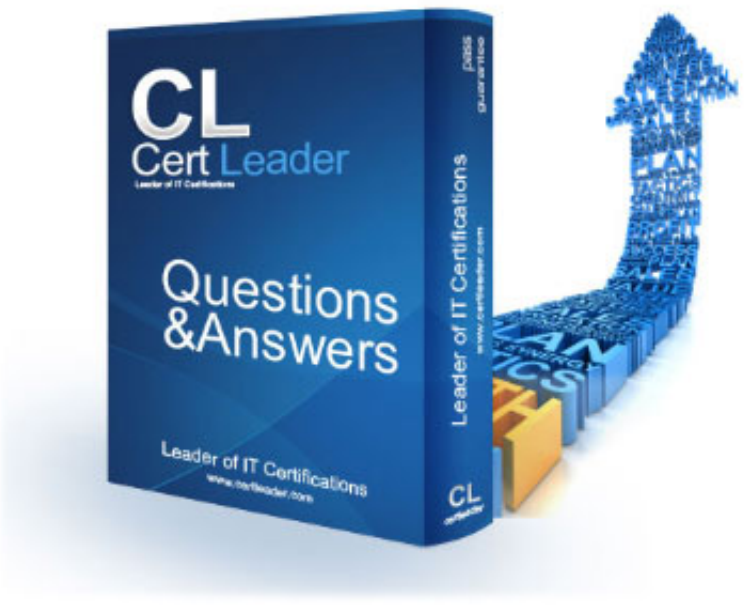
412-79v10 Dumps

EC-Council Certified Security Analyst (ECSA) V10

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



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

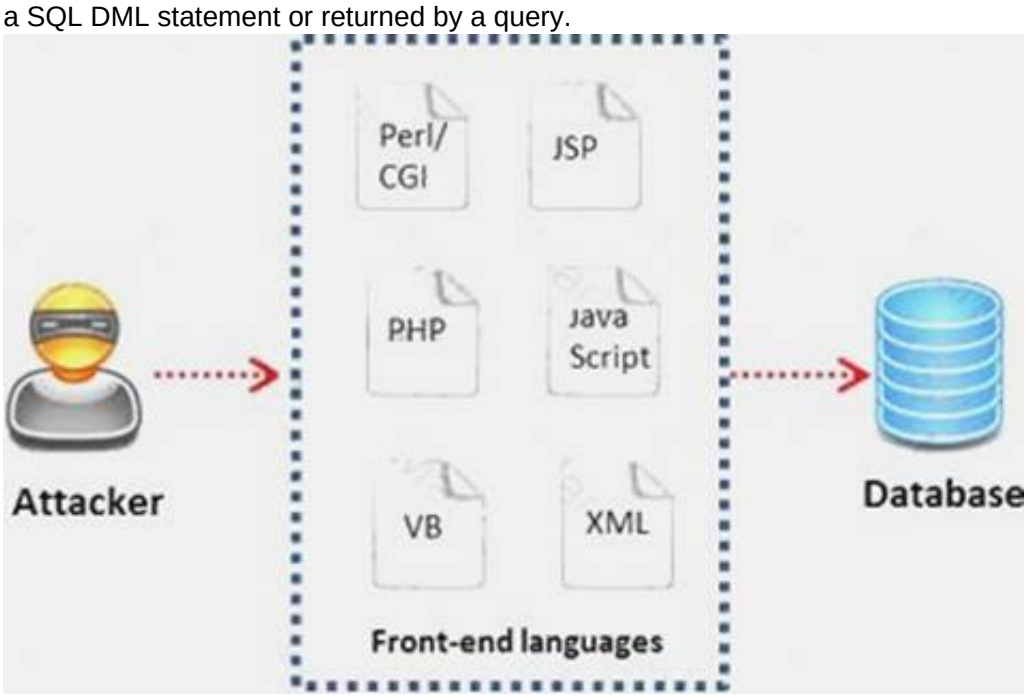
Answer: D

NEW QUESTION 2
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 3
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 4
How many possible sequence number combinations are there in TCP/IP protocol?

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

Answer: C

NEW QUESTION 5
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 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
Which one of the following acts related to the information security in the US fix the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

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

Answer: B

NEW QUESTION 9
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 10
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 10
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 11
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 12
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 17
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

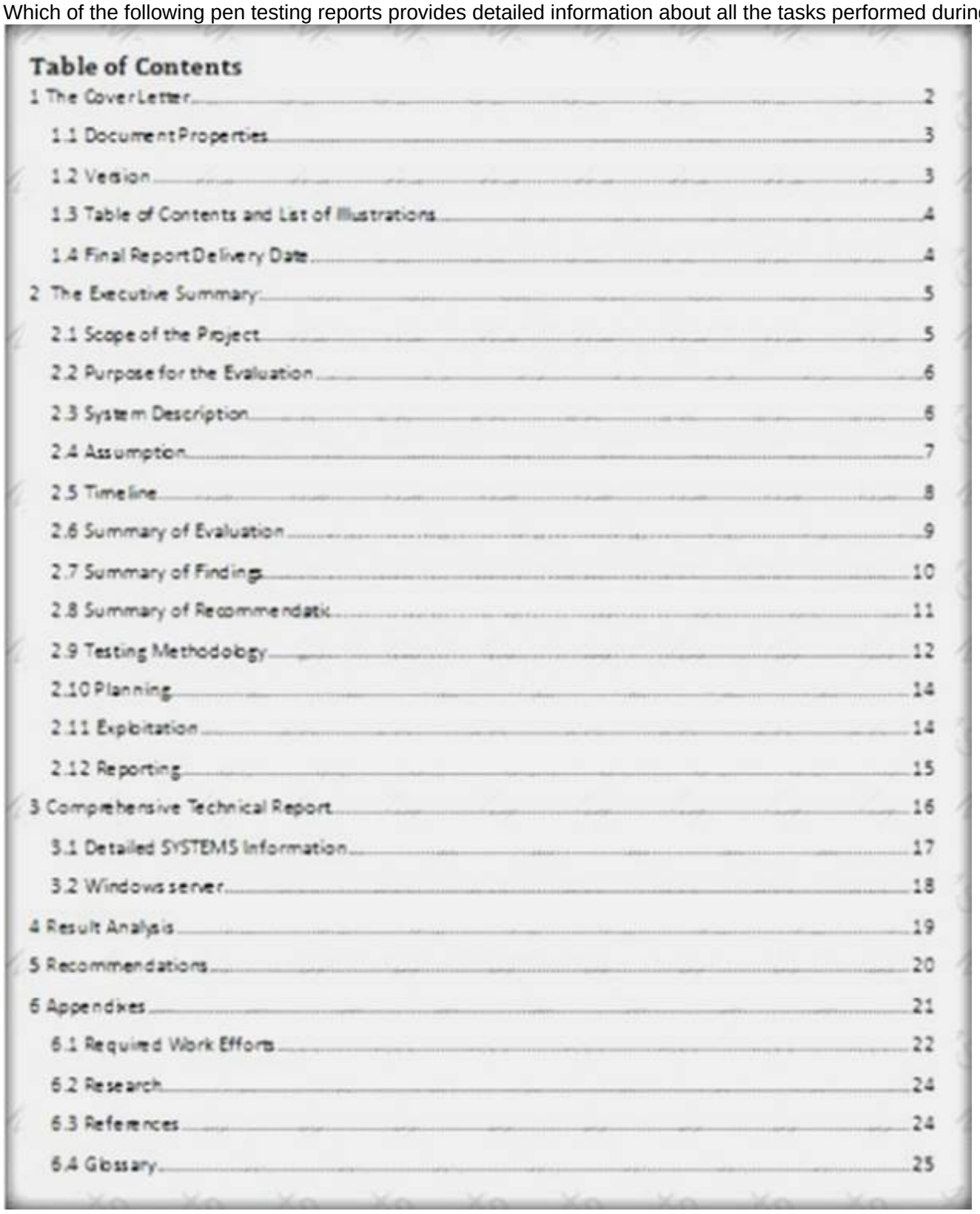


Table of Contents

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

Answer: A

NEW QUESTION 20
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 25
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 26
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

