



## EC-Council

### Exam Questions 412-79v10

EC-Council Certified Security Analyst (ECSA) V10

**NEW QUESTION 1**

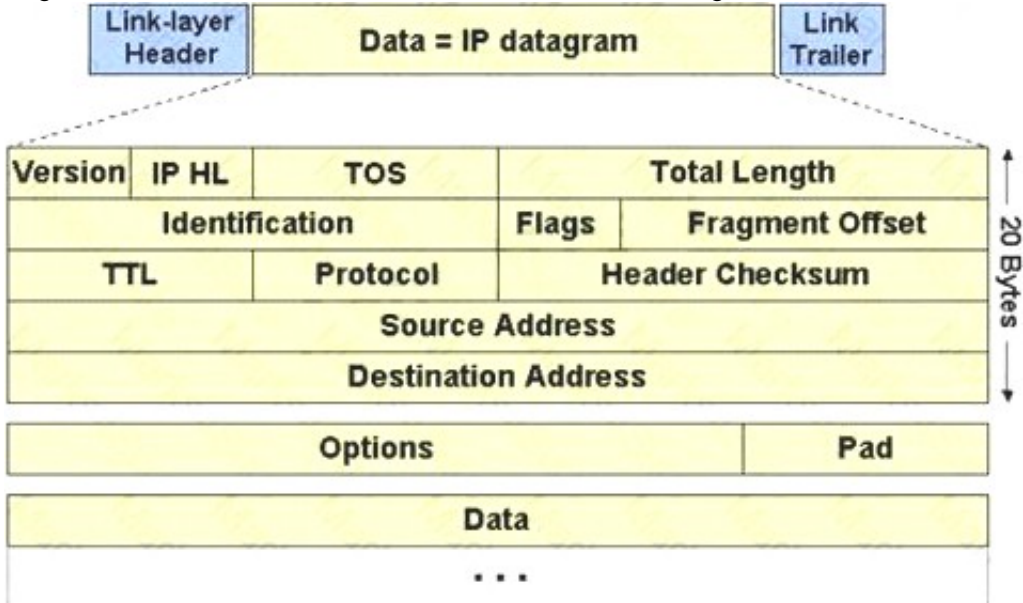
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram.  
 Each ICMP message contains three fields: type, code, and checksum. Different types of Internet 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 2**

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 3**

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 4**

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 5**

To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

- A. Circuit level gateway
- B. Stateful multilayer inspection firewall
- C. Packet filter
- D. Application level gateway

**Answer:** C

#### NEW QUESTION 6

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

- A. Use attack as a launching point to penetrate deeper into the network
- B. Demonstrate that no system can be protected against DoS attacks
- C. List weak points on their network
- D. Show outdated equipment so it can be replaced

**Answer:** C

#### NEW QUESTION 7

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 8

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 9

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

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

**Answer:** B

#### NEW QUESTION 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 15

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

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 24

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 26

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 30

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 34

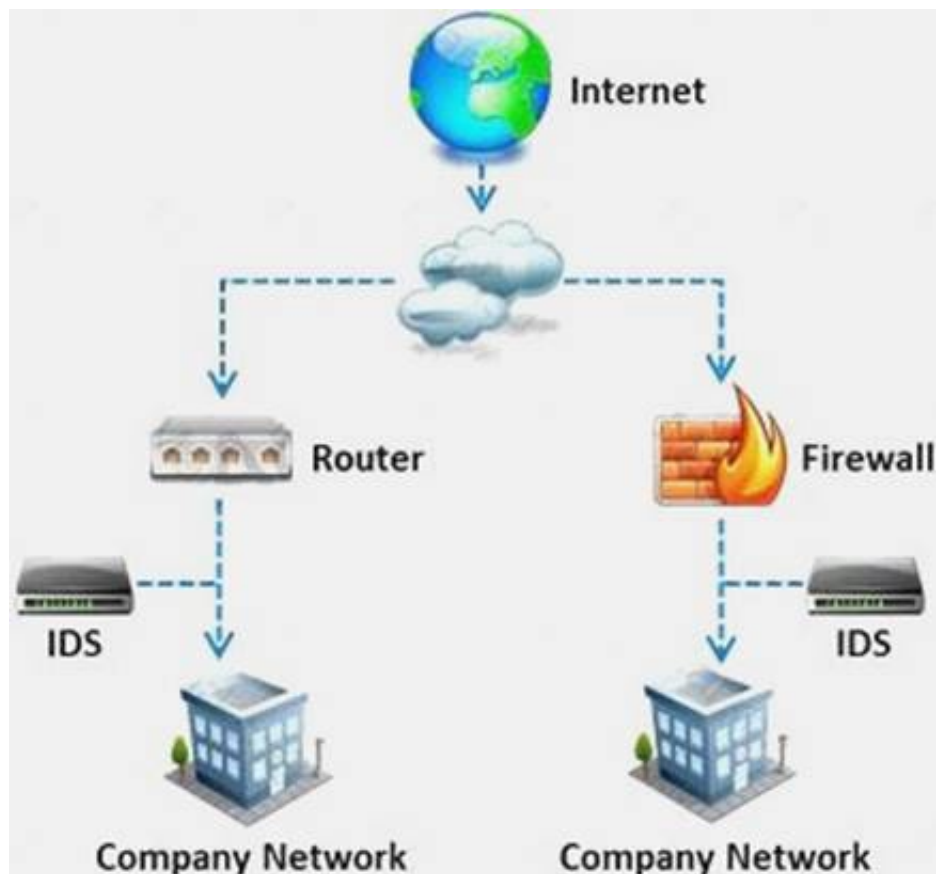
A framework is a fundamental structure used to support and resolve complex issues. The framework that delivers an efficient set of technologies in order to develop applications which are more secure in using Internet and Intranet is:

