

## ECSAv10 Dumps

# EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

<https://www.certleader.com/ECSAv10-dumps.html>



**NEW QUESTION 1**

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 2**

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 3**

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 4**

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 5**

Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

- A. SYN Scan
- B. Connect() scan
- C. XMAS Scan
- D. Null Scan

**Answer: A**

**NEW QUESTION 6**

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 7**

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 8**

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 9**

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 10**

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 10**

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 12**

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 16**

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 21**

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.

**Password hash using LM/NTLM**



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 22**

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

**Answer: C**

**NEW QUESTION 26**

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 29**

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 30**

Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?



- A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
- B. Examine Server Side Includes (SSI)
- C. Examine Hidden Fields
- D. Examine E-commerce and Payment Gateways Handled by the Web Server

**Answer: C**

**NEW QUESTION 32**

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 35**

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 40**

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 43**

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 45**

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 46**

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 48**

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 52**

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?

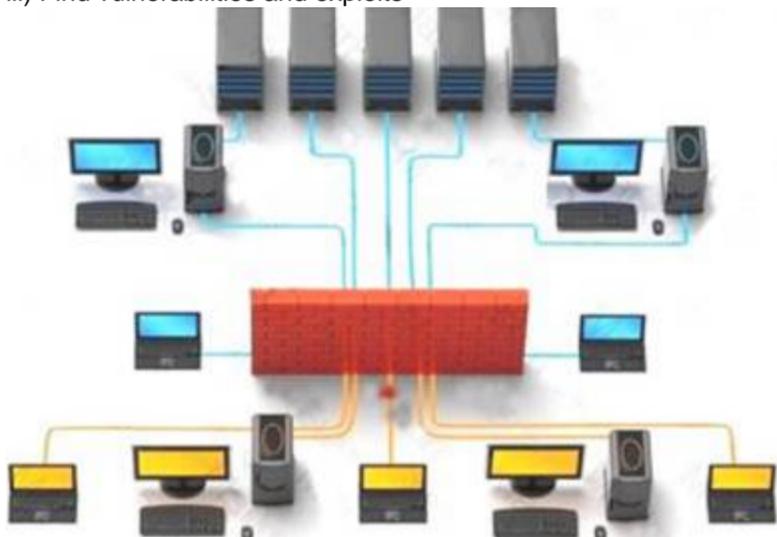
- A. Event Log Tracker
- B. Sawmill
- C. Syslog Manager
- D. Event Log Explorer

**Answer: B**

**NEW QUESTION 55**

Information gathering is performed to:

- i) Collect basic information about the target company and its network
- ii) Determine the operating system used, platforms running, web server versions, etc.
- iii) Find vulnerabilities and exploits



Which of the following pen testing tests yields information about a company's technology infrastructure?

- A. Searching for web page posting patterns
- B. Analyzing the link popularity of the company's website
- C. Searching for trade association directories
- D. Searching for a company's job postings

**Answer:** D

**NEW QUESTION 58**

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 60**

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 61**

In Linux, what is the smallest possible shellcode?

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

**Answer:** D

**NEW QUESTION 64**

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 68**

Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents	
1 The Cover Letter.....	2
1.1 Document Properties.....	3
1.2 Version.....	3
1.3 Table of Contents and List of Illustrations.....	4
1.4 Final Report Delivery Date.....	4
2 The Executive Summary.....	5
2.1 Scope of the Project.....	5
2.2 Purpose for the Evaluation.....	6
2.3 System Description.....	6
2.4 Assumption.....	7
2.5 Timeline.....	8
2.6 Summary of Evaluation.....	9
2.7 Summary of Findings.....	10
2.8 Summary of Recommendation.....	11
2.9 Testing Methodology.....	12
2.10 Planning.....	14
2.11 Exploitation.....	14
2.12 Reporting.....	15
3 Comprehensive Technical Report.....	16
3.1 Detailed SYSTEMS Information.....	17
3.2 Windows server.....	18
4 Result Analysis.....	19
5 Recommendations.....	20
6 Appendices.....	21
6.1 Required Work Efforts.....	22
6.2 Research.....	24
6.3 References.....	24
6.4 Glossary.....	25

- A. Client-Side Test Report
- B. Activity Report
- C. Host Report
- D. Vulnerability Report

**Answer: A**

**NEW QUESTION 71**

Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

- A. Active/Passive Tools
- B. Application-layer Vulnerability Assessment Tools
- C. Location/Data Examined Tools
- D. Scope Assessment Tools

**Answer: D**

**NEW QUESTION 73**

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 77**

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 78**

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 79**

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London.