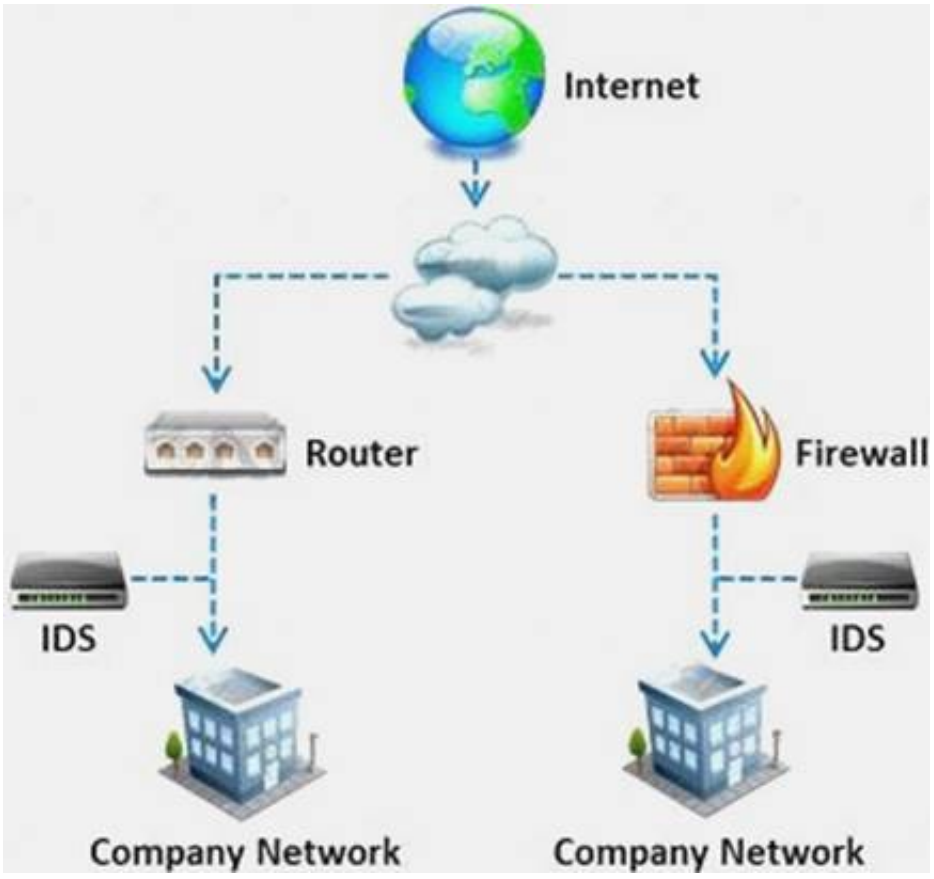
Answer: A

NEW QUESTION 30
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 35
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 36
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 40
The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the signal () function. Which one of the following functions is used as a programspecific signal and the handler for this calls the DropStats() function to output the current Snort statistics?

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

Answer: A

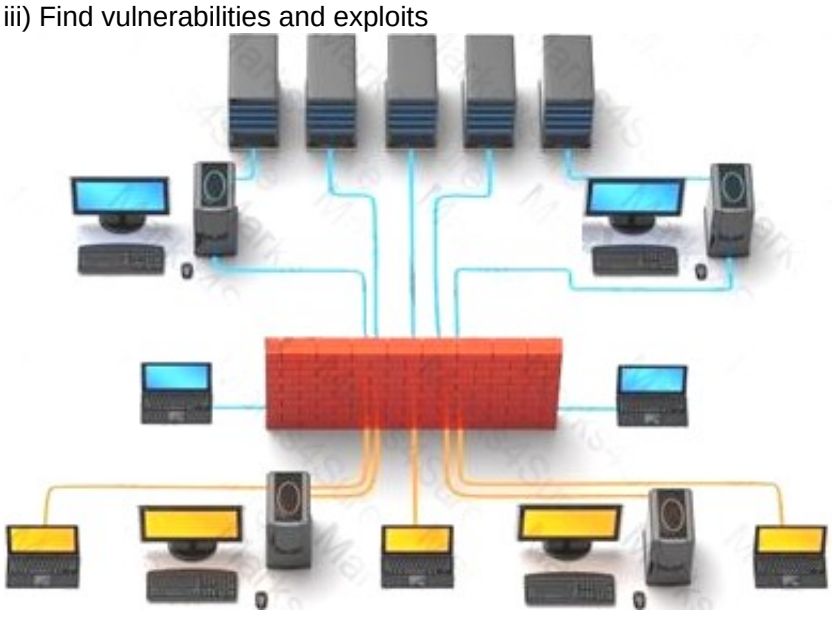
NEW QUESTION 41
An "idle" system is also referred to as what?

A. Zombie
B. PC not being used
C. Bot
D. PC not connected to the Internet

Answer: A

NEW QUESTION 45

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



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

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

Answer: D

NEW QUESTION 48
Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most people say 'Wireless' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and G.
Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

A. 802.11b
B. 802.11g
C. 802.11-Legacy
D. 802.11n

Answer: A

NEW QUESTION 52
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 57
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 59
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 63
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes

