

Exam Questions 412-79v10

EC-Council Certified Security Analyst (ECSA) V10

<https://www.2passeasy.com/dumps/412-79v10/>



NEW QUESTION 1

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.



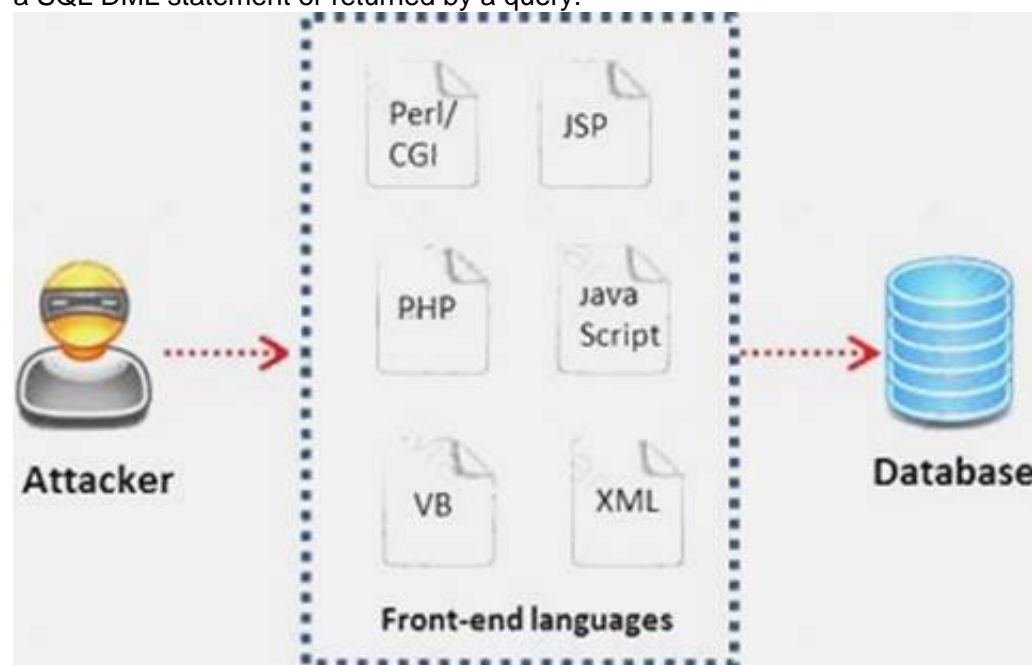
The SAM file in Windows Server 2008 is located in which of the following locations?

- 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 2

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 3

Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers.

Which one of the following cannot handle routing protocols properly?

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

Answer: B

NEW QUESTION 4

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

- A. OSPF
- B. BPG
- C. ATM
- D. UDP

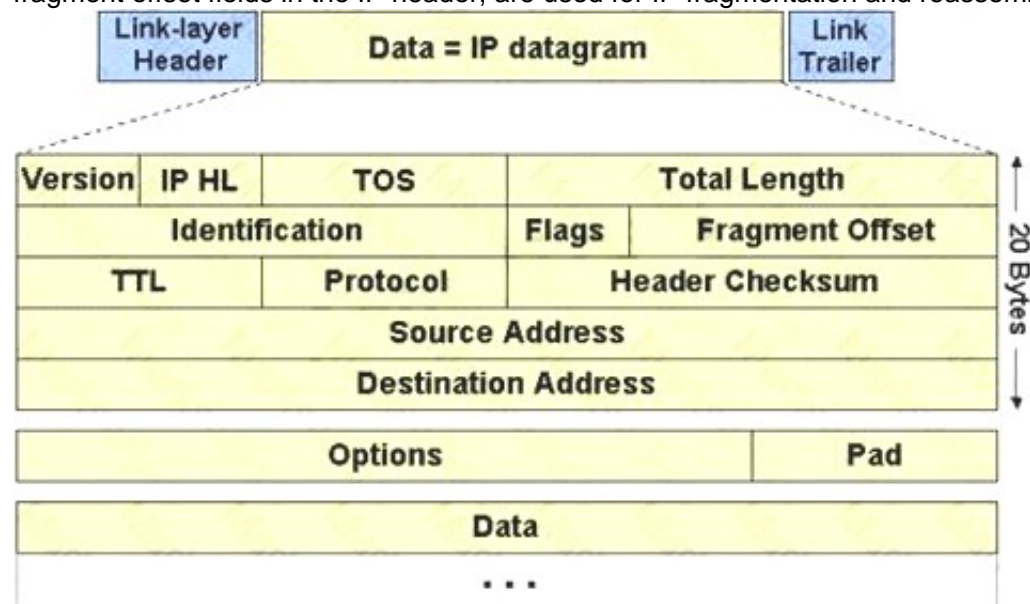
Answer: A

NEW QUESTION 5

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 6

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 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

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 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

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 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.

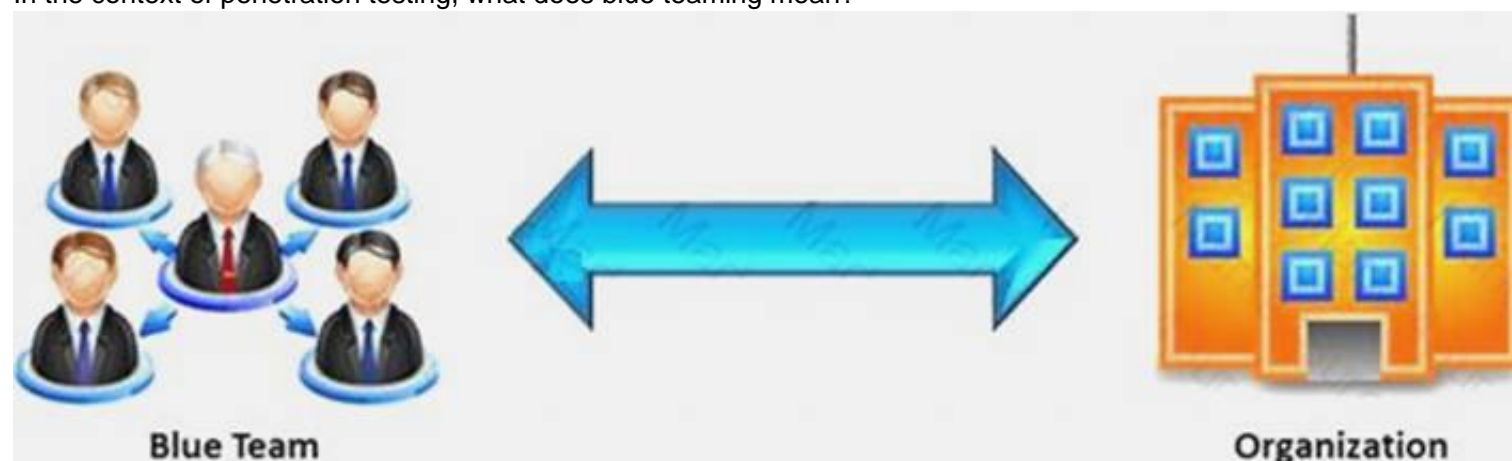
Which one of the following is well supported in most wireless applications?

