



## EC-Council

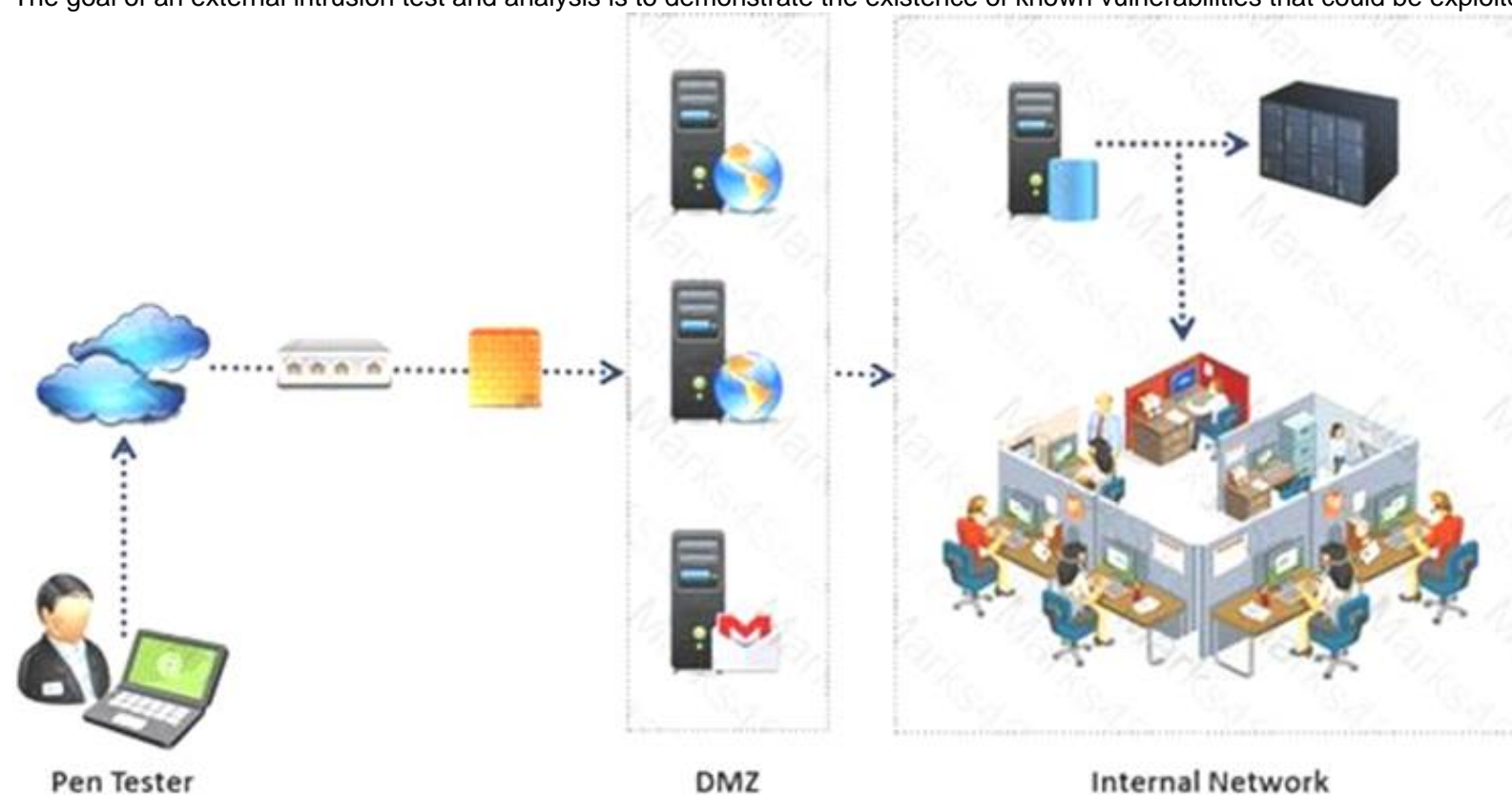
### Exam Questions 412-79v10

EC-Council Certified Security Analyst (ECSA) V10

### NEW QUESTION 1

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

**Answer: B**

### NEW QUESTION 2

Windows stores user passwords in the Security Accounts Manager database (SAM), or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.

NTLM and LM authentication protocols are used to securely store a user's password in the SAM database using different hashing methods.



The SAM file in Windows Server 2008 is located in which of the following locations?

- A. c:\windows\system32\config\SAM
- B. c:\windows\system32\drivers\SAM
- C. c:\windows\system32\Setup\SAM
- D. c:\windows\system32\Boot\SAM

**Answer: D**

### NEW QUESTION 3

What will the following URL produce in an unpatched IIS Web Server?

