DUMPSARENA

Certified Ethical Hacker Exam (CEHv12)

ECCouncil 312-50v12

Version Demo

Total Demo Questions: 20

Total Premium Questions: 503

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Pool A	140
Topic 2, Exam Pool B	182
Topic 3, Exam Pool C	181
Total	503

QUESTION NO: 1

What port number is used by LDAP protocol?

A. 110

B. 389

C. 464

D. 445

ANSWER: B

QUESTION NO: 2

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

] >

A. XXE

B. SQLi

C. IDOR

D. XXS

ANSWER: A

QUESTION NO: 3

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB

B. 44EFCE164AB921CQAAD3B435B51404EE

C. 0182BD0BD4444BF836077A718CCDF409

D. CEC52EB9C8E3455DC2265B23734E0DAC

E. B757BF5C0D87772FAAD3B435B51404EE

F. E52CAC67419A9A224A3B108F3FA6CB6D

ANSWER: B E

QUESTION NO: 4

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed

B. The right most portion of the hash is always the same

C. The hash always starts with AB923D

D. The left most portion of the hash is always the same

E. A portion of the hash will be all 0's

ANSWER: B

QUESTION NO: 5

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes. Which type of attack can she implement in order to continue?

A. LLMNR/NBT-NS poisoning

B. Internal monologue attack

C. Pass the ticket

D. Pass the hash

ANSWER: D

QUESTION NO: 6

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser

E. NMap

ANSWER: A B D

QUESTION NO: 7

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.

Identify the behavior of the adversary In the above scenario.

A. use of command-line interface

B. Data staging

C. Unspecified proxy activities

D. Use of DNS tunneling

ANSWER: C

QUESTION NO: 8

Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

ANSWER: A C D E

QUESTION NO: 9

jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

A. website mirroring

B. Session hijacking

C. Web cache poisoning

D. Website defacement

ANSWER: A

QUESTION NO: 10

Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS

B. A zone transfer is accomplished with the nslookup service

C. A zone transfer passes all zone information that a DNS server maintains

D. A zone transfer passes all zone information that a nslookup server maintains

E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections

F. Zone transfers cannot occur on the Internet

ANSWER: A C E

QUESTION NO: 11

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications

B. Harden DNS servers

C. Use split-horizon operation for DNS servers

D. Restrict Zone transfers

E. Have subnet diversity between DNS servers

ANSWER: B C D E

QUESTION NO: 12

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

A. Yagi antenna

B. Dipole antenna

C. Parabolic grid antenna

D. Omnidirectional antenna

ANSWER: A

QUESTION NO: 13

Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

ANSWER: B D E

QUESTION NO: 14

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. Honypot based

C. Behaviour based

D. Heuristics based

ANSWER: A

QUESTION NO: 15

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

A. Use port security on his switches.

B. Use a tool like ARPwatch to monitor for strange ARP activity.

C. Use a firewall between all LAN segments.

D. If you have a small network, use static ARP entries.

E. Use only static IP addresses on all PC's.

ANSWER: A B D

QUESTION NO: 16

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. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

ANSWER: B D

QUESTION NO: 17

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt

B. SAM file

C. wwwroot

D. Repair file

ANSWER: B

QUESTION NO: 18

Which of the following are well known password-cracking programs?

A. L0phtcrack

B. NetCat

C. Jack the Ripper

D. Netbus

E. John the Ripper

ANSWER: A E

QUESTION NO: 19

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

A. 110

B. 135

C. 139

D. 161

E. 445

F. 1024

ANSWER: B C E

QUESTION NO: 20

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Presentation tier

B. Application Layer

C. Logic tier

D. Data tier

ANSWER: C