



## EC-Council

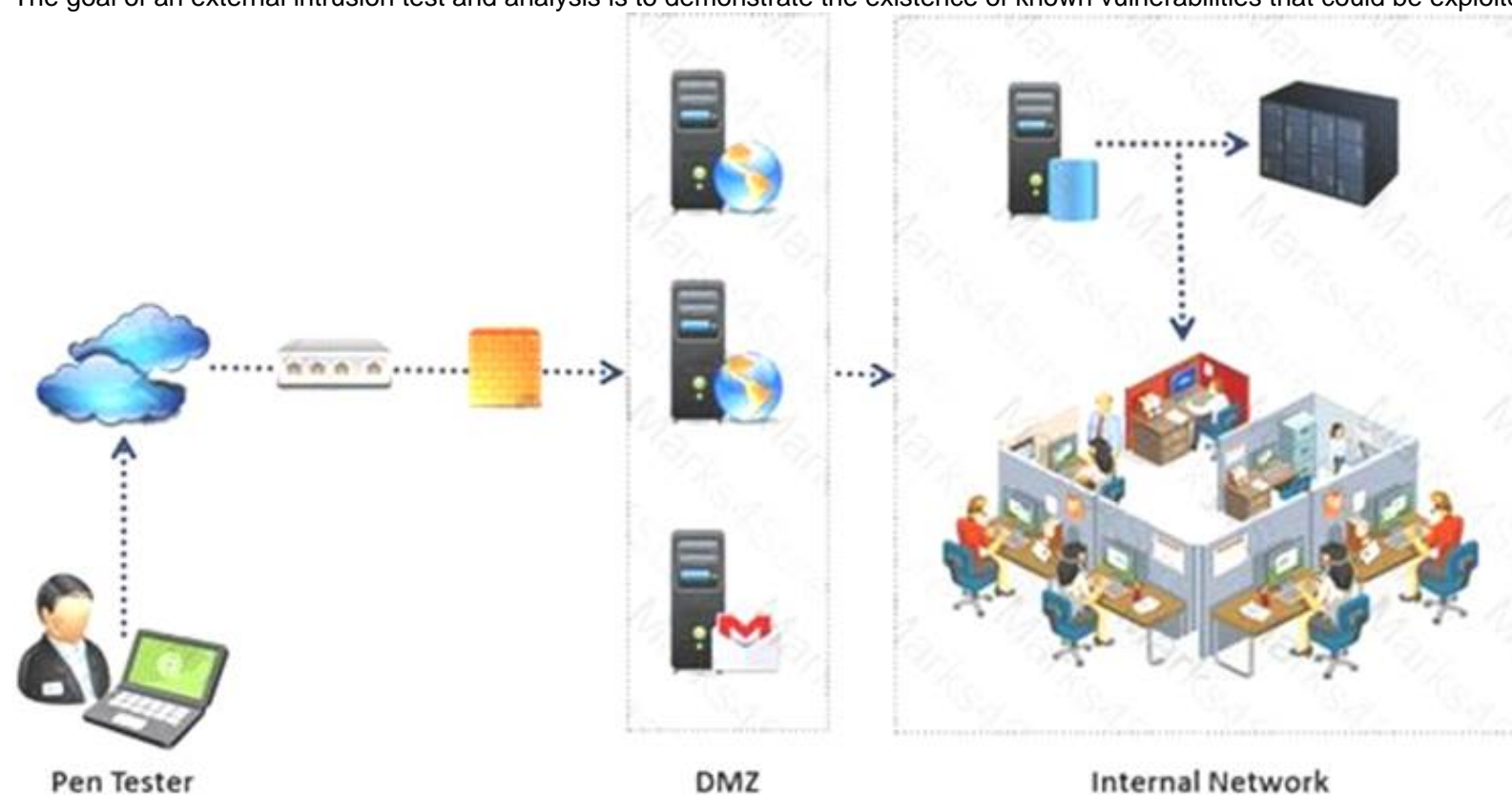
### Exam Questions 412-79v10

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

How many possible sequence number combinations are there in TCP/IP protocol?

