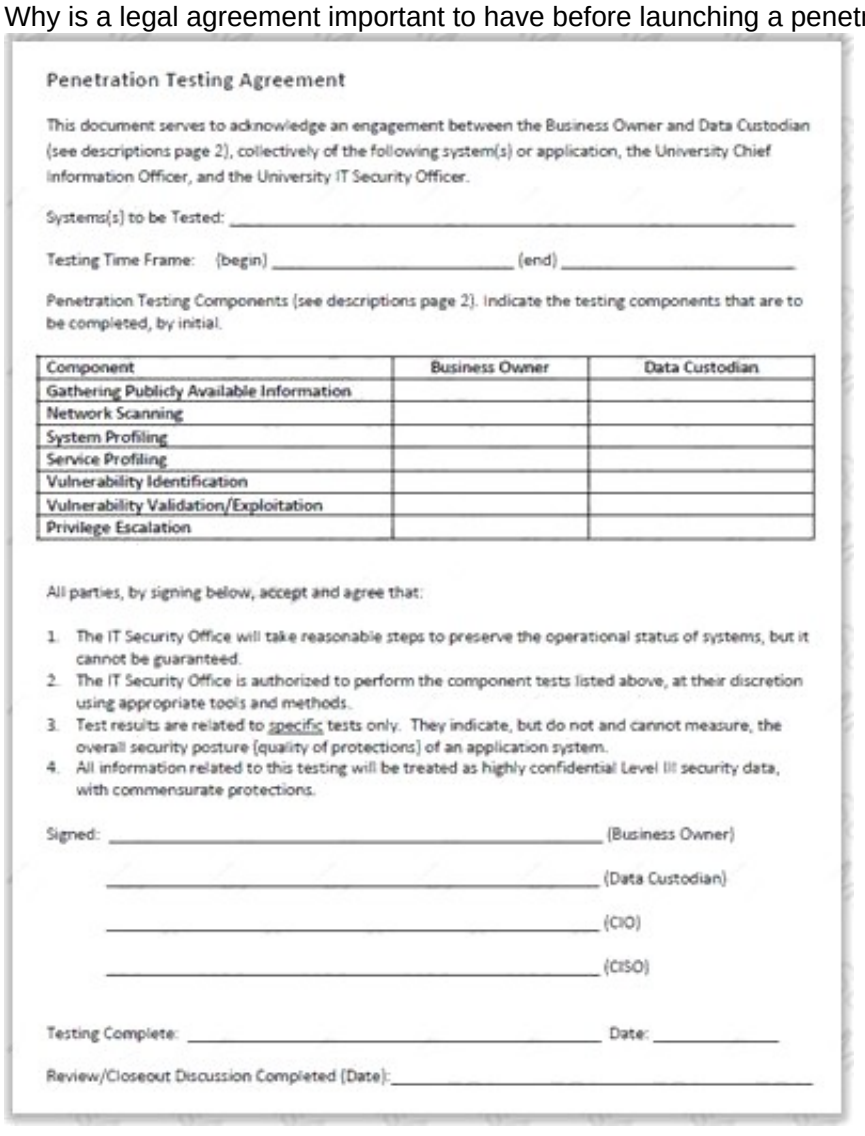
Exam Questions ECSAv10

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

https://www.2passeasy.com/dumps/ECSAv10/

NEW QUESTION 1
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 2
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers
many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

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

Answer: A

NEW QUESTION 3
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 4
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 5
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 6
Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

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

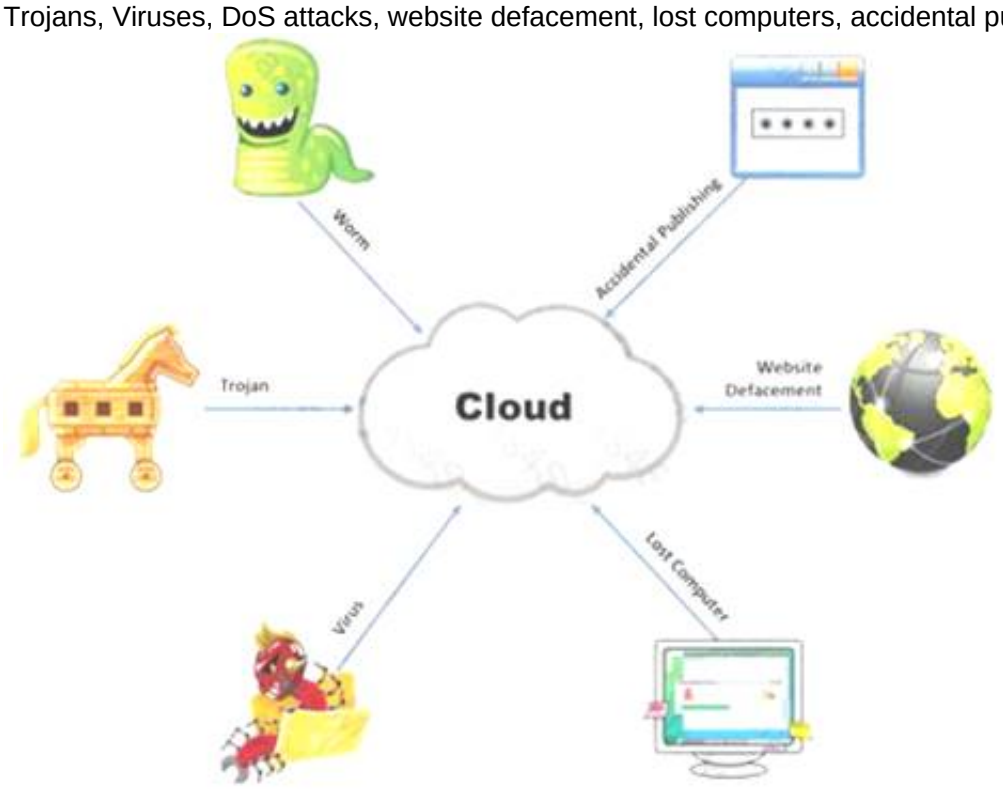
Answer: A

NEW QUESTION 7
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 8
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 9
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 10
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 10
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