After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

- A. RaidSniff
- B. Snort
- C. Ettercap
- D. Airsnort

**Answer:** C

**NEW QUESTION 81**

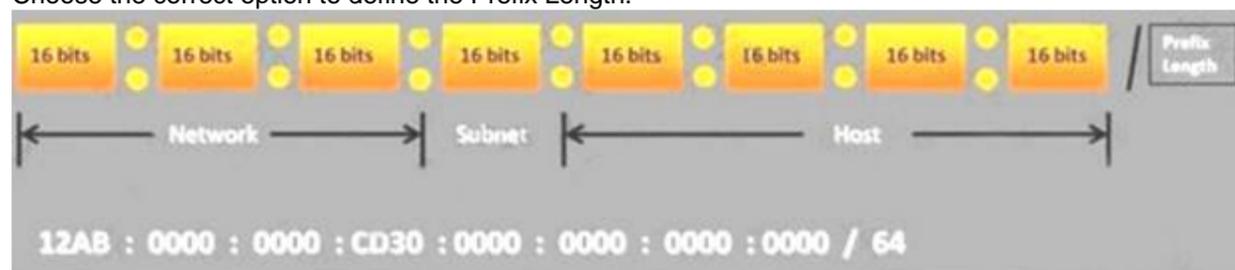
Logs are the record of the system and network activities. Syslog protocol is used for delivering log information across an IP network. Syslog messages can be sent via which one of the following?

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

**Answer:** A

**NEW QUESTION 82**

Choose the correct option to define the Prefix Length.



- A. Prefix Length = Subnet + Host portions
- B. Prefix Length = Network + Host portions
- C. Prefix Length = Network + Subnet portions
- D. Prefix Length = Network + Subnet + Host portions

**Answer:** C

**NEW QUESTION 87**

A framework for security analysis is composed of a set of instructions, assumptions, and limitations to analyze and solve security concerns and develop threat free applications.

Which of the following frameworks helps an organization in the evaluation of the company's information security with that of the industrial standards?

- A. Microsoft Internet Security Framework
- B. Information System Security Assessment Framework
- C. The IBM Security Framework
- D. Nortell's Unified Security Framework

**Answer:** B

**NEW QUESTION 88**

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 90**

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?

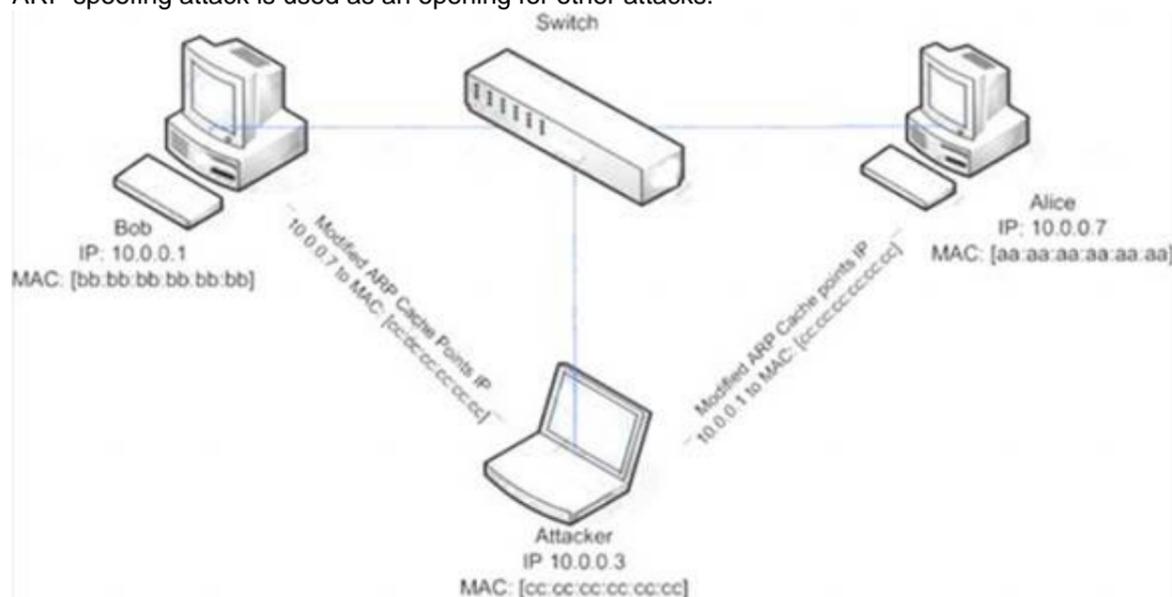
- A. Simple Network Management Protocol (SNMP)
- B. Network File system (NFS)
- C. Internet Control Message Protocol (ICMP)
- D. Transmission Control Protocol (TCP)