- A. Orinoco chipsets
- B. Prism II chipsets
- C. Atheros Chipset
- D. Cisco chipset

Answer: B

NEW QUESTION 15

In the context of penetration testing, what does blue teaming mean?



- A. A penetration test performed with the knowledge and consent of the organization's IT staff
- B. It is the most expensive and most widely used
- C. It may be conducted with or without warning
- D. A penetration test performed without the knowledge of the organization's IT staff but with permission from upper management

Answer: A

NEW QUESTION 18

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 20

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 25

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 27

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 32

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 35

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 37

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 38

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 40

Which of the following scan option is able to identify the SSL services?

- A. -sS
- B. -sV
- C. -sU
- D. -sT

Answer: B

NEW QUESTION 41

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 43

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 46

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 50

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 51

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 53

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 57

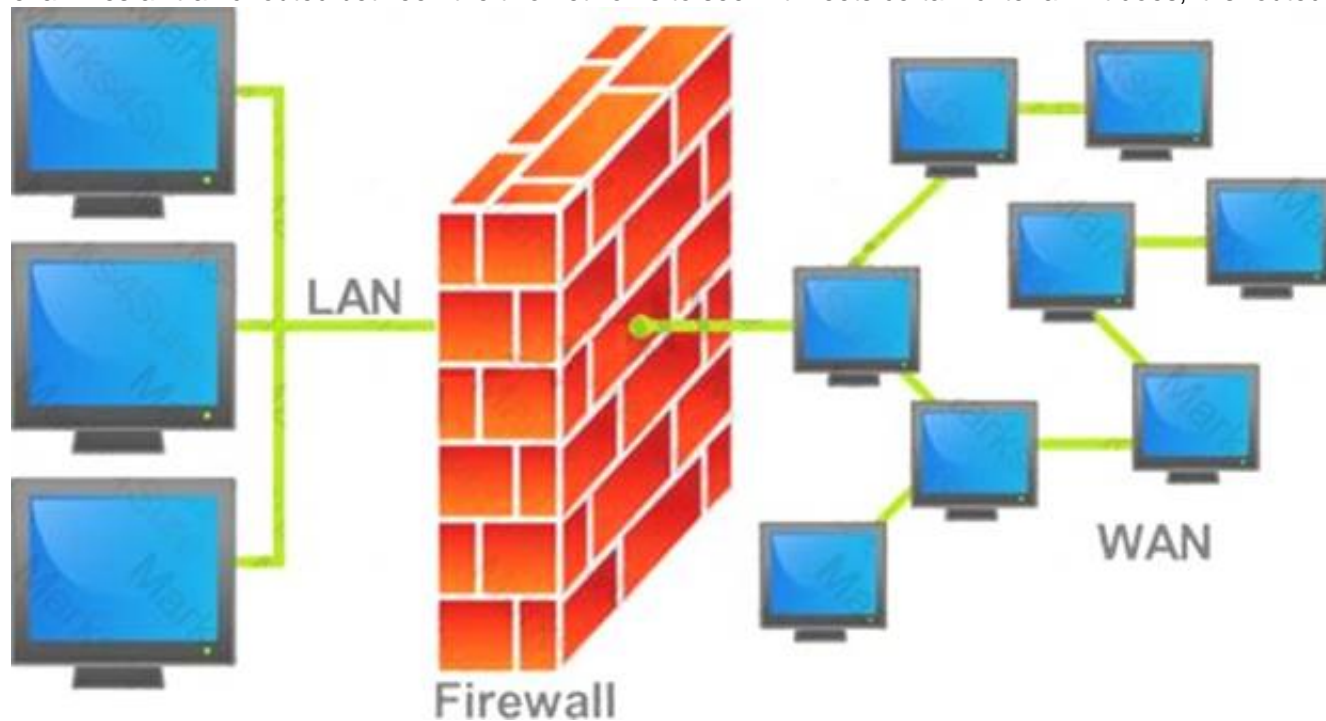
Which of the following acts related to information security in the US establish that the management of an organization is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

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

Answer: A

NEW QUESTION 58

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.