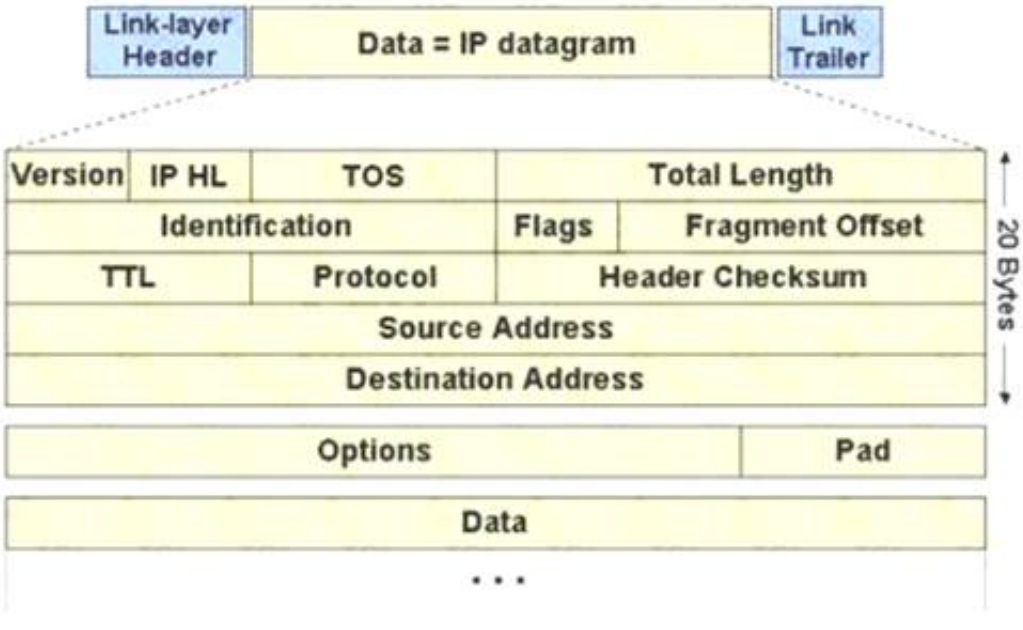
Answer: C

NEW QUESTION 11
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 12
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.

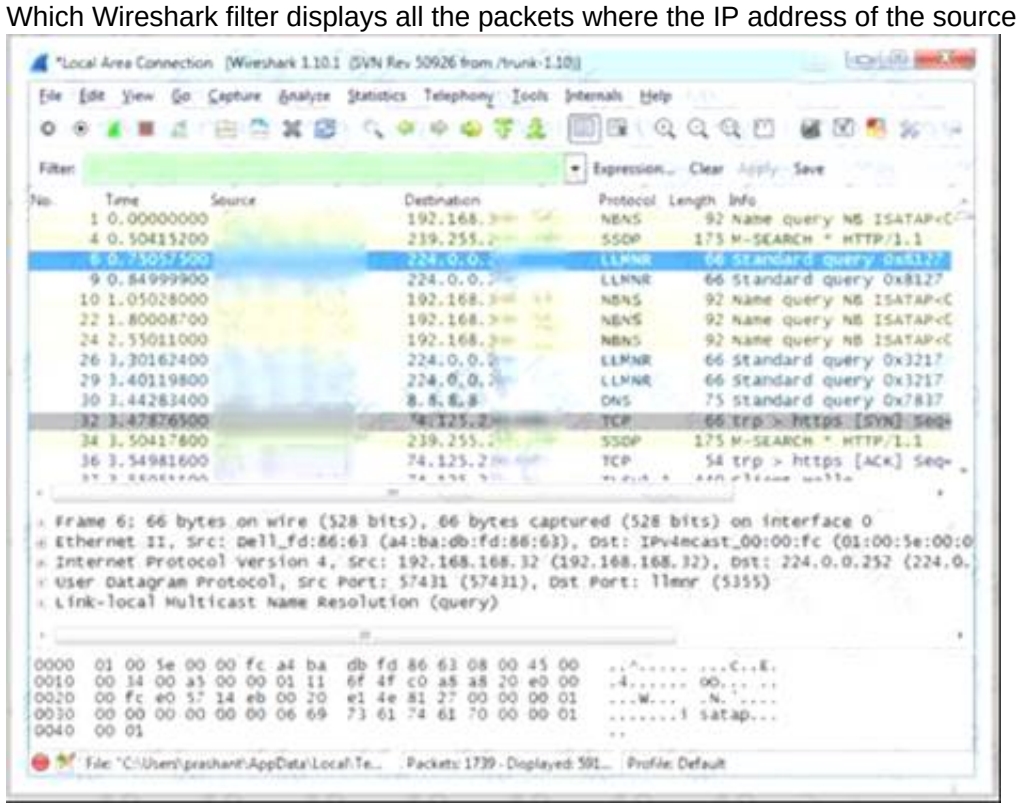


The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

A. Multiple of four bytes
B. Multiple of two bytes
C. Multiple of eight bytes
D. Multiple of six bytes

Answer: C

NEW QUESTION 13
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 15
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 17
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 19
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

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

Answer: C

NEW QUESTION 21
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 26
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 27
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

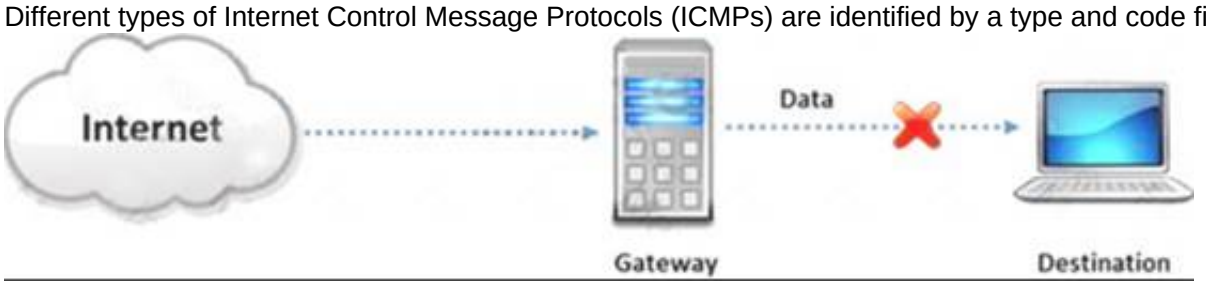
Answer: A

NEW QUESTION 30
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 34
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum.
Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.



