

412-79V10^{Q&As}

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

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

<https://www.leads4pass.com/412-79v10.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

John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

- A. C:\Windows\System32\Boot
- B. C:\WINNT\system32\drivers\etc
- C. C:\WINDOWS\system32\cmd.exe
- D. C:\Windows\System32\restore

Correct Answer: B

Reference: [http://en.wikipedia.org/wiki/Hosts_\(file\)](http://en.wikipedia.org/wiki/Hosts_(file)) (location in the file system, see the table)

QUESTION 2

Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

- A. SYN Scan
- B. Connect() scan
- C. XMAS Scan
- D. Null Scan

Correct Answer: A

QUESTION 3

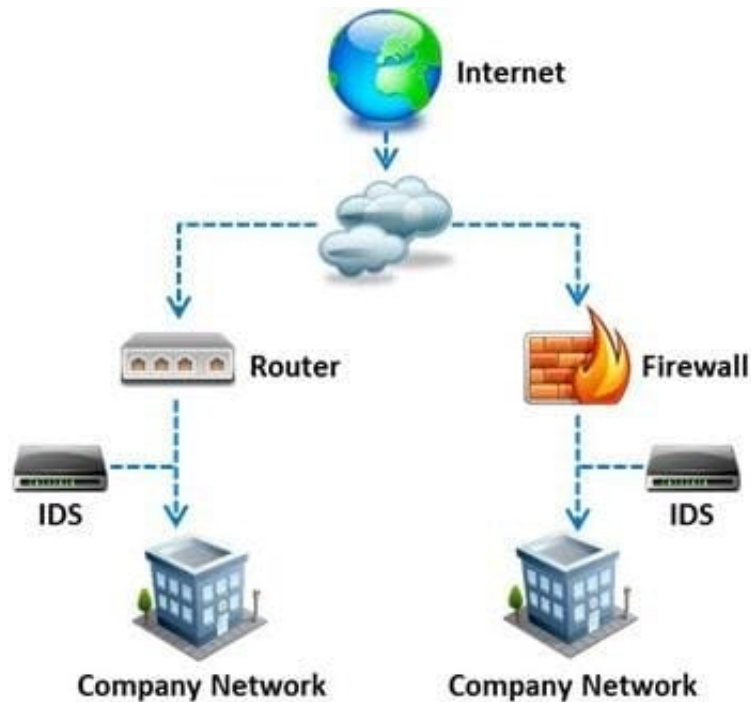
The framework primarily designed to fulfill a methodical and organized way of addressing five threat classes to network and that can be used to access, plan, manage, and maintain secure computers and communication networks is:

- A. Nortells Unified Security Framework
- B. The IBM Security Framework
- C. Bell Labs Network Security Framework
- D. Microsoft Internet Security Framework

Correct Answer: C

QUESTION 4

What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



- A. NIDS are usually a more expensive solution to implement compared to HIDS.
- B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
- C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.
- D. HIDS requires less administration and training compared to NIDS.

Correct Answer: C

QUESTION 5

Which of the following policies helps secure data and protects the privacy of organizational information?

- A. Special-Access Policy
- B. Document retention Policy
- C. Cryptography Policy
- D. Personal Security Policy

Correct Answer: C

[412-79V10 PDF Dumps](#)

[412-79V10 VCE Dumps](#)

[412-79V10 Study Guide](#)