412-79V8$^{\text{Q\&As}}$

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79V8 Exam with 100% Guarantee

QUESTION 1

Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools

B. Application-layer Vulnerability Assessment Tools

C. Location/Data Examined Tools

D. Scope Assessment Tools

Correct Answer: D

QUESTION 2

Output modules allow Snort to be much more flexible in the formatting and presentation of output to its users. Snort has 9 output plug-ins that push out data in different formats. Which one of the following output plug-ins allows alert data to be written in a format easily importable to a database?

A. unified

B. csv

C. alert_unixsock

D. alert_fast

Correct Answer: B

QUESTION 3

Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers. Which one of the following cannot handle routing protocols properly?

A. "Internet-router-firewall-net architecture"

B. "Internet-firewall-router-net architecture"

C. "Internet-firewall/router(edge device)-net architecture"

D. "Internet-firewall -net architecture"

Correct Answer: B

QUESTION 4

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes

B. Type 12 ICMP codes

C. Type 3 ICMP codes

D. Type 7 ICMP codes

Correct Answer: C

QUESTION 5

Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges. The port numbers above 1024 are considered as which one of the following? (Select all that apply)

A. Well-known port numbers

B. Dynamically assigned port numbers

C. Unregistered port numbers

D. Statically assigned port numbers

Correct Answer: B