- A. Microsoft Internet Security Framework
- B. Information System Security Assessment Framework (ISSAF)
- C. Bell Labs Network Security Framework
- D. The IBM Security Framework

**Answer:** A

#### NEW QUESTION 39

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

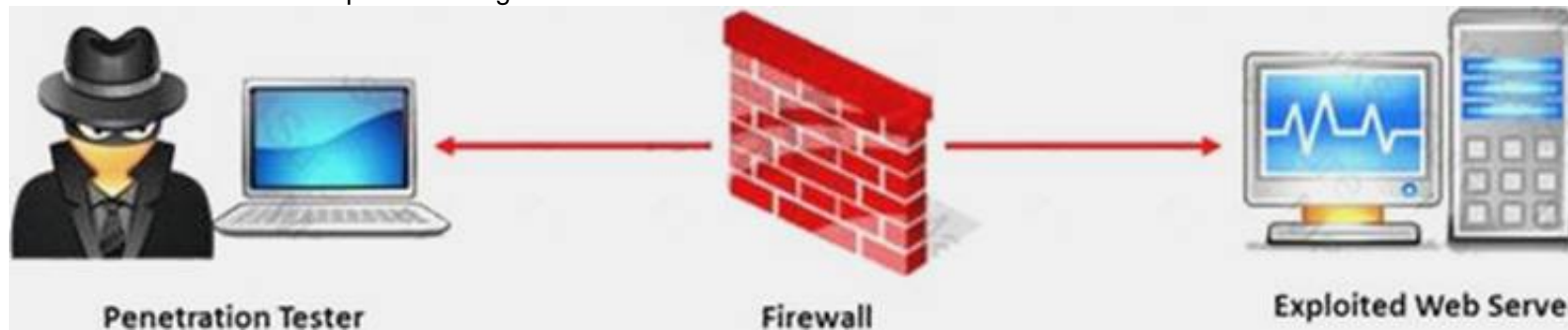


- A. NIDS are usually a more expensive solution to implement compared to HIDS.
- B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
- C. NIDS are standalone hardware appliances that include network intrusion detection capabilities 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 44

A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

- A. Announced testing and blind testing
- B. Blind testing and double blind testing
- C. Blind testing and unannounced testing
- D. Announced testing and unannounced testing

**Answer: D**

#### NEW QUESTION 45

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

- A. Testing to provide a more complete view of site security
- B. Testing focused on the servers, infrastructure, and the underlying software, including the target
- C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
- D. Testing performed from a number of network access points representing each logical and physical segment

**Answer: B**

#### NEW QUESTION 48

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

- A. Service account passwords in plain text
- B. Cached password hashes for the past 20 users
- C. IAS account names and passwords
- D. Local store PKI Kerberos certificates

**Answer: A**

#### NEW QUESTION 53

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 54

A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.



Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

- A. Post-attack phase
- B. Pre-attack phase and attack phase
- C. Attack phase
- D. Pre-attack phase

**Answer: D**

#### NEW QUESTION 59

What are the 6 core concepts in IT security?



- A. Server management, website domains, firewalls, IDS, IPS, and auditing
- B. Authentication, authorization, confidentiality, integrity, availability, and non-repudiation
- C. Passwords, logins, access controls, restricted domains, configurations, and tunnels
- D. Biometrics, cloud security, social engineering, DoS attack, viruses, and Trojans

**Answer: B**

#### NEW QUESTION 64

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 68

Which of the following is not a characteristic of a firewall?