- A. 320 billion
- B. 32 million
- C. 4 billion
- D. 1 billion

Answer: C

### NEW QUESTION 4

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 5

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

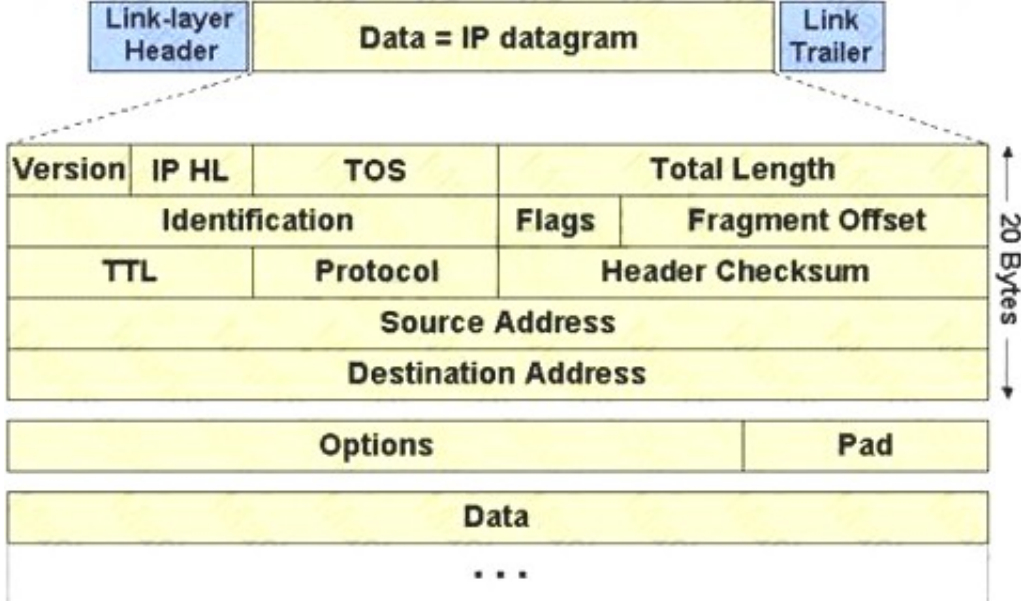
Answer: A

NEW QUESTION 6

The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.

The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.

IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.



The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

- A. Multiple of four bytes
- B. Multiple of two bytes
- C. Multiple of eight bytes
- D. Multiple of six bytes

Answer: C

NEW QUESTION 7

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 8

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. "?"

Answer: A

NEW QUESTION 9

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 10

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG. What is Simon trying to accomplish here?

- A. Enumerate all the users in the domain
- B. Perform DNS poisoning
- C. Send DOS commands to crash the DNS servers
- D. Perform a zone transfer

**Answer:** D

#### NEW QUESTION 10

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 12

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

**Answer:** B

#### NEW QUESTION 16

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 19

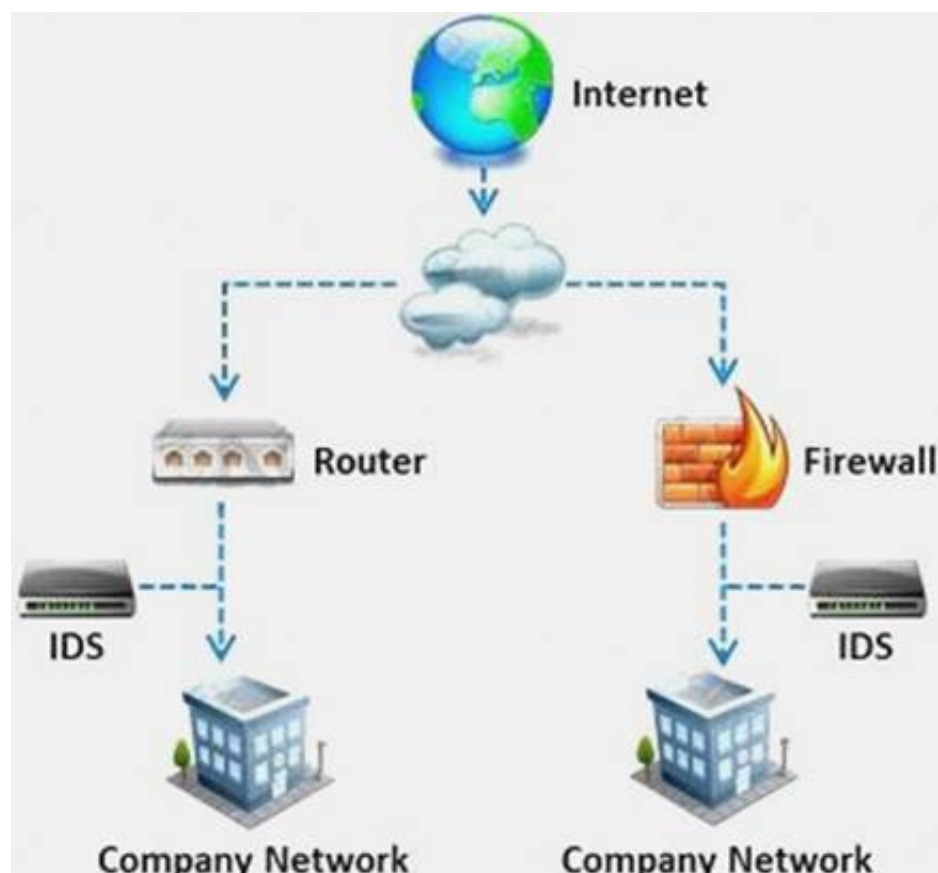
Which of the following policies helps secure data and protects the privacy of organizational information?

