

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.pass2lead.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 of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

- A. Truecrypt
- B. Sub7
- C. Nessus
- D. Clamwin

Correct Answer: C Section: (none)

QUESTION 2

You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

- A. Network-based IDS
- B. Firewall
- C. Proxy
- D. Host-based IDS

Correct Answer: A Section: (none)

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats. A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

References: <https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids>

QUESTION 3

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. DMZ
- D. Logical interface

Correct Answer: A Section: (none)

Risk assessment include: The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems

review.

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

References: https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

QUESTION 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

Correct Answer: A Section: (none)

QUESTION 5

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

- A. Semicolon
- B. Single quote
- C. Exclamation mark
- D. Double quote

Correct Answer: B Section: (none)

QUESTION 6

Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

- A. Timing options to slow the speed that the port scan is conducted
- B. Fingerprinting to identify which operating systems are running on the network
- C. ICMP ping sweep to determine which hosts on the network are not available
- D. Traceroute to control the path of the packets sent during the scan

Correct Answer: A Section: (none)

QUESTION 7

Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

- A. Cross-site scripting
- B. SQL injection
- C. VPath injection
- D. XML denial of service issues

Correct Answer: D Section: (none)

QUESTION 8

You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?

- A. Scan servers with Nmap
- B. Physically go to each server
- C. Scan servers with MBSA
- D. Telnet to every port on each server

Correct Answer: A Section: (none)

QUESTION 9

A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

- A. True negatives
- B. False negatives
- C. True positives

D. False positives

Correct Answer: D Section: (none)

QUESTION 10

An NMAP scan of a server shows port 25 is open. What risk could this pose?

- A. Open printer sharing
- B. Web portal data leak
- C. Clear text authentication
- D. Active mail relay

Correct Answer: D Section: (none)

QUESTION 11

Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

- A. Microsoft Security Baseline Analyzer
- B. Retina
- C. Core Impact
- D. Microsoft Baseline Security Analyzer

Correct Answer: D Section: (none)

QUESTION 12

Which of the following is an extremely common IDS evasion technique in the web world?

- A. unicode characters
- B. spyware
- C. port knocking
- D. subnetting

Correct Answer: A Section: (none)

Unicode attacks can be effective against applications that understand it. Unicode is the international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion. Unicode characters are normally represented with two bytes, but this is impractical in real life. One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded. What is worse is multiple representations of each character can exist.

Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.

References: <http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-chp-10-sect-8.html>

QUESTION 13

Which of the following is a symmetric cryptographic standard?

- A. DSA
- B. PKI
- C. RSA
- D. 3DES

Correct Answer: D Section: (none)

QUESTION 14

What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

- A. c:\compmgmt.msc
- B. c:\gpedit
- C. c:\ncpa.cpl
- D. c:\services.msc

Correct Answer: A Section: (none)

QUESTION 15

A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

- A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
- B. As long as the physical access to the network elements is restricted, there is no need for additional measures.
- C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- D. The operator knows that attacks and down time are inevitable and should have a backup site.

Correct Answer: A Section: (none)

[312-50V9 VCE Dumps](#)

[312-50V9 Study Guide](#)

[312-50V9 Braindumps](#)