312-50V9^{Q&As}

Certified Ethical Hacker Exam V9

Pass EC-COUNCIL 312-50V9 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v9.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

A. Reject all invalid email received via SMTP.

B. Allow full DNS zone transfers.

C. Remove A records for internal hosts.

D. Enable null session pipes.

Correct Answer: C Section: (none)

QUESTION 2

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 Section: (none)

QUESTION 3

A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

A. -sO

B. -sP

C. -sS

D. -sU

Correct Answer: B Section: (none)

QUESTION 4

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

Correct Answer: A Section: (none)

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

QUESTION 5

What is the benefit of performing an unannounced Penetration Testing?

A. The tester will have an actual security posture visibility of the target network.

B. Network security would be in a "best state" posture.

C. It is best to catch critical infrastructure unpatched.

D. The tester could not provide an honest analysis.

Correct Answer: A Section: (none)

Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry. A possible solution to this danger is to conduct intermittent "unannounced" penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with "announced" penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.

References: http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

QUESTION 6

A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.

B. Create a document that will crash the computer when opened and send it to friends.

C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.

D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Correct Answer: D Section: (none)

QUESTION 7

Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.

B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.

C. Configure the firewall to allow traffic on TCP port 53.

D. Configure the firewall to allow traffic on TCP port 8080.

Correct Answer: A Section: (none)

QUESTION 8

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

A. MD4

B. DES

C. SHA

D. SSL

Correct Answer: B Section: (none)

QUESTION 9

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

A. HIDS

B. WISS

C. WIPS

D. NIDS

Correct Answer: C Section: (none)

QUESTION 10

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to

believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender\\'s public key

B. Receiver\\'s private key

C. Receiver\\'s public key

D. Sender\\'s private key

Correct Answer: D Section: (none)

QUESTION 11

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.

B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.

C. Network firewalls can prevent attacks if they are properly configured.

D. Network firewalls cannot prevent attacks because they are too complex to configure.

Correct Answer: B Section: (none)

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.

References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters

QUESTION 12

Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. SHA-1

B. MD5

C. HAVAL D. MD4

Correct Answer: A Section: (none)

QUESTION 13

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. The amount of time it takes to convert biometric data into a template on a smart card.

B. The amount of time and resources that are necessary to maintain a biometric system.

C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.

D. How long it takes to setup individual user accounts.

Correct Answer: C Section: (none)

QUESTION 14

Which of the following is an example of an asymmetric encryption implementation?

A. SHA1

B. PGP

C. 3DES

D. MD5

Correct Answer: B Section: (none)

QUESTION 15

Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

A. A new username and password

B. A fingerprint scanner and his username and password.

C. Disable his username and use just a fingerprint scanner.

D. His username and a stronger password.

Correct Answer: B Section: (none)