B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

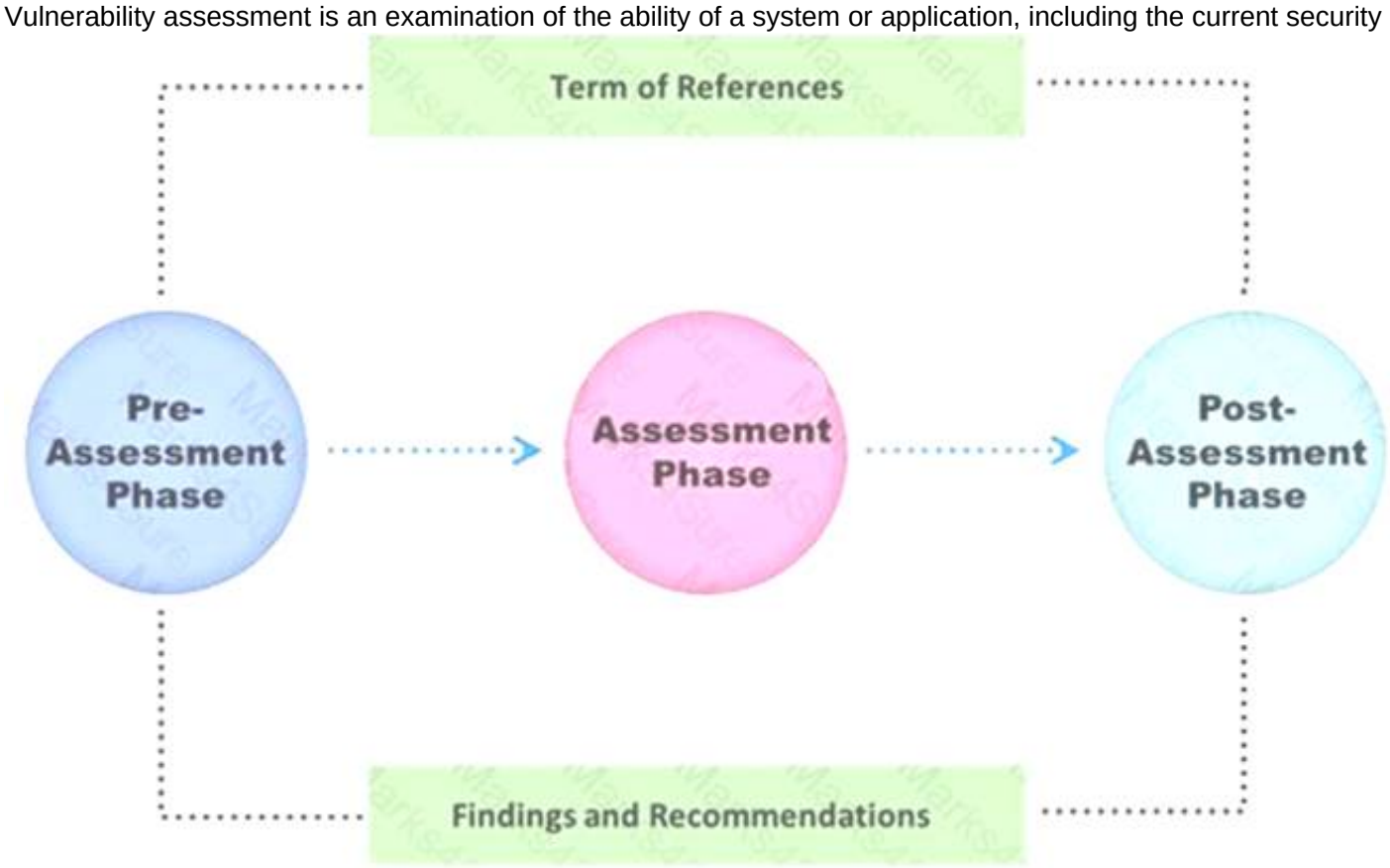
Answer: A

NEW QUESTION 66
An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Answer: D

NEW QUESTION 67
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.

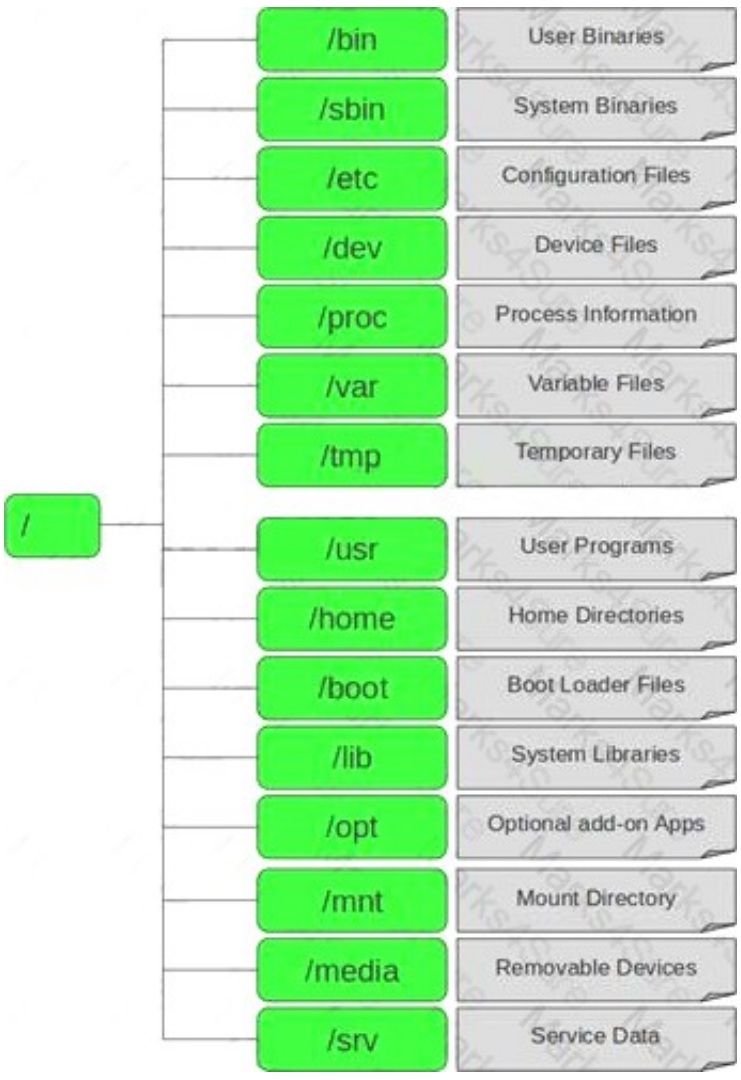


What does a vulnerability assessment identify?

A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure

Answer: B

NEW QUESTION 71
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: 1fnffc$GteyHdicpGOfffXX40w#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 72
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.
link:www.ghttech.net
What will this search produce?

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

Answer: A

NEW QUESTION 75
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

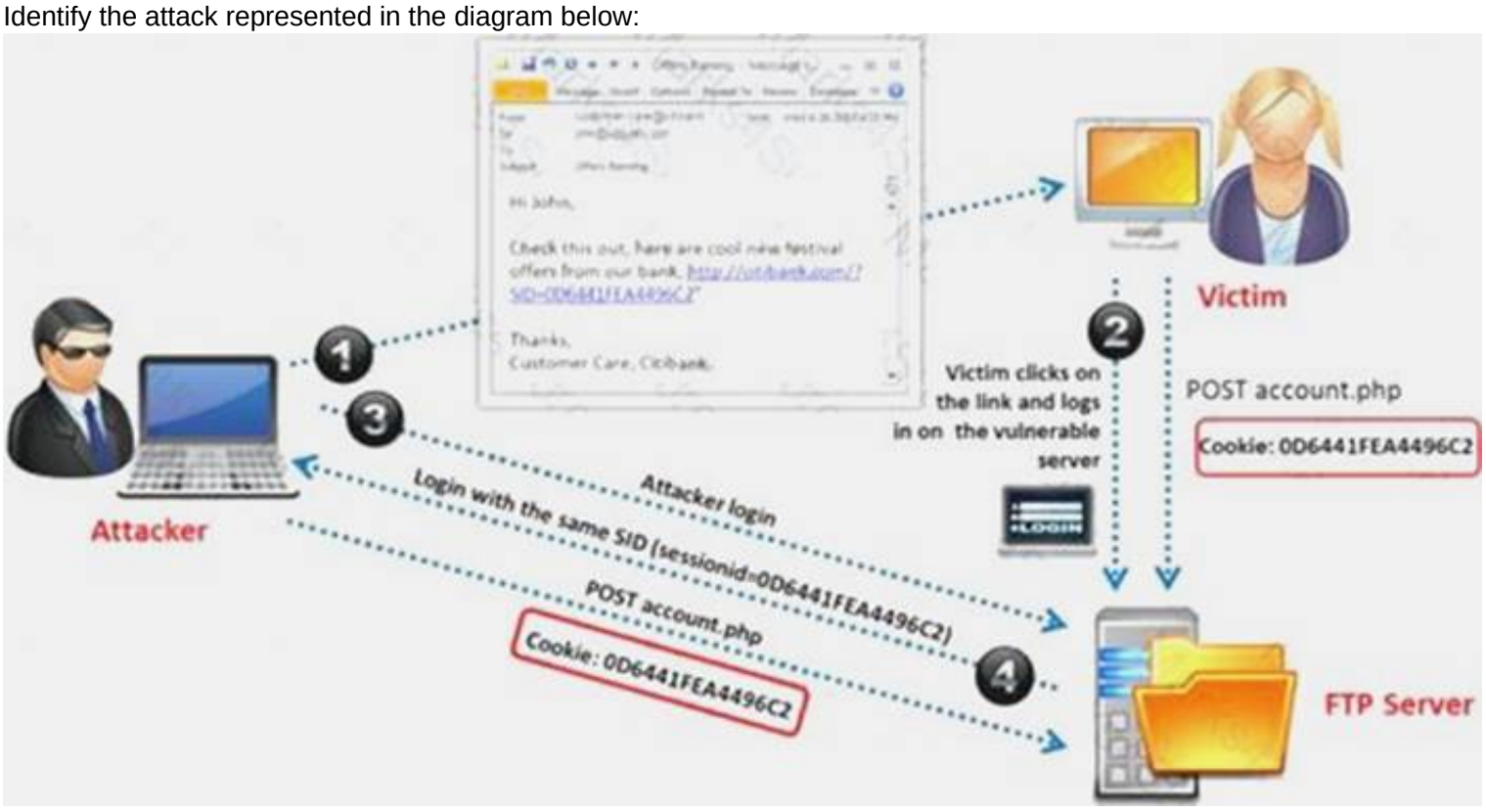
NEW QUESTION 78
The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirements, ROE, and budget.
Various components 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 81
Identify the attack represented in the diagram below:



