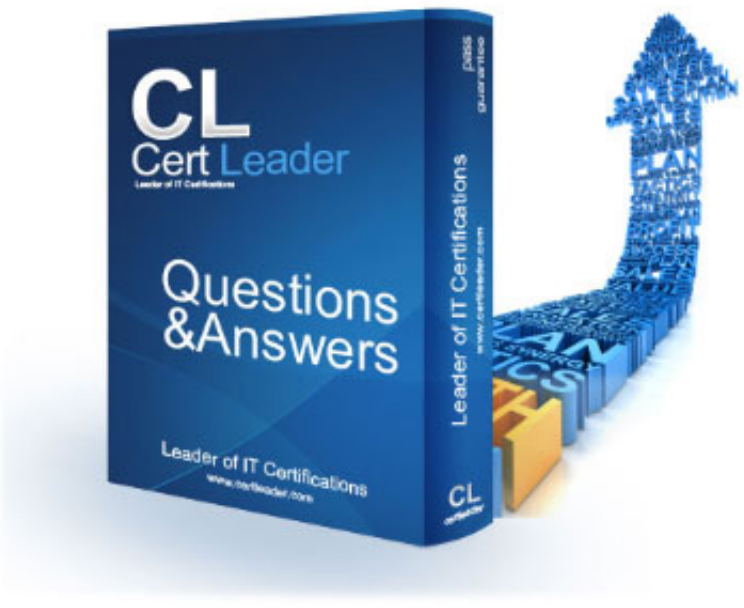
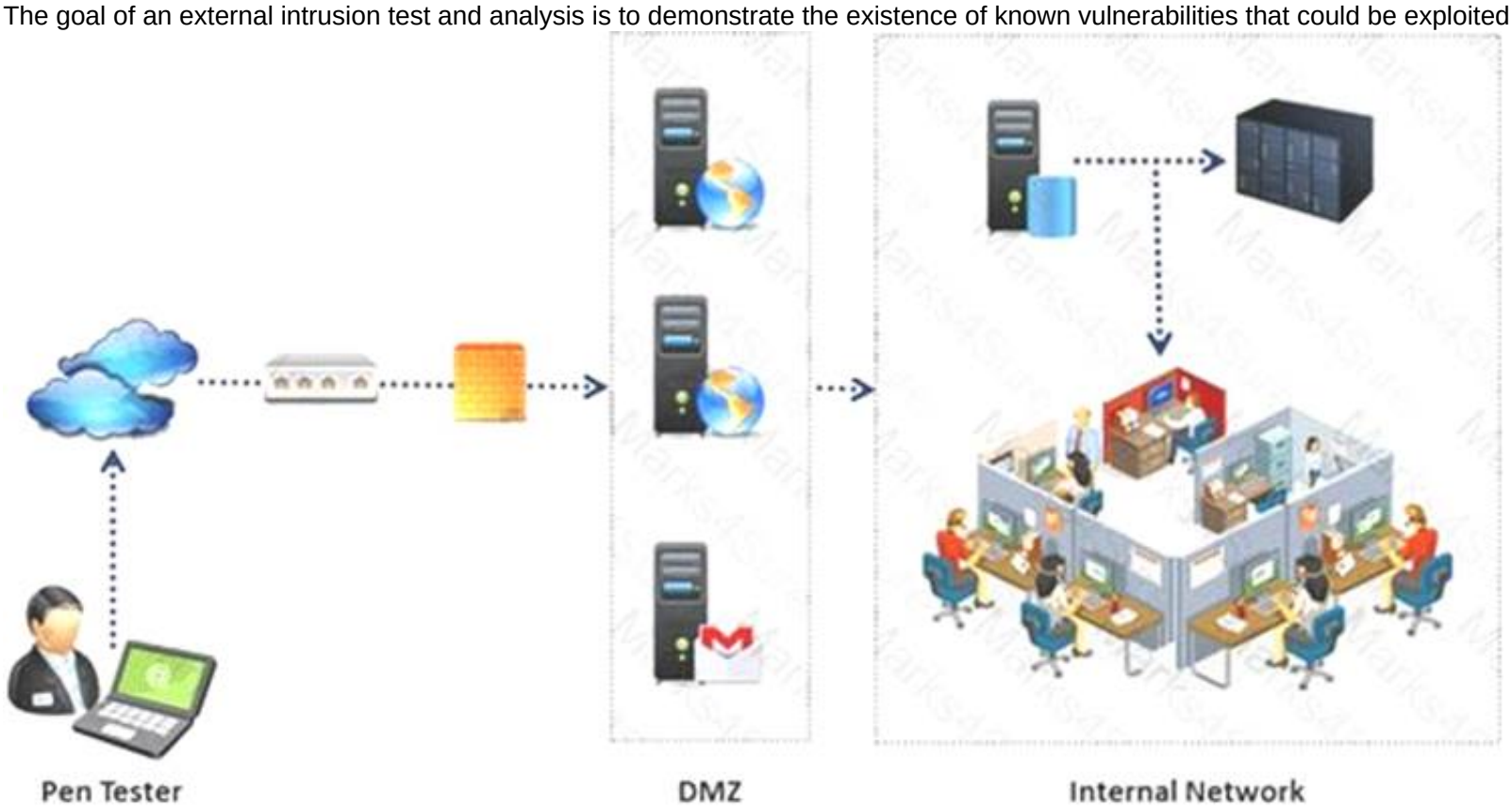
412-79v10 Dumps

EC-Council Certified Security Analyst (ECSA) V10

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



NEW QUESTION 1
An external intrusion test and analysis identify security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the Internet.
The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.

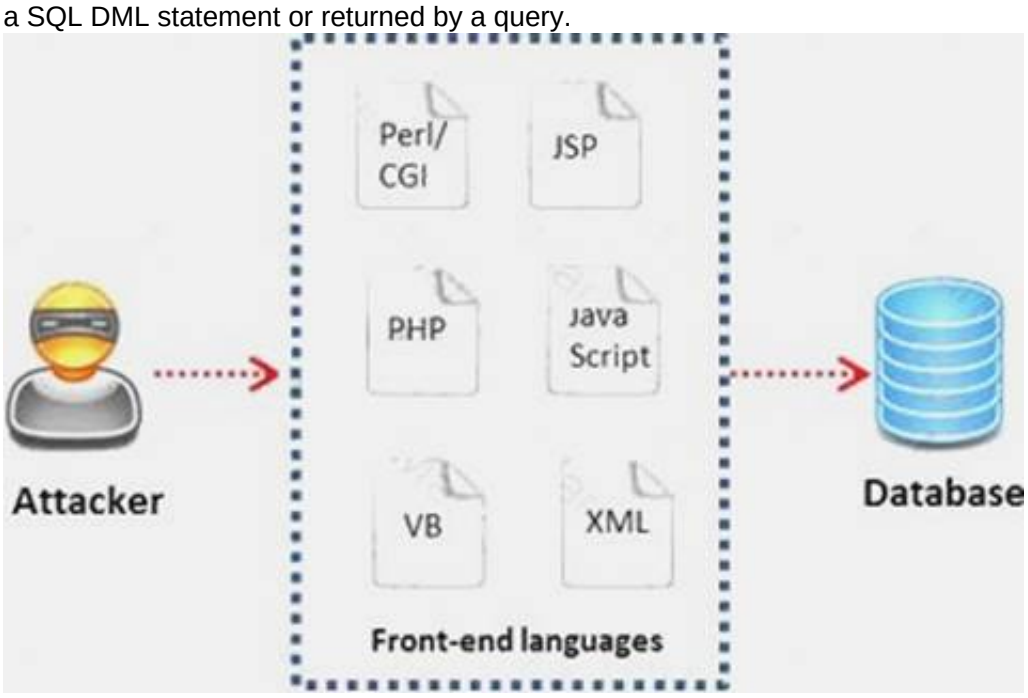


During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

A. XMAS Scan
B. SYN scan
C. FIN Scan
D. NULL Scan

Answer: B

NEW QUESTION 2
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
What will the following URL produce in an unpatched IIS Web Server?
http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Execute a buffer flow in the C: drive of the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Directory listing of the C:\windows\system32 folder on the web server