- A. Special-Access Policy
- B. Document retention Policy
- C. Cryptography Policy
- D. Personal Security Policy

**Answer:** C

#### NEW QUESTION 24

What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



- A. NIDS are usually a more expensive solution to implement compared to HIDS.
- B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
- C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.
- D. HIDS requires less administration and training compared to NIDS.

**Answer: C**

#### NEW QUESTION 28

Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

- A. Reverse Address Resolution Protocol (RARP)
- B. HTTP (Hypertext Transfer Protocol)
- C. SMTP (Simple Mail Transfer Protocol)
- D. Telnet

**Answer: A**

#### NEW QUESTION 33

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 38

War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks.

Which one of the following is a Linux based program that exploits the weak IV (Initialization Vector) problem documented with static WEP?

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

**Answer: A**

#### NEW QUESTION 42

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 44

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

link:www.ghitech.net

What will this search produce?

- A. All sites that link to ghttech.net
- B. Sites that contain the code: link:www.ghitech.net
- C. All sites that ghttech.net links to
- D. All search engines that link to .net domains

**Answer:** A

#### NEW QUESTION 49

Identify the person who will lead the penetration-testing project and be the client point of contact.

- A. Database Penetration Tester
- B. Policy Penetration Tester
- C. Chief Penetration Tester
- D. Application Penetration Tester

**Answer:** C

#### NEW QUESTION 52

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 54

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."

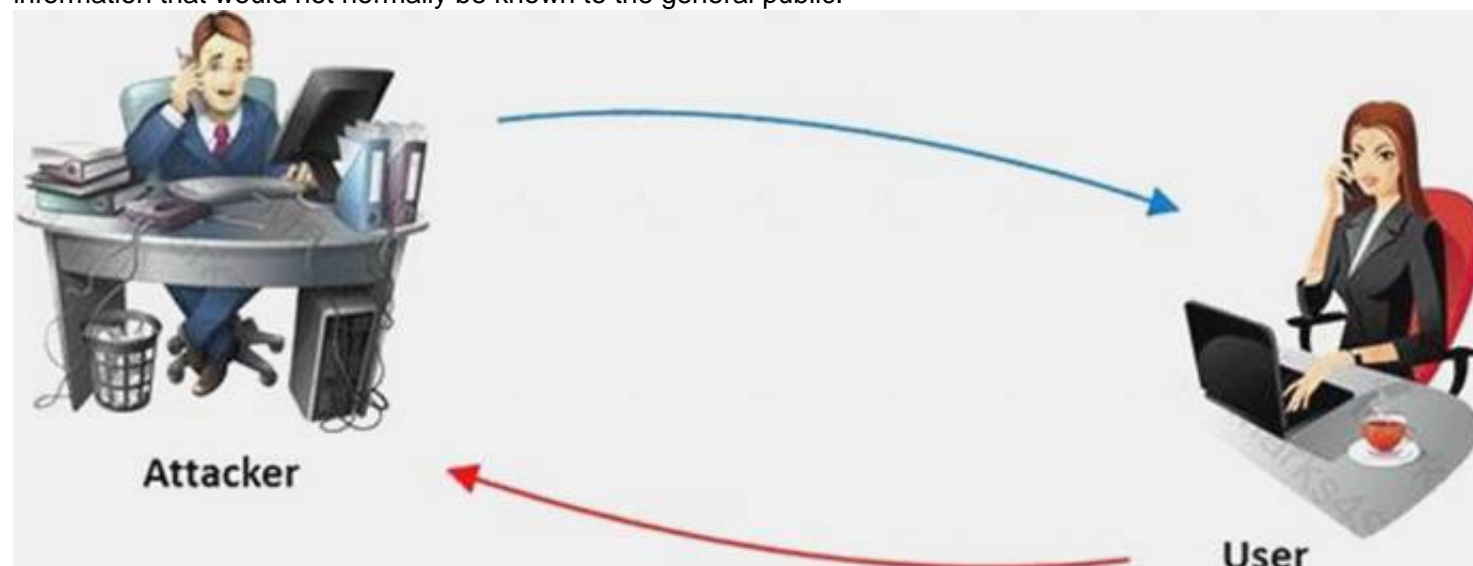
What is the result of this test?

