Vendor:EC-COUNCIL

Exam Code:412-79V8

Exam Name:EC-Council Certified Security Analyst (ECSA)

Version: Demo

QUESTION 1

Which one of the following architectures has the drawback of internally considering the hosted services individually?

A. Weak Screened Subnet Architecture

B. "Inside Versus Outside" Architecture

C. "Three-Homed Firewall" DMZ Architecture

D. Strong Screened-Subnet Architecture

Correct Answer: C

QUESTION 2

Which one of the following is false about Wireshark? (Select all that apply)

A. Wireshark offers some options to analyze the WEP-decrypted data

B. It does not support decrypting the TKIP or CCMP packets

C. In order for Wireshark to decrypt the contents of the WEP-encrypted packets, it must be given the appropriate WEP key for the network

D. Packet Sniffer Mode

Correct Answer: A

QUESTION 3

Which of the following scan option is able to identify the SSL services?

A. sS

B. sV C. sU

D. sT

Correct Answer: B

QUESTION 4

Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing

B. Double Blind Testing

C. Announced Testing

D. Blind Testing

Correct Answer: A

QUESTION 5

By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry

B. Netstat

C. Telnet

D. Tracert

Correct Answer: A

QUESTION 6

Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445

B. 134, 135, 136, 137

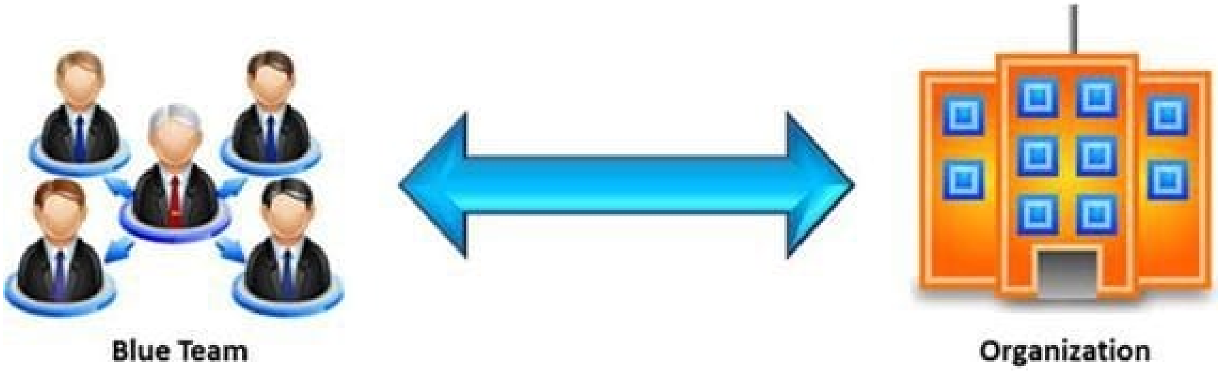
C. 137, 138, 139, 140

D. 133, 134, 139, 142

Correct Answer: A

QUESTION 7

In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization\\'s IT staff

B. It is the most expensive and most widely used

C. It may be conducted with or without warning

D. A penetration test performed without the knowledge of the organization\\'s IT staff but with permission from upper management

Correct Answer: A

QUESTION 8

Which one of the following 802.11 types has WLAN as a network support?

A. 802.11b

B. 802.11-Legacy

C. 802.11n

D. 802.11g

Correct Answer: C

QUESTION 9

The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the signal () function. Which one of the following functions is used as a programspecific signal and the handler for this calls the DropStats() function to output the current Snort statistics?

A. SIGUSR1

B. SIGTERM

C. SIGINT

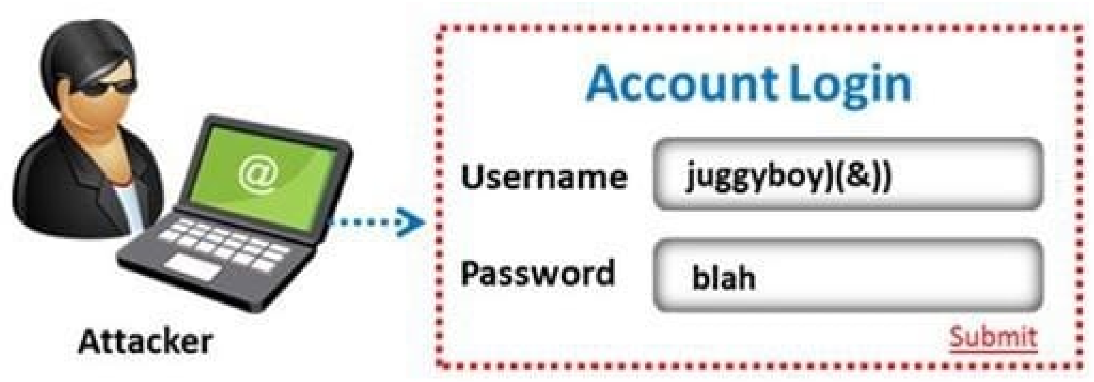
D. SIGHUP

Correct Answer: A

QUESTION 10

The amount of data stored in organizational databases has increased rapidly in recent years due to the rapid advancement of information technologies. A high percentage of these data is sensitive, private and critical to the organizations, their clients and partners.

Therefore, databases are usually installed behind internal firewalls, protected with intrusion detection mechanisms and accessed only by applications. To access a database, users have to connect to one of these applications and submit queries through them to the database. The threat to databases arises when these applications do not behave properly and construct these queries without sanitizing user inputs first. Identify the injection attack represented in the diagram below:



Account Login

Username juggyboy)(&))

Password blah

Submit

A. Frame Injection Attack

B. LDAP Injection Attack

C. XPath Injection Attack

D. SOAP Injection Attack

Correct Answer: B

QUESTION 11

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test

B. Techniques for data exclusion from systems upon termination of the test

C. Details on how data should be transmitted during and after the test

D. Details on how organizational data is treated throughout and after the test

Correct Answer: D

QUESTION 12

Nessus can test a server or a network for DoS vulnerabilities. Which one of the following script tries to kill a service?

A. ACT_DENIAL

B. ACT_FLOOD

C. ACT_KILL_HOST

D. ACT_ATTACK

Correct Answer: A