



ECSAV10^{Q&As}

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

<https://www.passapply.com/ecsav10.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

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

- A. CVE
- B. IANA
- C. RIPE
- D. APIPA

Correct Answer: A

QUESTION 2

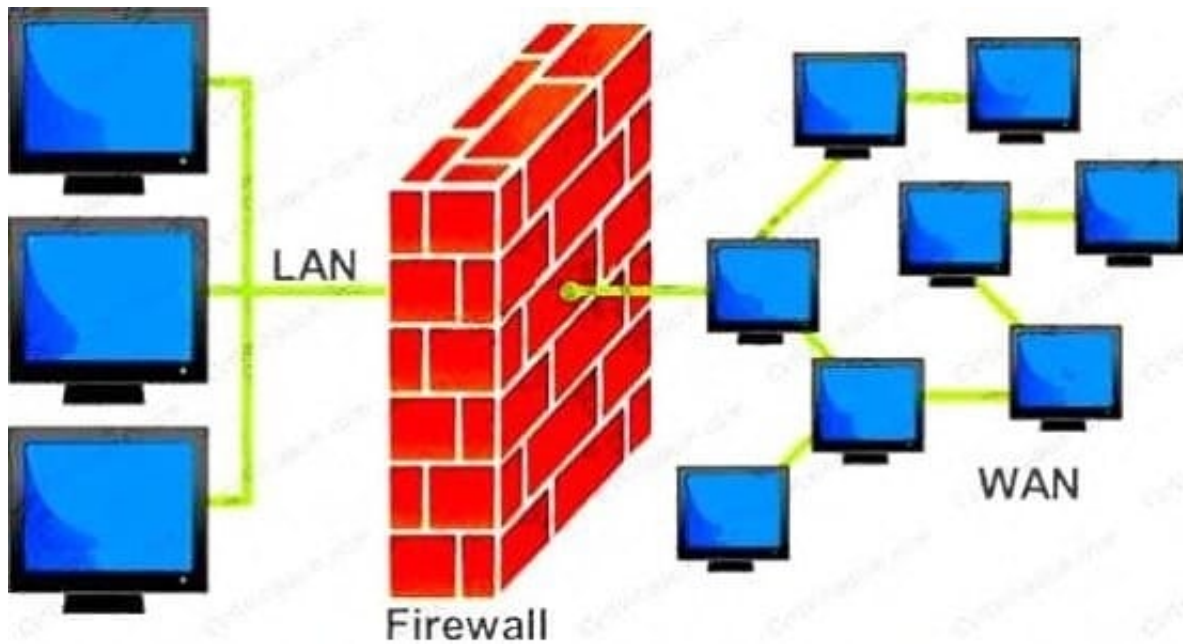
Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

- A. Reverse Address Resolution Protocol (RARP)
- B. HTTP (Hypertext Transfer Protocol)
- C. SMTP (Simple Mail Transfer Protocol)
- D. Telnet

Correct Answer: A

QUESTION 3

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria; If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

- A. Appliance based firewalls cannot be upgraded
- B. Firewalls implemented on a hardware firewall are highly scalable
- C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system
- D. Operating system firewalls are highly configured

Correct Answer: C

QUESTION 4

During an internal network audit, you are asked to see if there is any RPC server running on the network and if found, enumerate the associate RPC services. Which port would you scan to determine the RPC server and which command will you use to enumerate the RPC services?

- A. Port 111, rpcinfo
- B. Port 111, rpcenum
- C. Port 145, rpcinfo
- D. Port 145, rpcenum

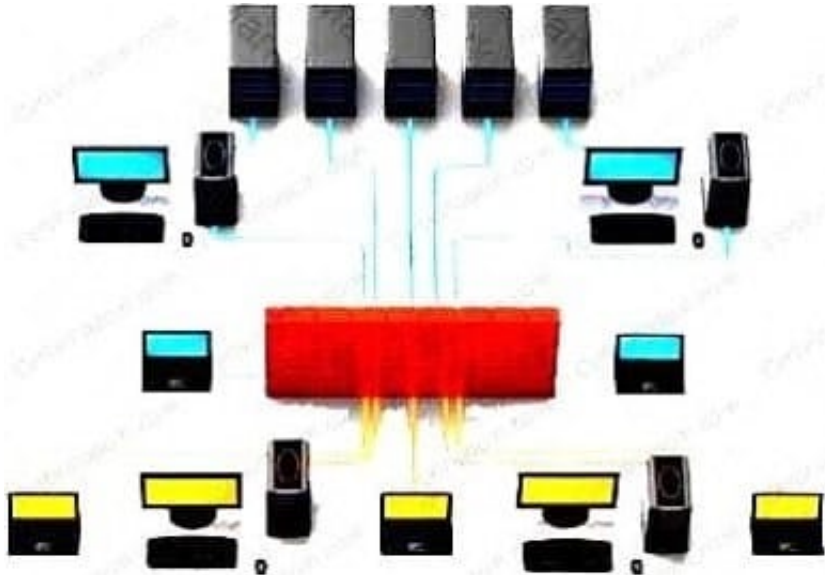
Correct Answer: A

QUESTION 5

Information gathering is performed to:



- i) Collect basic information about the target company and its network ii) Determine the operating system used, platforms running, web server versions, etc.
- iii) Find vulnerabilities and exploits



Which of the following pen testing tests yields information about a company's technology infrastructure?

- A. Searching for web page posting patterns
- B. Analyzing the link popularity of the company's website
- C. Searching for trade association directories
- D. Searching for a company's job postings

Correct Answer: D

[ECSAV10 Practice Test](#)

[ECSAV10 Study Guide](#)

[ECSAV10 Exam Questions](#)