- A. Manages public access to private networked resources
- B. Routes packets between the networks
- C. Examines all traffic routed between the two networks to see if it meets certain criteria
- D. Filters only inbound traffic but not outbound traffic

Answer: D

#### NEW QUESTION 69

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 72

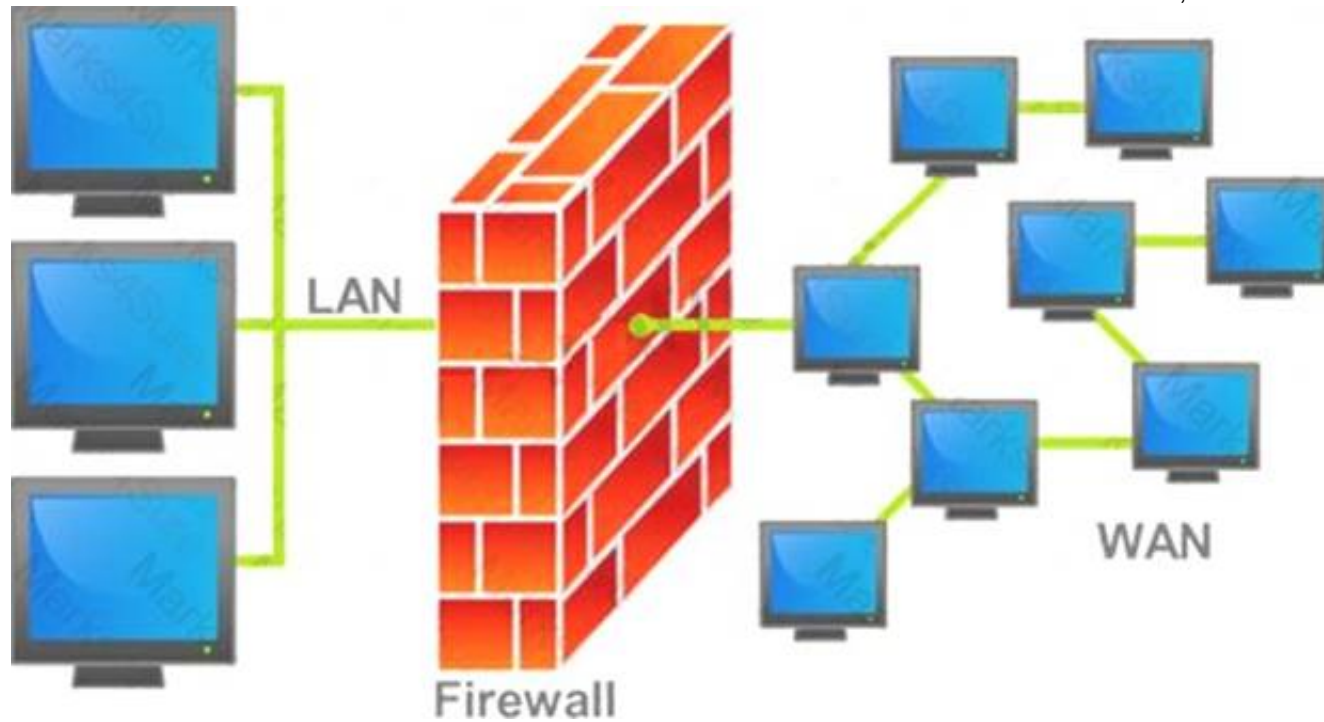
Which of the following acts related to information security in the US establish that the management of an organization is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

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

Answer: A

#### NEW QUESTION 76

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

- A. Appliance based firewalls cannot be upgraded
- B. Firewalls implemented on a hardware firewall are highly scalable
- C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system
- D. Operating system firewalls are highly configured

Answer: A

#### NEW QUESTION 78

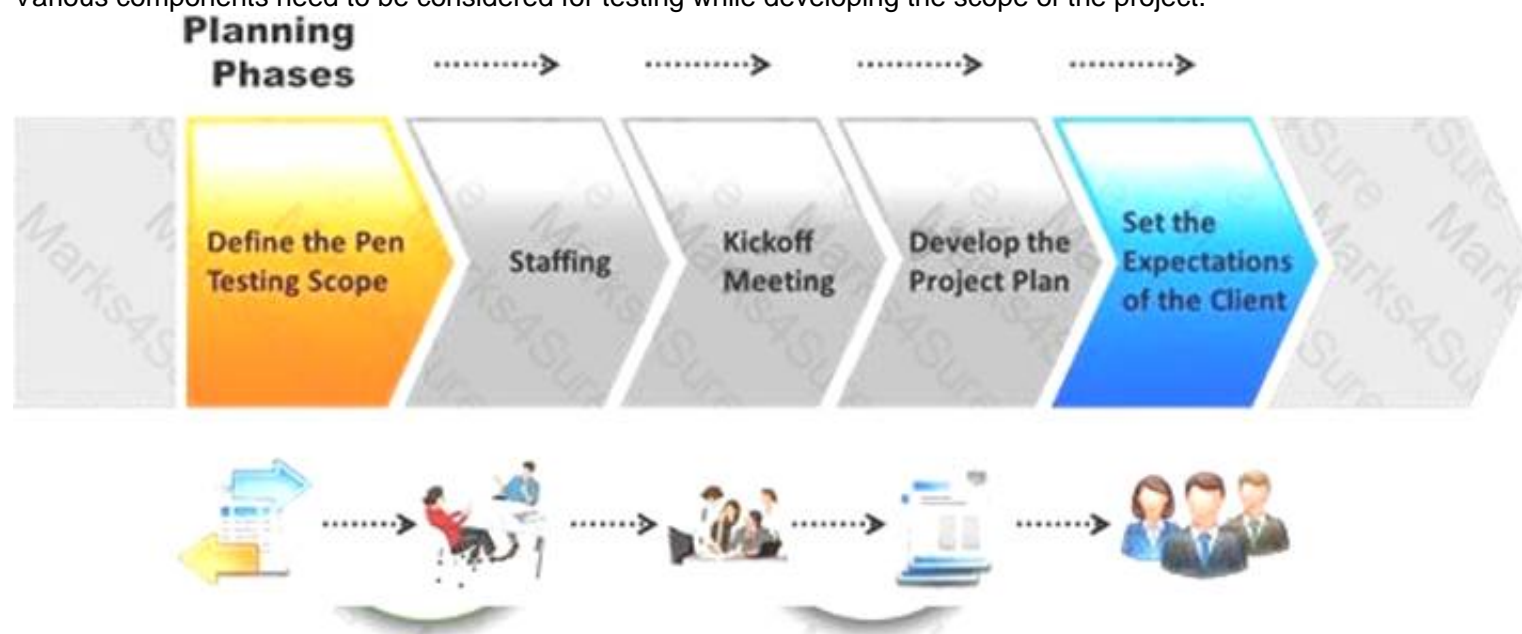
Which of the following has an offset field that specifies the length of the header and data?

