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

EC-Council Certified Security Analyst (ECSA)

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

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

https://www.geekcert.com/412-79v8.html

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Which one of the following log analysis tools is used for analyzing the server\\'s log files?

A. Performance Analysis of Logs tool

B. Network Sniffer Interface Test tool

C. Ka Log Analyzer tool

D. Event Log Tracker tool

Correct Answer: C

QUESTION 2

Which one of the following 802.11 types uses either FHSS or DSSS for modulation?

A. 802.11b

B. 802.11a

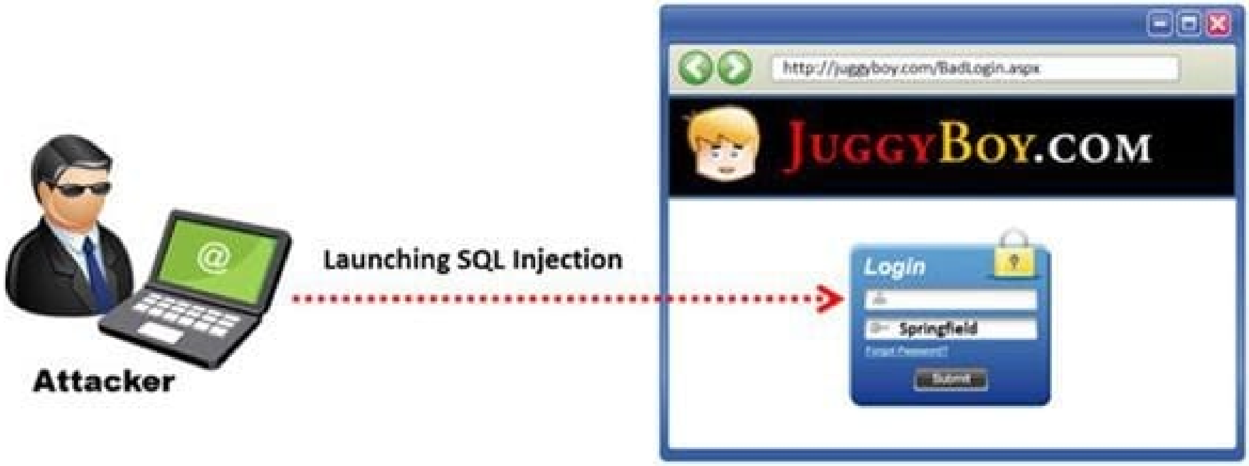
C. 802.11n

D. 802.11-Legacy

Correct Answer: D

QUESTION 3

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type. This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database. The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

A. Blah\\' "2=2 "

B. Blah\\' and 2=2 -

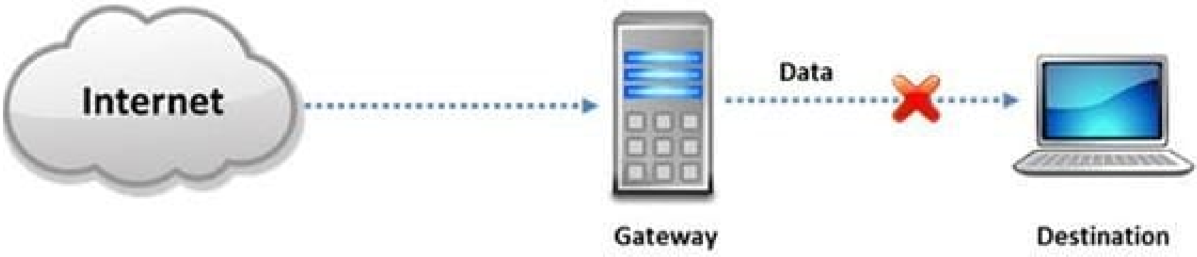
C. Blah\\' and 1=1 -

D. Blah\\' or 1=1 -

Correct Answer: D

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 and code field.



Which of the following ICMP messages will be generated if the destination port is not reachable?

A. ICMP Type 11 code 1

B. ICMP Type 5 code 3

C. ICMP Type 3 code 2

D. ICMP Type 3 code 3

Correct Answer: D

QUESTION 5

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