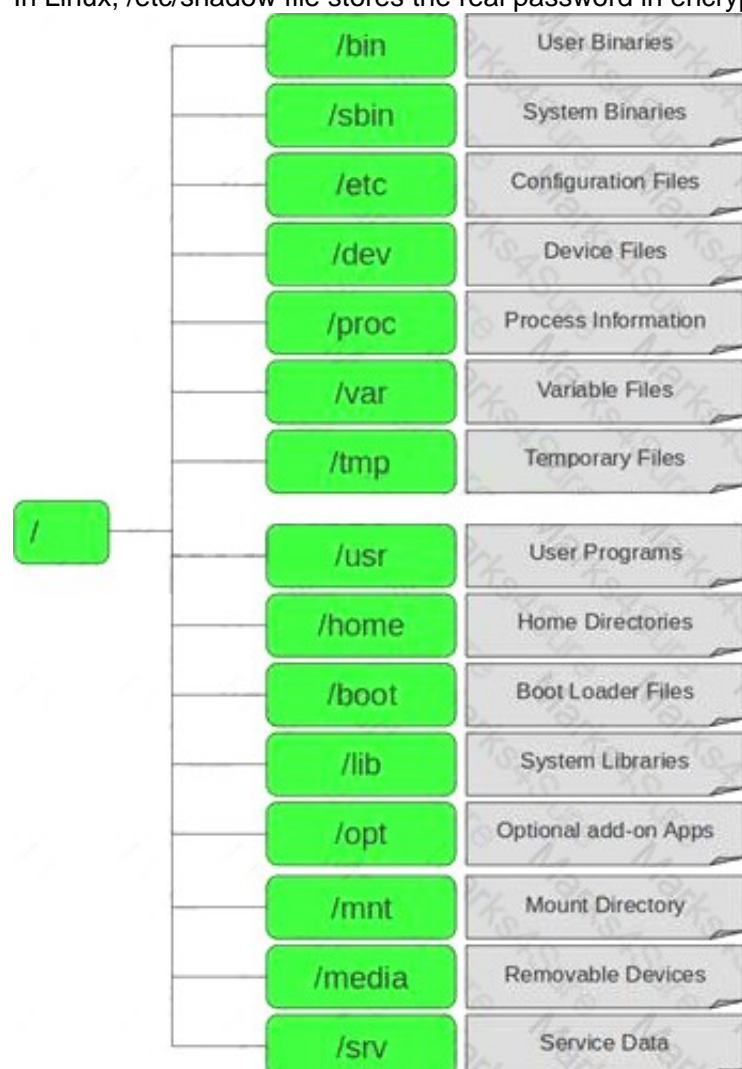
Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

- 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 63

In Linux, /etc/shadow file stores the real password in encrypted format for user's account with added properties associated with the user's password.



In the example of a /etc/shadow file below, what does the bold letter string indicate?

Vivek: \$1\$fnffc\$GteyHdicpGOffXX40w#5:13064:0:99999:7

- A. Number of days the user is warned before the expiration date
- B. Minimum number of days required between password changes
- C. Maximum number of days the password is valid
- D. Last password changed

Answer: B

NEW QUESTION 66

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 67

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 68

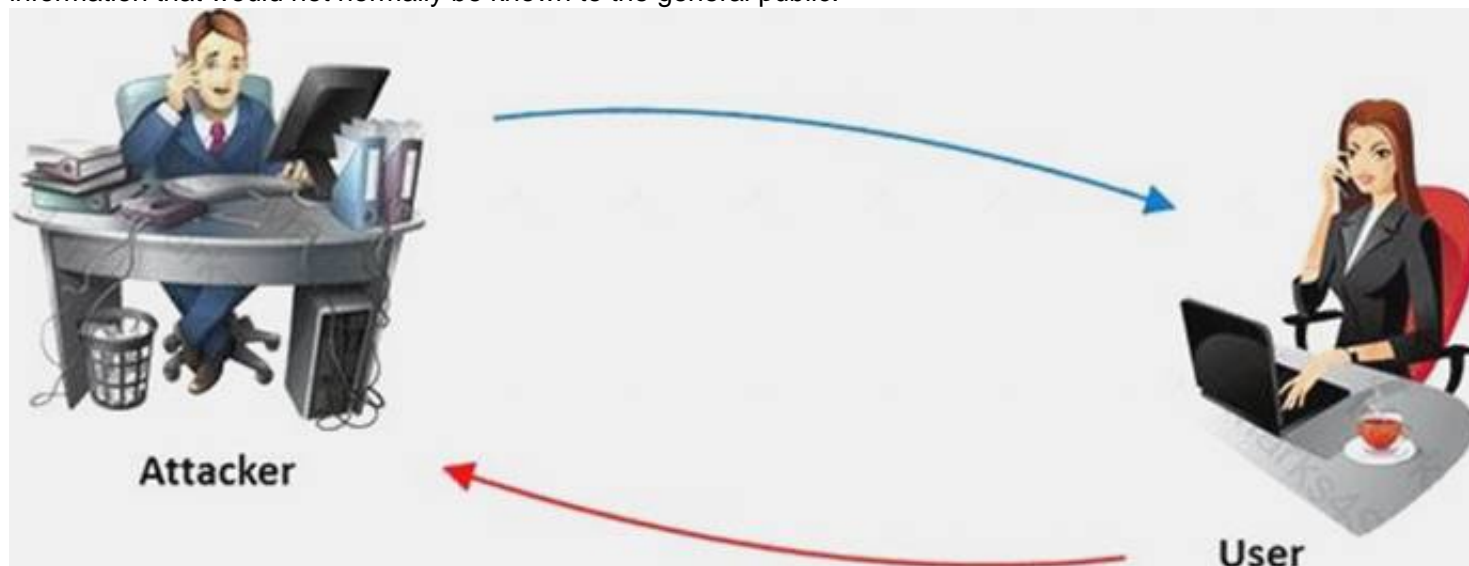
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

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

Answer: B

NEW QUESTION 72

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 74

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.



Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

- A. Passive Assessment
- B. Host-based Assessment
- C. External Assessment
- D. Application Assessment

Answer: D

NEW QUESTION 77

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 82

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. Aircrack
- B. Aircrack-ng
- C. Aircrack-ng
- D. WEPCrack