- A. IP Header
- B. UDP Header
- C. ICMP Header
- D. TCP Header

Answer: D

#### NEW QUESTION 81

The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirements, ROE, and budget. Various components need to be considered for testing while developing the scope of the project.



Which of the following is NOT a pen testing component to be tested?

- A. System Software Security
- B. Intrusion Detection
- C. Outside Accomplices
- D. Inside Accomplices

**Answer: C**

#### NEW QUESTION 84

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 88

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 90

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 92

Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

- A. PIPEDA
- B. PCI DSS
- C. Human Rights Act 1998
- D. Data Protection Act 1998

**Answer: B**

#### NEW QUESTION 94

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?

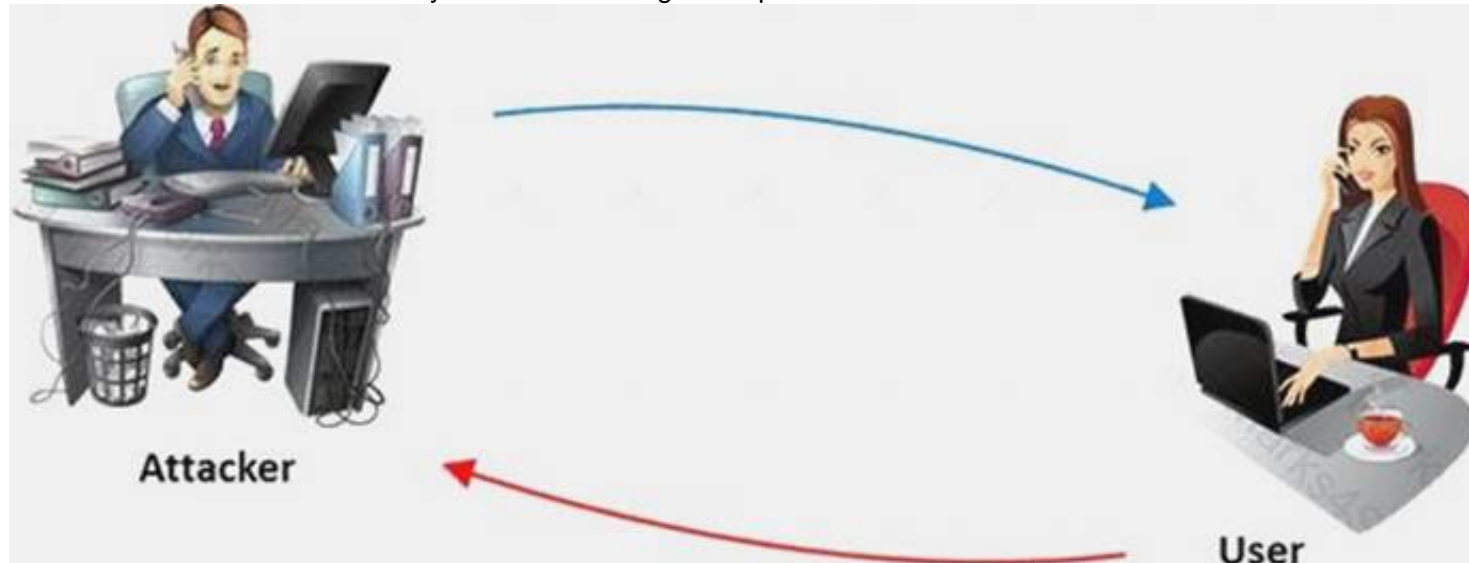


- A. Threat-Assessment Phase
- B. Pre-Assessment Phase
- C. Assessment Phase
- D. Post-Assessment Phase

