

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.pass2lead.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

Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

- A. RST flag scanning
- B. FIN flag scanning
- C. SYN flag scanning
- D. ACK flag scanning

Correct Answer: D

QUESTION 2

An Attacker creates a zuckerjournals.com website by copying and mirroring HACKERJOURNALS.COM site to spread the news that Hollywood actor Jason Jenkins died in a car accident. The attacker then submits his fake site for indexing in major search engines. When users search for "Jason Jenkins", attacker's fake site shows up and dupes victims by the fake news.



This is another great example that some people do not know what URL's are. Real website: Fake website:
<http://www.zuckerjournals.com>



The website is clearly not WWW.HACKERJOURNALS.COM. It is obvious for many, but unfortunately some people still do not know what an URL is. It\\'s the address that you enter into the address bar at the top your browser and this is clearly not legit site, its www.zuckerjournals.com

How would you verify if a website is authentic or not?

- A. Visit the site using secure HTTPS protocol and check the SSL certificate for authenticity
- B. Navigate to the site by visiting various blogs and forums for authentic links
- C. Enable Cache on your browser and lookout for error message warning on the screen
- D. Visit the site by clicking on a link from Google search engine

Correct Answer: D

QUESTION 3

A penetration tester is hired to do a risk assessment of a company\\'s DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

- A. white box
- B. grey box
- C. red box
- D. black box

Correct Answer: D

QUESTION 4

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 field.

```
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 5

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. "mountd 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

[312-50V7 PDF Dumps](#)

[312-50V7 VCE Dumps](#)

[312-50V7 Practice Test](#)