Answer: C

NEW QUESTION 84

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 85

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 90

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 94

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 95

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 98

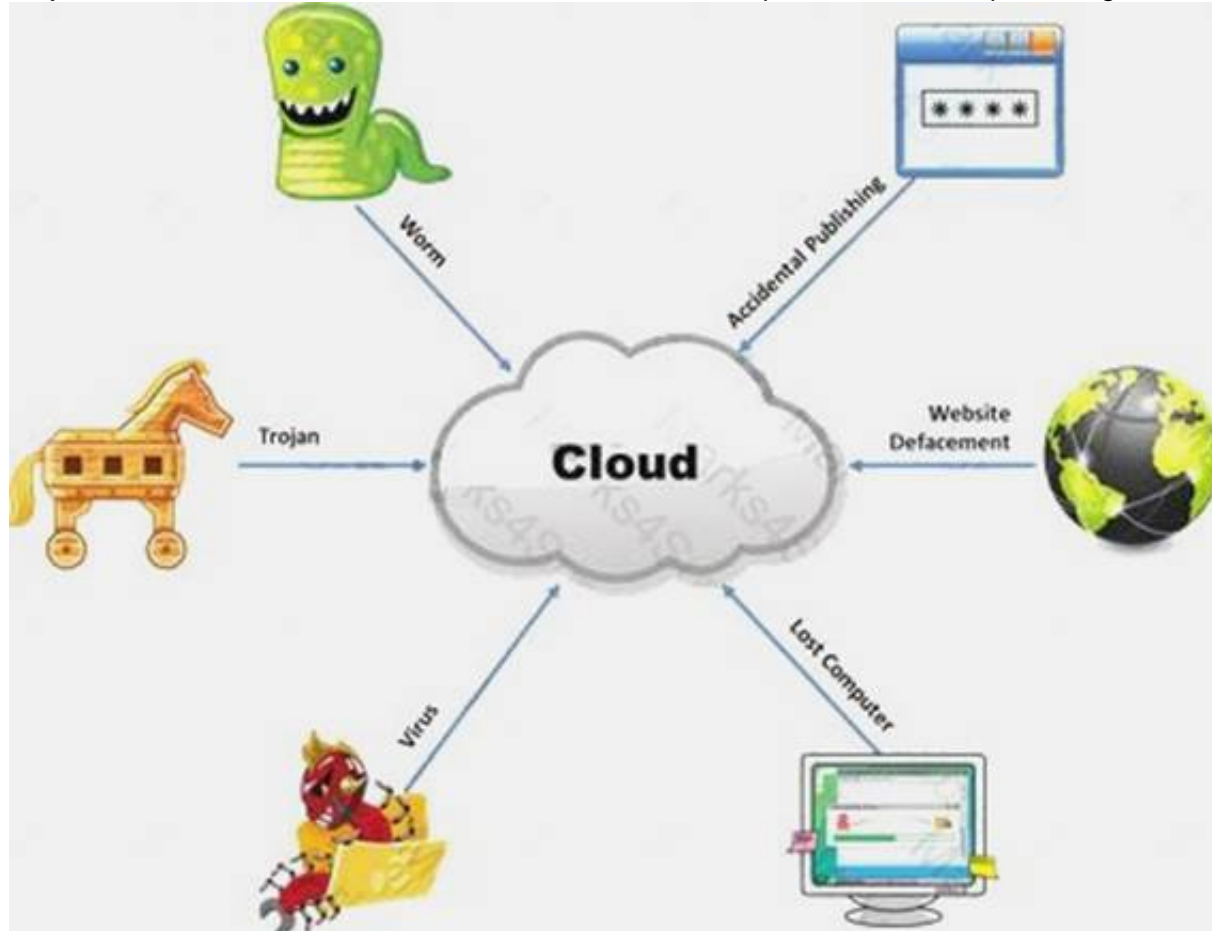
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

- A. DNSSEC
- B. Netsec
- C. IKE
- D. IPsec

Answer: D

NEW QUESTION 100

The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

- A. Weak passwords and lack of identity management
- B. Insufficient IT security budget
- C. Rogue employees and insider attacks
- D. Vulnerabilities, risks, and threats facing Web sites

Answer: C

NEW QUESTION 102

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 105

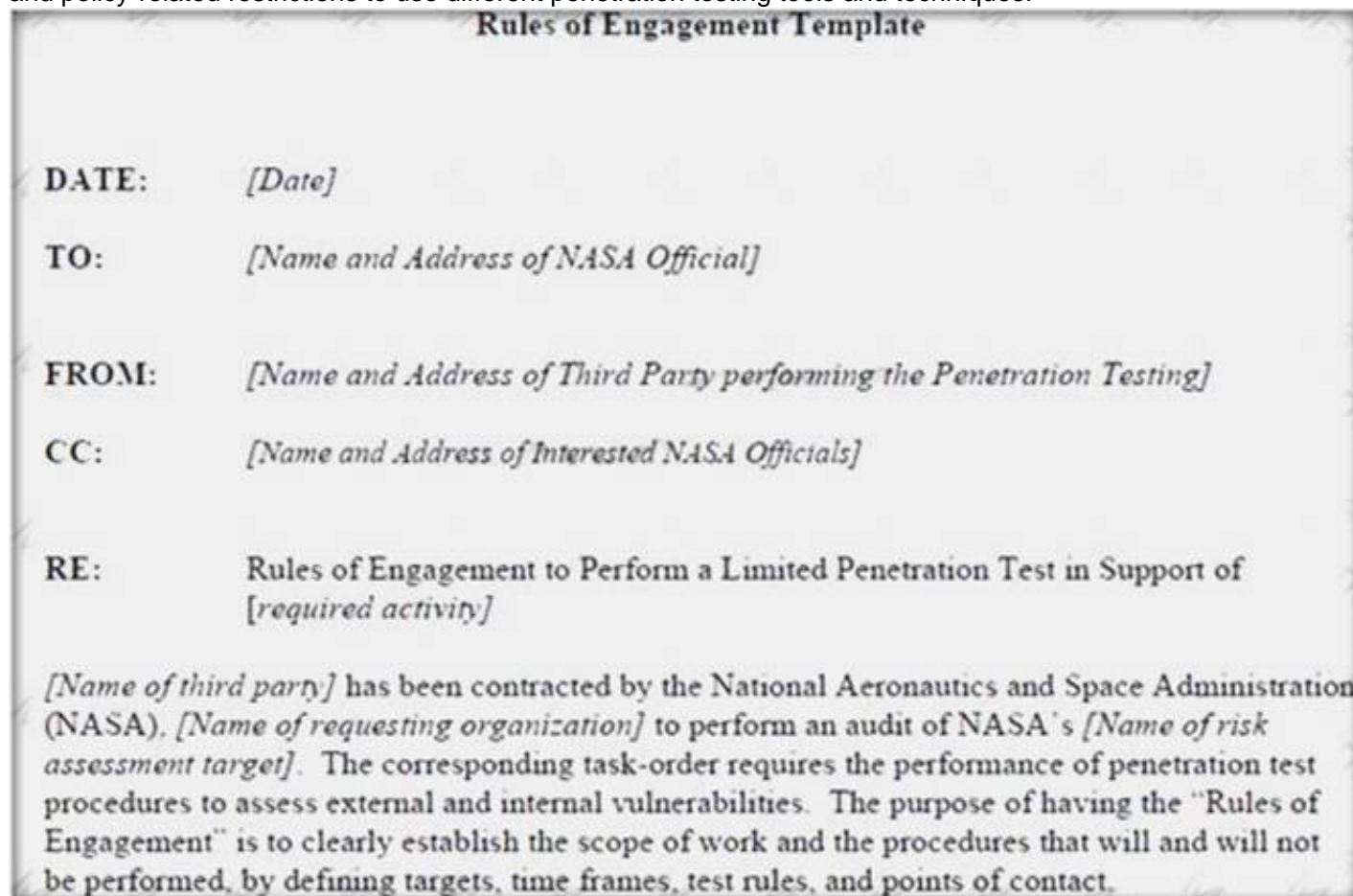
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

