

412-79v10 Dumps

EC-Council Certified Security Analyst (ECSA) V10

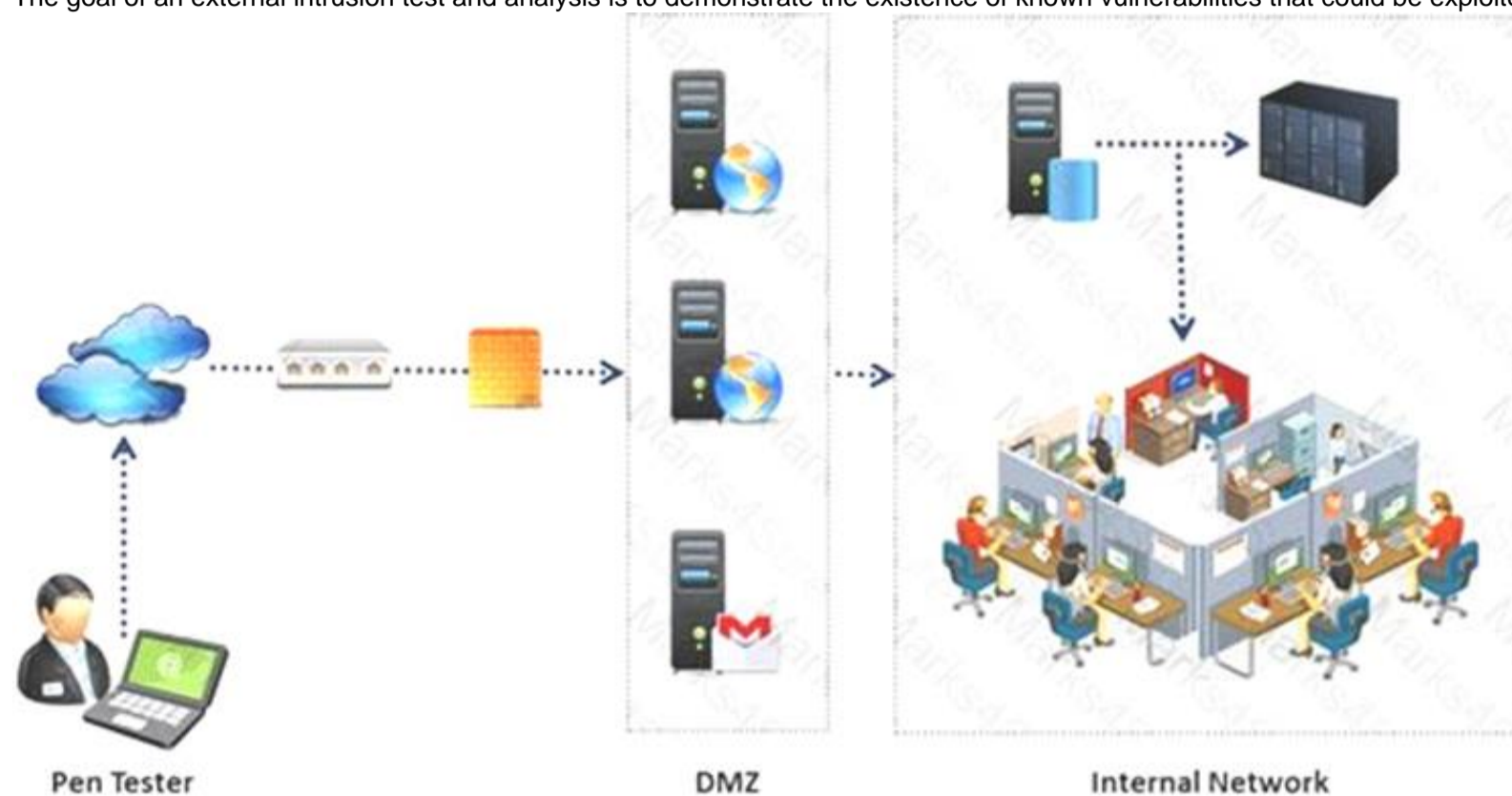
<https://www.certleader.com/412-79v10-dumps.html>



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

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 field.

If the destination is not reachable, which one of the following are generated?