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

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

Answer: D

NEW QUESTION 36
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 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
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 48
Identify the correct formula for Return on Investment (ROI).

A. ROI = ((Expected Returns – Cost of Investment) / Cost of Investment) * 100
B. ROI = (Expected Returns + Cost of Investment) / Cost of Investment
C. ROI = (Expected Returns Cost of Investment) / Cost of Investment
D. ROI = ((Expected Returns + Cost of Investment) / Cost of Investment) * 100

Answer: C

NEW QUESTION 53
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 58
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 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

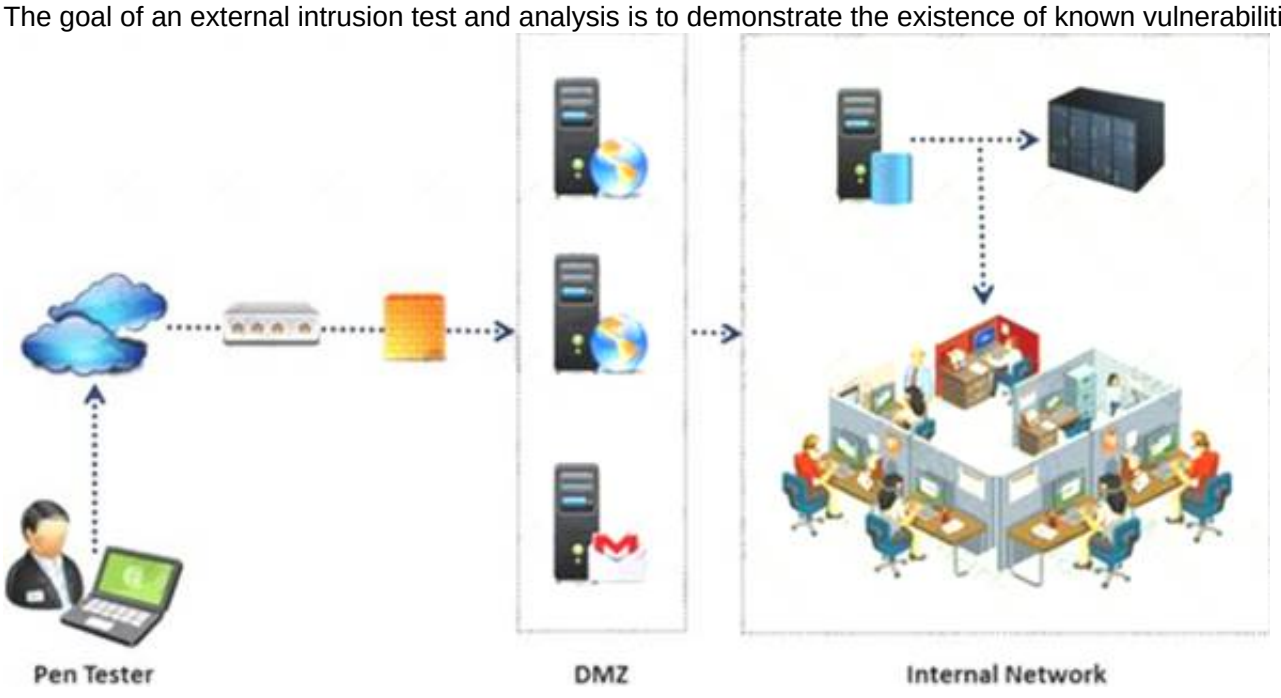
NEW QUESTION 62
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

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 63
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 68
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 72
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 73
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 75
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 78
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 82
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 83
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 85
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 90
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 92
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 93
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 96
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 101
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 104
Which of the following methods is used to perform server discovery?

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

Answer: B

NEW QUESTION 106
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 110
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 112
What does ICMP Type 3/Code 13 mean?

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

Answer: D

NEW QUESTION 116
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

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

Answer: D

NEW QUESTION 119
Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies.
A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces.
What could have prevented this information from being stolen from the laptops?

A. SDW Encryption
B. EFS Encryption
C. DFS Encryption
D. IPS Encryption

Answer: B

NEW QUESTION 121
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 124
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