- 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 59

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 64

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 69

Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

- A. Hash Key Length
- B. C/R Value Length
- C. C/R Key Length
- D. Hash Value Length

**Answer:** B

#### NEW QUESTION 72

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT.

Which firewall would be most appropriate for Harold?

- A. Application-level proxy firewall
- B. Data link layer firewall
- C. Packet filtering firewall
- D. Circuit-level proxy firewall

**Answer:** A

#### NEW QUESTION 77

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 78

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 79

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

`http://172.168.4.131/level/99/exec/show/config`

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

- A. URL Obfuscation Arbitrary Administrative Access Vulnerability
- B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
- C. HTTP Configuration Arbitrary Administrative Access Vulnerability
- D. HTML Configuration Arbitrary Administrative Access Vulnerability

**Answer:** C

#### NEW QUESTION 82

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 87

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 91

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 93

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 95

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 99

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 103

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 105

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 108

HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

- A. ASCII value of the character
- B. Binary value of the character
- C. Decimal value of the character
- D. Hex value of the character

**Answer:** D

#### NEW QUESTION 112

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 117

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 120

Which one of the following log analysis tools is a Cisco Router Log Format log analyzer and it parses logs, imports them into a SQL database (or its own built-in database), aggregates them, and generates the dynamically filtered reports, all through a web interface?

- A. Event Log Tracker
- B. Sawmill
- C. Syslog Manager
- D. Event Log Explorer

**Answer:** B

#### NEW QUESTION 125

What are the scanning techniques that are used to bypass firewall rules and logging mechanisms and disguise themselves as usual network traffic?

- A. Connect Scanning Techniques
- B. SYN Scanning Techniques
- C. Stealth Scanning Techniques
- D. Port Scanning Techniques

**Answer:** C

#### NEW QUESTION 129

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 134

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

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

**Answer:** A

#### NEW QUESTION 136

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses.

You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

- A. Metamorphic
- B. Oligomorph
- C. Polymorphic
- D. Transmorphic

**Answer:** A

#### NEW QUESTION 139

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 141

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. Nortell's Unified Security Framework
- D. Federal Information Technology Security Assessment Framework

**Answer:** D

#### NEW QUESTION 146

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 151

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 152

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 155

In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

- A. Circuit level firewalls
- B. Packet filters firewalls
- C. Stateful multilayer inspection firewalls
- D. Application level firewalls

**Answer:** D

#### NEW QUESTION 157

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 158

In Linux, what is the smallest possible shellcode?

- A. 800 bytes
- B. 8 bytes
- C. 80 bytes
- D. 24 bytes

**Answer:** D

#### NEW QUESTION 159

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 163

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 168

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 172

Which of the following statements is true about the LM hash?

- A. Disabled in Windows Vista and 7 OSs
- B. Separated into two 8-character strings
- C. Letters are converted to the lowercase
- D. Padded with NULL to 16 characters

Answer: A

#### NEW QUESTION 177

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the Restrict Anonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using User info tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

- A. Restrict Anonymous must be set to "2" for complete security
- B. Restrict Anonymous must be set to "3" for complete security
- C. There is no way to always prevent an anonymous null session from establishing
- D. Restrict Anonymous must be set to "10" for complete security

Answer: A

#### NEW QUESTION 179

What is the following command trying to accomplish?

```
C:\> nmap -sU -p445 192.168.0.0/24
```

- A. Verify that NETBIOS is running for the 192.168.0.0 network
- B. Verify that TCP port 445 is open for the 192.168.0.0 network
- C. Verify that UDP port 445 is open for the 192.168.0.0 network
- D. Verify that UDP port 445 is closed for the 192.168.0.0 networks

