# 412-79V10 Q&As

EC-Council Certified Security Analyst (ECSA) V10

## Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/412-79v10.html**

100% Passing Guarantee
100% Money Back Assurance

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

**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

Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration- Testing-NoRestriction (p.43)

**QUESTION 2**

Which one of the following acts related to the information security in the US fix the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

A. California SB 1386

B. Sarbanes-Oxley 2002

C. Gramm-Leach-Bliley Act (GLBA)

D. USA Patriot Act 2001

Correct Answer: B

**QUESTION 3**

Which one of the following is a useful formatting token that takes an int * as an argument, and writes the number of bytes already written, to that location?

A. "%n"

B. "%s"

C. "%p"

D. "%w"

Correct Answer: A

**QUESTION 4**

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 5**

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.


Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment

B. Host-based Assessment

C. External Assessment

D. Application Assessment

Correct Answer: D

**QUESTION 6**

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

A. 135, 136, 139, 445

B. 134, 135, 136, 137

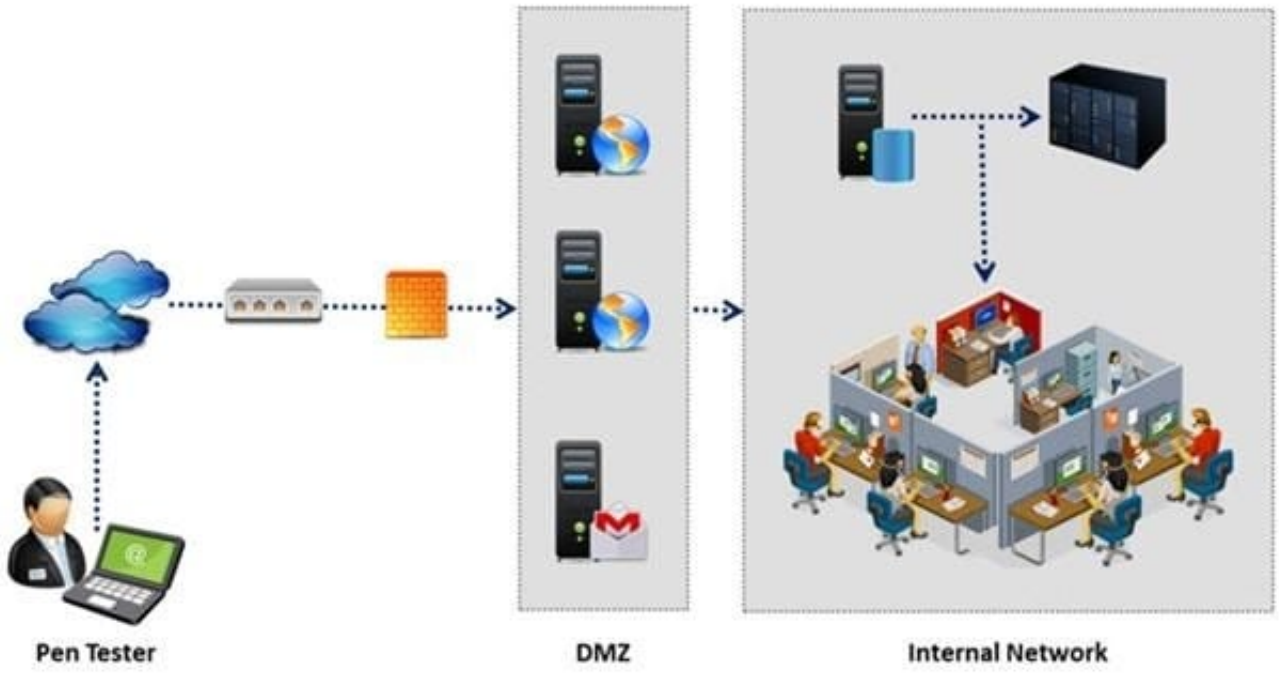
C. 137, 138, 139, 140

D. 133, 134, 139, 142

Correct Answer: A

**QUESTION 7**

An external intrusion test and analysis identify security weaknesses and strengths of the client\\'s systems and networks as they appear from outside the client\\'s security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.




During external penetration testing, which of the following scanning techniques allow you to determine a port\\'s state without making a full connection to the host?