- 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 109

Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



What is the last step in preparing a Rules of Engagement (ROE) document?

- A. Conduct a brainstorming session with top management and technical teams
- B. Decide the desired depth for penetration testing
- C. Conduct a brainstorming session with top management and technical teams
- D. Have pre-contract discussions with different pen-testers

Answer: C

NEW QUESTION 111

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 113

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 115

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.

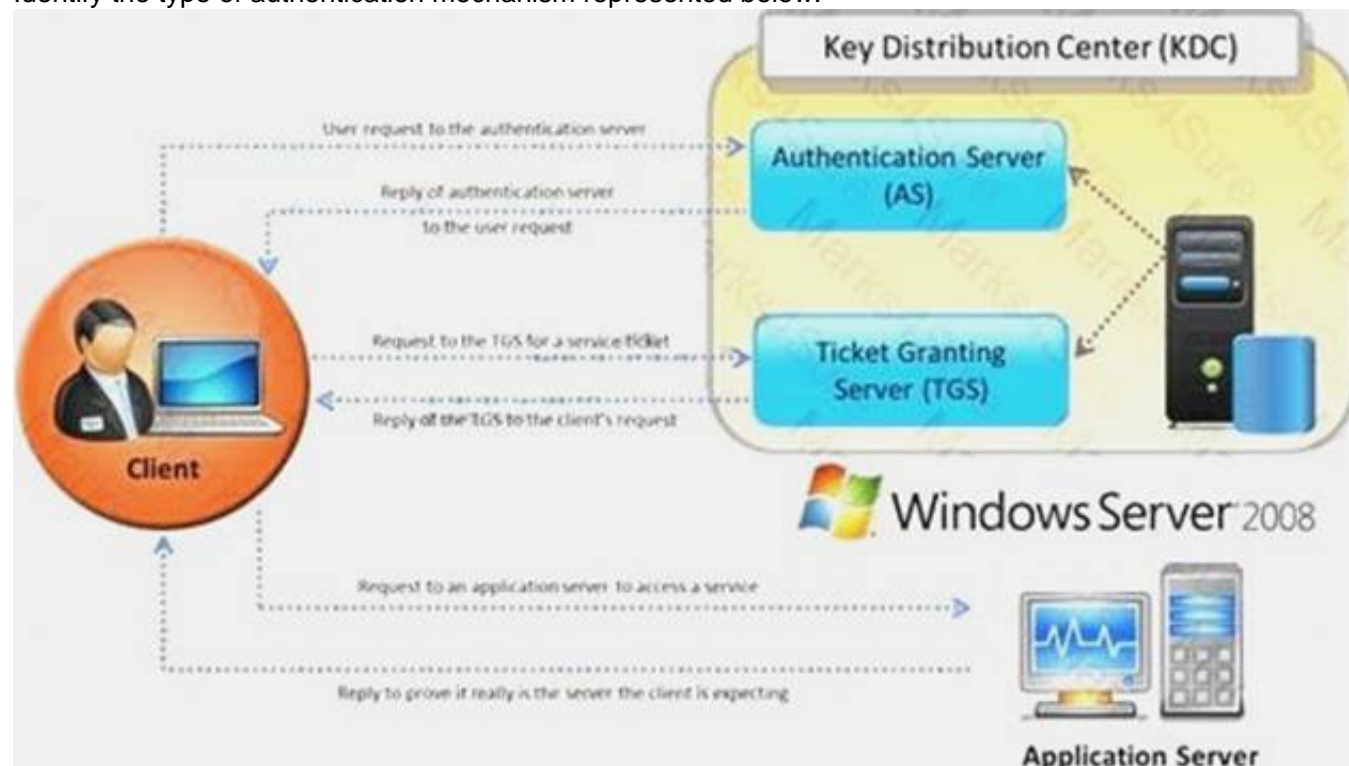
You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

- 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 120

Identify the type of authentication mechanism represented below:



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

Answer: D

NEW QUESTION 124

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 128

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 129

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 133

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 134

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 137

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 139

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 141

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 146

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

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

What could be Tyler issue with his home wireless network?

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

Answer: A

NEW QUESTION 151

Which of the following methods is used to perform server discovery?

- A. Banner Grabbing
- B. Who is Lookup
- C. SQL Injection
- D. Session Hijacking

Answer: B

NEW QUESTION 154

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 158

Which of the following are the default ports used by NetBIOS service?

- A. 135, 136, 139, 445
- B. 134, 135, 136, 137
- C. 137, 138, 139, 140
- D. 133, 134, 139, 142

Answer: A

NEW QUESTION 163

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 164

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

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

Answer: A

NEW QUESTION 165

John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

- A. C:\Windows\System32\Boot
- B. C:\WINNT\system32\drivers\etc
- C. C:\WINDOWS\system32\cmd.exe
- D. C:\Windows\System32\restore

Answer: B

NEW QUESTION 167

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 168

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 169

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 174

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 177

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 180

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 185

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 190

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 192

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 197

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 199

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 204

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 207

Many security and compliance projects begin with a simple idea: assess the organization's risk, vulnerabilities, and breaches. Implementing an IT security risk assessment is critical to the overall security posture of any organization. An effective security risk assessment can prevent breaches and reduce the impact of realized breaches.