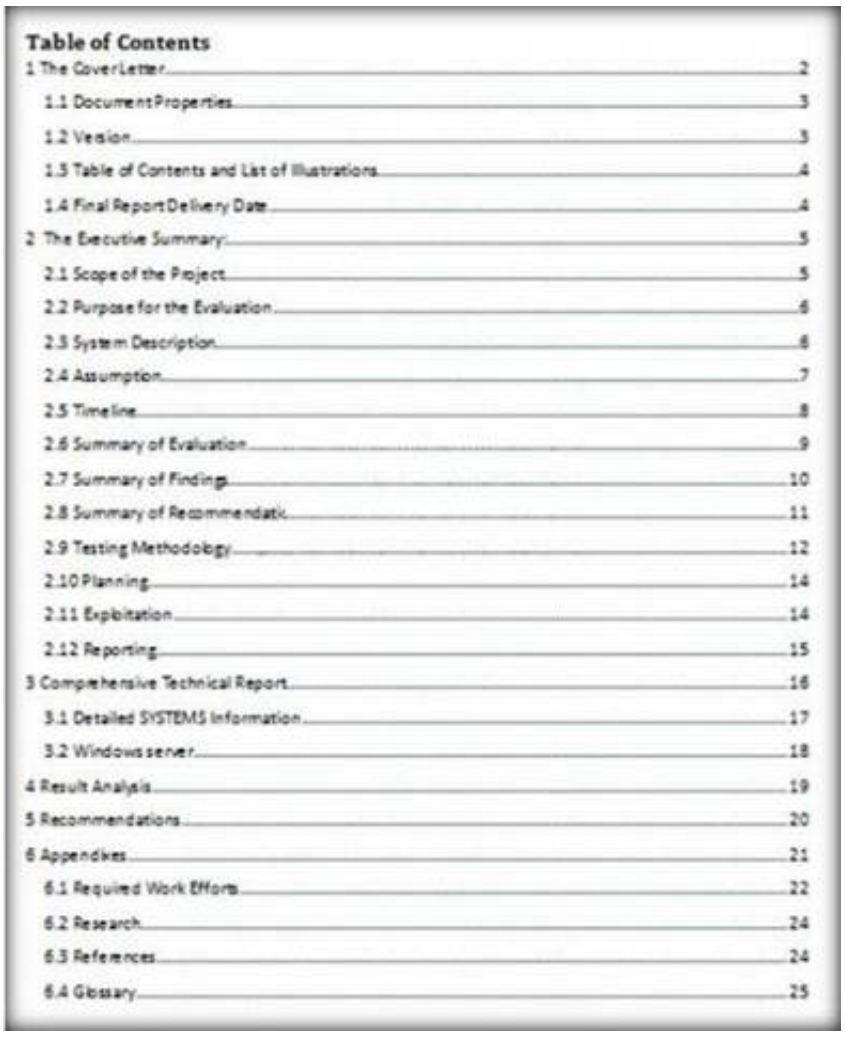


Table of Contents
1 The Cover Letter 2
1.1 Document Properties 3
1.2 Version 3
1.3 Table of Contents and List of Illustrations 4
1.4 Final Report Delivery Date 4
2 The Executive Summary: 5
2.1 Scope of the Project 5
2.2 Purpose for the Evaluation 6
2.3 System Description 6
2.4 Assumption 7
2.5 Timeline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

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

Answer: A

NEW QUESTION 129
As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

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

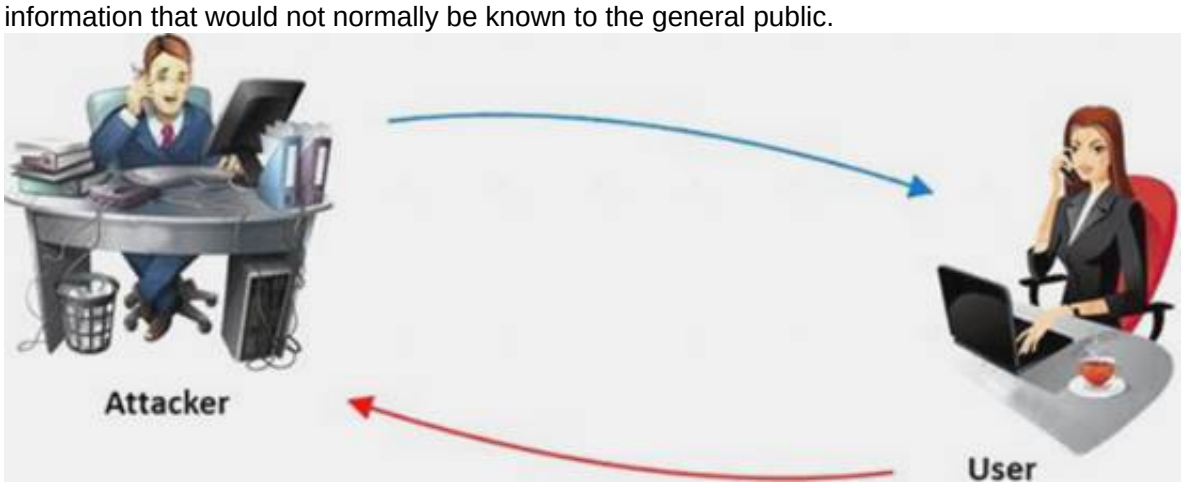
Answer: C

NEW QUESTION 134
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. URL Obfuscation Arbitrary Administrative Access Vulnerability
B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
C. HTTP Configuration Arbitrary Administrative Access Vulnerability
D. HTML Configuration Arbitrary Administrative Access Vulnerability

Answer: C

NEW QUESTION 135
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 136
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”

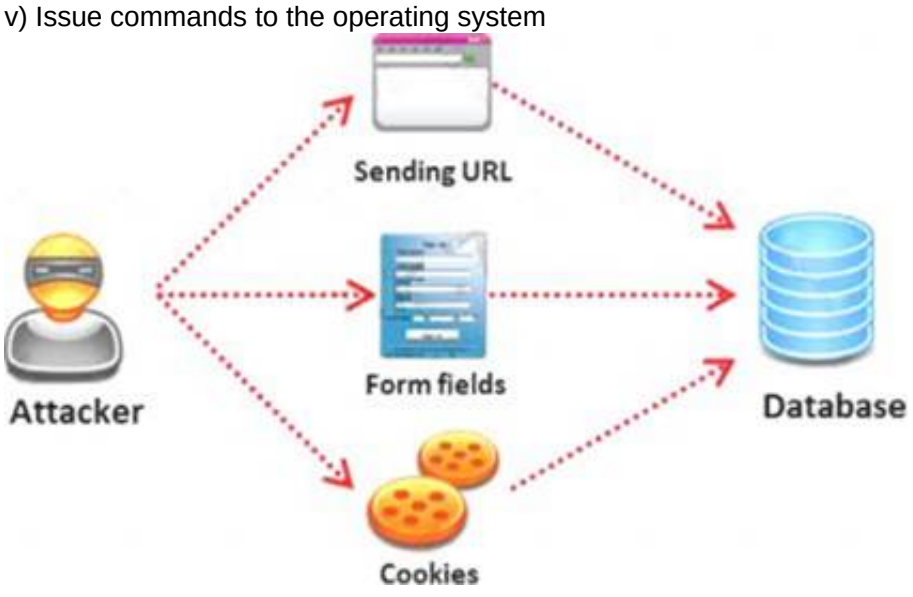
Answer: A

NEW QUESTION 140
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 145
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 148
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 151
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 153
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 155
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 159
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 161
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 164
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

