

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.leads4pass.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 is a detective control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

Correct Answer: C Section: (none)

QUESTION 2

Which definition among those given below best describes a covert channel?

- A. A server program using a port that is not well known.
- B. Making use of a protocol in a way it is not intended to be used.
- C. It is the multiplexing taking place on a communication link.
- D. It is one of the weak channels used by WEP which makes it insecure

Correct Answer: B Section: (none)

QUESTION 3

Which cipher encrypts the plain text digit (bit or byte) one by one?

- A. Classical cipher
- B. Block cipher
- C. Modern cipher
- D. Stream cipher

Correct Answer: D Section: (none)

QUESTION 4

It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?

- A. SNMP

- B. ICMP
- C. SYSLOG
- D. SMS

Correct Answer: C Section: (none)

QUESTION 5

During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

- A. Host
- B. Stateful
- C. Stateless
- D. Application

Correct Answer: C Section: (none)

QUESTION 6

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

- A. Cross-site scripting vulnerability
- B. Cross-site Request Forgery vulnerability
- C. SQL injection vulnerability
- D. Web site defacement vulnerability

Correct Answer: A Section: (none)

Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, **very** large), output encoding (such as `<big>` and `</big>`) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "**very** large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

QUESTION 7

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 8

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

- A. The tester must capture the WPA2 authentication handshake and then crack it.
- B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
- C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
- D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

Correct Answer: A Section: (none)

QUESTION 9

A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

- A. NMAP -P 192.168.1-5.
- B. NMAP -P 192.168.0/16
- C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
- D. NMAP -P 192.168.1/17

Correct Answer: A Section: (none)

QUESTION 10

While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model.

Which type of firewall is the tester trying to traverse?

- A. Packet filtering firewall
- B. Application-level firewall
- C. Circuit-level gateway firewall
- D. Stateful multilayer inspection firewall

Correct Answer: C Section: (none)

QUESTION 11

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.

Which command would you use?

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

Correct Answer: A Section: (none)

To start the Computer Management Console from command line just type `compmgmt.msc / computer:computername` in your run box or at the command line and it should automatically open the Computer Management console.

References: <http://www.waynezim.com/tag/compmgmtmsc/>

QUESTION 12

Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

- A. Detective
- B. Passive
- C. Intuitive
- D. Reactive

Correct Answer: B Section: (none)

QUESTION 13

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 14

Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

- A. Internal Whitebox
- B. External, Whitebox
- C. Internal, Blackbox
- D. External, Blackbox

Correct Answer: C Section: (none)

QUESTION 15

Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg. "mound access");

- A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
- B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
- C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
- D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Correct Answer: D Section: (none)