What is the formula to calculate risk?

- A. Risk = Budget x Time
- B. Risk = Goodwill x Reputation
- C. Risk = Loss x Exposure factor
- D. Risk = Threats x Attacks

Answer: C

NEW QUESTION 211

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 214

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type. This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database. The below diagram shows how attackers launched SQL injection attacks on web applications.



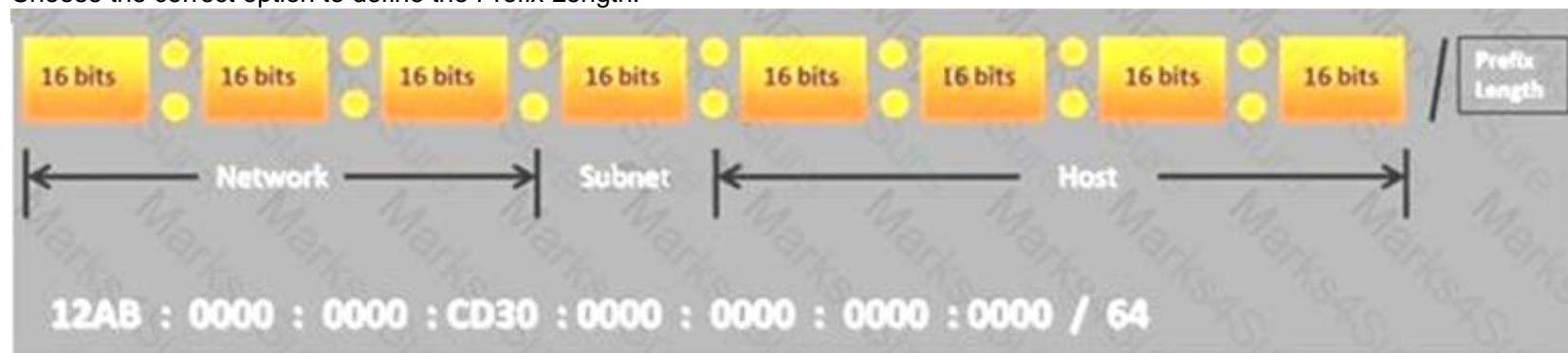
Which of the following can the attacker use to launch an SQL injection attack?

- A. Blah' "2=2 --"
- B. Blah' and 2=2 --
- C. Blah' and 1=1 --
- D. Blah' or 1=1 --

Answer: D

NEW QUESTION 218

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 221

Which of the following shields Internet users from artificial DNS data, such as a deceptive or mischievous address instead of the genuine address that was requested?

- A. DNSSEC
- B. Firewall
- C. Packet filtering
- D. IPSec

Answer: A

NEW QUESTION 224

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 229

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 232

External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.



Which of the following types of penetration testing is performed with no prior knowledge of the site?

- A. Blue box testing
- B. White box testing
- C. Grey box testing
- D. Black box testing

Answer: D

NEW QUESTION 233

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 234

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 237

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 241

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 244

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 247

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 249

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 253

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 258

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 261

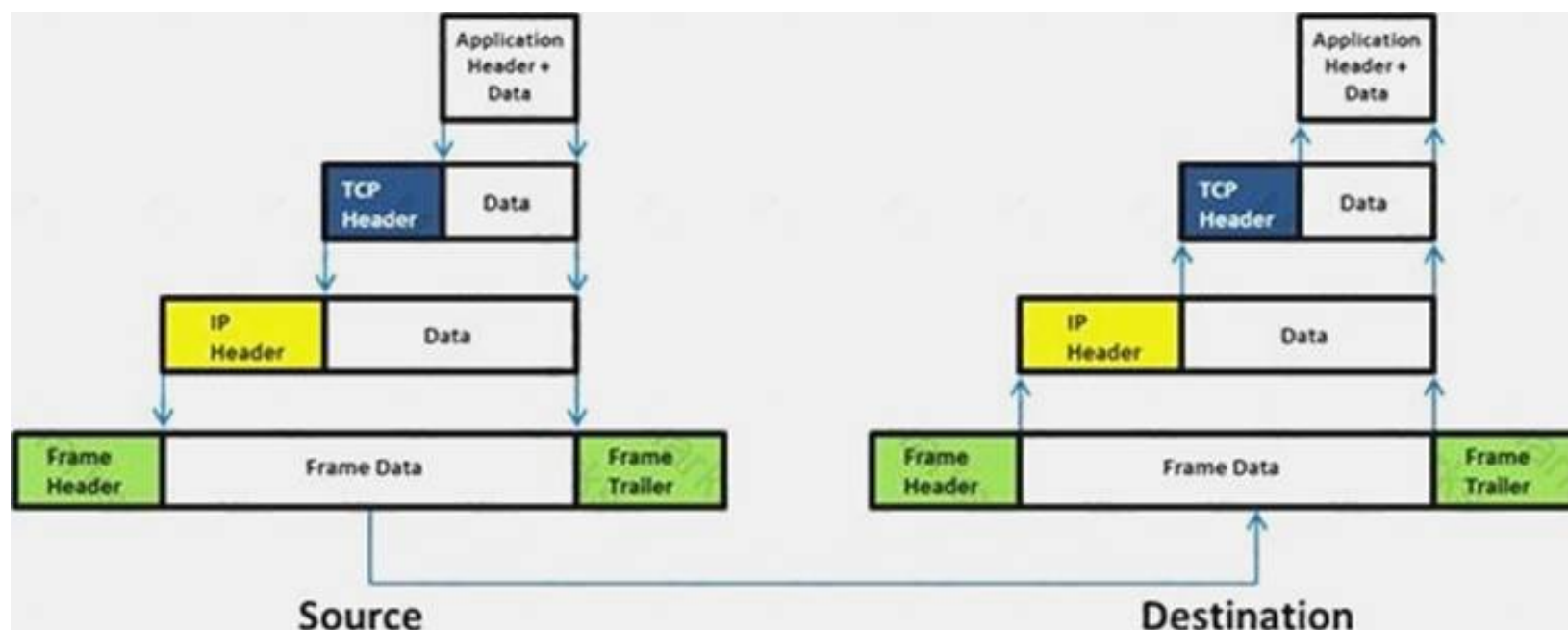
As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