A. Input Validation
B. Session Hijacking
C. SQL Injection
D. Denial-of-Service

Answer: B

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 86
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 87
You are carrying out the last round of testing for your new website before it goes live. The website has
many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:
<script>alert("This is a test.")</script>
When you type this and click on search, you receive a pop-up window that says: "This is a test."
What is the result of this test?

A. Your website is vulnerable to web bugs
B. Your website is vulnerable to XSS
C. Your website is not vulnerable
D. Your website is vulnerable to SQL injection

Answer: B

NEW QUESTION 88
Software firewalls work at which layer of the OSI model?

A. Data Link
B. Network
C. Transport
D. Application

Answer: A

NEW QUESTION 89
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 94
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 96
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

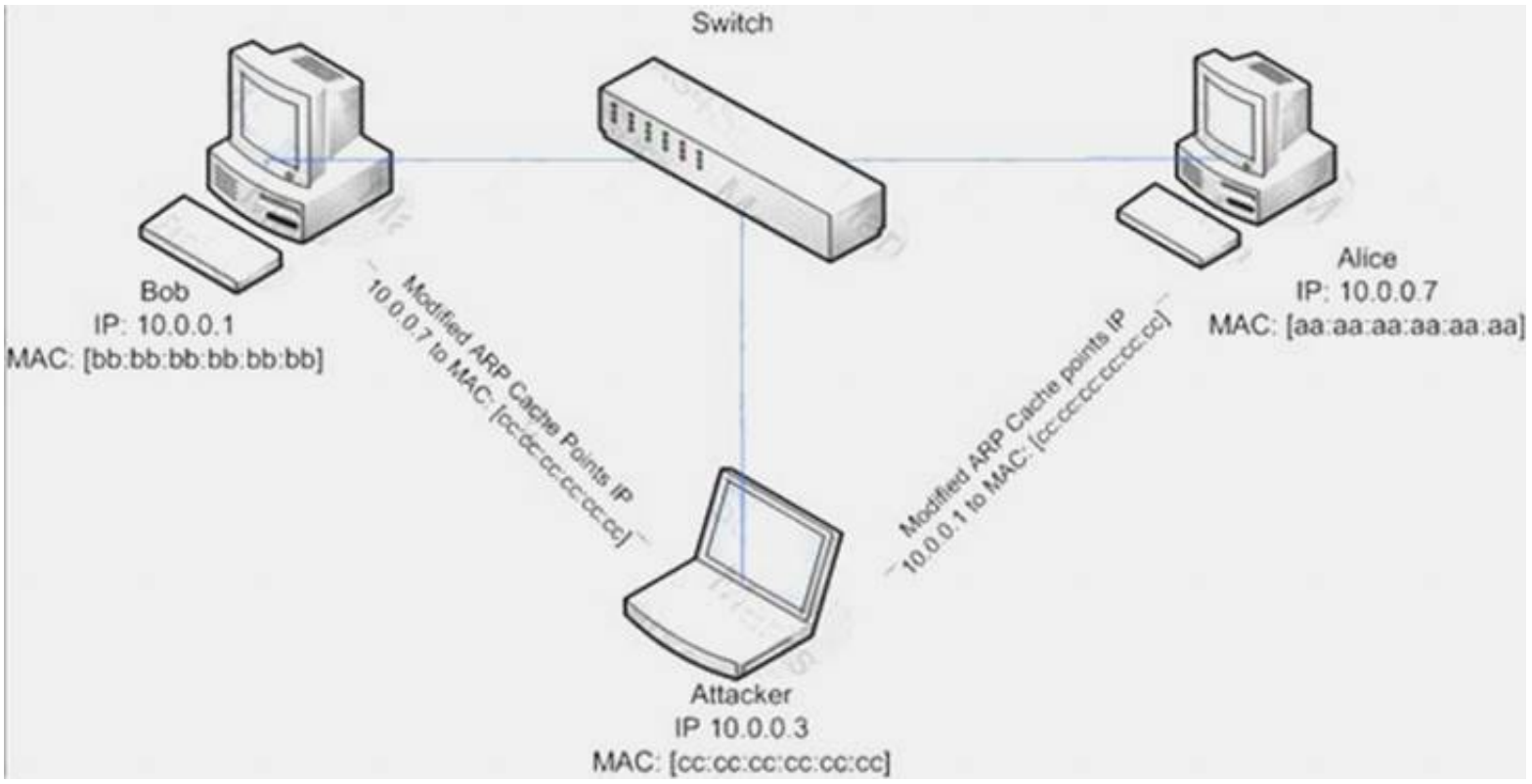
Answer: B

NEW QUESTION 97
Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.
D. public company boards, management and public accounting firms
E. To certify the accuracy of the reported financial statement

Answer: A

NEW QUESTION 101
ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.