D. Directory listing of C: drive on the web server

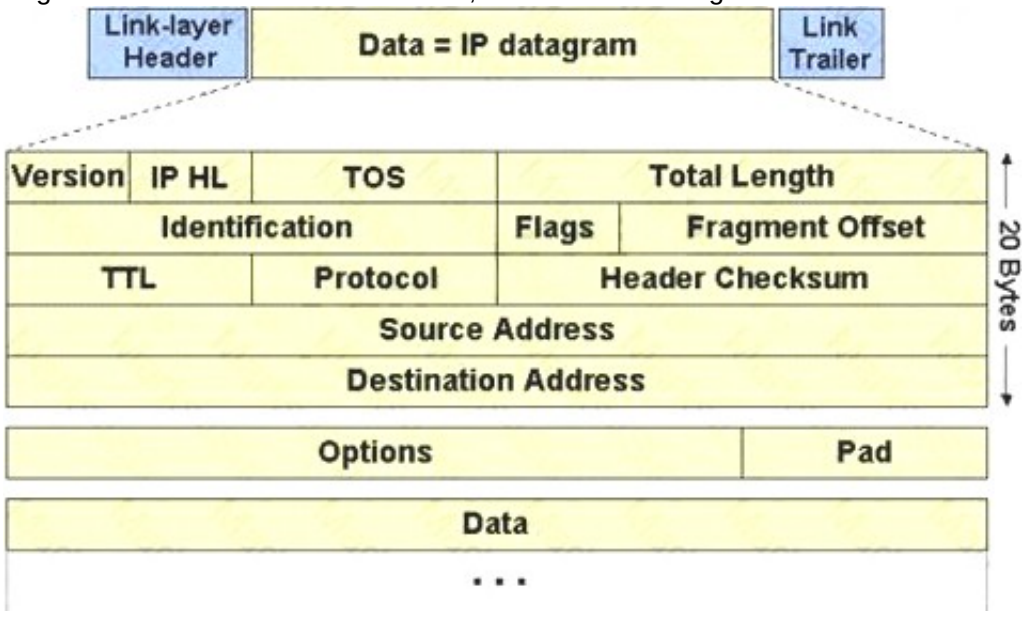
Answer: D

NEW QUESTION 4
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 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 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 7
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

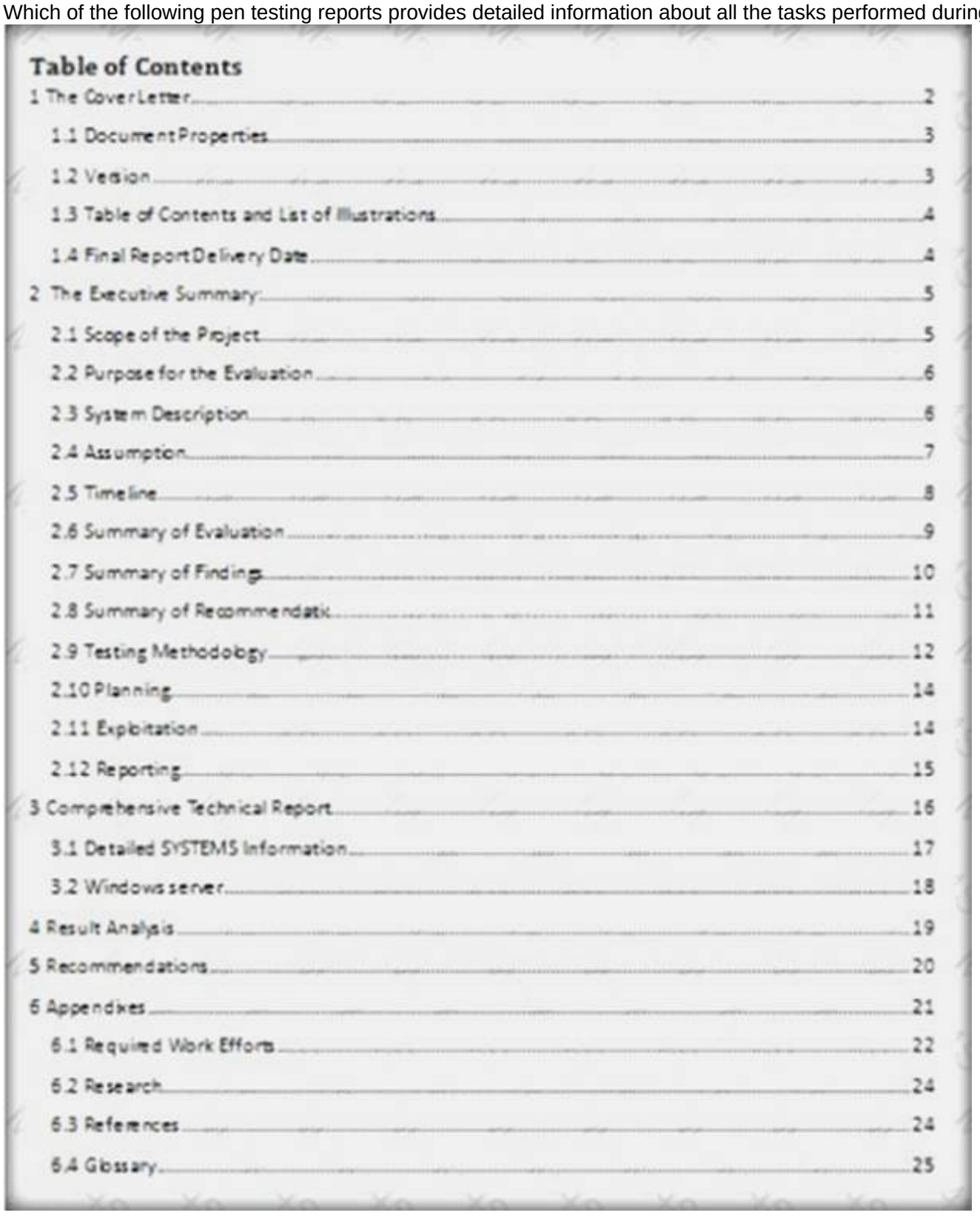
Answer: C

NEW QUESTION 8
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

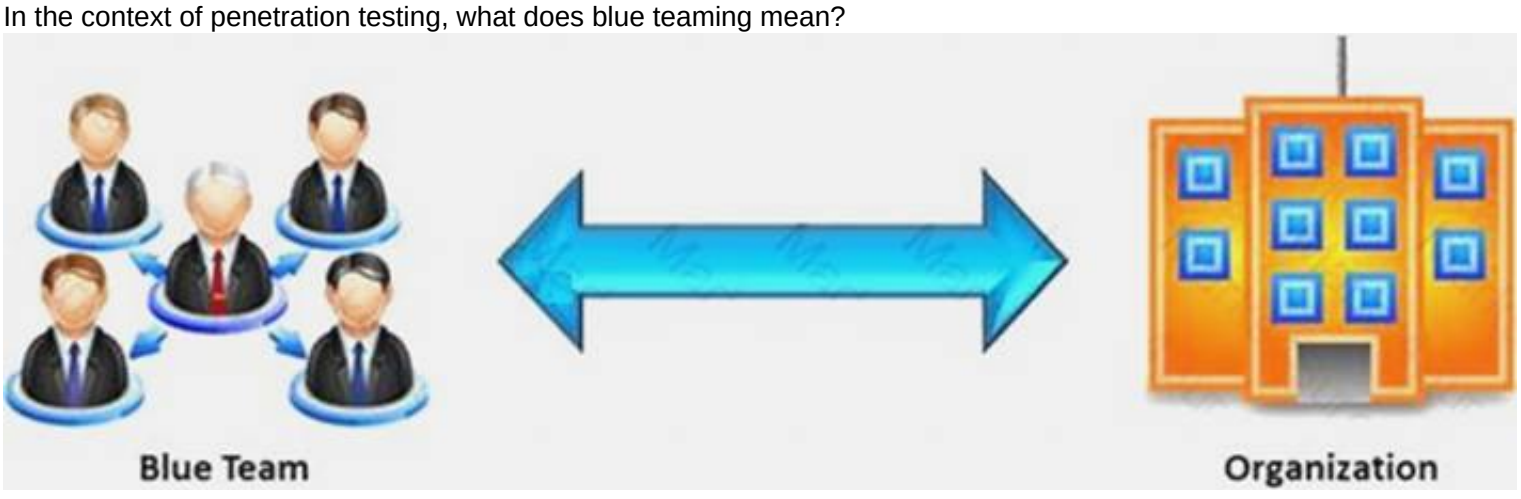
NEW QUESTION 9
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?