**Answer: B**

#### NEW QUESTION 98

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 101

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 102

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 106

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

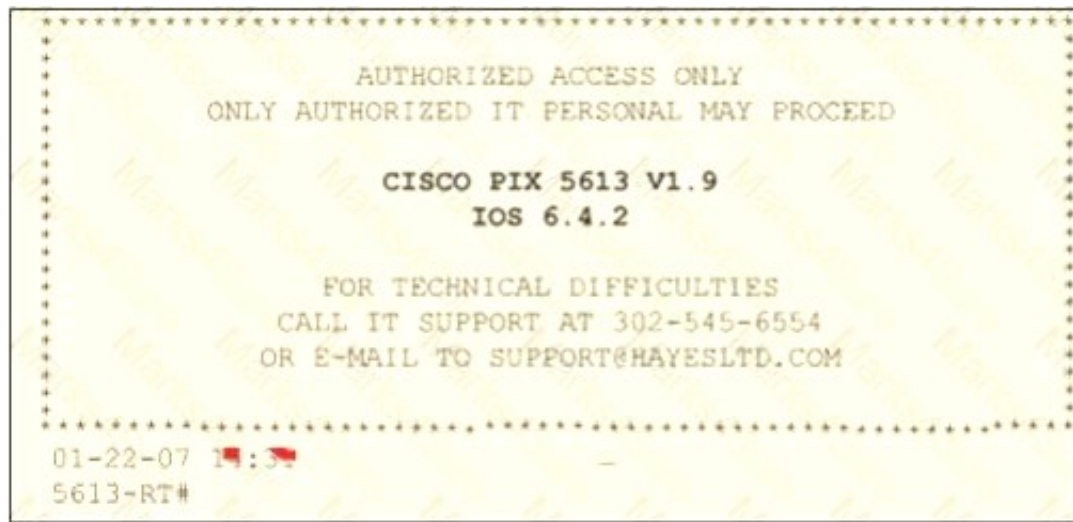
**Answer: A**

#### NEW QUESTION 109

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible.

Paulette presents the following screenshot to her boss so he can inform the clients about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:



- A. The banner should not state "only authorized IT personnel may proceed"
- B. Remove any identifying numbers, names, or version information
- C. The banner should include the Cisco tech support contact information as well
- D. The banner should have more detail on the version numbers for the network equipment

**Answer: B**

#### NEW QUESTION 113

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 114

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 119

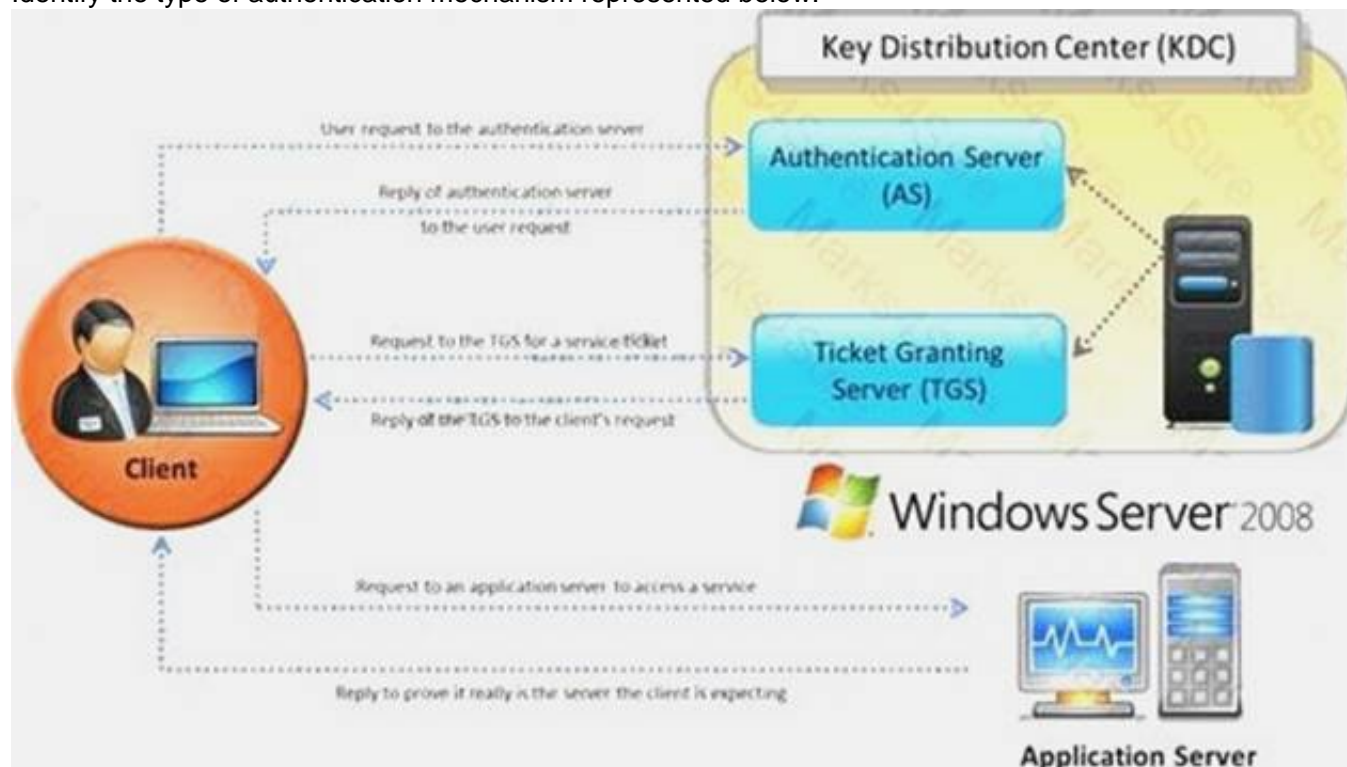
You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into 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 122