A. XMAS Scan

B. SYN scan

C. FIN Scan

D. NULL Scan

Correct Answer: B

**QUESTION 8**

Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug- in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting

B. HTTP fingerprinting

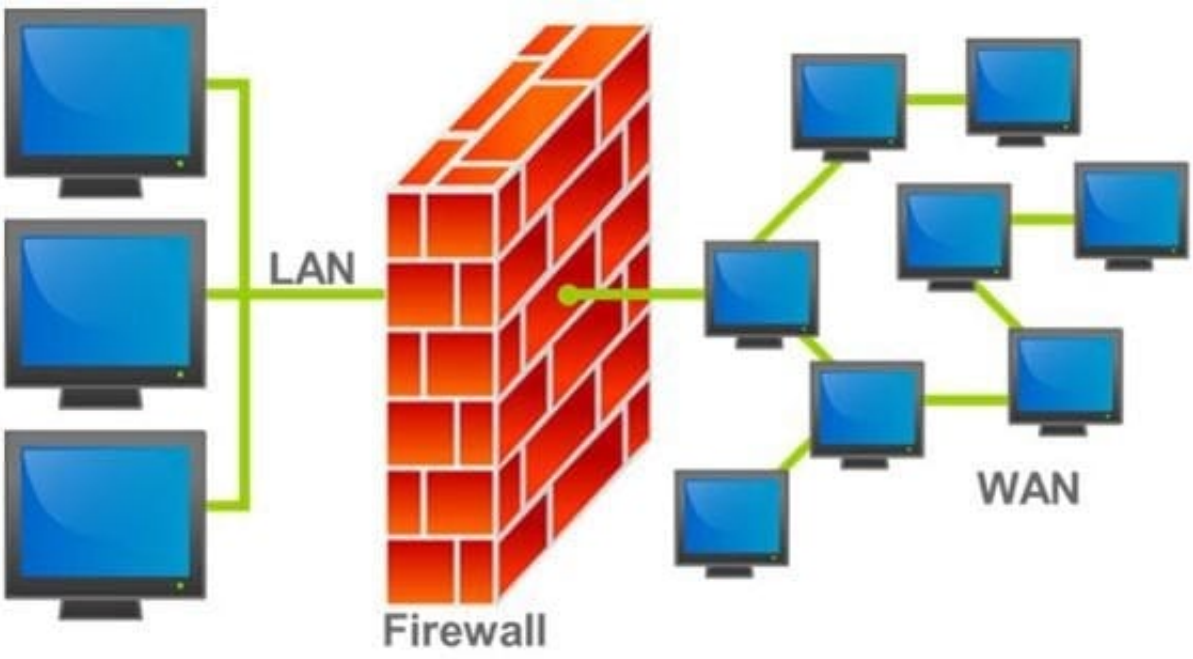
C. FTP fingerprinting

D. SNMP fingerprinting

Correct Answer: C

**QUESTION 9**

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.




Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

A. Appliance based firewalls cannot be upgraded

B. Firewalls implemented on a hardware firewall are highly scalable

C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system

D. Operating system firewalls are highly configured

Correct Answer: C

**QUESTION 10**

From where can clues about the underlying application environment can be collected?

A. From the extension of the file

B. From executable file

C. From file types and directories

D. From source code

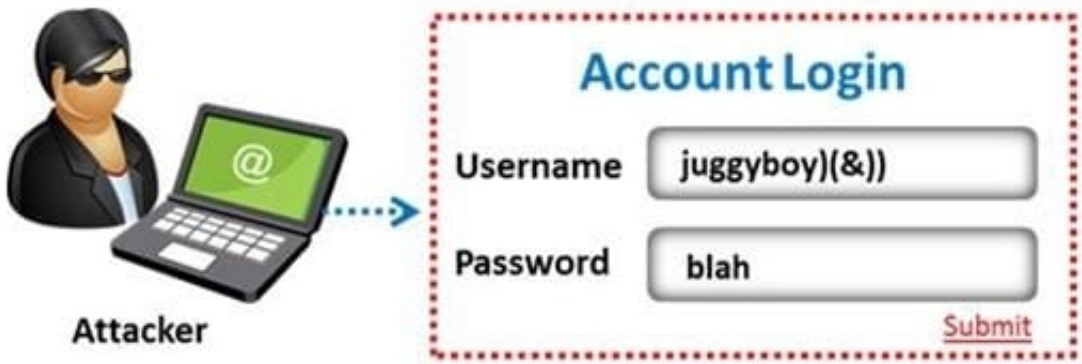
Correct Answer: A

**QUESTION 11**

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:




A. Frame Injection Attack

B. LDAP Injection Attack

C. XPath Injection Attack

D. SOAP Injection Attack

Correct Answer: B

Reference: e https://www.blackhat.com/presentations/bh-europe-08/Alonso- Parada/Whitepaper/bh-eu-08alonso-parada-WP.pdf ( page 3 to 5)

