ECCouncil.Premium.312-50v10.by.VCEplus.127q

Number: 312-50v10 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.2

Exam Code: 312-50v10
Exam Name: Certified Ethical Hacker v10 Exam
Certification Provider: ECCouncil
Corresponding Certification: CEH
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-312-50-v10/

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in 312-50 exam products and you get latest questions. We strive to deliver the best 312-50 exam product for top grades in your first attempt.

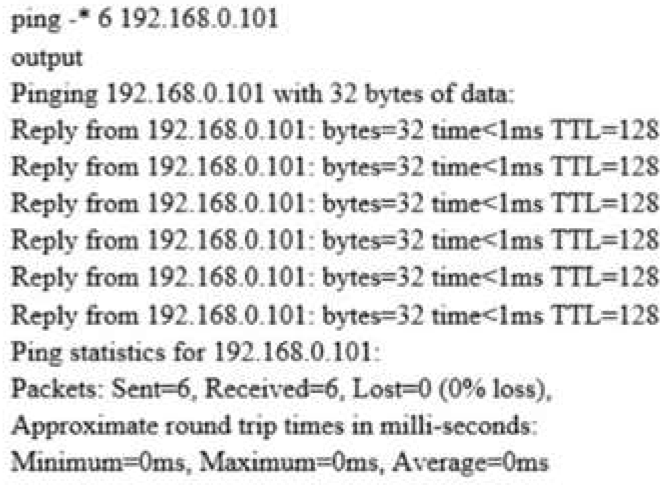
QUESTION 1
Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

A. Linux
B. Unix
C. OS X
D. Windows

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
What does the option * indicate?



```
ping -* 6 192.168.0.101
output
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.101:
Packets: Sent=6, Received=6, Lost=0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

A. s
B. t
C. n

D. a

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

A. Disk encryption
B. BIOS password
C. Hidden folders
D. Password protected files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer’s software and hardware without the owner's permission.
Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. White Hat
B. Suicide Hacker
C. Gray Hat
D. Black Hat

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

A. SHA-2
B. SHA-3
C. SHA-1
D. SHA-0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks.
What process would help him?

A. Banner Grabbing
B. IDLE/IPID Scanning
C. SSDP Scanning
D. UDP Scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

A. Discovery
B. Recovery
C. Containment
D. Eradication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

A. Bootrom Exploit
B. iBoot Exploit
C. Sandbox Exploit
D. Userland Exploit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system whose credentials are known. It was written by sysinternals and has been integrated within the framework. The penetration testers successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.
Which of the following is true hash type and sort order that is used in the psexec module's 'smbpass' option?

A. LM:NT
B. NTLM:LM
C. NT:LM
D. LMNTLM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?

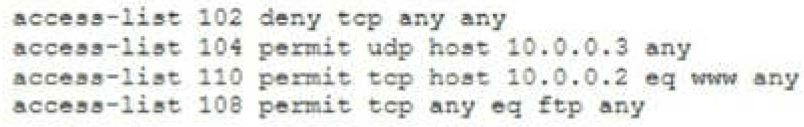
A. nmap-T4-q 10.10.0.0/24
B. nmap -T4-F 10.10.0.0/24
C. nmap -T4-r 10.10.1.0/24
D. nmap-T4-O 10.10.0.0/24

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

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 ACL 110 needs to be changed to port 80
C. The ACL for FTP must be before the ACL 110
D. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

A. wificracker
B. Airguard
C. WLAN-crack
D. Aircrack-ng

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

A. Metasploit
B. Cain & Abel
C. Maltego
D. Wireshark

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Keyed Hashing
B. Key Stretching
C. Salting
D. Double Hashing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. A web server and the database server facing the Internet, an application server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.
What is this type of DNS configuration commonly called?

A. DynDNS
B. DNS Scheme
C. DNSSEC
D. Split DNS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A virus that attempts to install itself inside the file it is infecting is called?

A. Tunneling virus
B. Cavity virus
C. Polymorphic virus
D. Stealth virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network.
What should Bob do to avoid this problem?

A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
You are the Network Admin, and you get a compliant that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?

A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on UDP Port 80
C. Traffic is Blocked on UDP Port 54
D. Traffic is Blocked on UDP Port 80

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

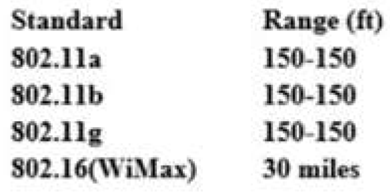
A. Omnidirectional antenna
B. Dipole antenna

C. Yagi antenna
D. Parabolic grid antenna

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
From the following table, identify the wrong answer in terms of Range (ft).



Standard	Range (ft)
802.11a	150-150
802.11b	150-150
802.11g	150-150
802.16(WiMax)	30 miles

A. 802.11b
B. 802.11g
C. 802.16(WiMax)
D. 802.11a

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Deferred risk
B. Impact risk
C. Inherent risk

D. Residual risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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. Bounding
C. Mutating
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Network security policy
B. Information protection policy
C. Access control policy
D. Remote access policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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. Network Time Protocol
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by Network-Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?

A. Out of band signaling
B. Protocol Isolation
C. Encryption
D. Alternate Data Streams

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which is the first step followed by Vulnerability Scanners for scanning a network?

A. TCP/UDP Port scanning
B. Firewall detection

C. OS Detection
D. Checking if the remote host is alive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Sam is working as s pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?

A. Denial-of-Service
B. False Positive Generation
C. Insertion Attack
D. Obfuscating

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
An attacker scans a host with the below command. Which three flags are set? (Choose three.) #nmap -sX host.domain.com

A. This is ACK scan. ACK flag is set
B. This is Xmas scan. SYN and ACK flags are set
C. This is Xmas scan. URG, PUSH and FIN are set
D. This is SYN scan. SYN flag is set

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following program infects the system boot sector and the executable files at the same time?

A. Stealth virus
B. Polymorphic virus
C. Macro virus
D. Multipartite Virus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
What two conditions must a digital signature meet?

A. Has to be legible and neat.
B. Has to be unforgeable, and has to be authentic.
C. Must be unique and have special characters.
D. Has to be the same number of characters as a physical signature and must be unique

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
An IT employee got a call from one of our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?

A. The employees cannot provide any information; but, anyway, he/she will provide the name of the person in charge.
B. Since the company's policy is all about Customer Service, he/she will provide information.

C. Disregarding the call, the employee should hang up.
D. The employee should not provide any information without previous management authorization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.
What should you do?

A. Confront the client in a respectful manner and ask her about the data.
B. Copy the data to removable media and keep it in case you need it.
C. Ignore the data and continue the assessment until completed as agreed.
D. Immediately stop work and contact the proper legal authorities.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

A. 123
B. 161
C. 69
D. 113

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
During the process of encryption and decryption, what keys are shared?

A. Private keys
B. User passwords
C. Public keys
D. Public and private keys

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
What is the purpose of a demilitarized zone on a network?

A. To scan all traffic coming through the DMZ to the internal network
B. To only provide direct access to the nodes within the DMZ and protect the network behind it
C. To provide a place to put the honeypot
D. To contain the network devices you wish to protect

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

A. Chosen-plaintext attack
B. Ciphertext-only attack

C. Adaptive chosen-plaintext attack
D. Known-plaintext attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks
B. To defend against webserver attacks
C. To defend against jailbreaking
D. To defend against wireless attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com', that the user is directed to a phishing site.
Which file does the attacker need to modify?

A. Boot.ini
B. Sudoers
C. Networks
D. Hosts

Correct Answer: D
Section: (none)
Explanation