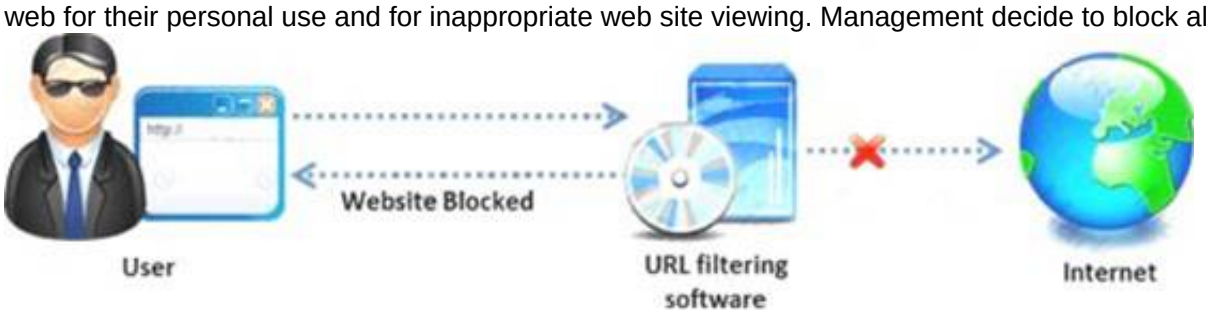
NEW QUESTION 168
Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers.
Which one of the following cannot handle routing protocols 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 171
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.

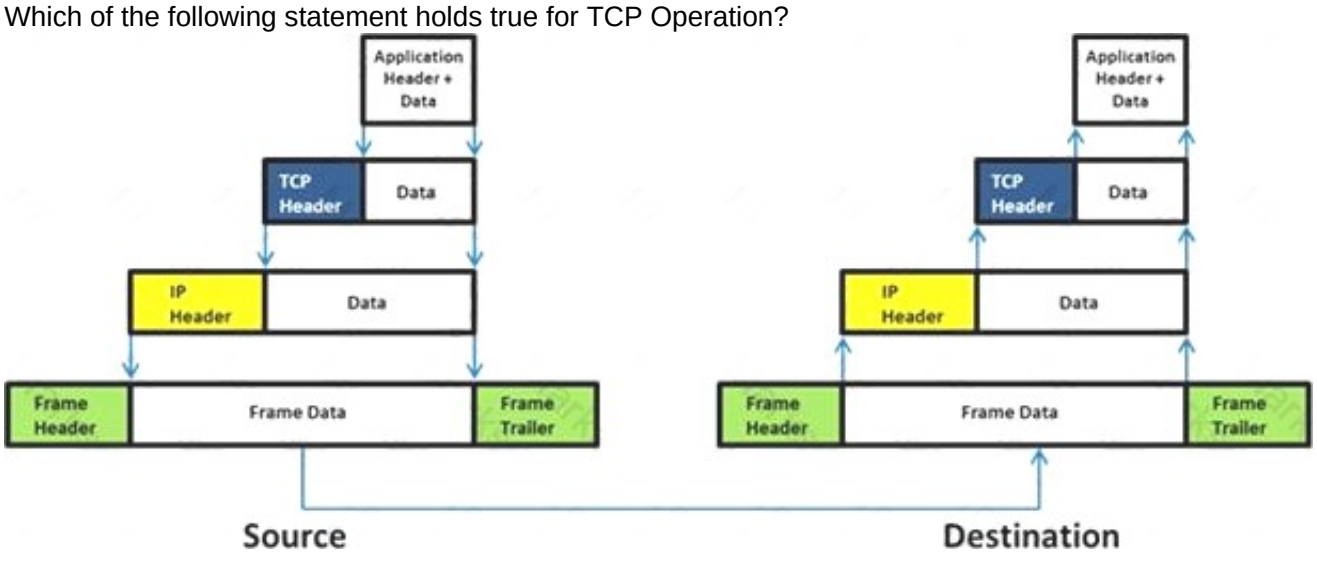


How can employees continue to see the blocked websites?

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

Answer: B

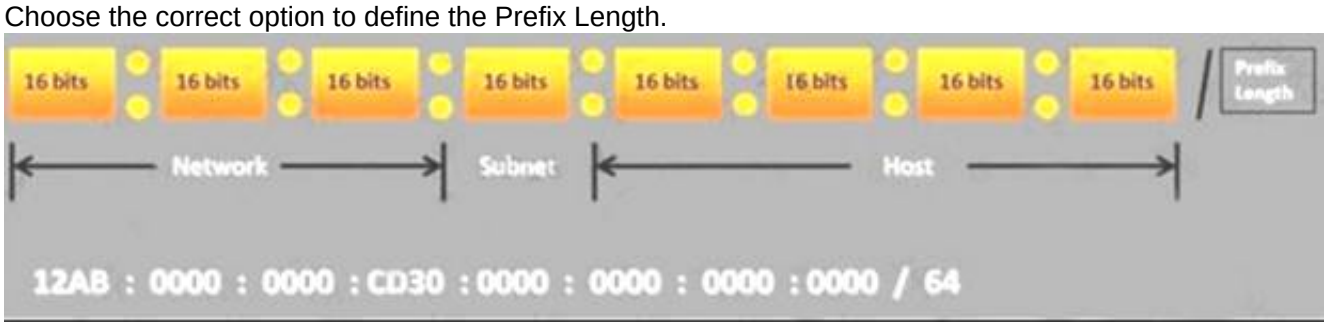
NEW QUESTION 172
Which of the following statement holds true for TCP Operation?



A. Port numbers are used to know which application the receiving host should pass the data to
B. Sequence numbers are used to track the number of packets lost in transmission
C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host
D. Data transfer begins even before the connection is established

Answer: D

NEW QUESTION 176
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 177
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