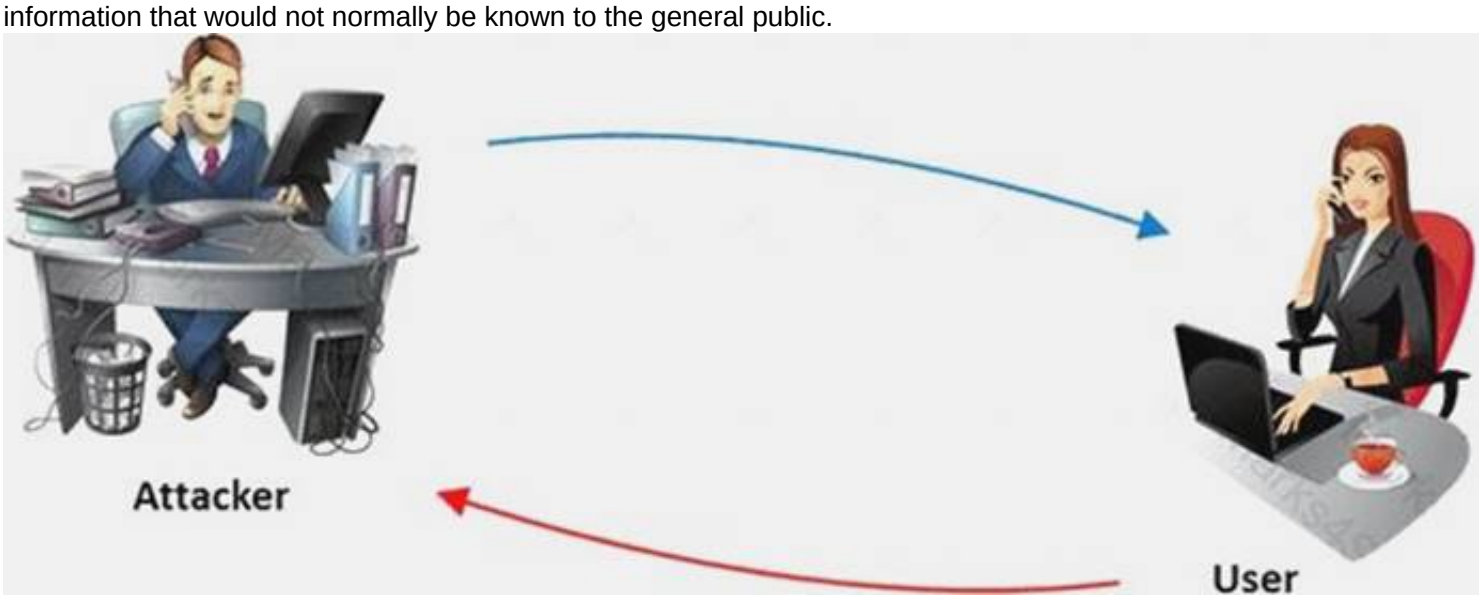


What type of attack would you launch after successfully deploying ARP spoofing?

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

Answer: D

NEW QUESTION 102
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 106
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 111
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information.
You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

A. Nmap
B. Netcraft

C. Ping sweep
D. Dig

Answer: B

NEW QUESTION 115
Which one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

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

Answer: C

NEW QUESTION 118
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 120
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

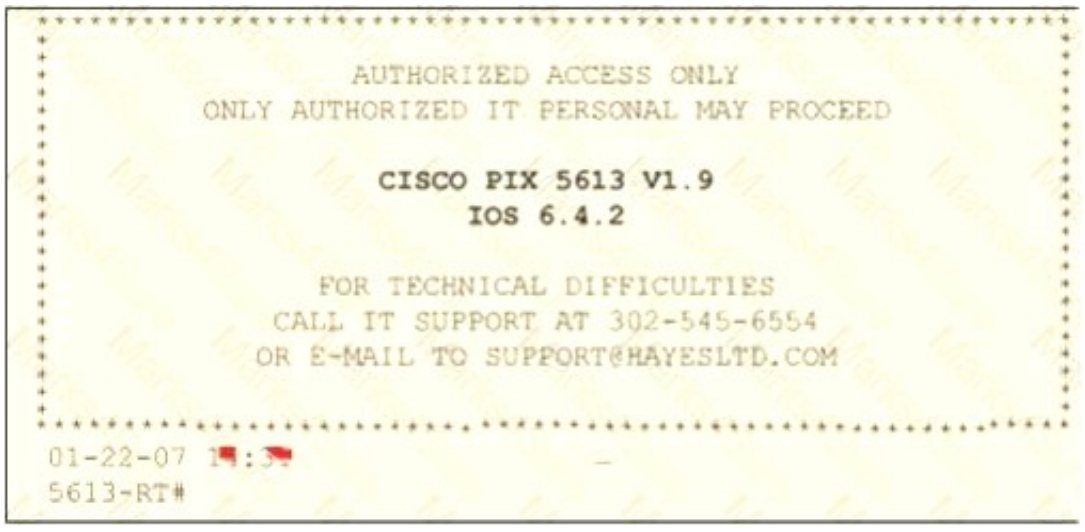
Answer: A

NEW QUESTION 123
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 127
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

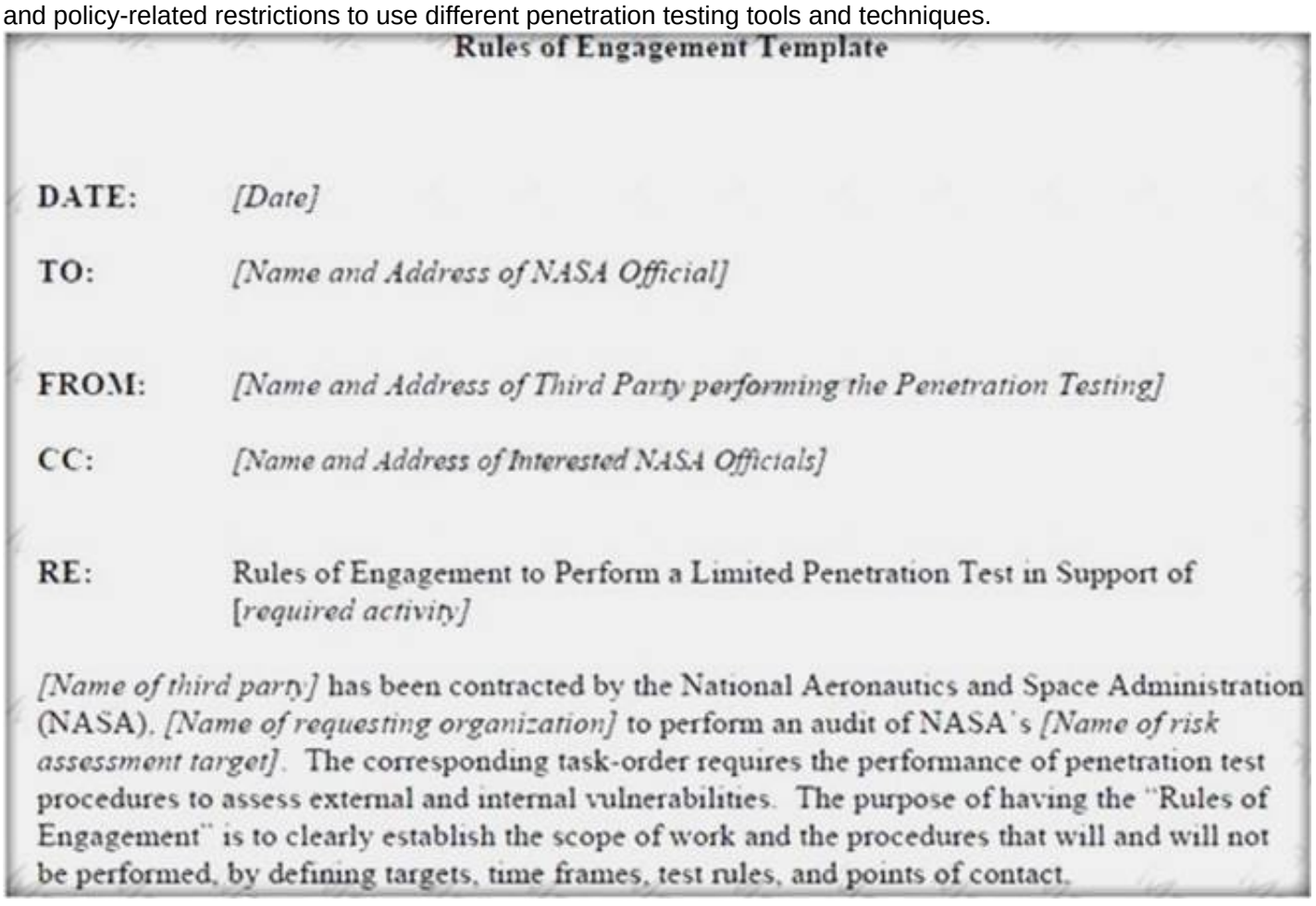
Answer: B

NEW QUESTION 128
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 131
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.


Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of *[required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA). *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

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 136
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 140
A Demilitarized Zone (DMZ) is a computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public

network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization.
Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

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

Answer: D

NEW QUESTION 145
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 150
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 151
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 152
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 153
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 155
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port 21

Answer: C

NEW QUESTION 159

Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?