**QUESTION 12**

Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most people say `Wireless\\' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and

A. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

B. 802.11b

C. 802.11g

D. 802.11-Legacy

E. 802.11n

Correct Answer: A

**QUESTION 13**

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

A. -sS

B. -sV

C. -sU

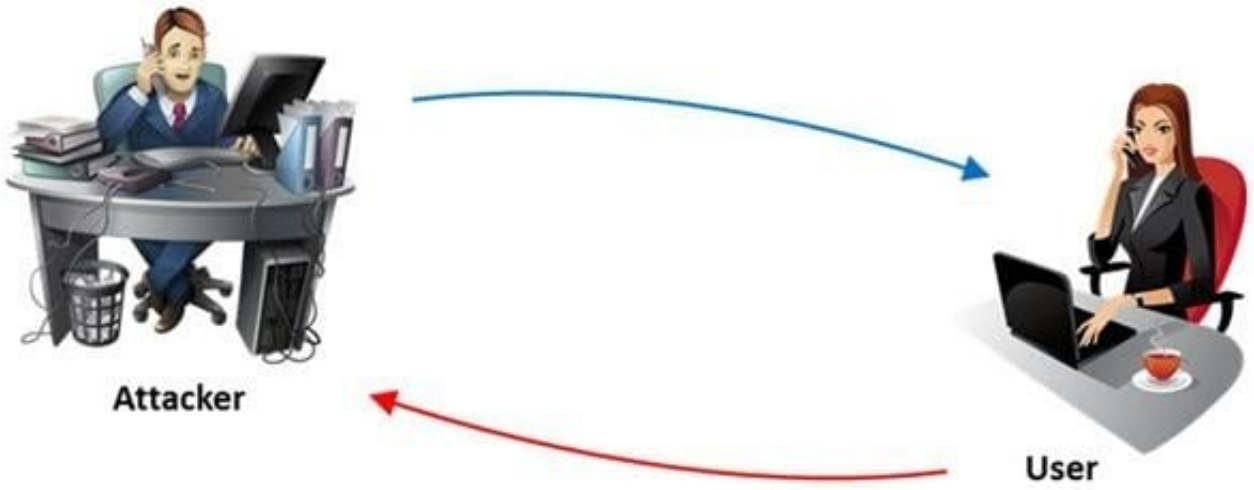
D. -sT

Correct Answer: B

Reference: https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001) (blackbox test and example, second para)

**QUESTION 14**

The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.




What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing

B. Spoofing

C. Tapping

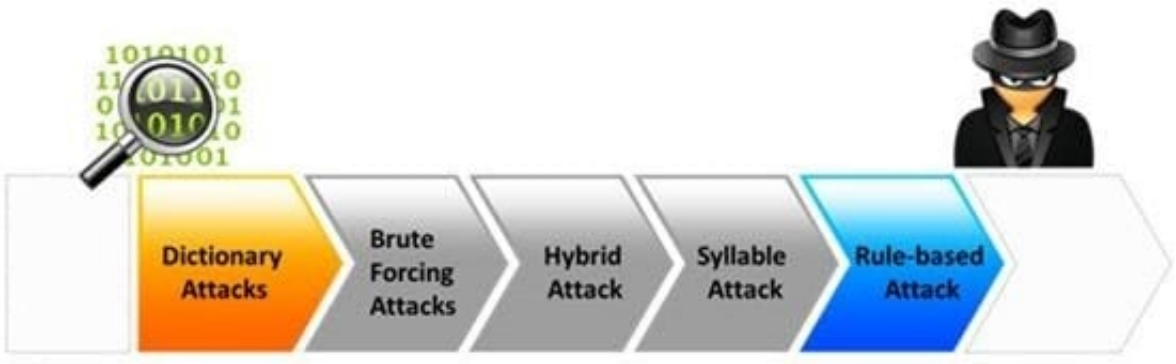
D. Vishing

Correct Answer: D

**QUESTION 15**

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

Reference:

http://books.google.com.pk/books?id=m2qZNW4dcyICandpg=PA237andlpg=PA237anddq=passw ord+cracking

+attacks+tries+every+combination+of+characters+until+the+password+is+bro

kenandsource=blandots=RKEUUo6LYjandsig=MPEfFBEpoO0yvOwMxYCoPQuqM5gandhl=enandsa=

Xandei=ZdwdVJm3CoXSaPXsgPgMandved=0CCEQ6AEwAQ#v=onepageandq=password%20cr acking%

20attacks%20tries%20every%20combination%20of%20characters%20until%20th e%20password%20is%

20brokenandf=false