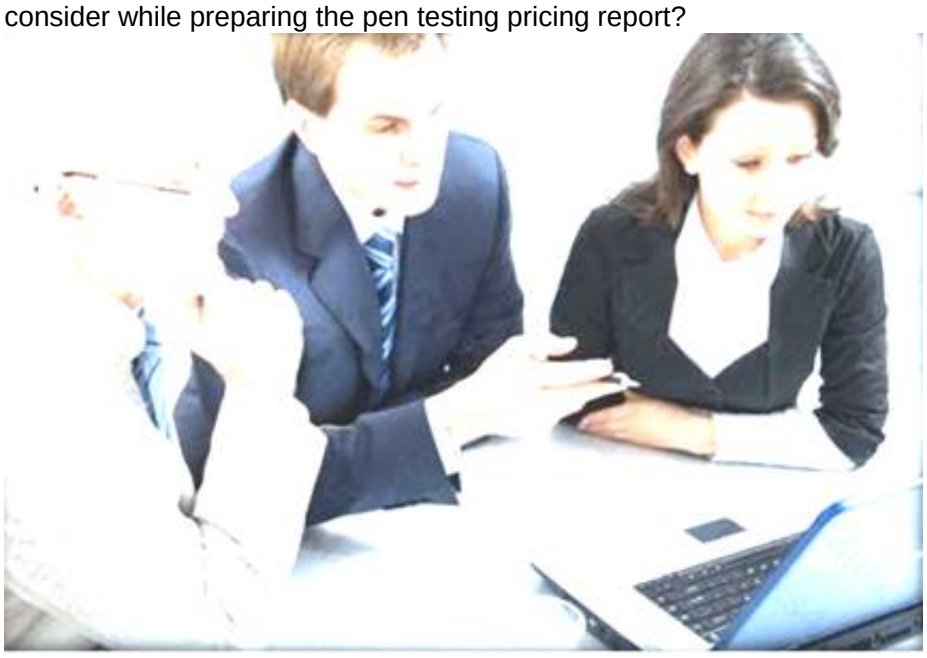
Answer: C

NEW QUESTION 182
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 186
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 191
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 193
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

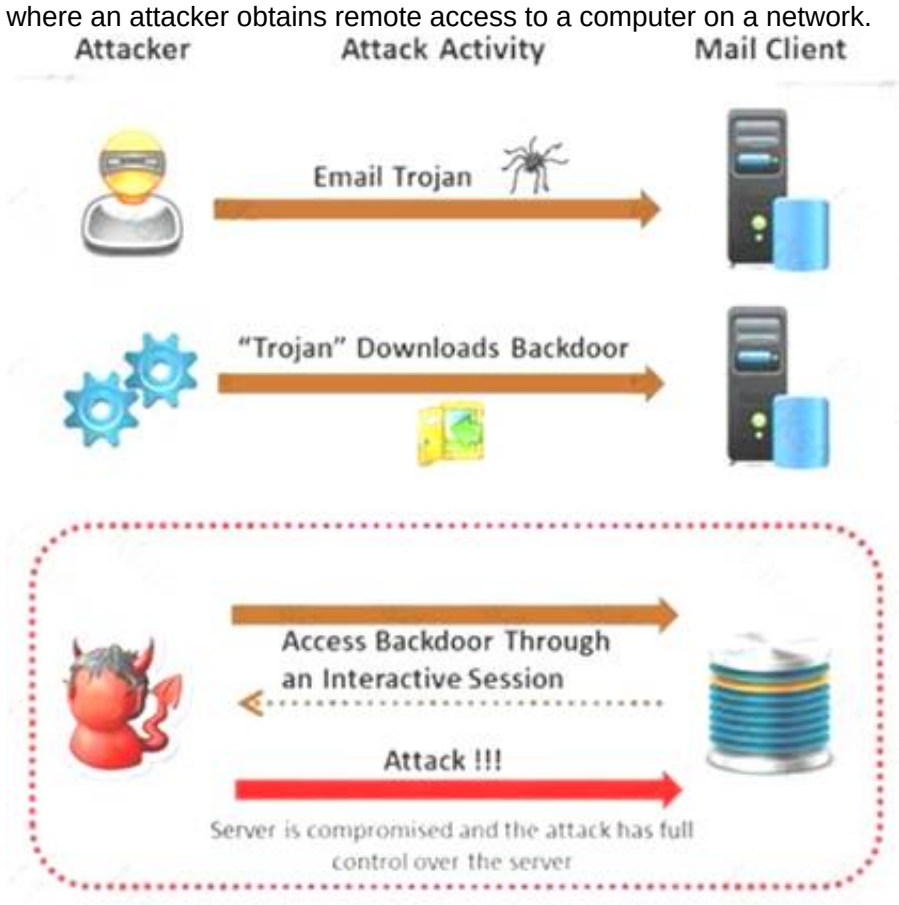
NEW QUESTION 196
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc.
Usually, this information is stored in cookies, hidden 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 199
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.



Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Answer: D

NEW QUESTION 204
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 209
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 213
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 218
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