A. Microsoft Baseline Security Analyzer (MBSA)
B. CORE Impact
C. Canvas
D. Network Security Analysis Tool (NSAT)

Answer: C

NEW QUESTION 162
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 164
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

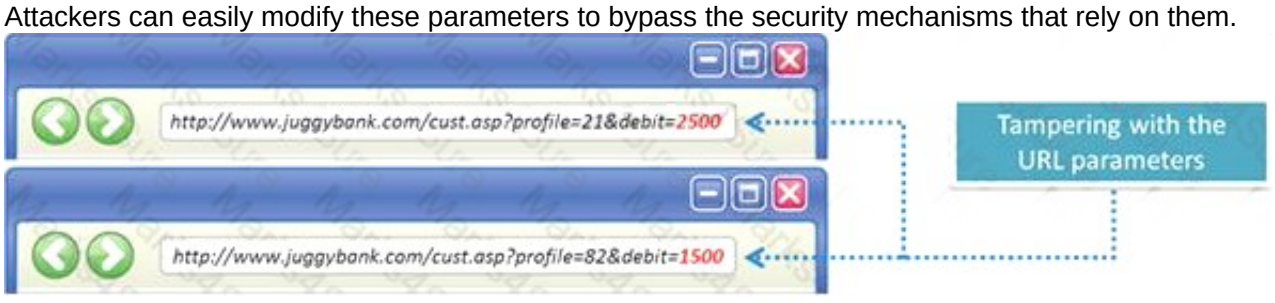
Answer: A

NEW QUESTION 167
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 170
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 171
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses.
You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Metamorphic
B. Oligomorhic

C. Polymorphic
D. Transmorphic

Answer: A

NEW QUESTION 173
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 174
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 178
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 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 180
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 184
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

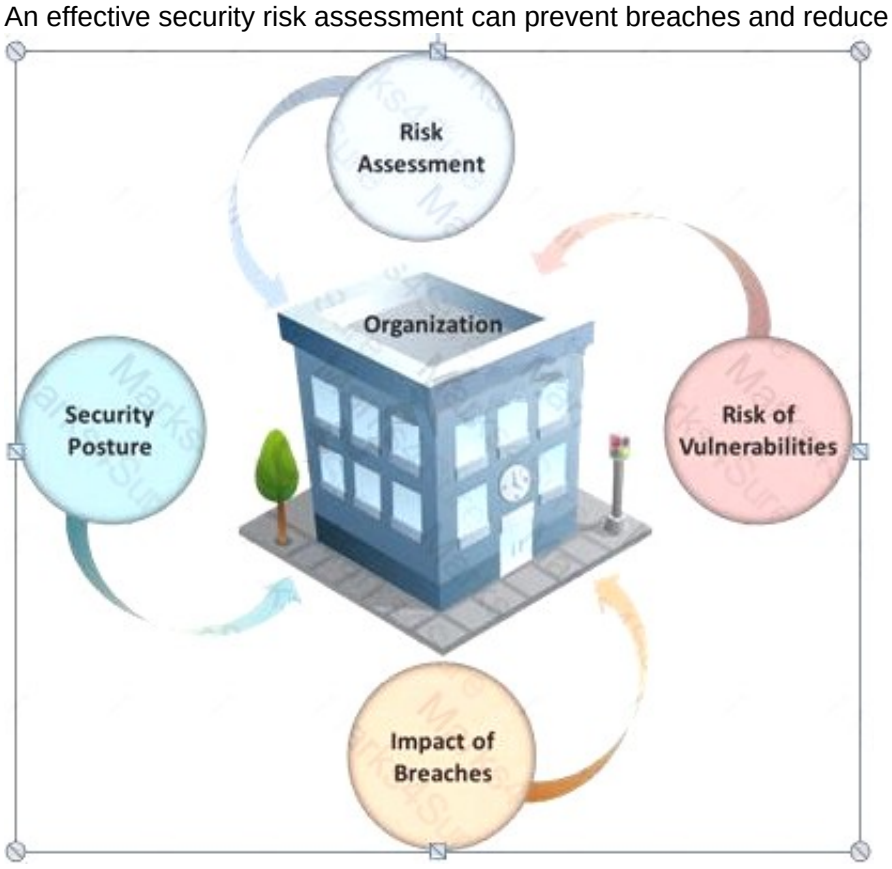
NEW QUESTION 187
In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique
B. IDS evasion technique

C. UDP evasion technique
D. TTL evasion technique

Answer: D

NEW QUESTION 192
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 197
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 200
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

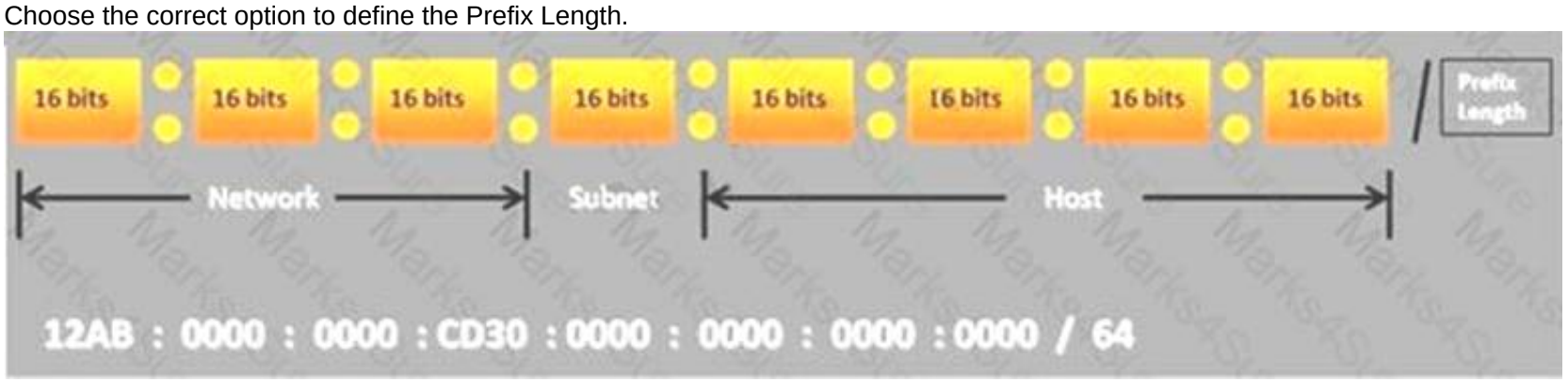
NEW QUESTION 204
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization
B. Type of testers involved
C. The budget required
D. Expected time required to finish the project

Answer: A

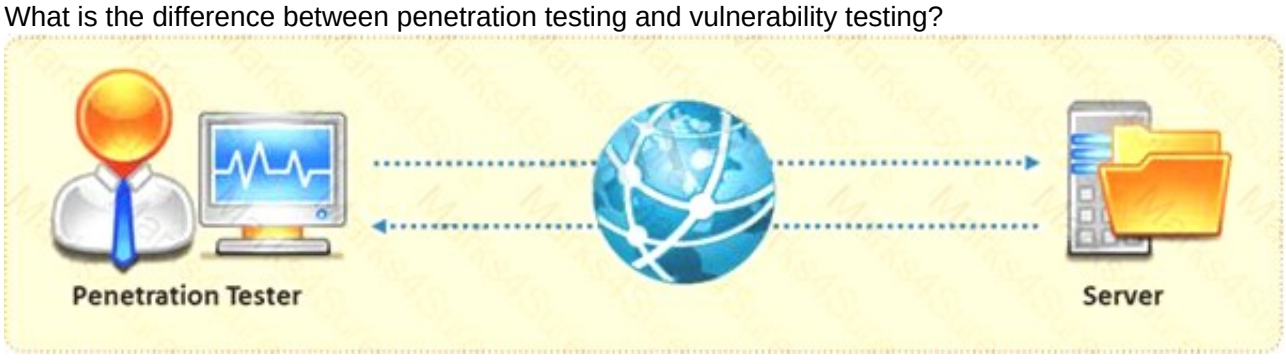
NEW QUESTION 206
Choose the correct option to define the Prefix Length.