Identify the type of authentication mechanism represented below:



- A. NTLMv1
- B. NTLMv2
- C. LAN Manager Hash
- D. Kerberos

**Answer:** D

#### NEW QUESTION 125

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 127

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 132

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 135

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 139

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network.

How would you answer?

- A. IBM Methodology
- B. LPT Methodology
- C. Google Methodology
- D. Microsoft Methodology

**Answer: B**

#### NEW QUESTION 142

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 145

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 148

Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs.

One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug-in uses four techniques to identify the presence of a WAP.

Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

- A. NMAP TCP/IP fingerprinting
- B. HTTP fingerprinting
- C. FTP fingerprinting
- D. SNMP fingerprinting

**Answer: C**

#### NEW QUESTION 151

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 153

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 157

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 161

The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc.

Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations.

Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.



What is the best way to protect web applications from parameter tampering attacks?

- A. Validating some parameters of the web application
- B. Minimizing the allowable length of parameters
- C. Using an easily guessable hashing algorithm
- D. Applying effective input field filtering parameters

**Answer: D**

#### NEW QUESTION 162

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

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

**Answer: A**

#### NEW QUESTION 167

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 171

Which one of the following architectures has the drawback of internally considering the hosted services individually?

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

**Answer: C**

#### NEW QUESTION 174

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 178

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 179

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 183

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 185

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 189

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 191

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 195

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 198

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 200

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 205

In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate.

A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.

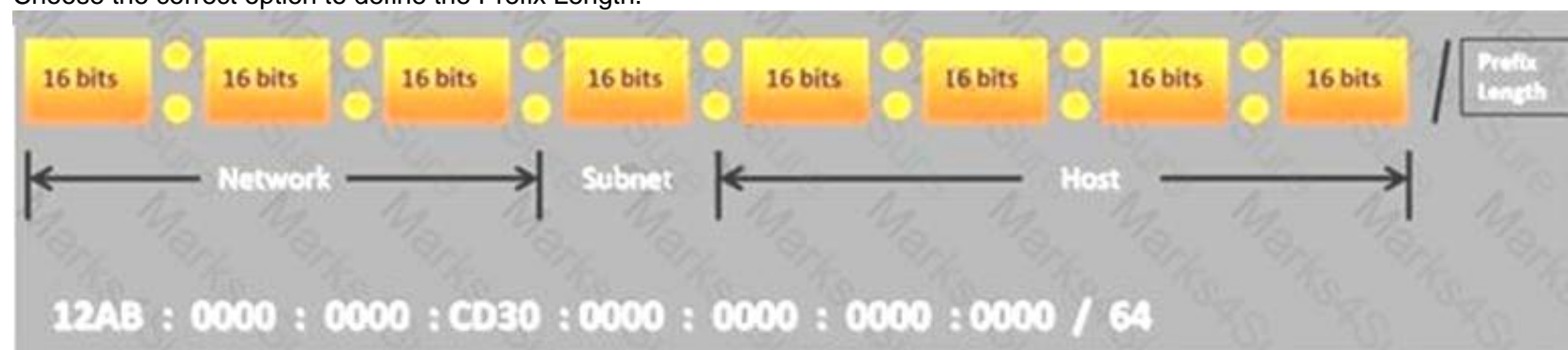


- A. Sliding Windows
- B. Windowing
- C. Positive Acknowledgment with Retransmission (PAR)
- D. Synchronization

**Answer:** C

#### NEW QUESTION 209

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 214

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 and code field.



Which of the following ICMP messages will be generated if the destination port is not reachable?