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

Answer: A

NEW QUESTION 10
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

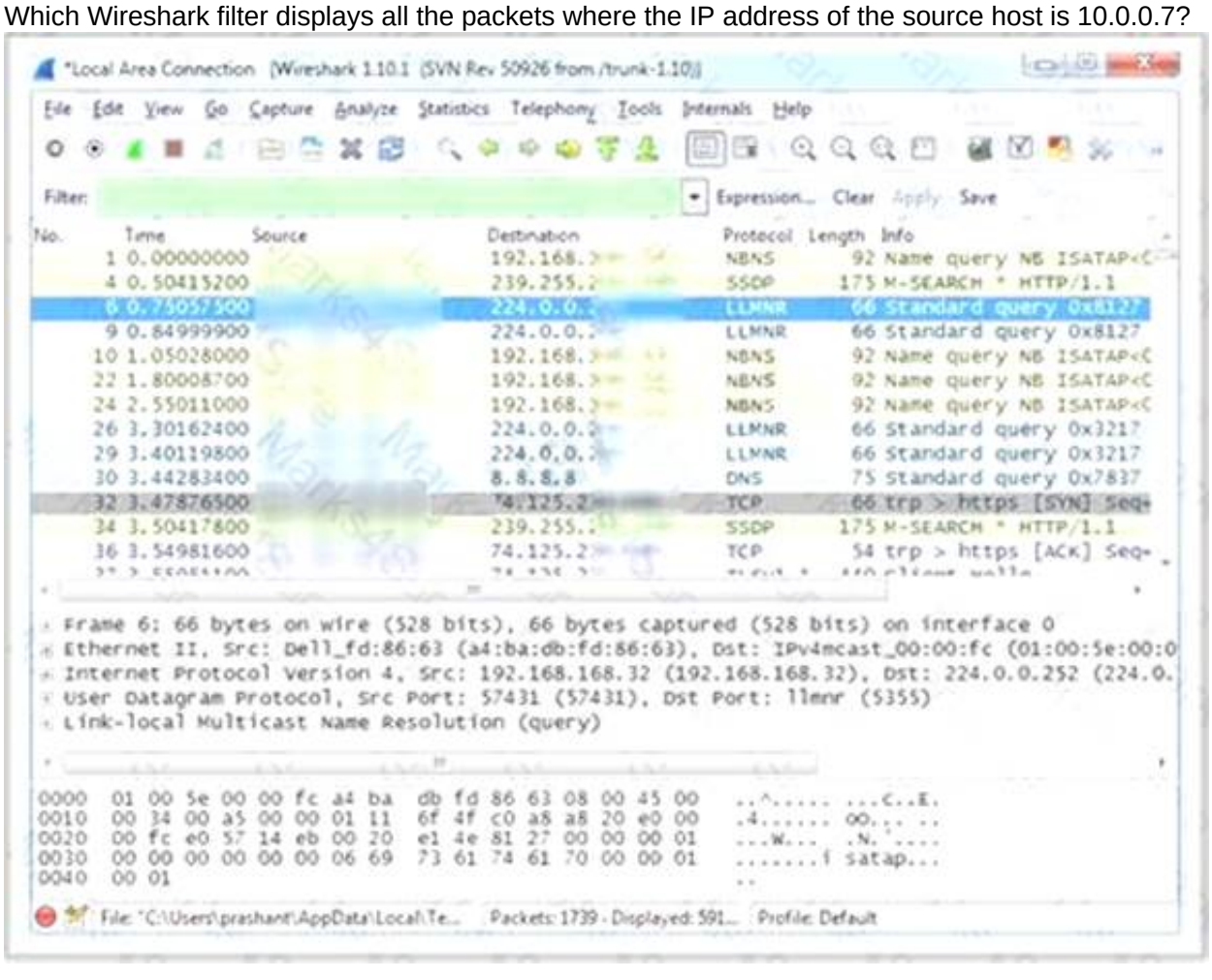
Answer: A

NEW QUESTION 10
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 11
Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



A. ip.dst==10.0.0.7
B. ip.port==10.0.0.7
C. ip.src==10.0.0.7
D. ip.dstport==10.0.0.7

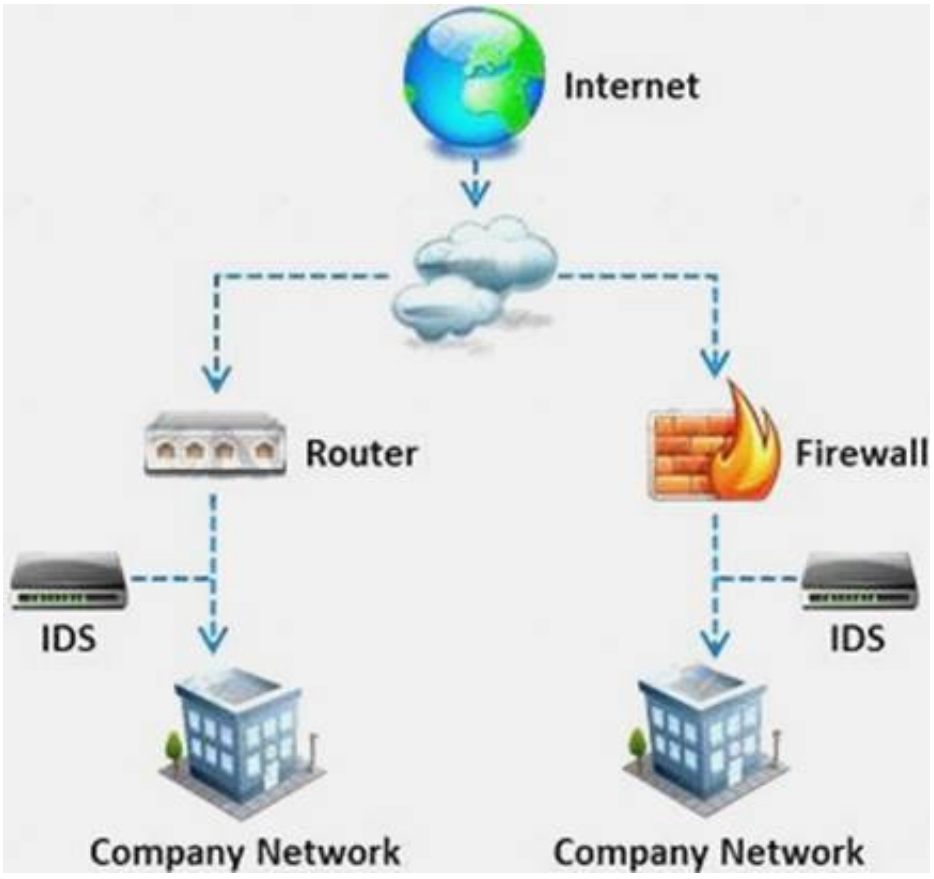
Answer: C

NEW QUESTION 12
Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?

A. AES
B. DES (ECB mode)
C. MD5
D. RC5

Answer: C

NEW QUESTION 17
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 19
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 24
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 29
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 32
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 35
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 37
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 Surfoffline 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 45
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 47
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 49
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
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 56
What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Port Unreachable
C. Protocol Unreachable
D. Administratively Blocked

Answer: D

NEW QUESTION 60
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

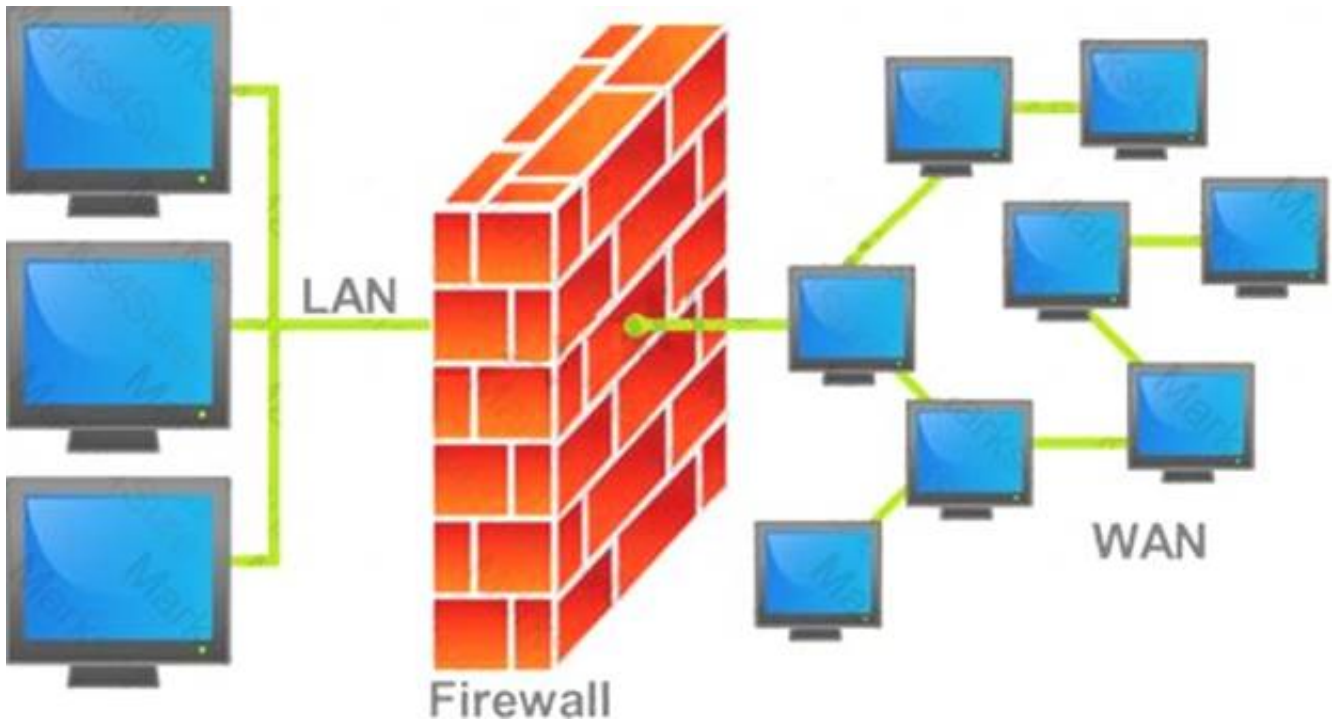
Answer: C

NEW QUESTION 62
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 64
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.