- A. Type 8 ICMP codes
- B. Type 12 ICMP codes
- C. Type 3 ICMP codes
- D. Type 7 ICMP codes

Answer: C

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 of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

- A. Vulnerabilities checklists
- B. Configuration checklists
- C. Action Plan
- D. Testing Plan

Answer: A

NEW QUESTION 6

Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
include <stdio.h>
#include <string.h>
int main(int argc, char *argv[])
{
char buffer[10]; if (argc < 2)
{
fprintf(stderr, "USAGE: %s string\n", argv[0]); return 1;
}
strcpy(buffer, argv[1]); return 0;
}
```

- A. Buffer overflow
- B. Format string bug
- C. Kernal injection
- D. SQL injection

Answer: A

NEW QUESTION 7

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

- A. Poison the switch's MAC address table by flooding it with ACK bits
- B. Enable tunneling feature on the switch
- C. Trick the switch into thinking it already has a session with Terri's computer
- D. Crash the switch with a DoS attack since switches cannot send ACK bits

Answer: C

NEW QUESTION 8

Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

- A. Special-Access Policy
- B. User Identification and Password Policy
- C. Personal Computer Acceptable Use Policy
- D. User-Account Policy

Answer: B

NEW QUESTION 9

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

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

- A. Techniques for data collection from systems upon termination of the test
- B. Techniques for data exclusion from systems upon termination of the test
- C. Details on how data should be transmitted during and after the test
- D. Details on how organizational data is treated throughout and after the test

Answer: A

NEW QUESTION 10

The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the signal () function. Which one of the following functions is used as a program-specific signal and the handler for this calls the DropStats() function to output the current Snort statistics?

- A. SIGUSR1
- B. SIGTERM
- C. SIGINT
- D. SIGHUP

Answer: A

NEW QUESTION 13

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 18

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 20

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 25

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 30

By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

- A. PortQry
- B. Netstat
- C. Telnet
- D. Tracert

Answer: A

NEW QUESTION 33

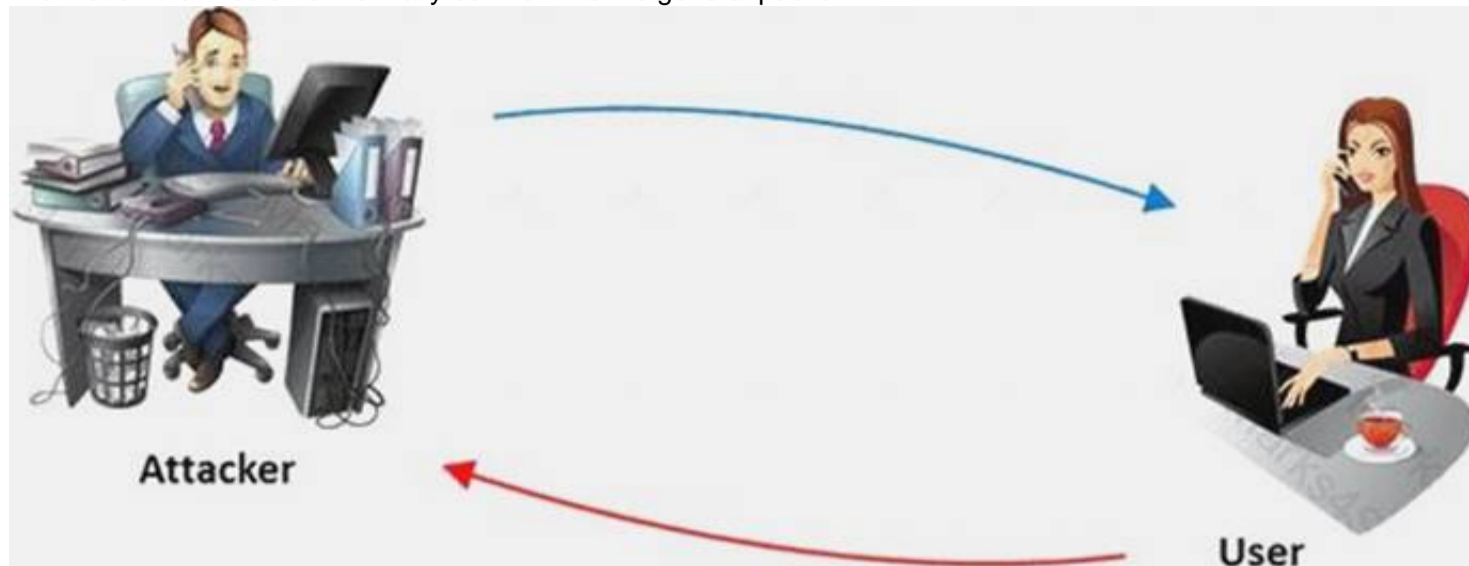
Which of the following is the objective of Gramm-Leach-Bliley Act?

- 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 38

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

Answer: D

NEW QUESTION 41

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information.

You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

- A. Nmap
- B. Netcraft
- C. Ping sweep
- D. Dig

Answer: B

NEW QUESTION 43

Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes. Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

- A. Packet Sniffer Mode
- B. Packet Logger Mode
- C. Network Intrusion Detection System Mode
- D. Inline Mode

Answer: A

NEW QUESTION 47

Which one of the following acts makes reputational risk of poor security a reality because it requires public disclosure of any security breach that involves personal information if it is unencrypted or if it is reasonably believed that the information has been acquired by an unauthorized person?

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

Answer: A

NEW QUESTION 51

Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

- A. Decreases consumed employee time and increases system uptime
- B. Increases detection and reaction time
- C. Increases response time
- D. Both Decreases consumed employee time and increases system uptime and Increases response time

Answer: A

NEW QUESTION 54

One of the steps in information gathering is to run searches on a company using complex keywords in Google.



Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?

- A. ROCHESTON fileformat:+ppt
- B. ROCHESTON ppt:filestring
- C. ROCHESTON filetype:ppt
- D. ROCHESTON +ppt:filesearch

Answer: C

NEW QUESTION 59

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 64

