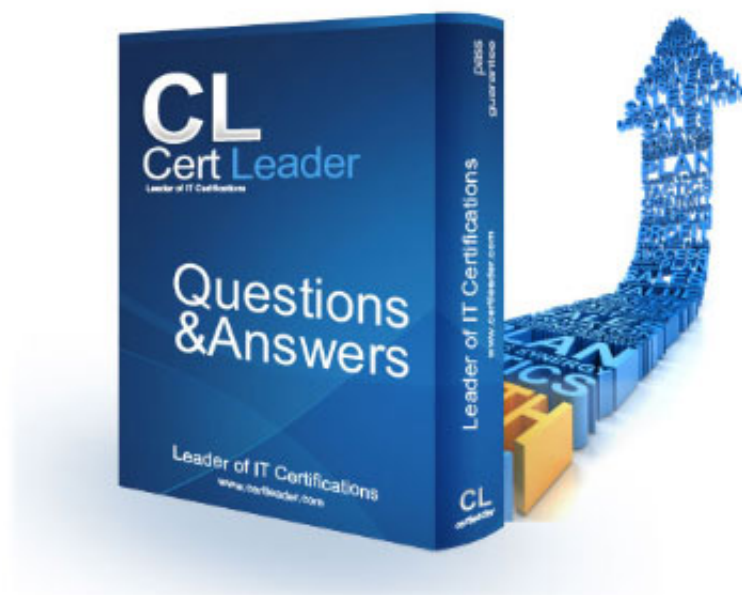


## 412-79v10 Dumps

### EC-Council Certified Security Analyst (ECSA) V10

<https://www.certleader.com/412-79v10-dumps.html>





**NEW QUESTION 1**

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 2**

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"

**Answer: B**

**NEW QUESTION 3**

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 4**

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet".

Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

- A. More RESET packets to the affected router to get it to power back up
- B. RESTART packets to the affected router to get it to power back up
- C. The change in the routing fabric to bypass the affected router
- D. STOP packets to all other routers warning of where the attack originated

**Answer: C**

**NEW QUESTION 5**

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 6**

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

- A. AES
- B. DES (ECB mode)
- C. MD5
- D. RC5

**Answer: C**

**NEW QUESTION 7**

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 8**

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and Zombies? What type of Penetration Testing is Larry planning to carry out?

- A. Internal Penetration Testing
- B. Firewall Penetration Testing
- C. DoS Penetration Testing
- D. Router Penetration Testing

**Answer:** C

**NEW QUESTION 9**

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 10**

An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

- A. Frame Injection Attack
- B. LDAP Injection Attack
- C. XPath Injection Attack
- D. SOAP Injection Attack

**Answer:** D

**NEW QUESTION 10**

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 13**

Which of the following acts related to information security in the US establish that the management of an organization is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

- A. USA Patriot Act 2001
- B. Sarbanes-Oxley 2002
- C. Gramm-Leach-Bliley Act (GLBA)
- D. California SB 1386

**Answer:** A

**NEW QUESTION 18**

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

**Answer:** D

**NEW QUESTION 22**

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

- A. %systemroot%\LSA
- B. %systemroot%\repair
- C. %systemroot%\system32\drivers\etc



D. %systemroot%\system32\LSA

**Answer:** B

#### NEW QUESTION 25

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

```
<script>alert("This is a test.")</script>
```

When you type this and click on search, you receive a pop-up window that says: "This is a test."

What is the result of this test?

- A. Your website is vulnerable to web bugs
- B. Your website is vulnerable to XSS
- C. Your website is not vulnerable
- D. Your website is vulnerable to SQL injection

**Answer:** B

#### NEW QUESTION 29

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 30

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 35

Which of the following is the objective of Gramm-Leach-Bliley Act?

- A. To ease the transfer of financial information between institutions and banks
- B. To protect the confidentiality, integrity, and availability of data
- C. To set a new or enhanced standards for all U.
- D. public company boards, management and public accounting firms
- E. To certify the accuracy of the reported financial statement

**Answer:** A

#### NEW QUESTION 39

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 40

Which one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

- A. Airsnort
- B. Aircrack
- C. Airpwn
- D. WEPCrack

**Answer:** C

#### NEW QUESTION 43

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 44

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code.

While searching through the code, you come across something abnormal:

```
<img  
src=http://coolwebsearch.com/ads/pixel.news.com width=1 height=1 border=0  
>
```

What have you found?

- A. Trojan.downloader
- B. Blind bug
- C. Web bug
- D. CGI code

**Answer:** C

#### NEW QUESTION 48

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 52

DMZ is a network designed to give the public access to the specific internal resources and you might want to do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories.

Identify the attacks that fall under Passive attacks category.

