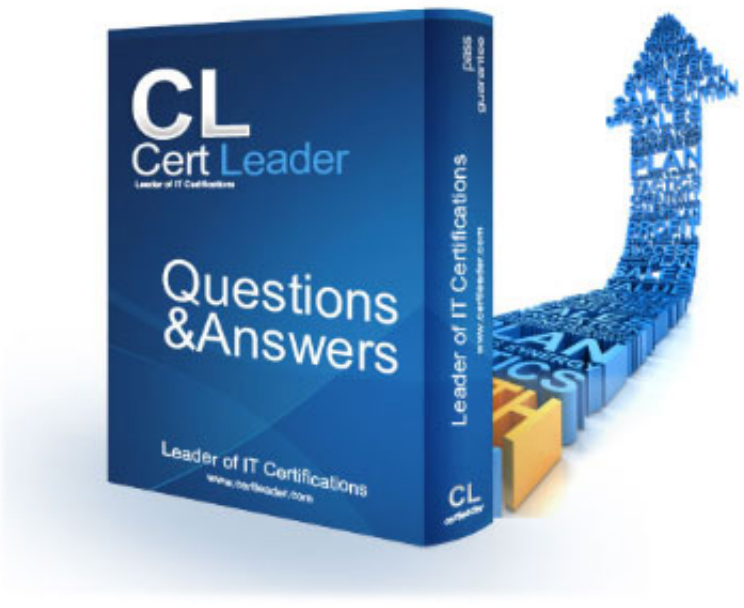
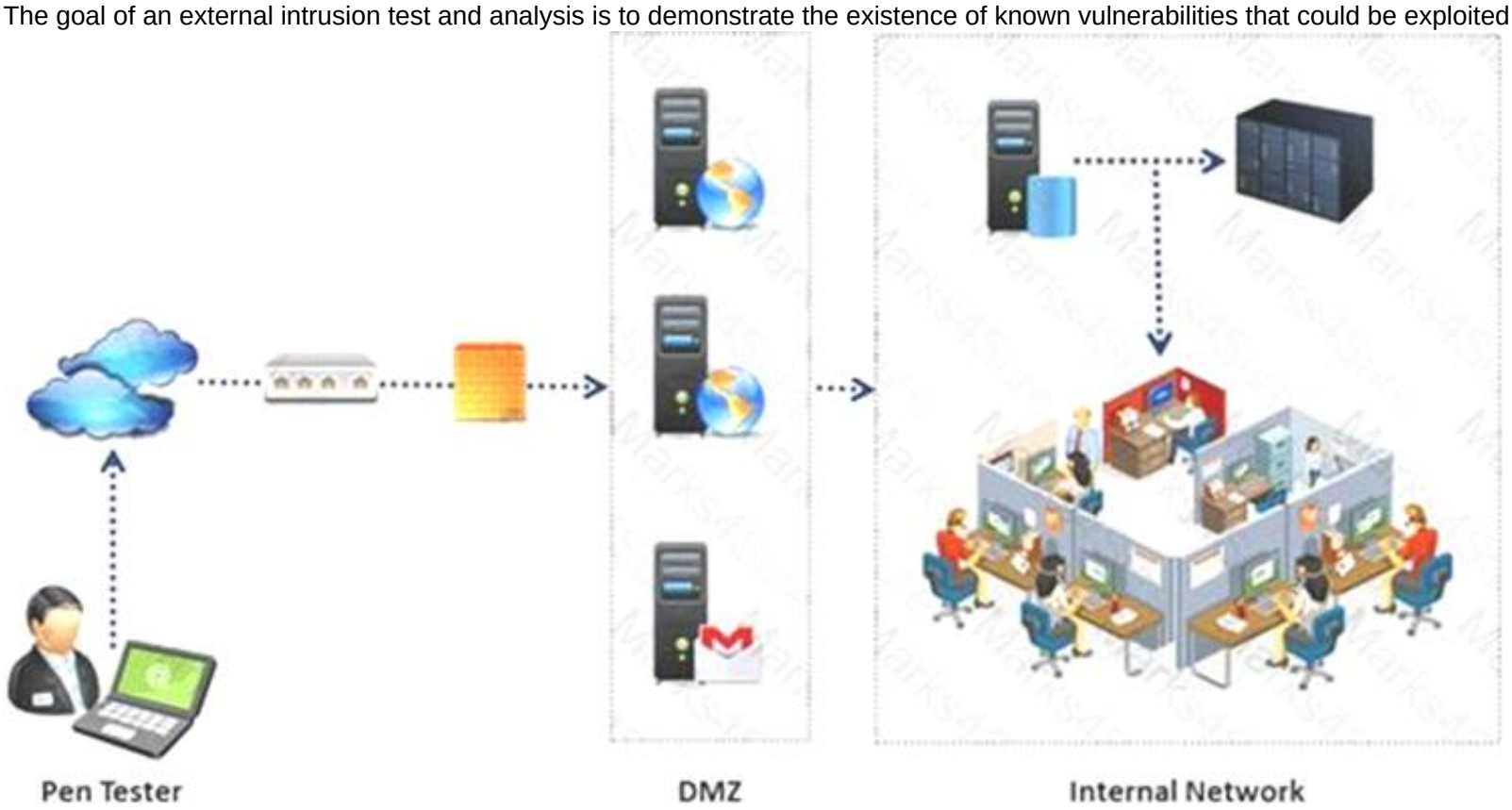
412-79v10 Dumps