`http://www.thetargetsite.com/scripts/../../../../windows/system32/cmd.exe?/c+dir+c:\`

- A. Execute a buffer flow in the C: drive of the web server
- B. Insert a Trojan horse into the C: drive of the web server
- C. Directory listing of the C:\windows\system32 folder on the web server
- D. Directory listing of C: drive on the web server

**Answer: D**

### NEW QUESTION 4

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

- A. OSPF
- B. BPG
- C. ATM
- D. UDP

**Answer:** A

#### NEW QUESTION 5

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

**Answer:** D

#### NEW QUESTION 6

During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

- A. Examine Source of the Available Pages
- B. Perform Web Spidering
- C. Perform Banner Grabbing
- D. Check the HTTP and HTML Processing by the Browser

**Answer:** D

#### NEW QUESTION 7

What is a good security method to prevent unauthorized users from "tailgating"?

- A. Electronic key systems
- B. Man trap
- C. Pick-resistant locks
- D. Electronic combination locks

**Answer:** B

#### NEW QUESTION 8

Identify the policy that defines the standards for the organizational network connectivity and security standards for computers that are connected in the organizational network.

- A. Information-Protection Policy
- B. Special-Access Policy
- C. Remote-Access Policy
- D. Acceptable-Use Policy

**Answer:** C

#### NEW QUESTION 9

DNS information records provide important data about:

- A. Phone and Fax Numbers
- B. Location and Type of Servers
- C. Agents Providing Service to Company Staff
- D. New Customer

**Answer:** B

#### NEW QUESTION 10

Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

- A. 3001-3100
- B. 5000-5099
- C. 6666-6674
- D. 0 – 1023

**Answer:** D

#### NEW QUESTION 10

Mason is footprinting an organization to gather competitive intelligence. He visits the company's website for contact information and telephone numbers but does not find any. He knows the entire staff directory was listed on their website 12 months. How can he find the directory?

- A. Visit Google's search engine and view the cached copy
- B. Crawl and download the entire website using the Surffoffline tool and save them to his computer
- C. Visit the company's partners' and customers' website for this information
- D. Use Way Back Machine in Archive.org web site to retrieve the Internet archive

**Answer:** D

#### NEW QUESTION 11

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

- A. -sS
- B. -sV
- C. -sU
- D. -sT

**Answer:** B

#### NEW QUESTION 16

What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

- A. Server Side Includes
- B. Sort Server Includes
- C. Server Sort Includes
- D. Slide Server Includes

**Answer:** A

#### NEW QUESTION 18

Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

- A. ./snort -dvr packet.log icmp
- B. ./snort -dev -l ./log
- C. ./snort -dv -r packet.log
- D. ./snort -l ./log -b

**Answer:** C

#### NEW QUESTION 19

The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

- A. HIPAA
- B. Sarbanes-Oxley 2002
- C. Gramm-Leach-Bliley Act
- D. California SB 1386a

**Answer:** C

#### NEW QUESTION 22

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

**Answer:** C

#### NEW QUESTION 26

Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

- A. Threat-Assessment Phase
- B. Pre-Assessment Phase
- C. Assessment Phase
- D. Post-Assessment Phase

**Answer:** B

#### NEW QUESTION 31

Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

- A. Weak Screened Subnet Architecture
- B. "Inside Versus Outside" Architecture
- C. "Three-Homed Firewall" DMZ Architecture
- D. Strong Screened-Subnet Architecture

**Answer:** A

#### NEW QUESTION 34

One needs to run "Scan Server Configuration" tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound

interface of the Nessus daemon to be configured.

By default, the Nessus daemon listens to connections on which one of the following?

- A. Localhost (127.0.0.1) and port 1241
- B. Localhost (127.0.0.1) and port 1240
- C. Localhost (127.0.0.1) and port 1246
- D. Localhost (127.0.0.0) and port 1243

**Answer:** A

#### NEW QUESTION 39

Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

- A. DNSSEC
- B. Netsec
- C. IKE
- D. IPsec

**Answer:** D

#### NEW QUESTION 43

Which of the following protocols cannot be used to filter VoIP traffic?

- A. Media Gateway Control Protocol (MGCP)
- B. Real-time Transport Control Protocol (RTCP)
- C. Session Description Protocol (SDP)
- D. Real-Time Publish Subscribe (RTPS)

**Answer:** D

#### NEW QUESTION 44

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

- A. From source code
- B. From file types and directories
- C. From executable file
- D. From the extension of the file

**Answer:** D

#### NEW QUESTION 46

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

- A. Avoid cross talk
- B. Avoid over-saturation of wireless signals
- C. So that the access points will work on different frequencies
- D. Multiple access points can be set up on the same channel without any issues

**Answer:** A

#### NEW QUESTION 48

Traffic on which port is unusual for both the TCP and UDP ports?