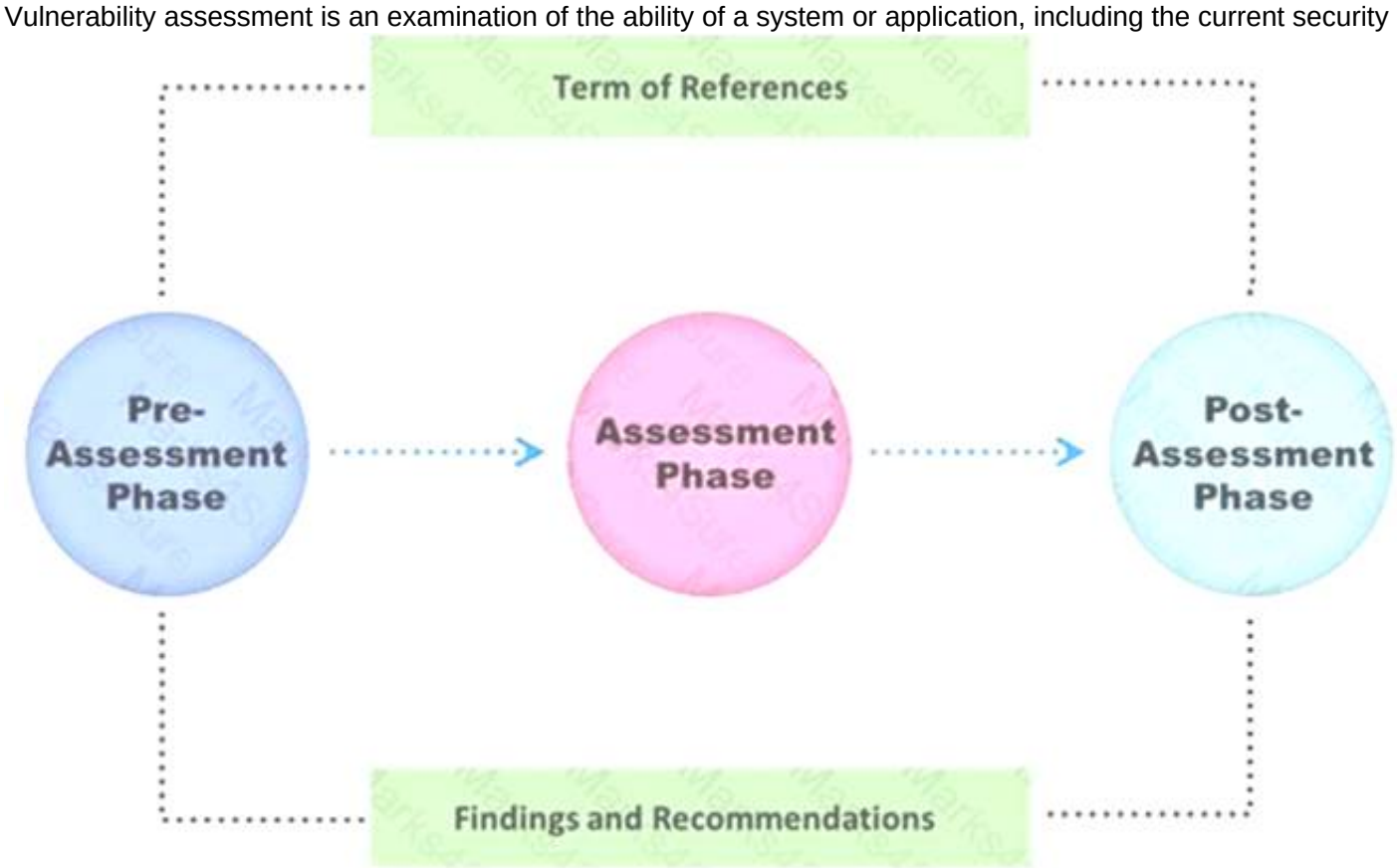


Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

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 68
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.

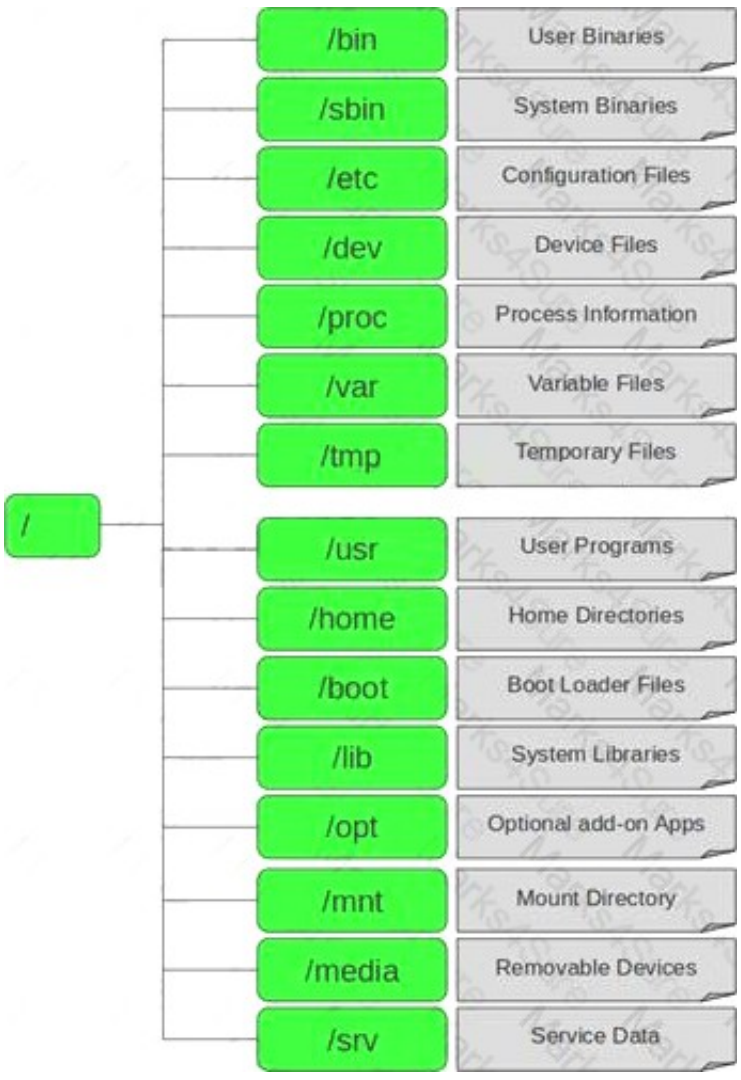


What does a vulnerability assessment identify?