- A. ICMP Type 11 code 1
- B. ICMP Type 5 code 3
- C. ICMP Type 3 code 2
- D. ICMP Type 3 code 3

**Answer: D**

#### NEW QUESTION 215

What is the difference between penetration testing and vulnerability testing?



- A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
- B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
- C. Vulnerability testing is more expensive than penetration testing
- D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

**Answer: A**

#### NEW QUESTION 219

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 223

SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. A successful SQL injection attack can:

- i) Read sensitive data from the database
- iii) Modify database data (insert/update/delete)
- iii) Execute administration operations on the database (such as shutdown the DBMS)
- iv) Recover the content of a given file existing on the DBMS file system or write files into the file system
- v) Issue commands to the operating system





Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error. In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

- A. Automated Testing
- B. Function Testing
- C. Dynamic Testing
- D. Static Testing

**Answer:** D

#### NEW QUESTION 225

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 229

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 233

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 238

The first and foremost step for a penetration test is information gathering. The main objective of this test is to gather information about the target system which can be used in a malicious manner to gain access to the target systems.



Which of the following information gathering terminologies refers to gathering information through social engineering on-site visits, face-to-face interviews, and direct questionnaires?

- A. Active Information Gathering
- B. Pseudonymous Information Gathering
- C. Anonymous Information Gathering
- D. Open Source or Passive Information Gathering

**Answer:** A

#### NEW QUESTION 243

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

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

**Answer: D**

#### NEW QUESTION 245

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 246

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 251

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes. Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.  
 What can a pen tester do to detect input sanitization issues?

- A. Send single quotes as the input data to catch instances where the user input is not sanitized
- B. Send double quotes as the input data to catch instances where the user input is not sanitized
- C. Send long strings of junk data, just as you would send strings to detect buffer overruns
- D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