Answer: C

#### NEW QUESTION 184

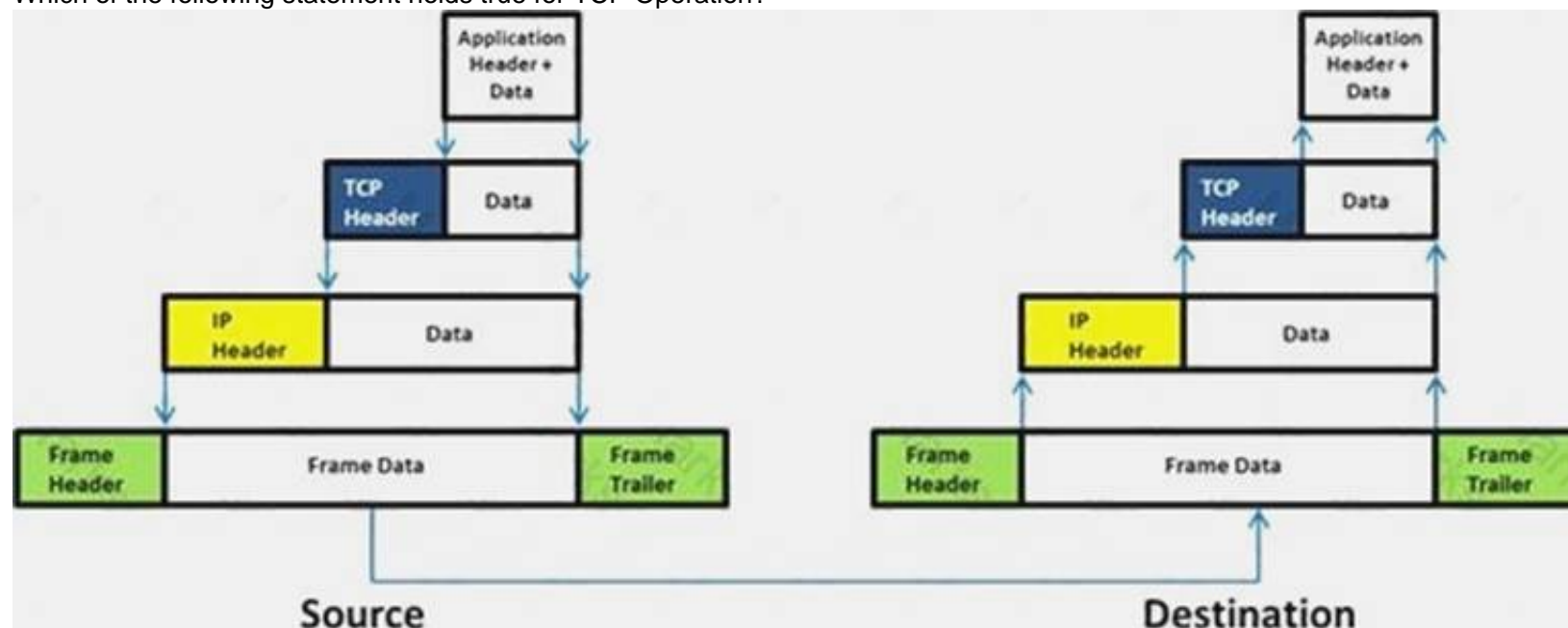
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

- A. A switched network will not respond to packets sent to the broadcast address
- B. Only IBM AS/400 will reply to this scan
- C. Only Unix and Unix-like systems will reply to this scan
- D. Only Windows systems will reply to this scan

Answer: C

#### NEW QUESTION 186

Which of the following statement holds true for TCP Operation?



- A. Port numbers are used to know which application the receiving host should pass the data to
- B. Sequence numbers are used to track the number of packets lost in transmission
- C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host
- D. Data transfer begins even before the connection is established

Answer: D

#### NEW QUESTION 190

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 195

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 198

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 202

Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

- A. Tcpdump
- B. Capinfos
- C. Tshark
- D. Idl2wrs

**Answer:** B

#### NEW QUESTION 204

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 207

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 208

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 211

Why is a legal agreement important to have before launching a penetration test?

**Penetration Testing Agreement**

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: \_\_\_\_\_

Testing Time Frame: (begin) \_\_\_\_\_ (end) \_\_\_\_\_

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: \_\_\_\_\_ (Business Owner)

\_\_\_\_\_ (Data Custodian)

\_\_\_\_\_ (CIO)

\_\_\_\_\_ (CISO)

Testing Complete: \_\_\_\_\_ Date: \_\_\_\_\_

Review/Closeout Discussion Completed (Date): \_\_\_\_\_

- A. Guarantees your consultant fees
- B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
- C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
- D. It is important to ensure that the target organization has implemented mandatory security policies

**Answer: C**

### NEW QUESTION 214

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 215

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 217

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 222

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 224

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 228

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 231

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**