

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

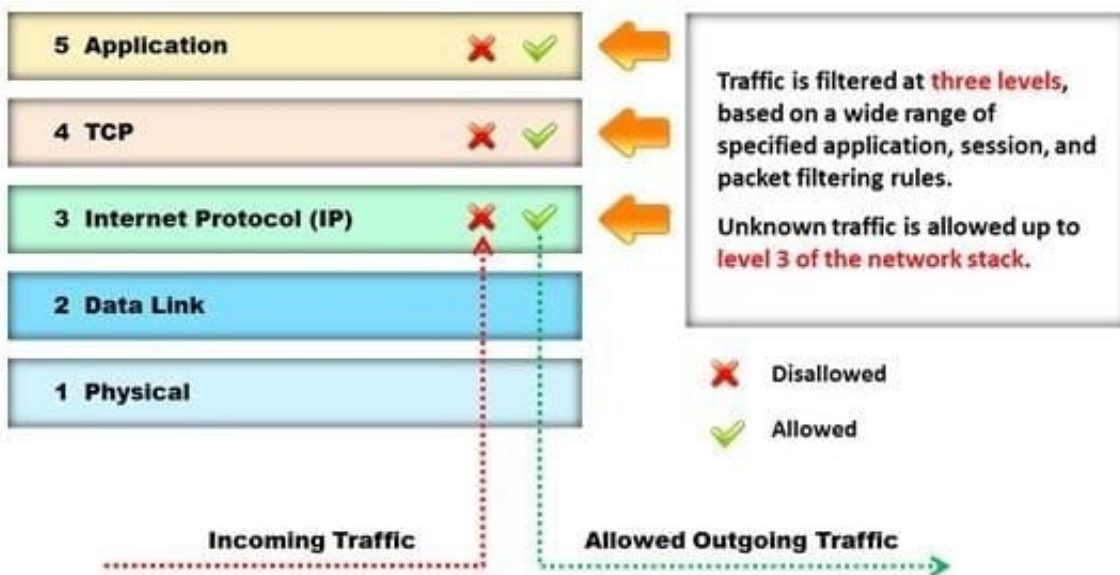
TCP/IP provides a broad range of communication protocols for the various applications on the network. The TCP/IP model has four layers with major protocols included within each layer. Which one of the following protocols is used to collect information from all the network devices?

- A. Simple Network Management Protocol (SNMP)
- B. Network File system (NFS)
- C. Internet Control Message Protocol (ICMP)
- D. Transmission Control Protocol (TCP)

Correct Answer: A

QUESTION 2

Identify the type of firewall represented in the diagram below:



- A. Stateful multilayer inspection firewall
- B. Application level gateway
- C. Packet filter
- D. Circuit level gateway

Correct Answer: A

Reference: <http://www.technicolorbroadbandpartner.com/getfile.php?id=4159> (page 13)

QUESTION 3

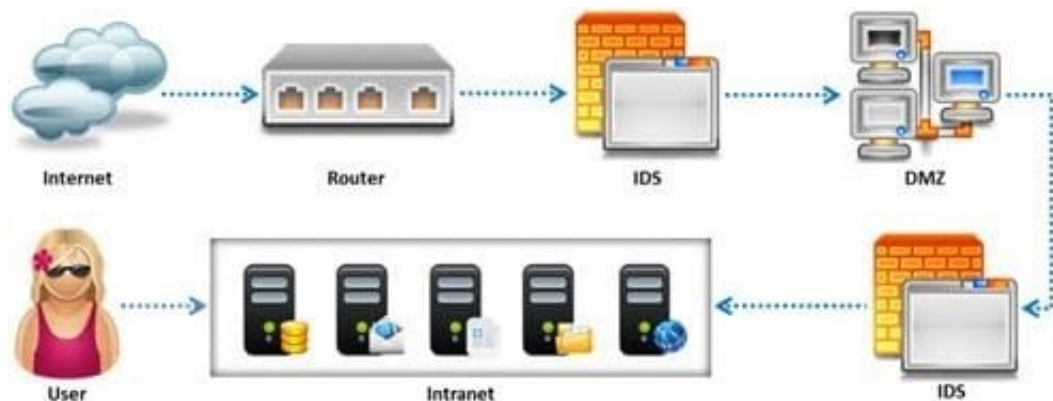
Identify the framework that comprises of five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement:

- A. Information System Security Assessment Framework (ISSAF)
- B. Microsoft Internet Security Framework
- C. Nortells Unified Security Framework
- D. Federal Information Technology Security Assessment Framework

Correct Answer: D

QUESTION 4

Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/ FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS.

Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

- A. SYN/RST/ACK
- B. SYN/FIN/ACK
- C. SYN/FIN
- D. All Flags

Correct Answer: D

Reference:

<http://books.google.com.pk/books?id=tUCumJot0ocCandpg=PA63andlpg=PA63anddq=TCP+flag+combinations+combines+the+problem+of+initiation,+midstream,+and+termination+flags+with+the+PSH+and>

+URGandsource=blandots=mIGSXBli15andsig=WMnXIEChVSU4RhK65W_V

3tzNjnsandhl=enandsa=Xandei=H7AfVJctLaufygO1v4DQDgandved=0CBsQ6AEwAA#v=onepageand q=TCP%

20flag%20combinations%20combines%20the%20problem%20of%20initiation%20C%20midstream%20C%

20and%20termination%20flags%20with%20the%20PSH%20and%20URGandf=false (see the highlighted

sentence in Table 3-1 at the end of the page)

QUESTION 5

What is the difference between penetration testing and vulnerability testing?



- A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
- B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
- C. Vulnerability testing is more expensive than penetration testing
- D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A

[412-79V10 PDF Dumps](#)

[412-79V10 VCE Dumps](#)

[412-79V10 Study Guide](#)