312-50V7 Q&As

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/312-50v7.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design

B. Elimination

C. Incorporation

D. Replication

E. Launch

F. Detection

Correct Answer: E

QUESTION 2

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key

B. 1025 bit key

C. 1536 bit key

D. 2048 bit key

Correct Answer: C

QUESTION 3

Which of the following is a strong post designed to stop a car?

A. Gate

B. Fence

C. Bollard

D. Reinforced rebar

Correct Answer: C

QUESTION 4

The SNMP Read-Only Community String is like a password. The string is sent along with each SNMP Get-Request and allows (or denies) access to a device. Most network vendors ship their equipment with a default password of "public". This is the so-called "default public community string". How would you keep

intruders from getting sensitive information regarding the network devices using SNMP? (Select 2 answers)

A. Enable SNMPv3 which encrypts username/password authentication

B. Use your company name as the public community string replacing the default \\'public\\'

C. Enable IP filtering to limit access to SNMP device

D. The default configuration provided by device vendors is highly secure and you don\\'t need to change anything

Correct Answer: AC

QUESTION 5

E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.

Select a feature, which you will NOT be able to accomplish with this probe?

A. When the e-mail was received and read

B. Send destructive e-mails

C. GPS location and map of the recipient

D. Time spent on reading the e-mails

E. Whether or not the recipient visited any links sent to them

F. Track PDF and other types of attachments

G. Set messages to expire after specified time

H. Remote control the User\\'s E-mail client application and hijack the traffic

Correct Answer: H

QUESTION 6

Kevin is an IT security analyst working for Emerson Time Makers, a watch manufacturing company in Miami. Kevin and his girlfriend Katy recently broke up after a big fight. Kevin believes that she was seeing another person. Kevin, who has an online email account that he uses for most of his mail, knows that Katy has an account with that same company. Kevin logs into his email account online and gets the following URL after successfully logged in: http://www.youremailhere.com/ mail.asp? mailbox=KevinandSmith=121%22 Kevin changes the URL to: http://www.youremailhere.com/mail.asp? mailbox=KatyandSanchez=121%22 Kevin is trying to access her email account to see if he can find out any information. What is Kevin attempting here to gain access to Katy\\'s mailbox?

A. This type of attempt is called URL obfuscation when someone manually changes a URL to try and gain unauthorized access

B. By changing the mailbox\\'s name in the URL, Kevin is attempting directory transversal

C. Kevin is trying to utilize query string manipulation to gain access to her email account

D. He is attempting a path-string attack to gain access to her mailbox

Correct Answer: C

QUESTION 7

Which type of hacker represents the highest risk to your network?

A. black hat hackers

B. grey hat hackers

C. disgruntled employees

D. script kiddies

Correct Answer: C

QUESTION 8

How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80 HEAD / HTTP/1.0

B. telnet webserverAddress 80 PUT / HTTP/1.0

C. telnet webserverAddress 80 HEAD / HTTP/2.0

D. telnet webserverAddress 80 PUT / HTTP/2.0

Correct Answer: A

QUESTION 9

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.

B. Perform a full restore.

C. Read the first 512 bytes of the tape.

D. Read the last 512 bytes of the tape.

Correct Answer: B

QUESTION 10

Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

A. Port Security

B. IPSec Encryption

C. Network Admission Control (NAC)

D. 802.1q Port Based Authentication

E. 802.1x Port Based Authentication

F. Intrusion Detection System (IDS)

Correct Answer: ACE

QUESTION 11

Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning

B. Banner grabbing

C. Injecting arbitrary data

D. Analyzing service response

Correct Answer: D

QUESTION 12

A company has made the decision to host their own email and basic web services. The administrator needs to set up the external firewall to limit what protocols should be allowed to get to the public part of the company\\'s network. Which

ports should the administrator open? (Choose three.)

A. Port 22

B. Port 23

C. Port 25

D. Port 53

E. Port 80

F. Port 139

G. Port 445

Correct Answer: CDE

QUESTION 13

When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

A. Drops the packet and moves on to the next one

B. Continues to evaluate the packet until all rules are checked

C. Stops checking rules, sends an alert, and lets the packet continue

D. Blocks the connection with the source IP address in the packet

Correct Answer: B

QUESTION 14

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Hping

B. Traceroute

C. TCP ping

D. Broadcast ping

Correct Answer: A

QUESTION 15

What is the default Password Hash Algorithm used by NTLMv2?

A. MD4

B. DES

C. SHA-1

D. MD5

Correct Answer: D