# 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.leads4pass.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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

**QUESTION 1**

Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment

B. Penetration testing

C. Risk assessment

D. Security auditing

Correct Answer: D

**QUESTION 2**

Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

A. 150

B. 161

C. 169

D. 69

Correct Answer: B

**QUESTION 3**

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

**QUESTION 4**

What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.

B. To get messaging programs to function with this algorithm requires complex configurations.

C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.

D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

Correct Answer: D

**QUESTION 5**

Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

A. WebBugs

B. WebGoat

C. VULN_HTML

D. WebScarab

Correct Answer: B

**QUESTION 6**

Blane is a network security analyst for his company. From an outside IP, Blane performs an XMAS scan using Nmap. Almost every port scanned does not illicit a response. What can he infer from this kind of response?

A. These ports are open because they do not illicit a response.

B. He can tell that these ports are in stealth mode.

C. If a port does not respond to an XMAS scan using NMAP, that port is closed.

D. The scan was not performed correctly using NMAP since all ports, no matter what their state, will illicit some sort of response from an XMAS scan.

Correct Answer: A

**QUESTION 7**

WWW wanderers or spiders are programs that traverse many pages in the World Wide Web by recursively retrieving linked pages. Search engines like Google, frequently spider web pages for indexing. How will you stop web spiders from crawling certain directories on your website?

A. Place robots.txt file in the root of your website with listing of directories that you don\\'t want to be crawled

B. Place authentication on root directories that will prevent crawling from these spiders

C. Enable SSL on the restricted directories which will block these spiders from crawling

D. Place "HTTP:NO CRAWL" on the html pages that you don\\'t want the crawlers to index

Correct Answer: A

**QUESTION 8**

Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

A. Image Hide

B. Snow

C. Gif-It-Up

D. NiceText

Correct Answer: B

**QUESTION 9**

A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application\\'s search form and introduces the following code in the search input fieID.

IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable". Which web applications vulnerability did the analyst discover?

A. Cross-site request forgery

B. Command injection

C. Cross-site scripting

D. SQL injection

Correct Answer: C

**QUESTION 10**

Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)

B. Sarbanes-Oxley Act (SOX)

C. Health Insurance Portability and Accountability Act (HIPAA)

D. Payment Card Industry Data Security Standards (PCI DSS)

Correct Answer: D

**QUESTION 11**

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 192.168.0.0/16

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

**QUESTION 12**

A majority of attacks come from insiders, people who have direct access to a company\\'s computer system as part of their job function or a business relationship. Who is considered an insider?

A. A competitor to the company because they can directly benefit from the publicity generated by making such an attack

B. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants

C. The CEO of the company because he has access to all of the computer systems

D. A government agency since they know the company\\'s computer system strengths and weaknesses

Correct Answer: B

**QUESTION 13**

Your company has blocked all the ports via external firewall and only allows port 80/443 to connect to the Internet. You want to use FTP to connect to some remote server on the Internet. How would you accomplish this?

A. Use HTTP Tunneling

B. Use Proxy Chaining

C. Use TOR Network

D. Use Reverse Chaining

Correct Answer: A

**QUESTION 14**

There is a WEP encrypted wireless access point (AP) with no clients connected. In order to crack the WEP key, a fake authentication needs to be performed. What information is needed when performing fake authentication to an AP? (Choose two.)

A. The IP address of the AP

B. The MAC address of the AP

C. The SSID of the wireless network

D. A failed authentication packet

Correct Answer: BC

**QUESTION 15**

The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence numbers of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. false

B. true

Correct Answer: B

Latest 312-50V7 Dumps 312-50V7 PDF Dumps 312-50V7 Study Guide