**Answer: D**

#### NEW QUESTION 256

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**

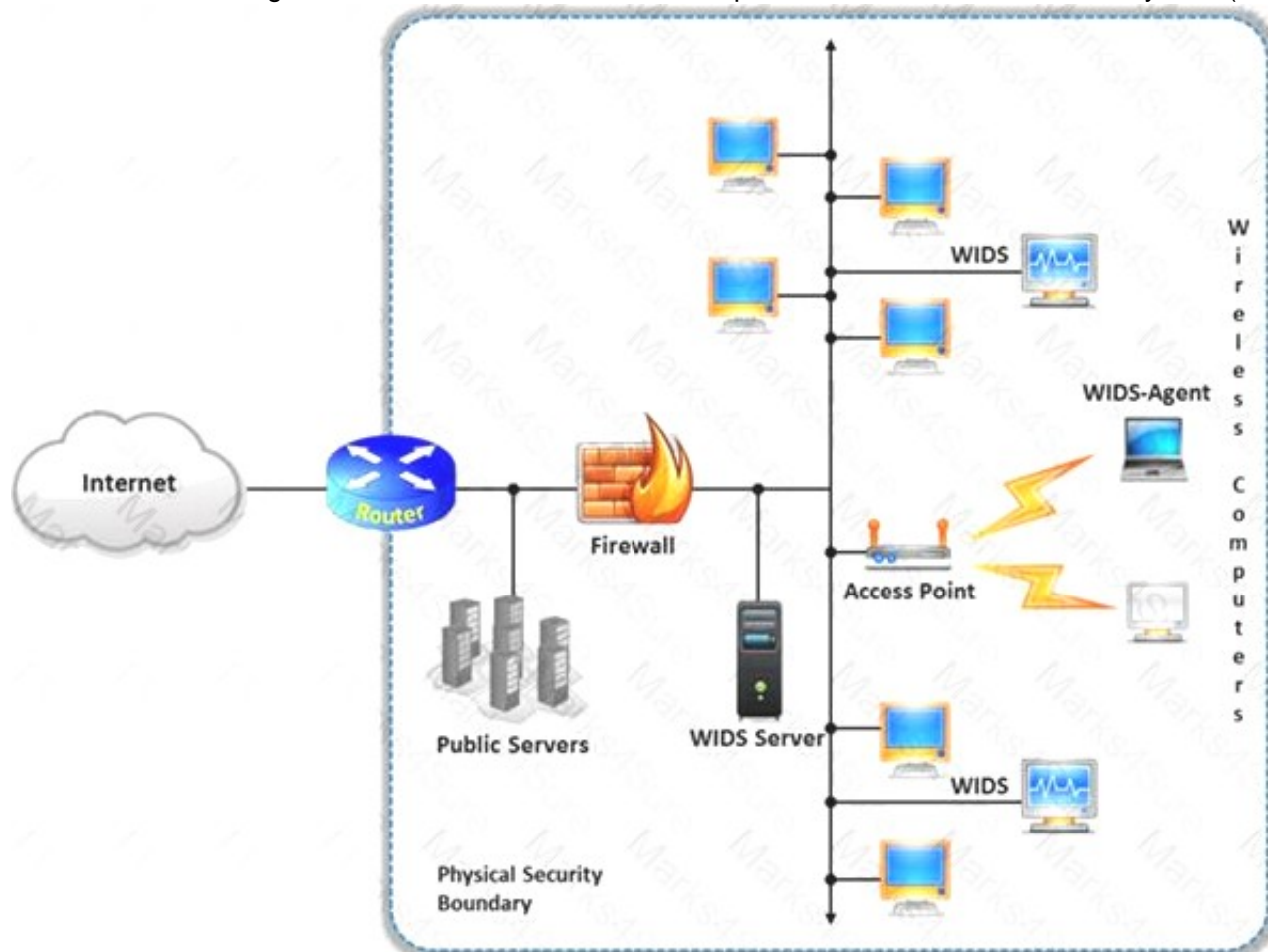
#### NEW QUESTION 261

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools.

The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected.

Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



- A. Social engineering
- B. SQL injection
- C. Parameter tampering
- D. Man-in-the-middle attack

**Answer: D**

#### NEW QUESTION 265

Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

- A. Using session hijacking
- B. Using proxy servers
- C. Using authentication
- D. Using encryption

**Answer: B**

#### NEW QUESTION 267

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 272

Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.



Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

- A. SSI injection attack
- B. Insecure cryptographic storage attack
- C. Hidden field manipulation attack
- D. Man-in-the-Middle attack

**Answer: B**

#### NEW QUESTION 275

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 277

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 281

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 285

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 288

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

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



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

**Answer:** C

#### NEW QUESTION 289

What is the target host IP in the following command?

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

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

**Answer:** A

#### NEW QUESTION 290

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 294

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 298

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 301

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:

- The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
- The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
- 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.
- 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

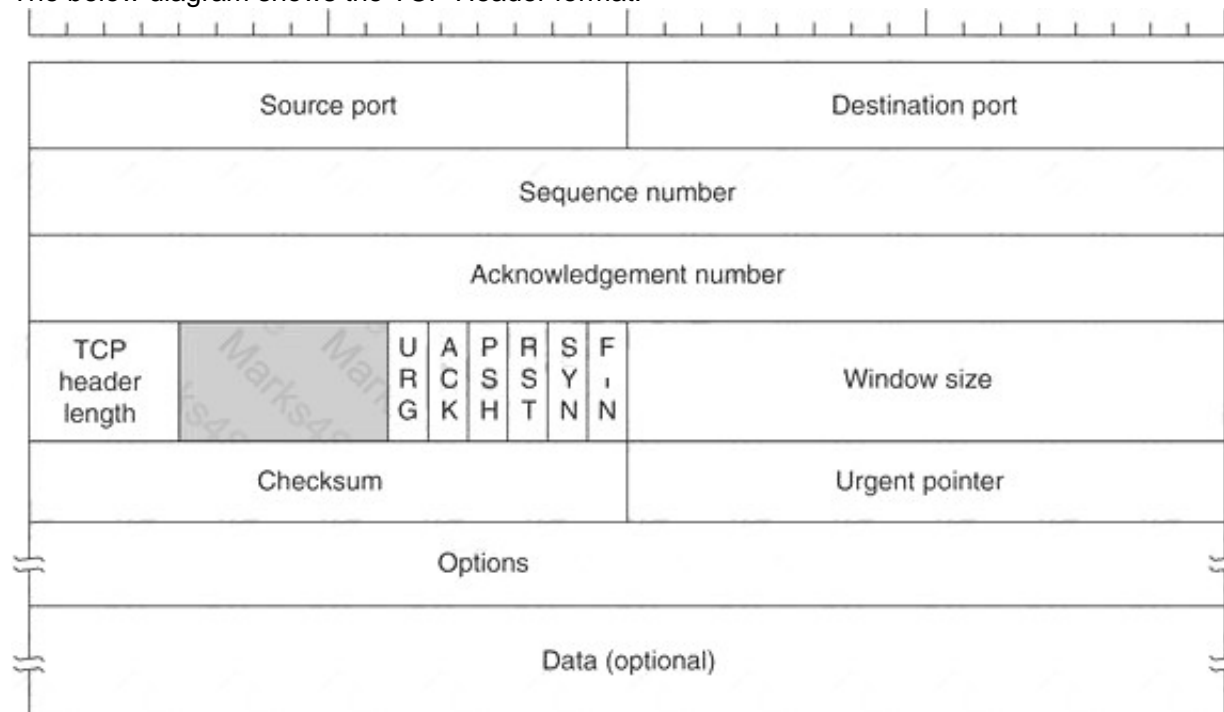
**Answer: C**

#### NEW QUESTION 304

Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.

For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side

The below diagram shows the TCP Header format:



- A. 16 bits
- B. 32 bits
- C. 8 bits
- D. 24 bits

**Answer:** B

**NEW QUESTION 308**

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 312**

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 317**

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 320**

.....

## 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](#)**