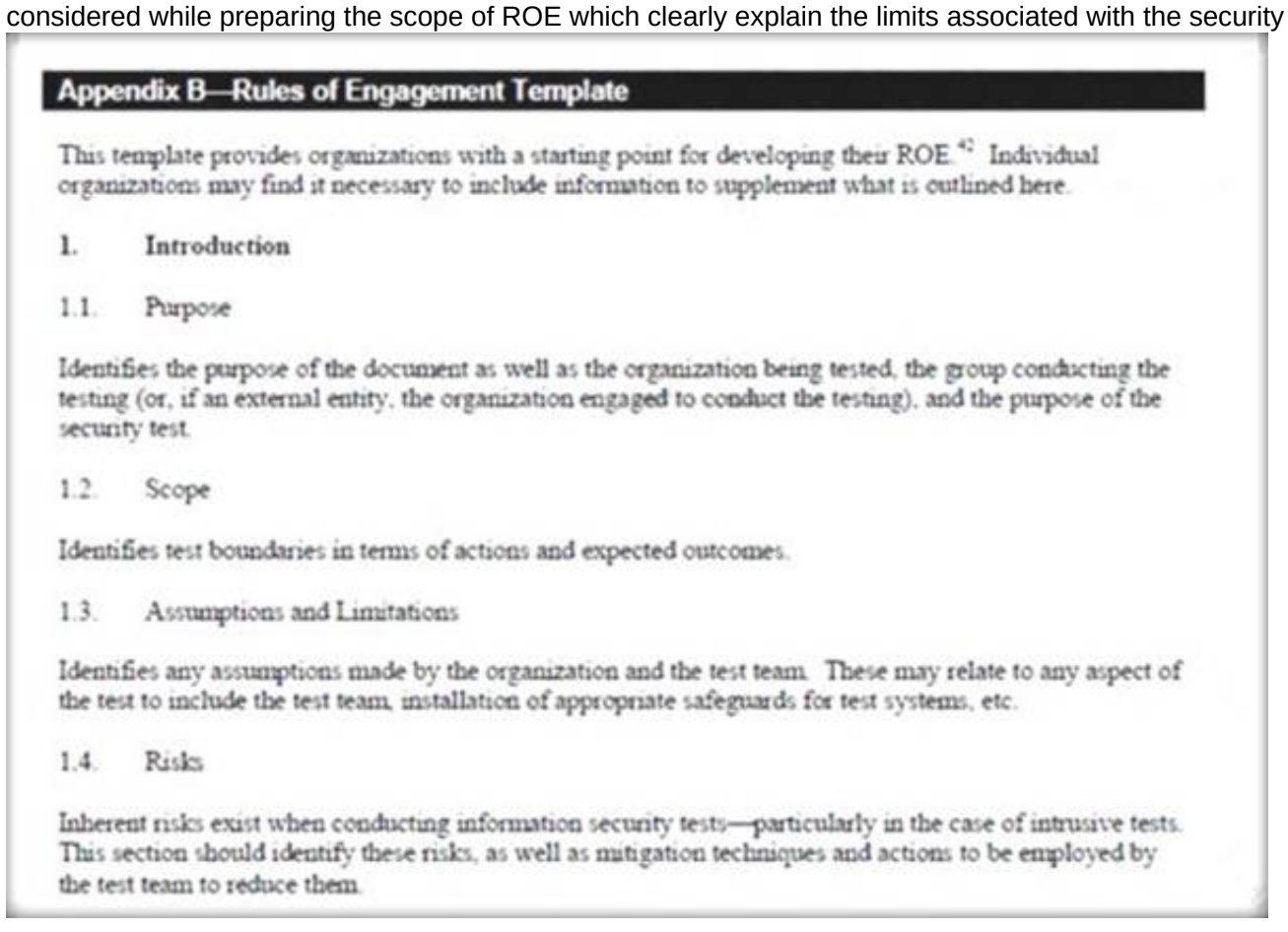
NEW QUESTION 221
External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, 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 222
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.

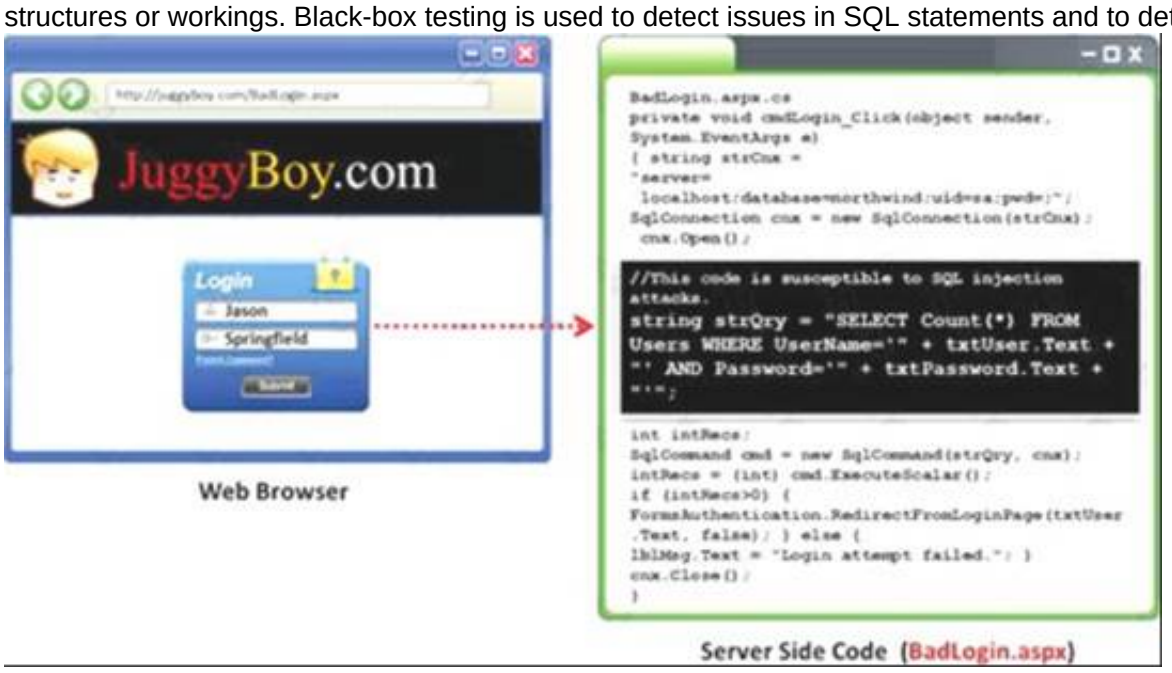
Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

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 223

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 227
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 231
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

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

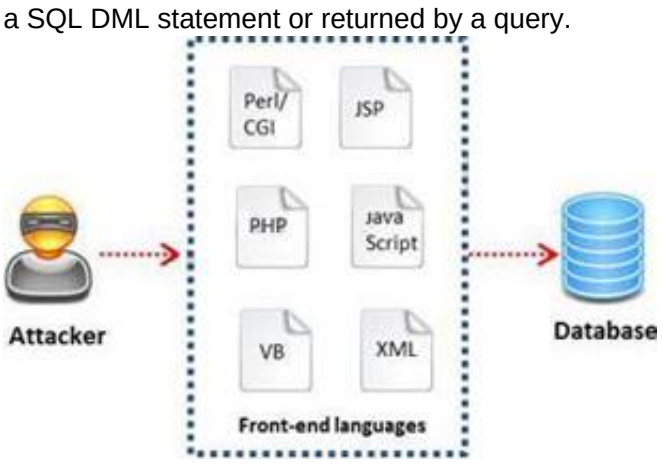
Answer: C

NEW QUESTION 236
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 239
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.