Which one of the following tools of trade is an automated, comprehensive penetration testing product for assessing the specific information security threats to an organization?

- A. Sunbelt Network Security Inspector (SNSI)
- B. CORE Impact
- C. Canvas
- D. Microsoft Baseline Security Analyzer (MBSA)

Answer: C

NEW QUESTION 65

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 67

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 68

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 69

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

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

Answer: A

NEW QUESTION 70

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 73

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

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 77

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

- A. Filtered
- B. Stealth
- C. Closed
- D. Open

Answer: D

NEW QUESTION 78

Identify the port numbers used by POP3 and POP3S protocols.

- A. 113 and 981
- B. 111 and 982
- C. 110 and 995
- D. 109 and 973

Answer: C

NEW QUESTION 81

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 84

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet

filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

- A. IPSEC does not work with packet filtering firewalls
- B. NAT does not work with IPSEC
- C. NAT does not work with statefull firewalls
- D. Statefull firewalls do not work with packet filtering firewalls

Answer: B

NEW QUESTION 86

Which of the following defines the details of services to be provided for the client's organization and the list of services required for performing the test in the organization?

- A. Draft
- B. Report
- C. Requirement list
- D. Quotation

Answer: D

NEW QUESTION 89

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 94

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs.

He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

- A. CVE
- B. IANA
- C. RIPE
- D. APIPA

Answer: A

NEW QUESTION 97

In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc.

They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

- A. XPath Injection Attack
- B. Authorization Attack
- C. Authentication Attack
- D. Frame Injection Attack

Answer: B

NEW QUESTION 101

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 106

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"

Answer: A

NEW QUESTION 111

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 115

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 119

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa.

She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for.

What principal of social engineering did Julia use?

- A. Reciprocation
- B. Friendship/Liking
- C. Social Validation
- D. Scarcity

Answer: A

NEW QUESTION 122

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

- A. Passive IDS
- B. Active IDS
- C. Progressive IDS
- D. NIPS

Answer: B

NEW QUESTION 126

NTP protocol is used to synchronize the system clocks of computers with a remote time server or time source over a network. Which one of the following ports is used by NTP as its transport layer?

- A. TCP port 152
- B. UDP port 177
- C. UDP port 123
- D. TCP port 113

Answer: C

NEW QUESTION 130

Metasploit framework in an open source platform for vulnerability research, development, and penetration testing. Which one of the following metasploit options is used to exploit multiple systems at once?

- A. NinjaDontKill
- B. NinjaHost
- C. RandomNops
- D. EnablePython

Answer: A

NEW QUESTION 133

What operating system would respond to the following command?

```
C:\> nmap -sW 10.10.145.65
```

- A. Mac OS X
- B. Windows XP

- C. Windows 95
- D. FreeBSD

Answer: D

NEW QUESTION 134

What are the security risks of running a "repair" installation for Windows XP?

- A. There are no security risks when running the "repair" installation for Windows XP
- B. Pressing Shift+F1 gives the user administrative rights
- C. Pressing Ctrl+F10 gives the user administrative rights
- D. Pressing Shift+F10 gives the user administrative rights

Answer: D

NEW QUESTION 139

.....

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>