DUMPSARENA

Certified Professional Ethical Hacker (CPEH)

GAQM CPEH-001

Version Demo

Total Demo Questions: 20

Total Premium Questions: 736

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	102
Topic 2, Exam Pool B	169
Topic 3, Exam Pool C	63
Topic 4, Exam Pool D	83
Topic 5, Exam Pool E	104
Topic 6, Exam Pool F	106
Topic 7, Exam Pool G	109
Total	736

QUESTION NO: 1

Name two software tools used for OS guessing? (Choose two.)

A. Nmap

B. Snadboy

C. Queso

D. UserInfo

E. NetBus

ANSWER: A C

QUESTION NO: 2

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: 3

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. Containment

B. Eradication

C. Recovery

D. Discovery

ANSWER: A

QUESTION NO: 4

An NMAP scan of a server shows port 69 is open. What risk could this pose?

A. Unauthenticated access

B. Weak SSL version

C. Cleartext login

D. Web portal data leak

ANSWER: A

QUESTION NO: 5

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: B

QUESTION NO: 6

Which of these is capable of searching for and locating rogue access points?

A. HIDS

B. WISS

C. WIPS

D. NIDS

ANSWER: C

QUESTION NO: 7

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

A. Converts passwords to uppercase.

B. Hashes are sent in clear text over the network.

C. Makes use of only 32-bit encryption.

D. Effective length is 7 characters.

ANSWER: A B D

QUESTION NO: 8

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: 9

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: 10

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: 11

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: 12

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

ANSWER: C

QUESTION NO: 13

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account

B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer

C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques

D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

ANSWER: C

QUESTION NO: 14

Which DNS resource record can indicate how long any "DNS poisoning" could last?

A. MX

B. SOA

C. NS

D. TIMEOUT

ANSWER: B

QUESTION NO: 15

When tuning security alerts, what is the best approach?

A. Tune to avoid False positives and False Negatives

B. Rise False positives Rise False Negatives

C. Decrease the false positives

D. Decrease False negatives

ANSWER: A

QUESTION NO: 16

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

ANSWER: A

QUESTION NO: 17

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 corporate network. What tool should the analyst use to perform a

Blackjacking attack?

A. Paros Proxy

B. BBProxy

C. BBCrack

D. Blooover

ANSWER: B

Explanation:

:

Blackberry users warned of hacking tool threat.

Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.

References:

http://www.computerweekly.com/news/2240062112/Technology-news-in-brief

QUESTION NO: 18

What does a type 3 code 13 represent? (Choose two.)

A. Echo request

B. Destination unreachable

C. Network unreachable

D. Administratively prohibited

E. Port unreachable

F. Time exceeded

ANSWER: B D

QUESTION NO: 19

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: 20

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