



312-50V12^{Q&As}

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/312-50v12.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

You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?

- A. wireshark --fetch '\\\\192.168.8*\\'
- B. wireshark --capture --local masked 192.168.8.0 ---range 24
- C. tshark -net 192.255.255.255 mask 192.168.8.0
- D. sudo tshark -f\\'\\'net 192 .68.8.0/24\\'\\'

Correct Answer: D

QUESTION 2

What is the role of test automation in security testing?

- A. It is an option but it tends to be very expensive.
- B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- C. Test automation is not usable in security due to the complexity of the tests.
- D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Correct Answer: D

QUESTION 3

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

- A. search.com
- B. EarthExplorer
- C. Google image search
- D. FCC ID search

Correct Answer: D

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc. pg. 5052 ECHv11 manual



https://en.wikipedia.org/wiki/FCC_mark An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless devices in the US, manufacturers must: ?Have the device evaluated by an independent lab to ensure it conforms to FCC standards ?Provide documentation to the FCC of the lab results ?Provide User Manuals, Documentation, and Photos relating to the device ?Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application) The FCC gets its authority from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

QUESTION 4

Consider the following Nmap output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

what command-line parameter could you use to determine the type and version number of the web server?

- A. -sv
- B. -Pn
- C. -V
- D. -ss

Correct Answer: A

C:\Users\moi>nmap -h | findstr " -sV" -sV: Probe open ports to determine service/version info

QUESTION 5

What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

- A. Session hijacking



- B. Server side request forgery
- C. Cross-site request forgery
- D. Cross-site scripting

Correct Answer: C

[312-50V12 Practice Test](#)

[312-50V12 Study Guide](#)

[312-50V12 Exam Questions](#)