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
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram.
Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field.
If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes
B. Type 12 ICMP codes
C. Type 3 ICMP codes
D. Type 7 ICMP codes

Answer: C

NEW QUESTION 3
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
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers
many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

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

Answer: A

NEW QUESTION 5
To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

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

Answer: C

NEW QUESTION 6
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

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D. Show outdated equipment so it can be replaced

Answer: C

NEW QUESTION 7
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 8
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 9
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG. What is Simon trying to accomplish here?

A. Enumerate all the users in the domain
B. Perform DNS poisoning
C. Send DOS commands to crash the DNS servers
D. Perform a zone transfer

Answer: D

NEW QUESTION 10
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
include <stdio.h>
#include <string.h>
int main(int argc, char *argv[])
{
char buffer[10]; if (argc < 2)
{
fprintf(stderr, "USAGE: %s string\n", argv[0]); return 1;
}
strcpy(buffer, argv[1]); return 0;
}
```

A. Buffer overflow
B. Format string bug
C. Kernal injection
D. SQL injection

Answer: A

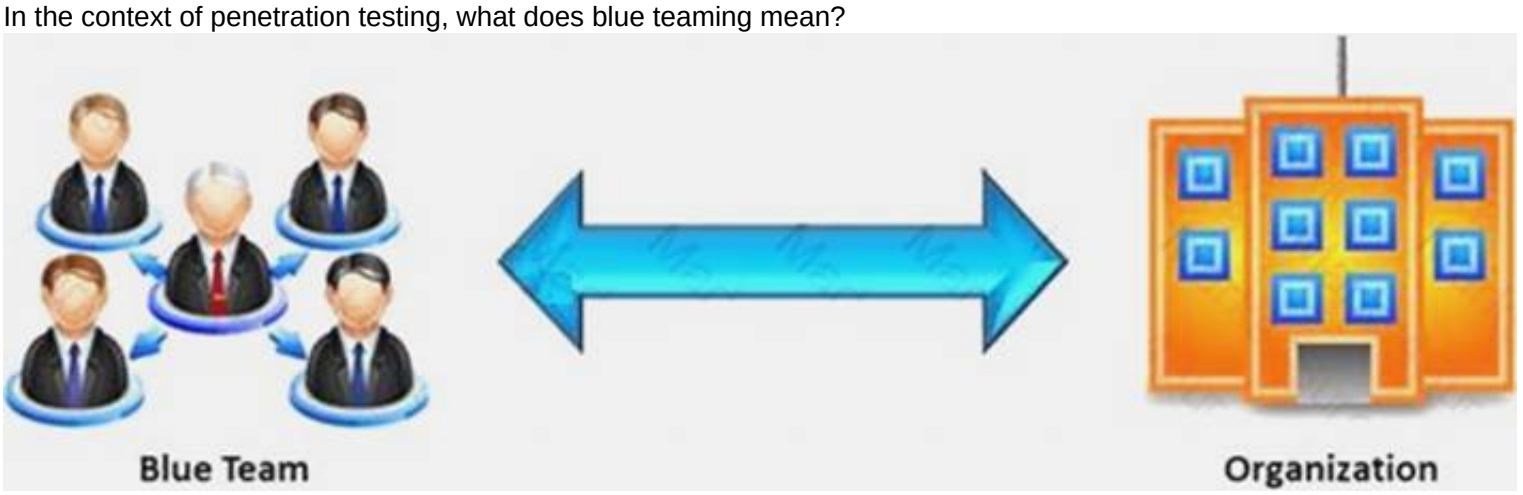
NEW QUESTION 10
A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card.
Which one of the following is well supported in most wireless applications?

A. Orinoco chipsets
B. Prism II chipsets

C. Atheros Chipset
D. Cisco chipset

Answer: B

NEW QUESTION 14
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 17
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 18
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Poison the switch's MAC address table by flooding it with ACK bits
B. Enable tunneling feature on the switch
C. Trick the switch into thinking it already has a session with Terri's computer
D. Crash the switch with a DoS attack since switches cannot send ACK bits

Answer: C

NEW QUESTION 21
DNS information records provide important data about:

A. Phone and Fax Numbers
B. Location and Type of Servers
C. Agents Providing Service to Company Staff
D. New Customer