- A. Wardriving
- B. Spoofing
- C. Sniffing
- D. Network Hijacking

**Answer:** A

#### NEW QUESTION 55

You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable.

You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

- A. The firewall failed-open
- B. The firewall failed-bypass
- C. The firewall failed-closed
- D. The firewall ACL has been purged

**Answer:** A

#### NEW QUESTION 57

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 61

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 62

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 66

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast.

On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently.

What could be Tyler issue with his home wireless network?

- A. 2.4 Ghz Cordless phones
- B. Satellite television
- C. CB radio
- D. Computers on his wired network

**Answer:** A

#### NEW QUESTION 71

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable.

What kind of results did Jim receive from his vulnerability analysis?

- A. True negatives
- B. False negatives
- C. False positives
- D. True positives

**Answer:** B

#### NEW QUESTION 73

Which of the following is not the SQL injection attack character?

- A. \$
- B. PRINT
- C. #
- D. @@variable

**Answer:** A

#### NEW QUESTION 74

Identify the correct formula for Return on Investment (ROI).

- A.  $ROI = ((\text{Expected Returns} - \text{Cost of Investment}) / \text{Cost of Investment}) * 100$
- B.  $ROI = (\text{Expected Returns} + \text{Cost of Investment}) / \text{Cost of Investment}$
- C.  $ROI = (\text{Expected Returns Cost of Investment}) / \text{Cost of Investment}$
- D.  $ROI = ((\text{Expected Returns} + \text{Cost of Investment}) / \text{Cost of Investment}) * 100$

**Answer:** C

#### NEW QUESTION 77

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 81

If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

- A. Parameter tampering Attack
- B. Sql injection attack
- C. Session Hijacking
- D. Cross-site request attack



**Answer:** D

**NEW QUESTION 84**

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 85**

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

**Answer:** B

**NEW QUESTION 90**

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

`http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--`

`http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--`

`http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--`

`http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—`

What is the table name?

- A. CTS
- B. QRT
- C. EMP
- D. ABC

**Answer:** C

**NEW QUESTION 93**

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

**Answer:** D

**NEW QUESTION 94**

In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

- A. IPS evasion technique
- B. IDS evasion technique
- C. UDP evasion technique
- D. TTL evasion technique

**Answer:** D

**NEW QUESTION 99**

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers.

Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

- A. net port 22
- B. udp port 22 and host 172.16.28.1/24
- C. src port 22 and dst port 22
- D. src port 23 and dst port 23

**Answer:** C



**NEW QUESTION 104**

Which of the following will not handle routing protocols properly?

- A. "Internet-router-firewall-net architecture"
- B. "Internet-firewall-router-net architecture"
- C. "Internet-firewall -net architecture"
- D. "Internet-firewall/router(edge device)-net architecture"

**Answer:** B

**NEW QUESTION 107**

As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

- A. The employees network usernames and passwords
- B. The MAC address of the employees' computers
- C. The IP address of the employees computers
- D. Bank account numbers and the corresponding routing numbers

**Answer:** C

**NEW QUESTION 112**

Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

- A. Penetration Testing Agreement
- B. Rules of Behavior Agreement
- C. Liability Insurance
- D. Non-Disclosure Agreement

**Answer:** D

**NEW QUESTION 117**

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 118**

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 119**

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

**Answer:** A

**NEW QUESTION 124**

Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

- A. Information-Protection Po
- B. Paranoid Policy
- C. Promiscuous Policy
- D. Prudent Policy

**Answer:** B

**NEW QUESTION 126**

Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?



- A. Wireshark: Capinfos
- B. Wireshark: Tcpdump
- C. Wireshark: Text2pcap
- D. Wireshark: Dumpcap

**Answer:** D

#### NEW QUESTION 129

Output modules allow Snort to be much more flexible in the formatting and presentation of output to its users. Snort has 9 output plug-ins that push out data in different formats. Which one of the following output plug-ins allows alert data to be written in a format easily importable to a database?

- A. unified
- B. csv
- C. alert\_unixsock
- D. alert\_fast

**Answer:** B

#### NEW QUESTION 133

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 136

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

- A. Circuit-level proxy firewall
- B. Packet filtering firewall
- C. Application-level proxy firewall
- D. Statefull firewall

**Answer:** D

#### NEW QUESTION 137

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 142

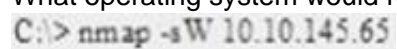
Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

- A. 6566 TCP port
- B. 6771 TCP port
- C. 6667 TCP port
- D. 6257 TCP port

**Answer:** C

#### NEW QUESTION 146

What operating system would respond to the following command?



- A. Mac OS X
- B. Windows XP
- C. Windows 95
- D. FreeBSD

**Answer:** D

#### NEW QUESTION 148



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 153**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 412-79v10 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/412-79v10-dumps.html>