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

Answer: C

NEW QUESTION 266

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

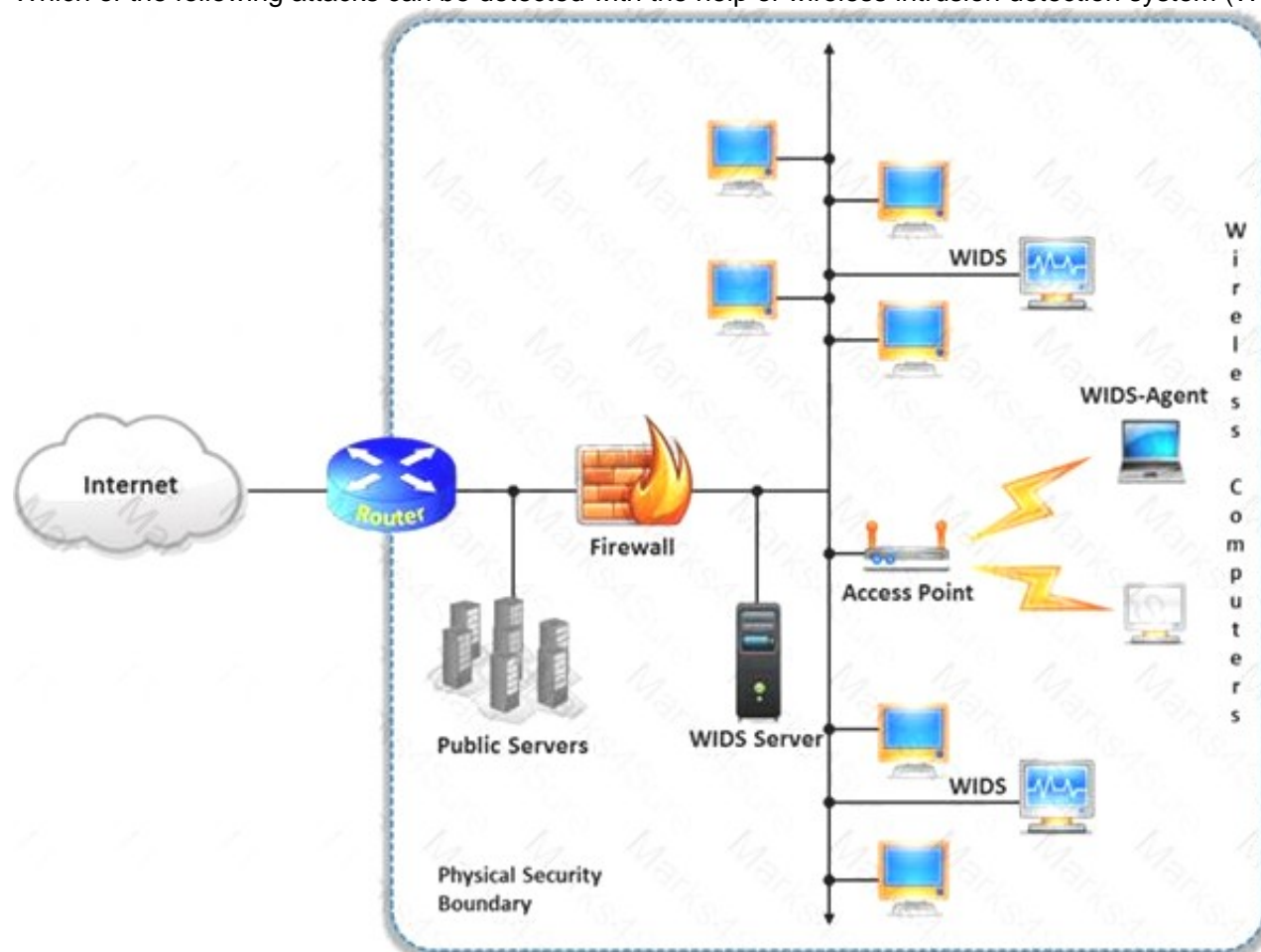
NEW QUESTION 269

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 272

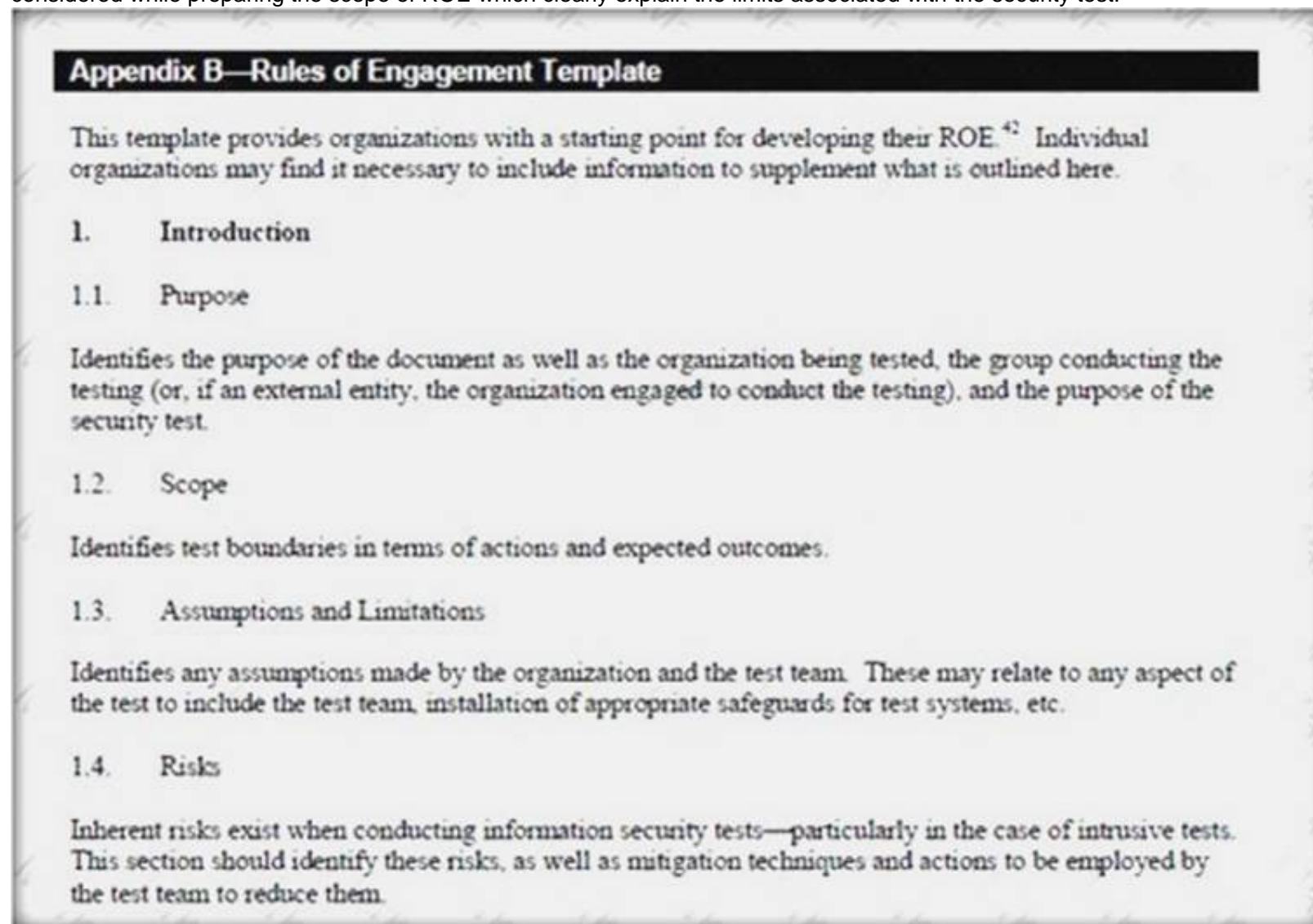
The framework primarily designed to fulfill a methodical and organized way of addressing five threat classes to network and that can be used to access, plan, manage, and maintain secure computers and communication networks is:

- 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 275

Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Which of the following factors is NOT considered while preparing the scope of the Rules of Engagement (ROE)?

- A. A list of employees in the client organization
- B. A list of acceptable testing techniques
- C. Specific IP addresses/ranges to be tested
- D. Points of contact for the penetration testing team

Answer: A

NEW QUESTION 279

The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. It is often used to raise the level of security awareness among employees.



The tester should demonstrate extreme care and professionalism during a social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.

Which of the following methods of attempting social engineering is associated with bribing, handing out gifts, and becoming involved in a personal relationship to befriend someone inside the company?

- A. Accomplice social engineering technique
- B. Identity theft
- C. Dumpster diving