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 211
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 215

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 219
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 t 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 224
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 227
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 228
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 231
In Linux, what is the smallest possible shellcode?

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

Answer: D

NEW QUESTION 234
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 Lophtcrack 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 236
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 237
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs.
He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

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

Answer: A

NEW QUESTION 242
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

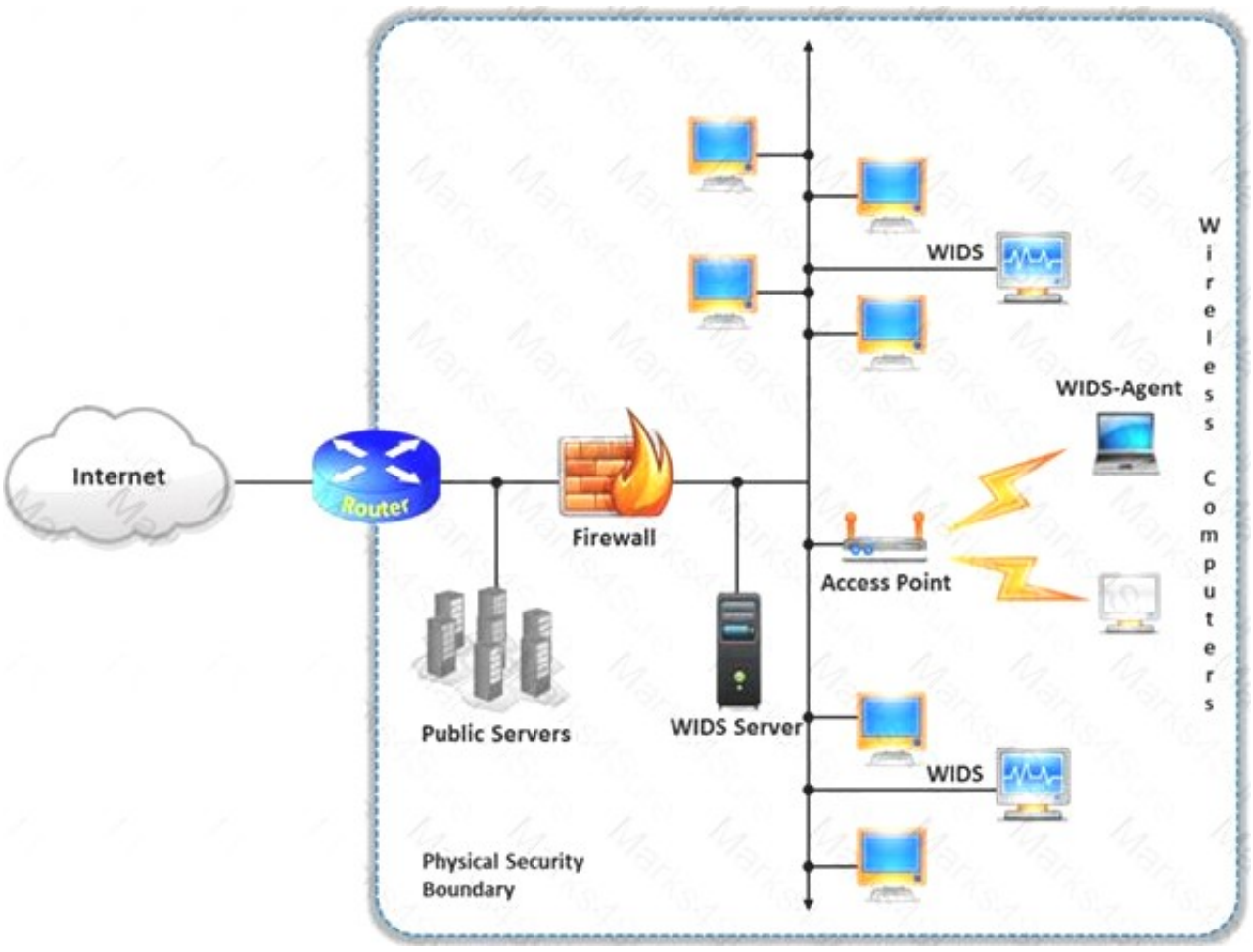
Answer: A

NEW QUESTION 244
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the Restrict Anonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server.
Using User info tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

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

Answer: A

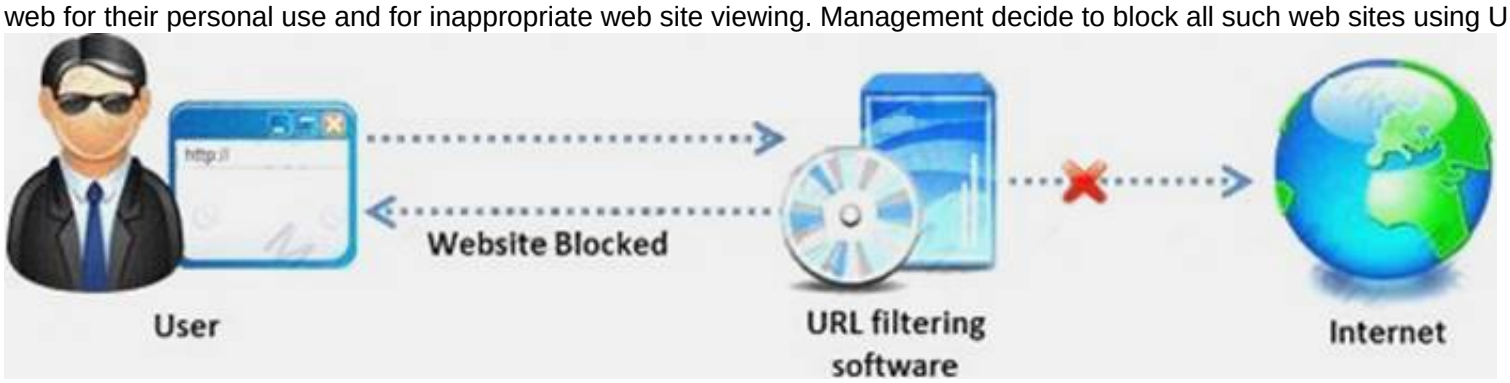
NEW QUESTION 246
A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools.
The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a 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 251
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 256
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