- A. Port 81
- B. Port 443
- C. Port 0
- D. Port 21

**Answer:** C

#### NEW QUESTION 51

Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?

- A. Microsoft Baseline Security Analyzer (MBSA)
- B. CORE Impact
- C. Canvas
- D. Network Security Analysis Tool (NSAT)

**Answer:** C

#### NEW QUESTION 53

Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

- A. Project Goal

- B. Success Factors
- C. Objectives
- D. Assumptions

**Answer:** D

#### NEW QUESTION 54

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

**Answer:** C

#### NEW QUESTION 57

Which of the following methods is used to perform server discovery?

- A. Banner Grabbing
- B. Who is Lookup
- C. SQL Injection
- D. Session Hijacking

**Answer:** B

#### NEW QUESTION 61

You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

- A. Analyzing, categorizing and prioritizing resources
- B. Evaluating the existing perimeter and internal security
- C. Checking for a written security policy
- D. Analyzing the use of existing management and control architecture

**Answer:** C

#### NEW QUESTION 63

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs.

The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

- A. Pattern matching
- B. Statistical-based anomaly detection
- C. Real-time anomaly detection
- D. Signature-based anomaly detection

**Answer:** C

#### NEW QUESTION 68

Logs are the record of the system and network activities. Syslog protocol is used for delivering log information across an IP network. Syslog messages can be sent via which one of the following?

- A. UDP and TCP
- B. TCP and SMTP
- C. SMTP
- D. UDP and SMTP

**Answer:** A

#### NEW QUESTION 71

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

**Answer:** C

#### NEW QUESTION 72

Identify the framework that comprises of five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement:



- A. Information System Security Assessment Framework (ISSAF)
- B. Microsoft Internet Security Framework
- C. Nortells Unified Security Framework
- D. Federal Information Technology Security Assessment Framework

**Answer:** D

#### NEW QUESTION 76

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

- A. Web Services Footprinting Attack
- B. Service Level Configuration Attacks
- C. URL Tampering Attacks
- D. Inside Attacks

**Answer:** A

#### NEW QUESTION 79

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.

What are you trying to accomplish here?

- A. Poison the DNS records with false records
- B. Enumerate MX and A records from DNS
- C. Establish a remote connection to the Domain Controller
- D. Enumerate domain user accounts and built-in groups

**Answer:** D

#### NEW QUESTION 80

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

- A. intitle:"exchange server"
- B. outlook:"search"
- C. locate:"logon page"
- D. allinurl:"exchange/logon.asp"

**Answer:** D

#### NEW QUESTION 81

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

- A. Smurf scan
- B. Tracert
- C. Ping trace
- D. ICMP ping sweep

**Answer:** D

#### NEW QUESTION 85

John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtrcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found.

What information will he be able to gather from this?

- A. The SID of Hillary's network account
- B. The network shares that Hillary has permissions
- C. The SAM file from Hillary's computer
- D. Hillary's network username and password hash

**Answer:** D

#### NEW QUESTION 90

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies.

A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces.

What could have prevented this information from being stolen from the laptops?

- A. SDW Encryption
- B. EFS Encryption
- C. DFS Encryption
- D. IPS Encryption

**Answer:** B

#### NEW QUESTION 94

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

**Answer:** C

#### NEW QUESTION 95

A firewall's decision to forward or reject traffic in network filtering is dependent upon which of the following?

- A. Destination address
- B. Port numbers
- C. Source address
- D. Protocol used

**Answer:** D

#### NEW QUESTION 96

An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

- A. Leaky Wave Antennas
- B. Aperture Antennas
- C. Reflector Antenna
- D. Directional Antenna

**Answer:** B

#### NEW QUESTION 100

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted.

Which one of the following scanned timing options in NMAP's scan is useful across slow WAN links or to hide the scan?

- A. Paranoid
- B. Sneaky
- C. Polite
- D. Normal

**Answer:** C

#### NEW QUESTION 105

What is the target host IP in the following command?

```
C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP
```

- A. Firewalk does not scan target hosts
- B. 172.16.28.95
- C. This command is using FIN packets, which cannot scan target hosts
- D. 10.10.150.1

**Answer:** A

#### NEW QUESTION 107

Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

- A. Vulnerability Report
- B. Executive Report
- C. Client-side test Report
- D. Host Report

**Answer:** B

#### NEW QUESTION 108

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)

**Answer:** A



**NEW QUESTION 113**

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

**Answer:** C

**NEW QUESTION 115**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### 412-79v10 Practice Exam Features:

- \* 412-79v10 Questions and Answers Updated Frequently
- \* 412-79v10 Practice Questions Verified by Expert Senior Certified Staff
- \* 412-79v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 412-79v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 412-79v10 Practice Test Here](#)**