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

Answer: B

NEW QUESTION 69
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

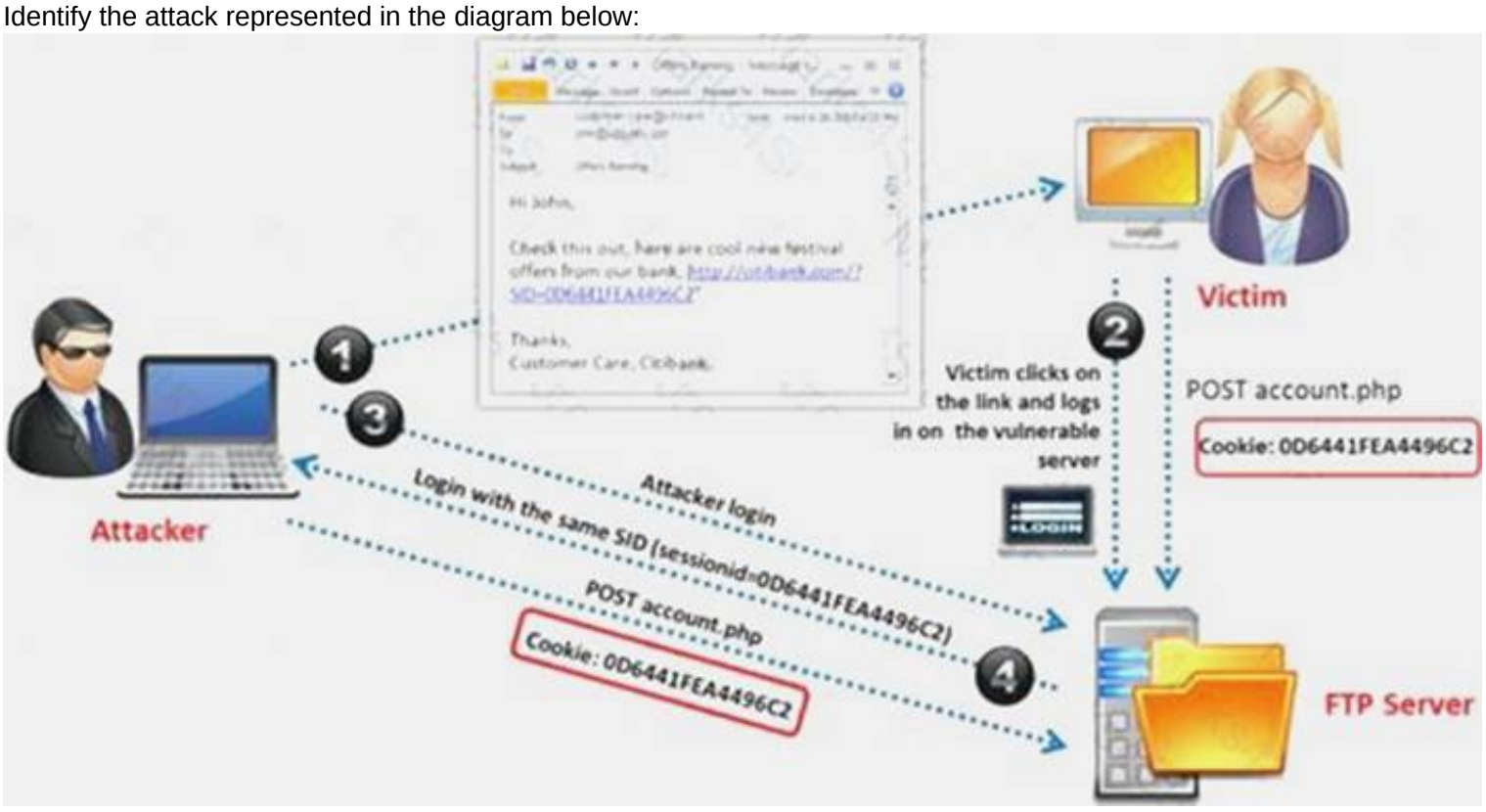
NEW QUESTION 78
The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirements, ROE, and budget.
Various components 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 80
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 82
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 84
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 86
Software firewalls work at which layer of the OSI model?

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

Answer: A

NEW QUESTION 88
Which one of the following log analysis tools is used for analyzing the server's log files?

A. Performance Analysis of Logs tool
B. Network Sniffer Interface Test tool
C. Ka Log Analyzer tool
D. Event Log Tracker tool

Answer: C

NEW QUESTION 93
Which of the following acts is a proprietary information security standard for organizations that handle
cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

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

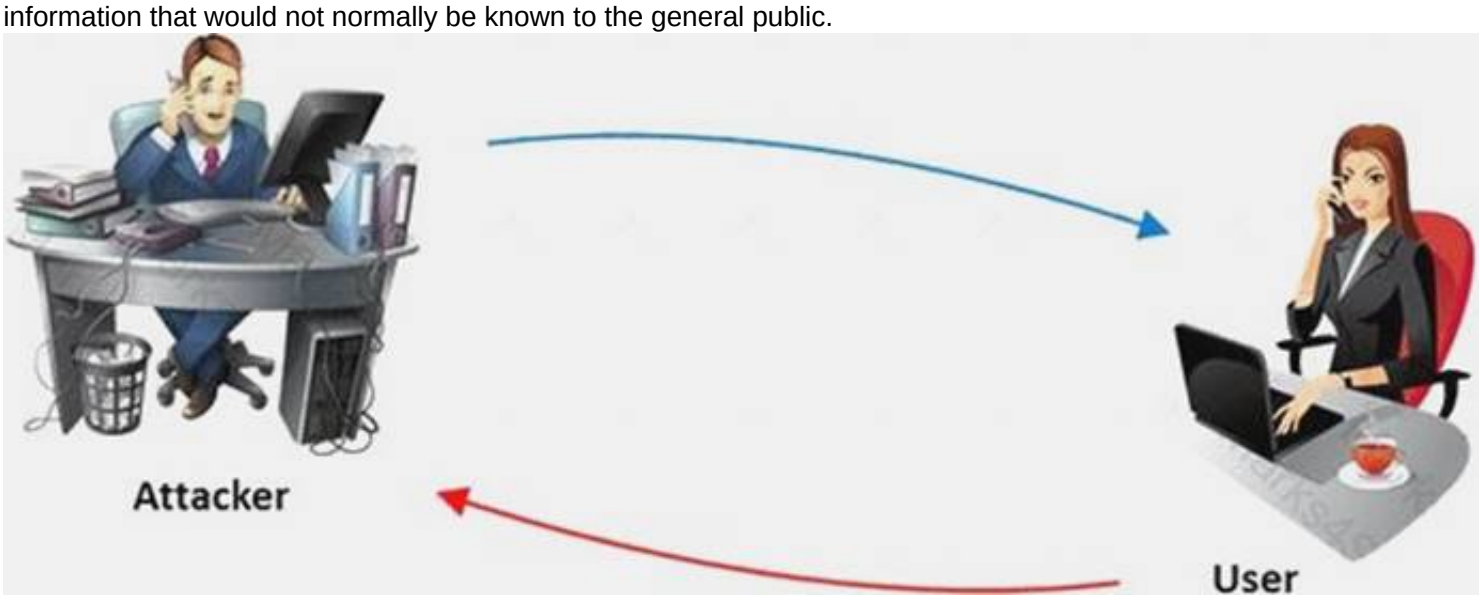
Answer: B

NEW QUESTION 94
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

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

Answer: B

NEW QUESTION 99
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 104
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 107
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 111
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 115
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

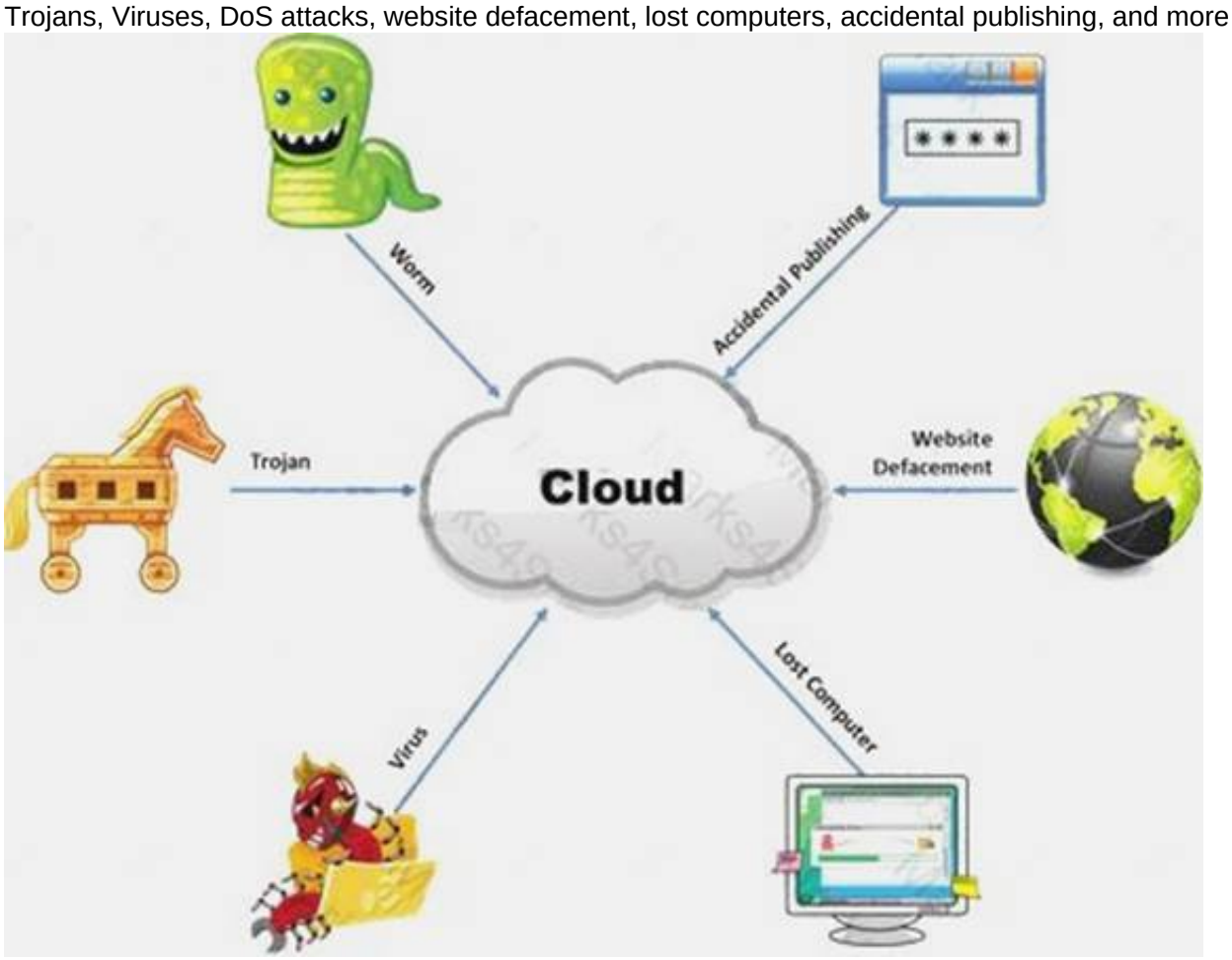
NEW QUESTION 120
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com 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 121
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.

