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.passapply.com/412-79v8.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

During external penetration testing, which of the following techniques uses tools like Nmap to predict the sequence numbers generated by the targeted server and use this information to perform session hijacking techniques?

A. TCP Sequence Number Prediction

B. IPID State Number Prediction

C. TCP State Number Prediction

D. IPID Sequence Number Prediction

Correct Answer: A

QUESTION 2

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security

B. Testing focused on the servers, infrastructure, and the underlying software, including the target

C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections

D. Testing performed from a number of network access points representing each logical and physical segment

Correct Answer: D

QUESTION 3

Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?

A. AES

B. DES (ECB mode)

C. MD5

D. RC5

Correct Answer: C

QUESTION 4

Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars

B. Painted ultraviolet material

C. Microphone

D. All the above

Correct Answer: A

QUESTION 5

A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?

A. Orinoco chipsets

B. Prism II chipsets

C. Atheros Chipset

D. Cisco chipset

Correct Answer: B

QUESTION 6

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf

B. Trinoo

C. Fraggle

D. SYN flood

Correct Answer: A

QUESTION 7

Which of the following has an offset field that specifies the length of the header and data?

A. IP Header

B. UDP Header

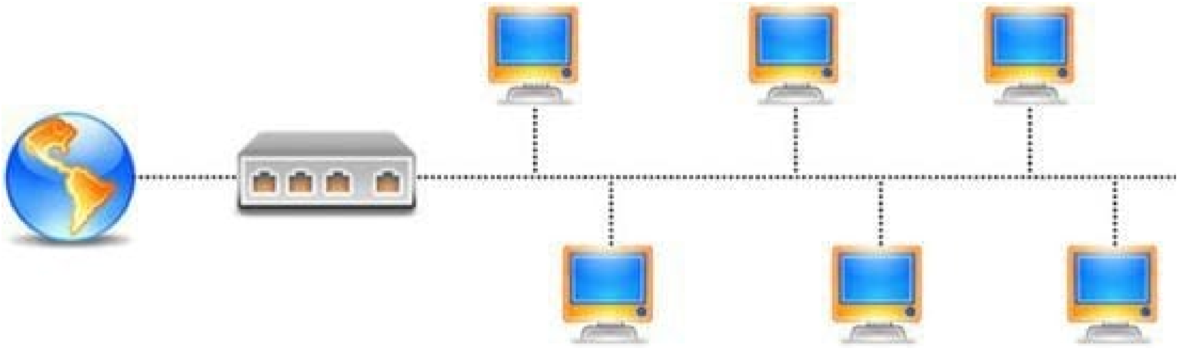
C. ICMP Header

D. TCP Header

Correct Answer: A

QUESTION 8

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.



Port numbers above 1024 are considered which one of the following?

A. Dynamically assigned port numbers

B. Statically assigned port numbers

C. Well-known port numbers

D. Unregistered port numbers

Correct Answer: A

QUESTION 9

Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack

B. Mac Flooding

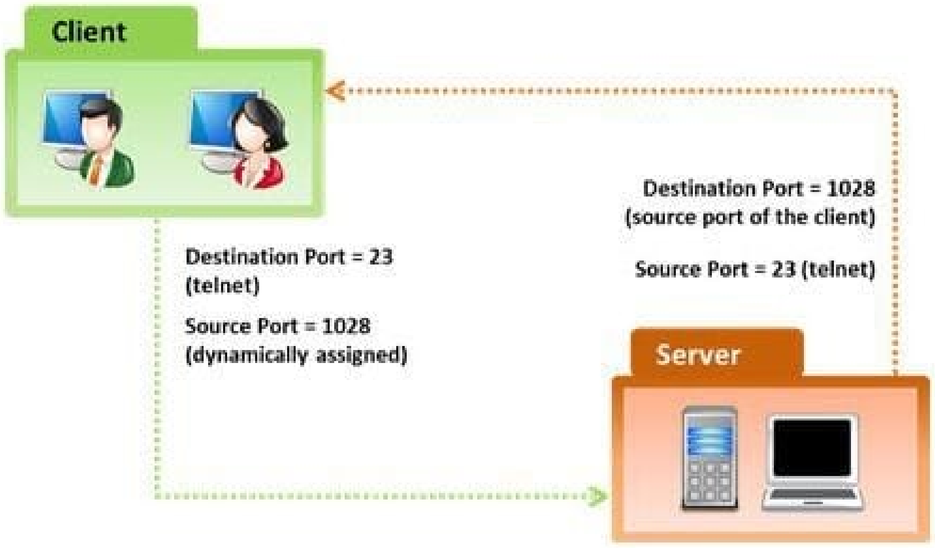
C. Man-in-the Middle Attack

D. DNS Poisoning

Correct Answer: B

QUESTION 10

In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows

B. Windowing

C. Positive Acknowledgment with Retransmission (PAR)

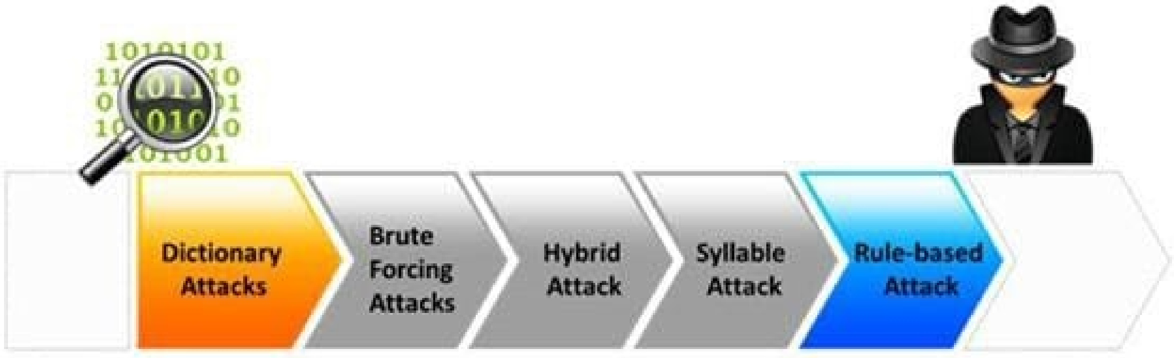
D. Synchronization

Correct Answer: C

QUESTION 11

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 12

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 13

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

QUESTION 14

What is the maximum value of a "tinyint" field in most database systems?

A. 222

B. 224 or more

C. 240 or less

D. 225 or more

Correct Answer: D

QUESTION 15

A framework is a fundamental structure used to support and resolve complex issues. The framework that delivers an efficient set of technologies in order to develop applications which are more secure in using Internet and Intranet is:

A. Microsoft Internet Security Framework

B. Information System Security Assessment Framework (ISSAF)

C. Bell Labs Network Security Framework

D. The IBM Security Framework

Correct Answer: A

Latest 412-79V8 Dumps 412-79V8 Practice Test 412-79V8 Exam Questions