- D. Phishing social engineering technique

Answer: A

NEW QUESTION 280

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 282

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 286

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 289

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 293

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 294

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 297

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 302

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 307

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 308

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

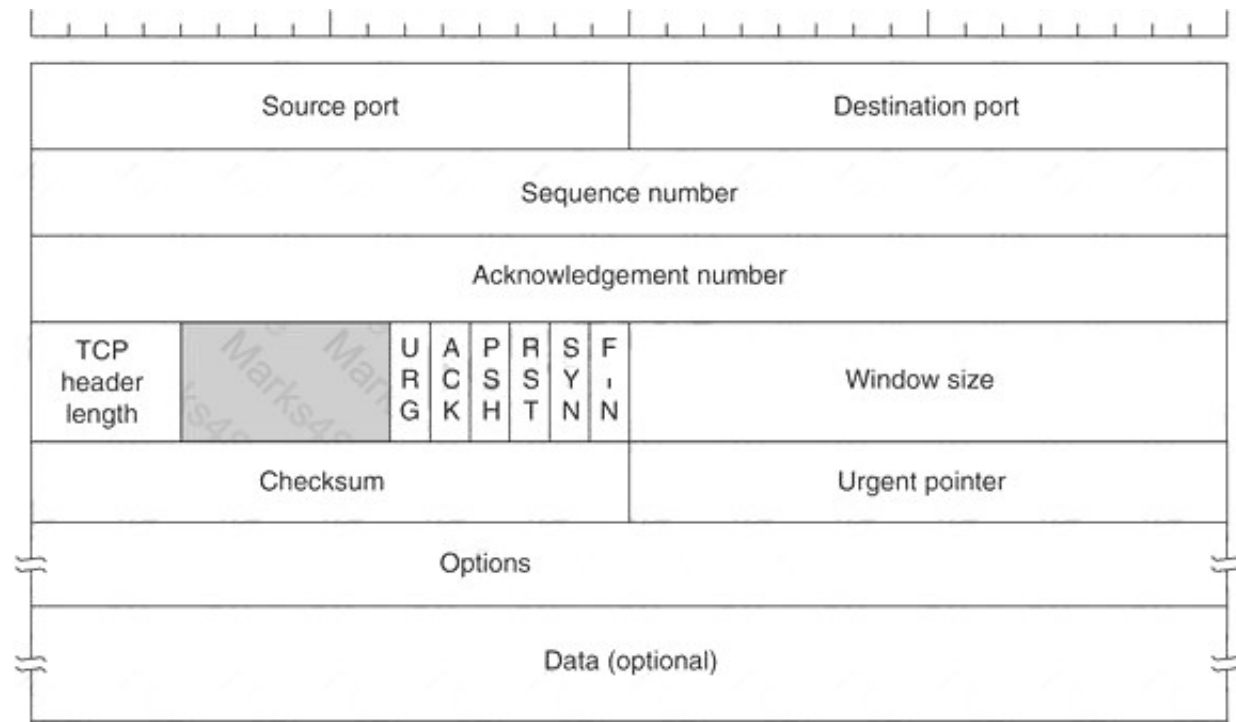
Answer: B

NEW QUESTION 311

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 314

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 319

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 321

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 323

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 326

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 329

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 331

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

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

Answer: D

NEW QUESTION 335

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 412-79v10 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 412-79v10 Product From:

<https://www.2passeasy.com/dumps/412-79v10/>

Money Back Guarantee

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