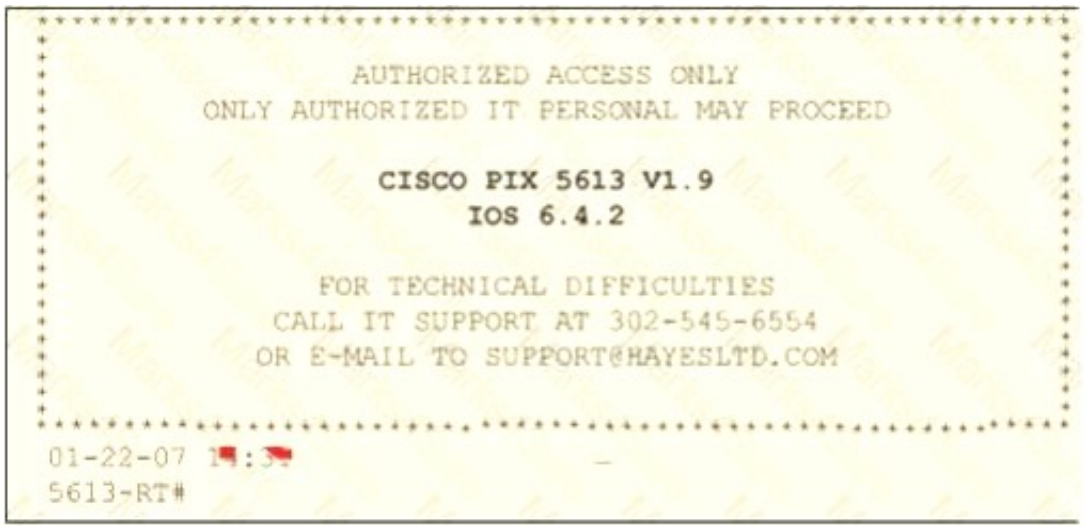


What is the biggest source of data leaks in organizations today?

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 122
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 124
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 125
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 126
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 129
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 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 139
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 141
Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal
B. Success Factors
C. Objectives
D. Assumptions

Answer: D

NEW QUESTION 145
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

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

Answer: D

NEW QUESTION 146
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 149
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 154
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 155

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

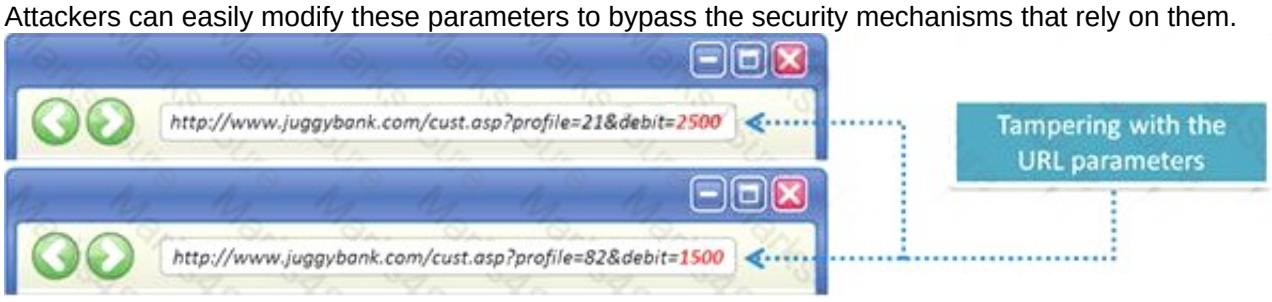
Answer: B

NEW QUESTION 156
You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

A. Analyzing, categorizing and prioritizing resources
B. Evaluating the existing perimeter and internal security
C. Checking for a written security policy
D. Analyzing the use of existing management and control architecture

Answer: C

NEW QUESTION 159
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 163
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 168
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 172
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 176
Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businesService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack
B. Service Level Configuration Attacks
C. URL Tampering Attacks
D. Inside Attacks

Answer: A

NEW QUESTION 179
If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

A. Parameter tampering Attack
B. Sql injection attack
C. Session Hijacking
D. Cross-site request attack

Answer: D

NEW QUESTION 181
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 183
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London.
After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

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

Answer: C

NEW QUESTION 184
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 189
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 191
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

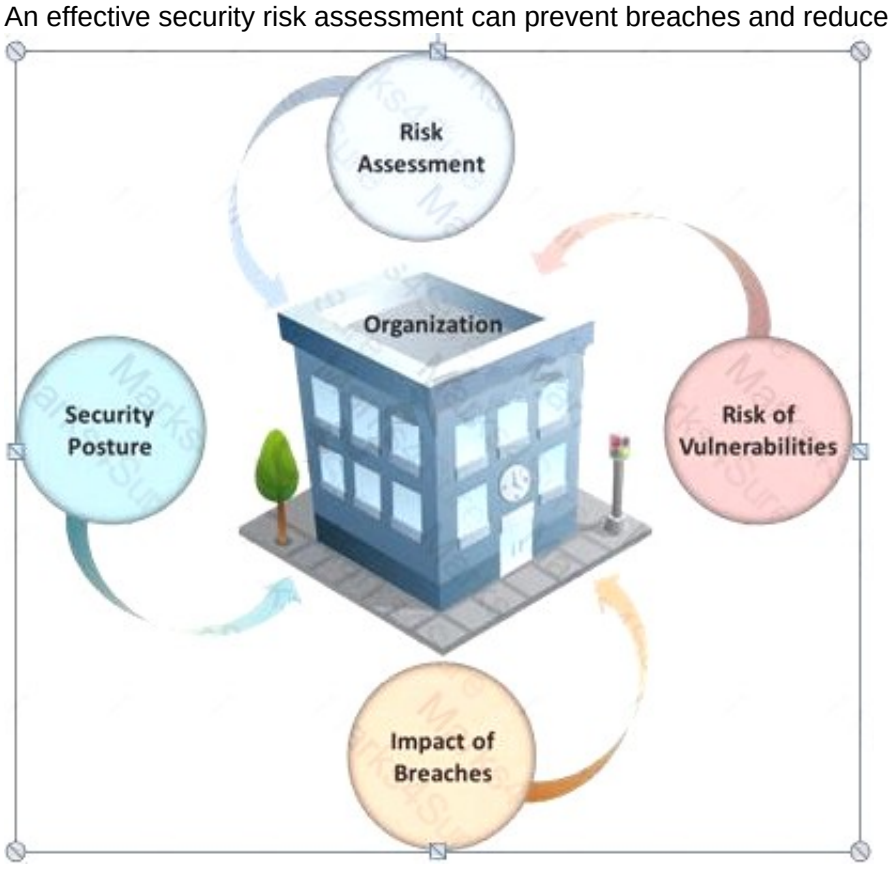
Answer: D

NEW QUESTION 196
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Filtered
B. Stealth
C. Closed
D. Open

Answer: D

NEW QUESTION 201
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 205
Identify the injection attack represented in the diagram below:

A. XPath Injection Attack
B. XML Request Attack
C. XML Injection Attack
D. Frame Injection Attack

Answer: C

NEW QUESTION 210
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 211
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"