**Answer: A**

**NEW QUESTION 92**

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

- A. Parameter Filtering
- B. Social Engineering
- C. Input Validation
- D. Session Hijacking

**Answer: D**

**NEW QUESTION 96**

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 98**

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 101**

How many bits is Source Port Number in TCP Header packet?

- A. 48
- B. 32
- C. 64
- D. 16

**Answer: D**

**NEW QUESTION 103**

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 107**

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 108**

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 111**

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 114**

Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?



- A. Service-based Assessment Solutions
- B. Product-based Assessment Solutions
- C. Tree-based Assessment
- D. Inference-based Assessment

**Answer: C**

**NEW QUESTION 116**

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?

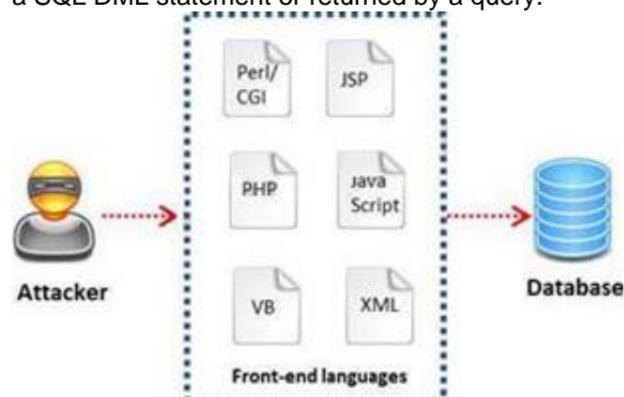
- A. 6566 TCP port
- B. 6771 TCP port

- C. 6667 TCP port
- D. 6257 TCP port

**Answer: C**

**NEW QUESTION 121**

A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable). What query does he need to write to retrieve the information?

- A. `EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000`
- B. `DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—`
- C. `SELECT * FROM StudentTable WHERE roll_number = " or '1' = '1'`
- D. `RETRIVE * FROM StudentTable WHERE roll_number = 1'#`

**Answer: C**

**NEW QUESTION 124**

A Demilitarized Zone (DMZ) is a computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization.

Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

- A. Lightweight Directory Access Protocol (LDAP)
- B. Simple Network Management Protocol (SNMP)
- C. Telnet
- D. Secure Shell (SSH)

**Answer: D**

**NEW QUESTION 126**

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame.

What ports should you open for SNMP to work through Firewalls. (Select 2)

- A. 162
- B. 160
- C. 161
- D. 163

**Answer: AC**

**NEW QUESTION 131**

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 136**

Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.



New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies.

In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.

What is the biggest threat to Web 2.0 technologies?

- A. SQL Injection Attacks
- B. Service Level Configuration Attacks
- C. Inside Attacks
- D. URL Tampering Attacks

**Answer:** A

**NEW QUESTION 138**

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 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 ECSAv10 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/ECSAv10-dumps.html>