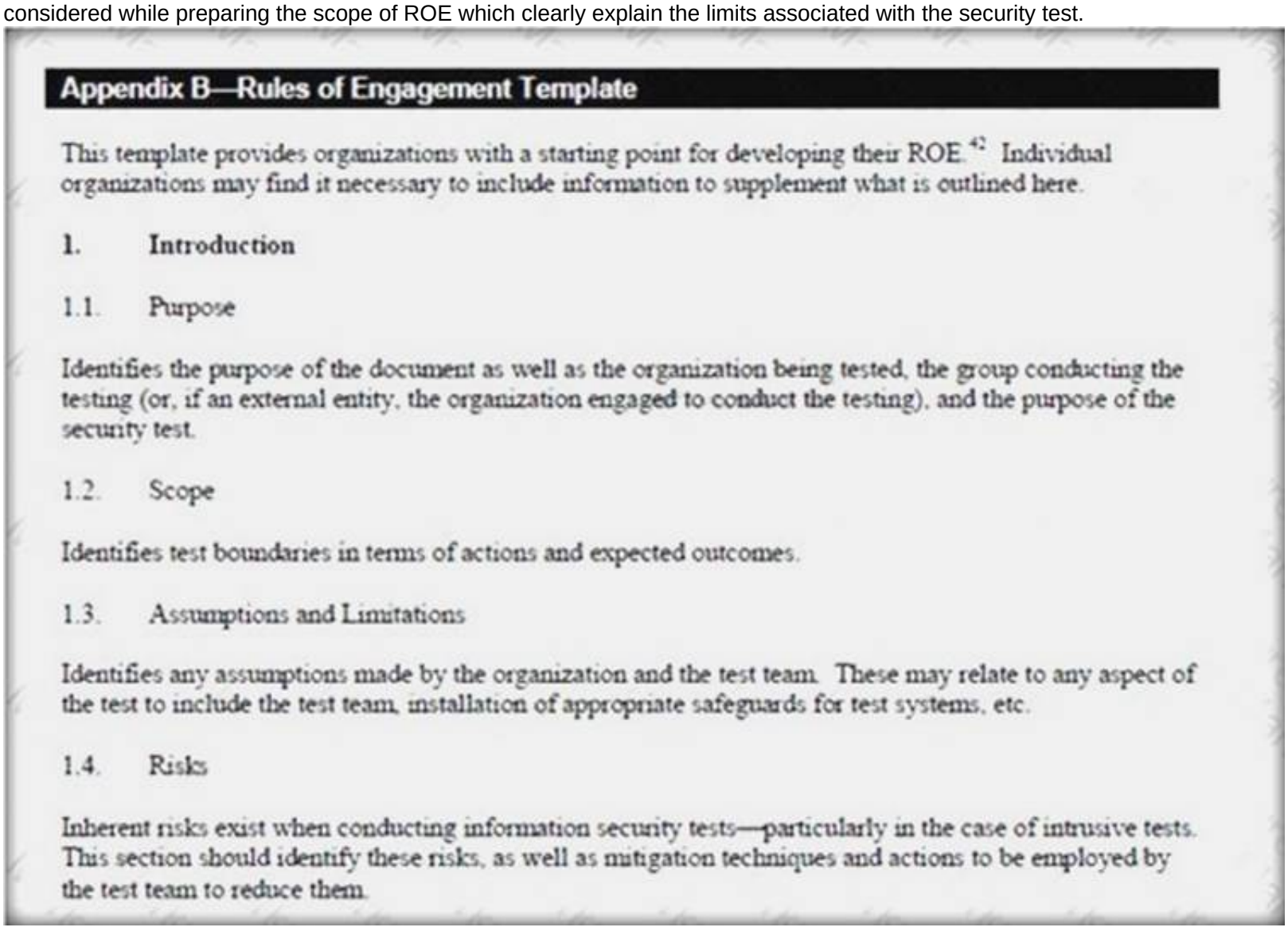
Answer: D

NEW QUESTION 261
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 262
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.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (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 264
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 265
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 267
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 272
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 276
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

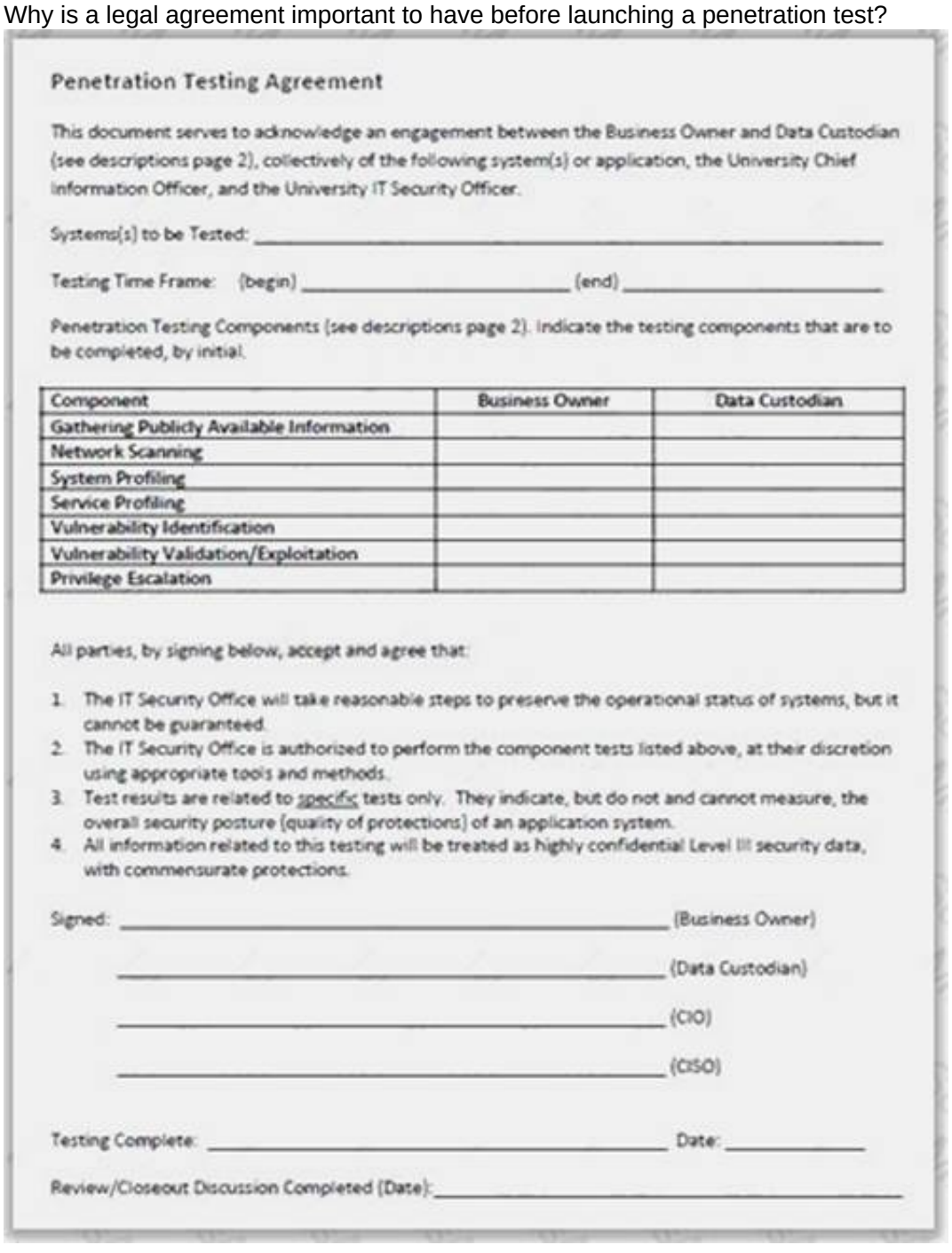
Answer: B

NEW QUESTION 280
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 281
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.

System(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 282
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 287
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 292
John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client. Which of the following factors does he need to consider while preparing the pen testing pricing report?

A. Number of employees in the client organization
B. Complete structure of the organization
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Answer: C

NEW QUESTION 293
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 296
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 299
Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

A. 6566 TCP port
B. 6771 TCP port
C. 6667 TCP port
D. 6257 TCP port

Answer: C

NEW QUESTION 302
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 303
What operating system would respond to the following command?

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

A. Mac OS X
B. Windows XP
C. Windows 95
D. FreeBSD

Answer: D

NEW QUESTION 304
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

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

Answer: A

NEW QUESTION 307
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 412-79v10 Exam with Our Prep Materials Via below:

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