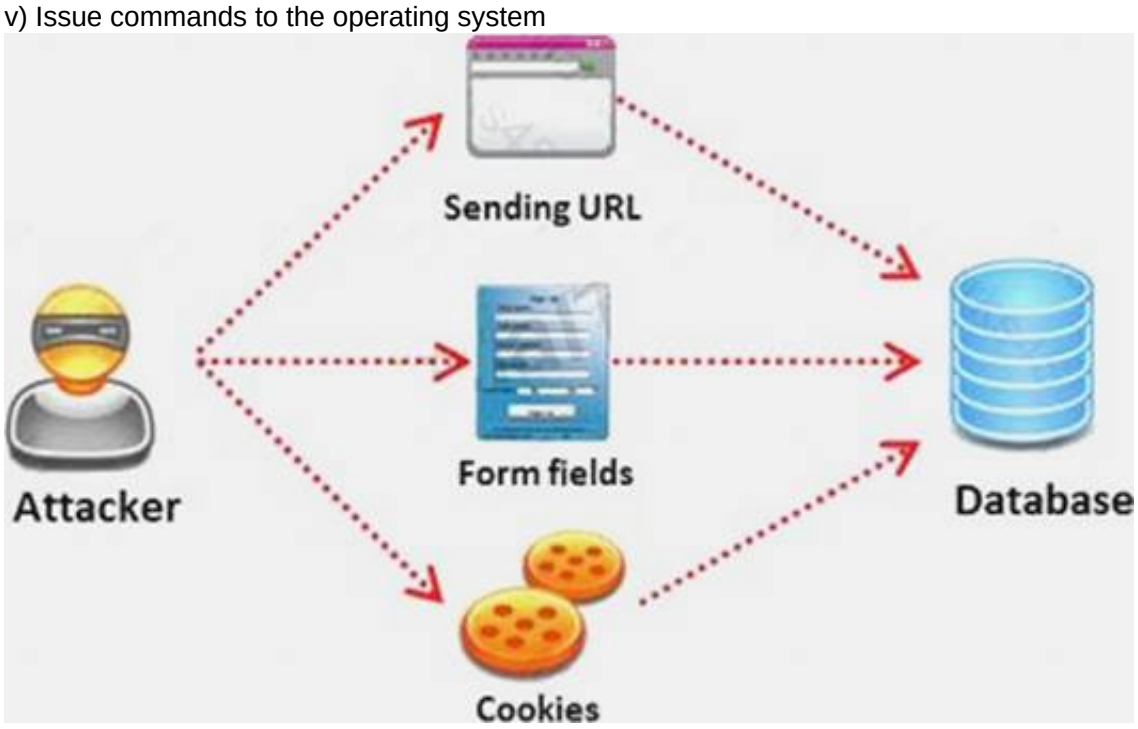
Answer: D

NEW QUESTION 212
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 215
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

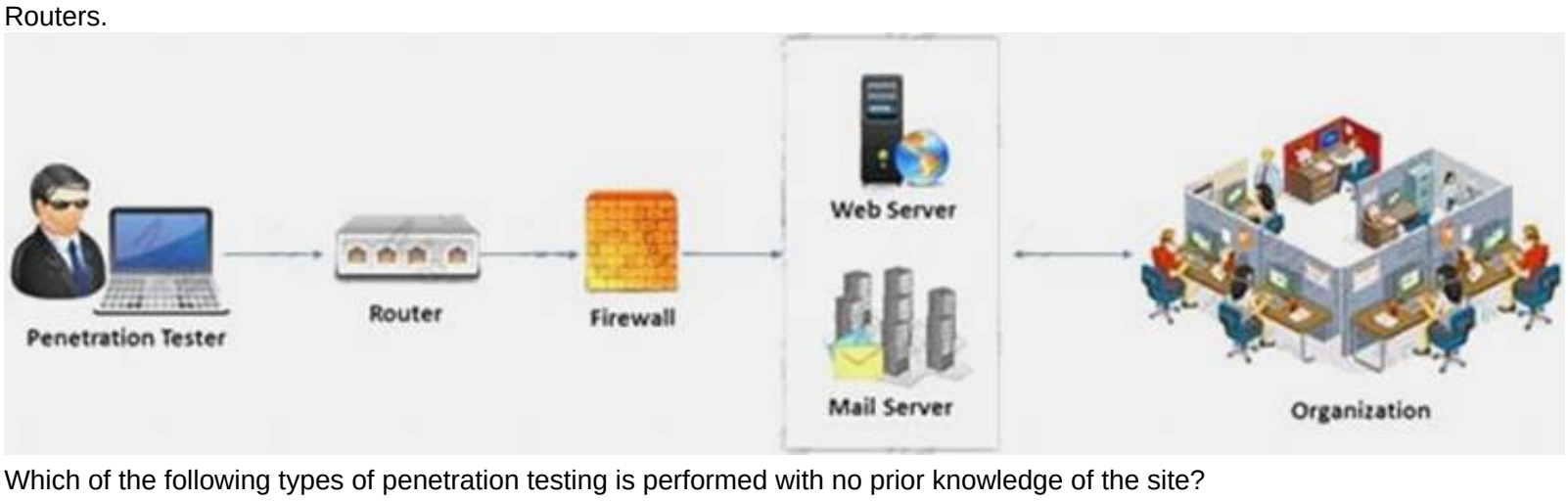


Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate 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 218
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 221
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 223
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 224
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 228
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 233
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 234
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 238
In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc.
They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

A. XPath Injection Attack
B. Authorization Attack
C. Authentication Attack
D. Frame Injection Attack

Answer: B

NEW QUESTION 243
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”

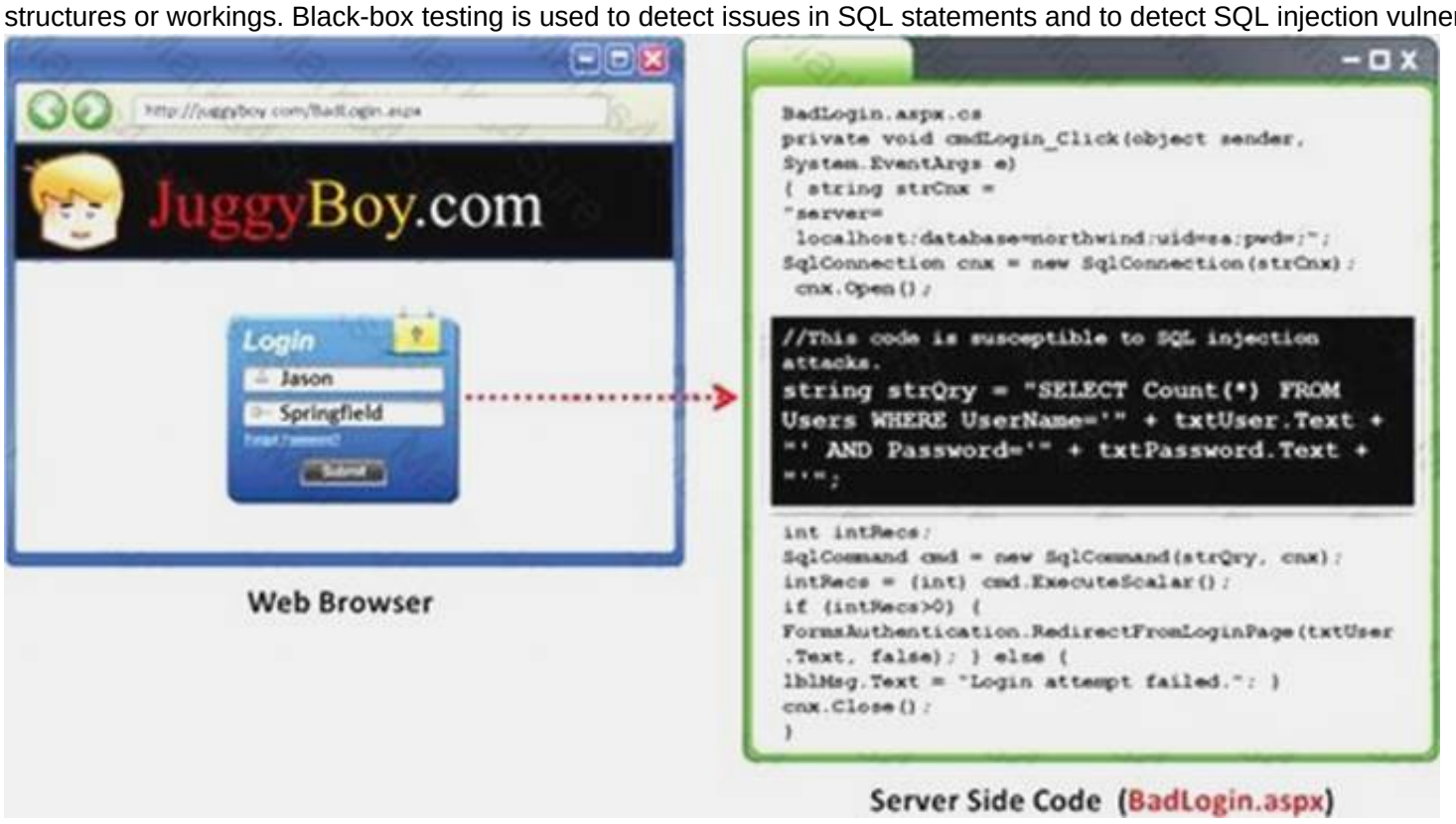
Answer: B

NEW QUESTION 248
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 253
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