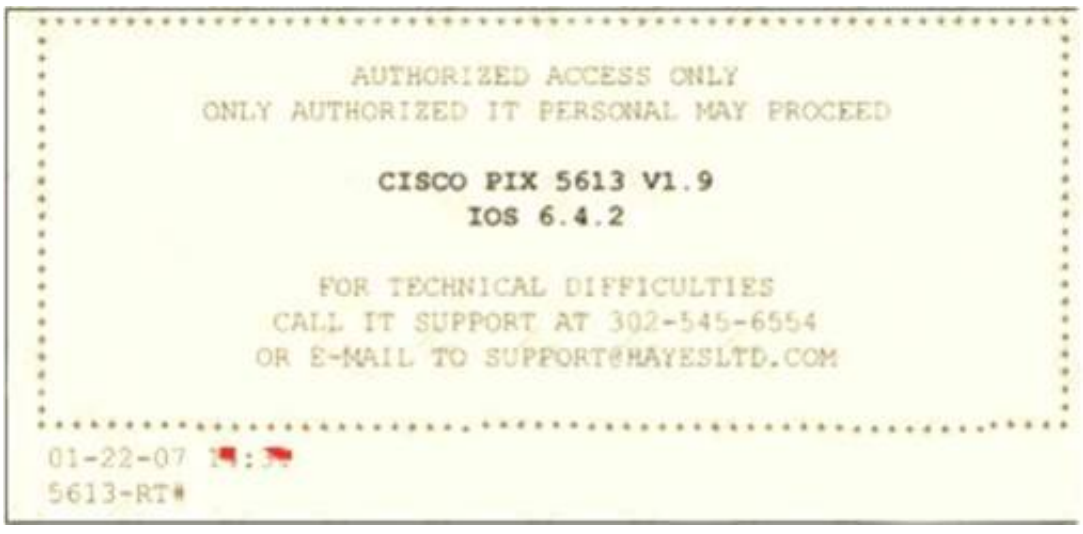
A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?

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 241
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

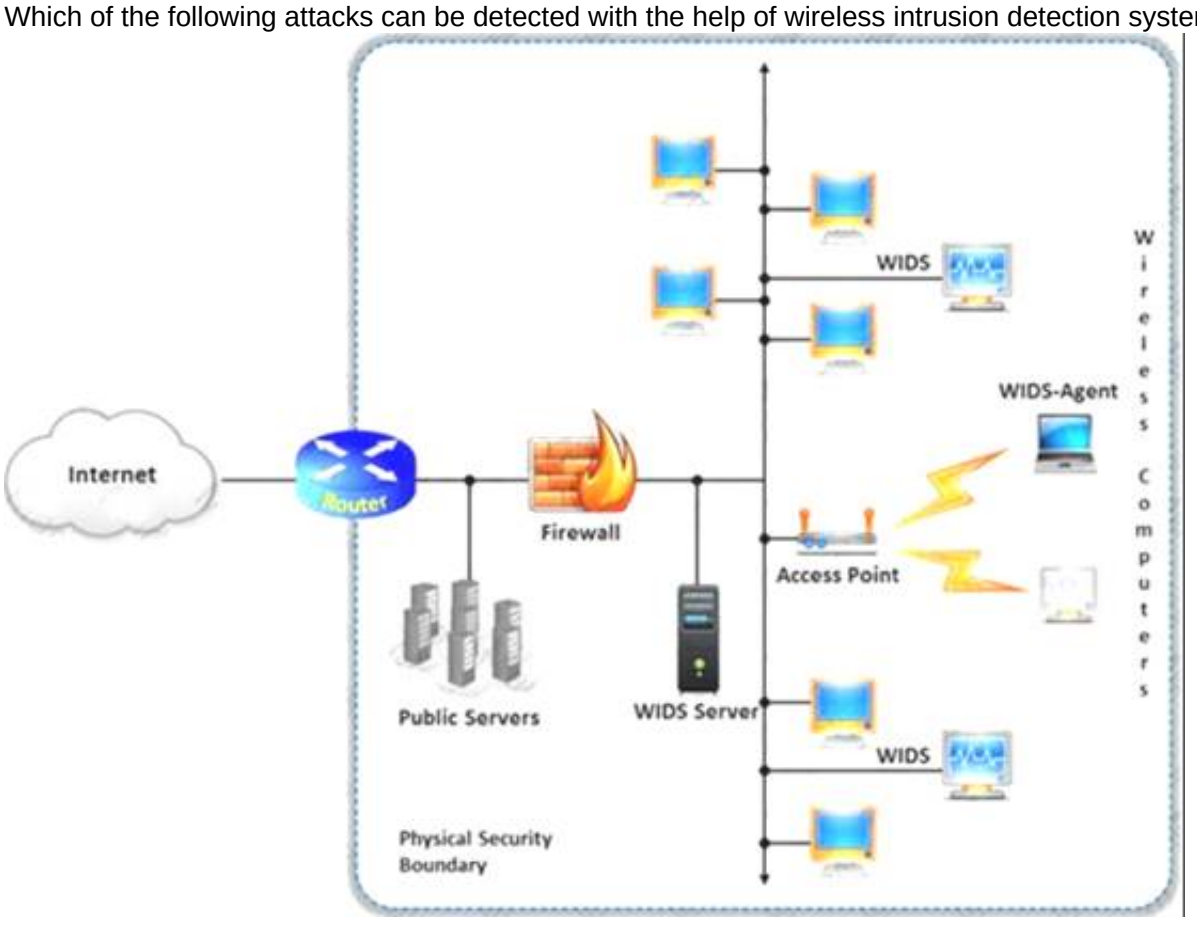
Answer: B

NEW QUESTION 245
Which of the following shields Internet users from artificial DNS data, such as a deceptive or mischievous address instead of the genuine address that was requested?

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

Answer: A

NEW QUESTION 248
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 250

HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

A. ASCII value of the character
B. Binary value of the character
C. Decimal value of the character
D. Hex value of the character

Answer: D

NEW QUESTION 255
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 257
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 262
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 263
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 265
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual ECSAv10 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the ECSAv10 Product From:

https://www.2passeasy.com/dumps/ECSAv10/

Money Back Guarantee

ECSAv10 Practice Exam Features:

* ECSAv10 Questions and Answers Updated Frequently

* ECSAv10 Practice Questions Verified by Expert Senior Certified Staff

* ECSAv10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* ECSAv10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year