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.pass4itsure.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

Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS

B. IANA

C. CAPTCHA

D. IETF

Correct Answer: A Section: (none)

QUESTION 2

Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP

B. Nikto

C. Ike-scan

D. Arp-scan

Correct Answer: C Section: (none)

QUESTION 3

In the OSI model, where does PPTP encryption take place?

A. Transport layer

B. Application layer

C. Data link layer

D. Network layer

Correct Answer: C Section: (none)

QUESTION 4

During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential

B. Invoking the stored procedure xp_shell to spawn a Windows command shell

C. Invoking the stored procedure cmd_shell to spawn a Windows command shell

D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Correct Answer: D Section: (none)

QUESTION 5

What is the algorithm used by LM for Windows2000 SAM?

A. MD4

B. DES

C. SHA

D. SSL

Correct Answer: B Section: (none)

QUESTION 6

A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

A. Issue the pivot exploit and set the meterpreter.

B. Reconfigure the network settings in the meterpreter.

C. Set the payload to propagate through the meterpreter.

D. Create a route statement in the meterpreter.

Correct Answer: D Section: (none)

QUESTION 7

A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A. IP Security (IPSEC)

B. Multipurpose Internet Mail Extensions (MIME)

C. Pretty Good Privacy (PGP)

D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Correct Answer: C Section: (none)

QUESTION 8

How can a policy help improve an employee\\'s security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security

B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees

C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line

D. By decreasing an employee\\'s vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

Correct Answer: A Section: (none)

QUESTION 9

If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

A. Running a network scan to detect network services in the corporate DMZ

B. Reviewing the need for a security clearance for each employee

C. Using configuration management to determine when and where to apply security patches

D. Training employees on the security policy regarding social engineering

Correct Answer: A Section: (none)

QUESTION 10

When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification

B. At least once every three years or after any significant upgrade or modification

C. At least twice a year or after any significant upgrade or modification

D. At least once every two years and after any significant upgrade or modification

Correct Answer: A Section: (none)

QUESTION 11

The "black box testing" methodology enforces which kind of restriction?

A. Only the external operation of a system is accessible to the tester.

B. Only the internal operation of a system is known to the tester.

C. The internal operation of a system is only partly accessible to the tester.

D. The internal operation of a system is completely known to the tester.

Correct Answer: A Section: (none)

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

References: https://en.wikipedia.org/wiki/Black-box_testing

QUESTION 12

A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

A. Ignore it.

B. Try to sell the information to a well-paying party on the dark web.

C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.

D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

Correct Answer: C Section: (none)

QUESTION 13

The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?

A. Accept

B. Mitigate

C. Delegate

D. Avoid

Correct Answer: C Section: (none)

QUESTION 14

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

A. Validate and escape all information sent to a server

B. Use security policies and procedures to define and implement proper security settings

C. Verify access right before allowing access to protected information and UI controls

D. Use digital certificates to authenticate a server prior to sending data

Correct Answer: A Section: (none)

Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.

References: https://en.wikipedia.org/wiki/Crosssite_scripting#Contextual_output_encoding.2Fescaping_of_string_input

QUESTION 15

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment

test.

While conducting a port scan she notices open ports in the range of 135 to 139.

What protocol is most likely to be listening on those ports?

A. Finger

B. FTP C. Samba

D. SMB

Correct Answer: D Section: (none)