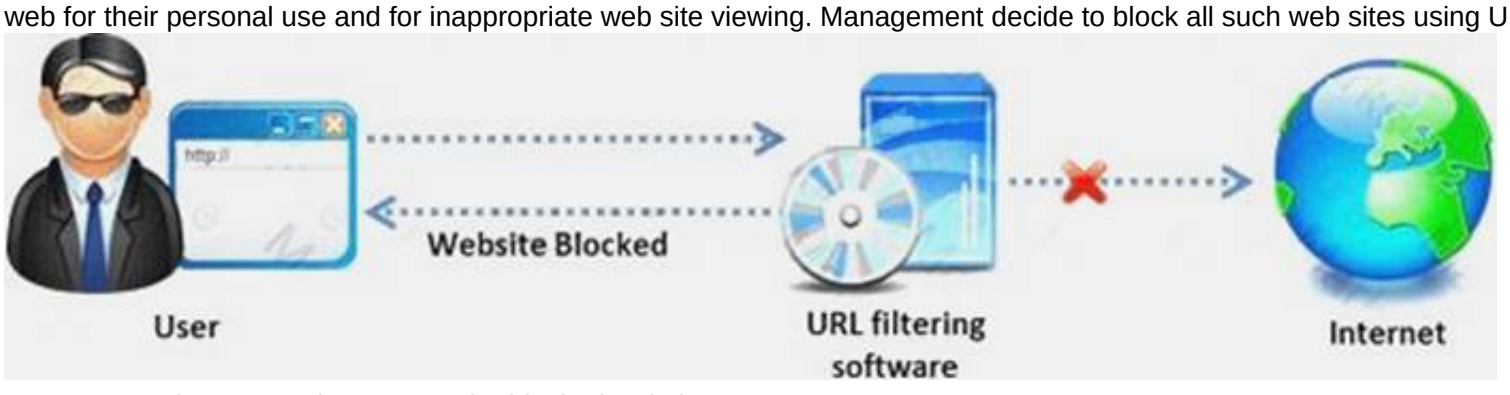
Answer: D

NEW QUESTION 254
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 258
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 259
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 261
Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

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

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

Answer: B

NEW QUESTION 262
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
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 270
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 271
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

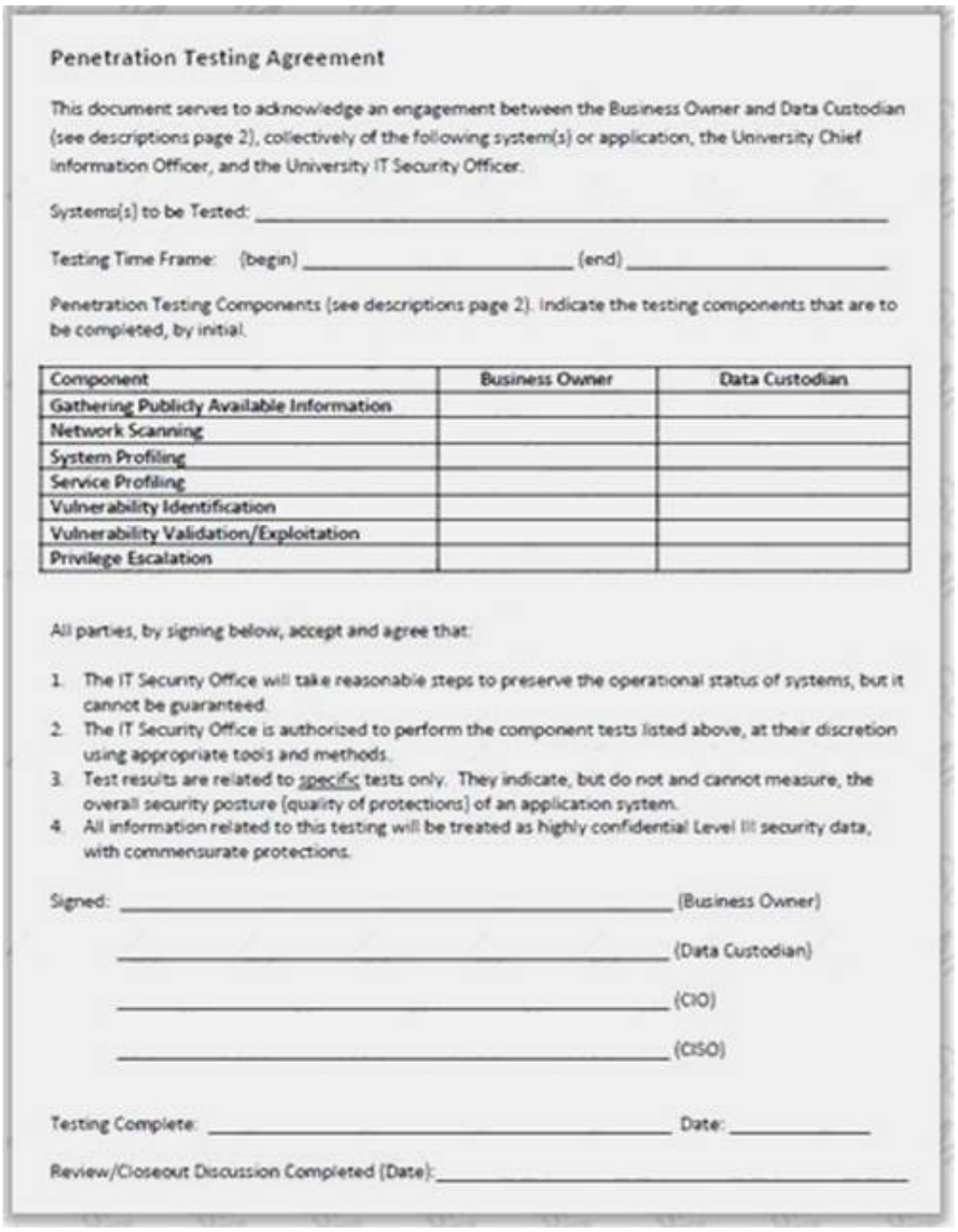
Answer: C

NEW QUESTION 273
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 277
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)

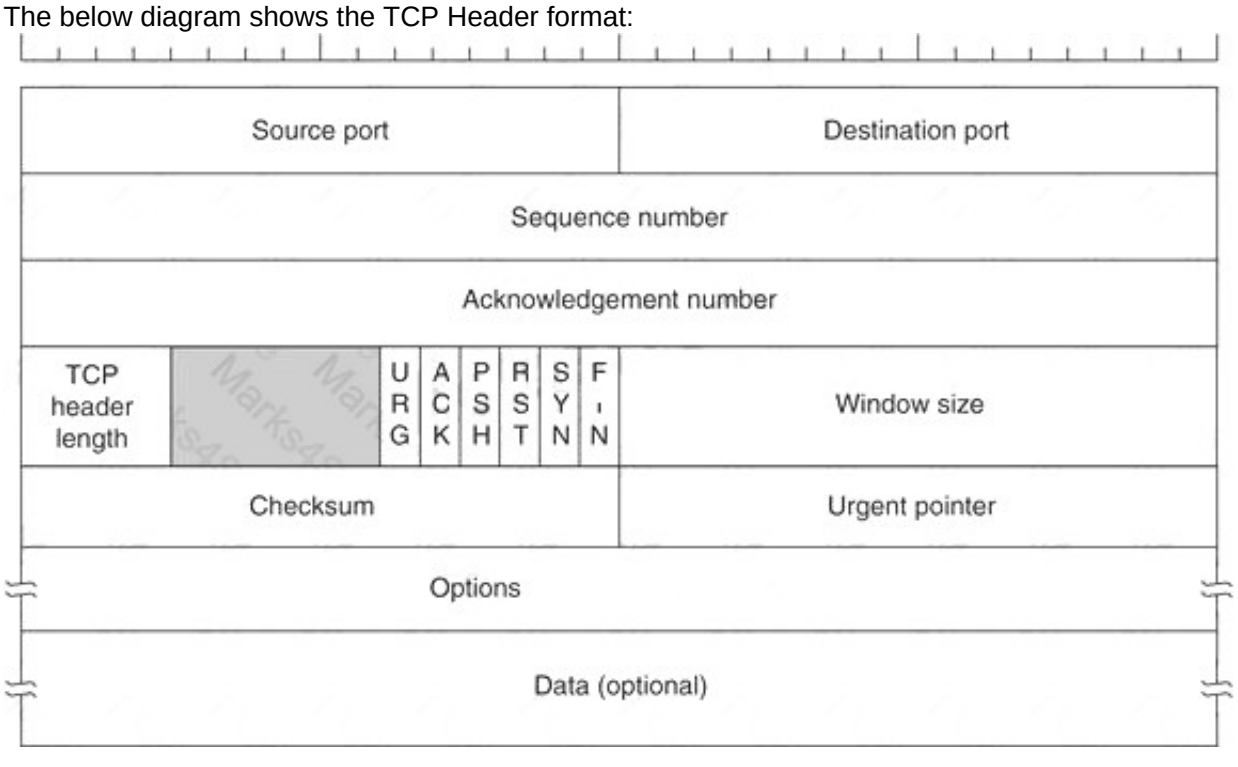
Testing Complete: _____ Date: _____

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 278
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 280
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 282
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 286
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 289
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 291
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 296
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 297
.....

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