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 of the following is not a characteristic of a firewall?

A. Manages public access to private networked resources

B. Routes packets between the networks

C. Examines all traffic routed between the two networks to see if it meets certain criteria

D. Filters only inbound traffic but not outbound traffic

Correct Answer: B

QUESTION 3

Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businesService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack

B. Service Level Configuration Attacks

C. URL Tampering Attacks

D. Inside Attacks

Correct Answer: A

QUESTION 4

An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing

B. SMTP Message Bouncing

C. SMTP Server Bouncing

D. SMTP Mail Bouncing

Correct Answer: B

QUESTION 5

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 6

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)

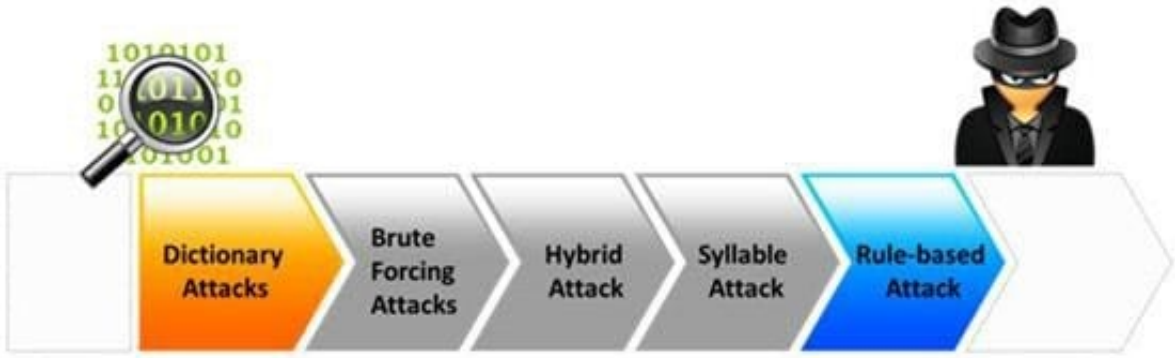
D. Transmission Control Protocol (TCP)

Correct Answer: A

QUESTION 7

Passwords protect computer resources and files from unauthorized access by malicious users. Using passwords is the most capable and effective way to protect information and to increase the security level of a company.

Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system to gain unauthorized access to a system.



Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack

B. Rule-based attack

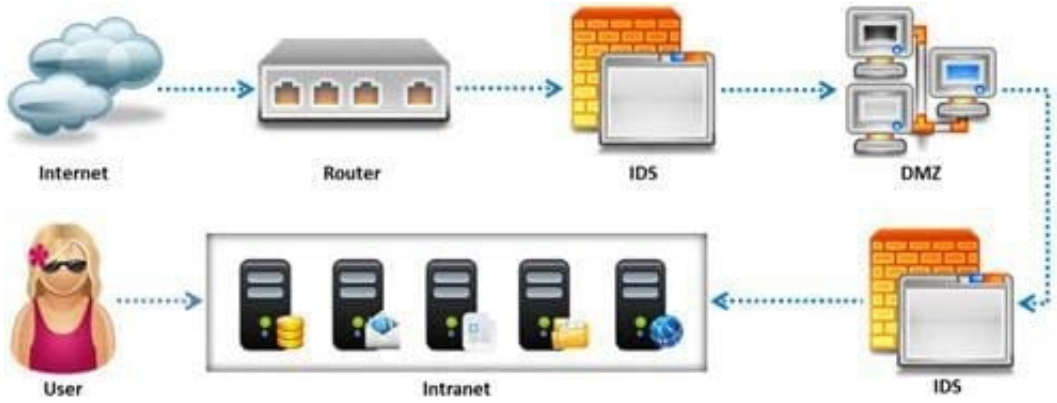
C. Hybrid attack

D. Dictionary attack

Correct Answer: A

QUESTION 8

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

QUESTION 9

Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword. Which one of the following operator is used to define meta- variables?

A. "$"

B. "#"

C. "*"

D. "?"

Correct Answer: A

QUESTION 10

Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information B. Suspiciously good grammar and capitalization

C. They trigger warning pop-ups

D. Suspicious attachments

Correct Answer: D

QUESTION 11

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 12

Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

A. Hash Key Length

B. C/R Value Length

C. C/R Key Length

D. Hash Value Length

Correct Answer: B