Answer: B

NEW QUESTION 23
Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy
B. User Identification and Password Policy
C. Personal Computer Acceptable Use Policy
D. User-Account Policy

Answer: B

NEW QUESTION 25
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 30
Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)
B. HTTP (Hypertext Transfer Protocol)
C. SMTP (Simple Mail Transfer Protocol)
D. Telnet

Answer: A

NEW QUESTION 33
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100
B. 5000-5099
C. 6666-6674
D. 0 – 1023

Answer: D

NEW QUESTION 34
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 38
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 42
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 44
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

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and Zombies? What type of Penetration Testing is Larry planning to carry out?

A. Internal Penetration Testing
B. Firewall Penetration Testing
C. DoS Penetration Testing
D. Router Penetration Testing

Answer: C

NEW QUESTION 51
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 54
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 55
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 56
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 59
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 63
Software firewalls work at which layer of the OSI model?

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

Answer: A

NEW QUESTION 65

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 66
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 67
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 69
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 72
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 73
Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

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

Answer: A

NEW QUESTION 75
Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

A. Hash Key Length
B. C/R Value Length
C. C/R Key Length
D. Hash Value Length

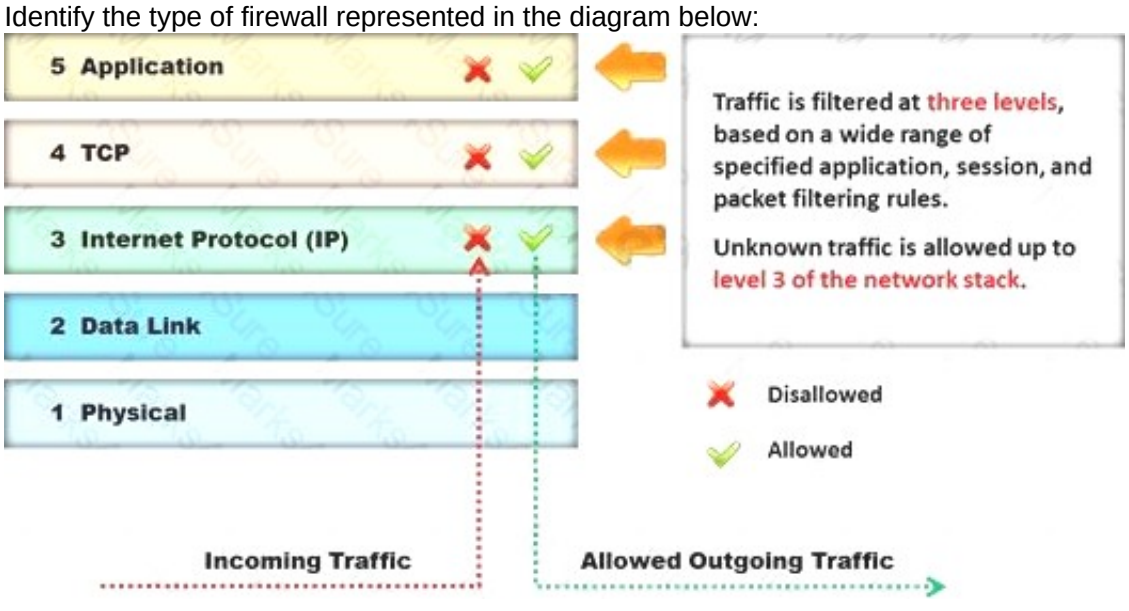
Answer: B

NEW QUESTION 76
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 80
Identify the type of firewall represented in the diagram below:



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

Answer: A

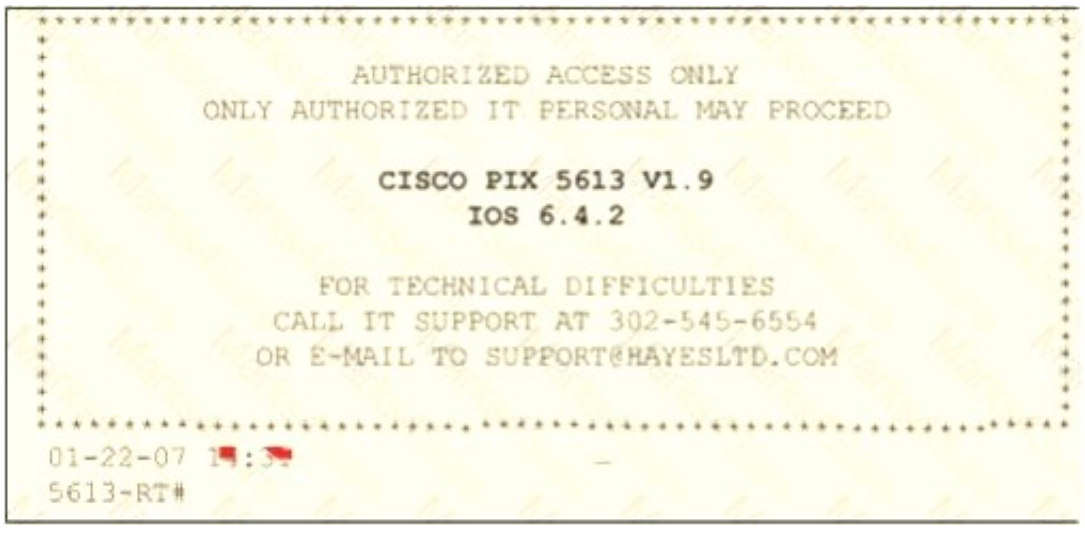
NEW QUESTION 84
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

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

Answer: D

NEW QUESTION 86
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

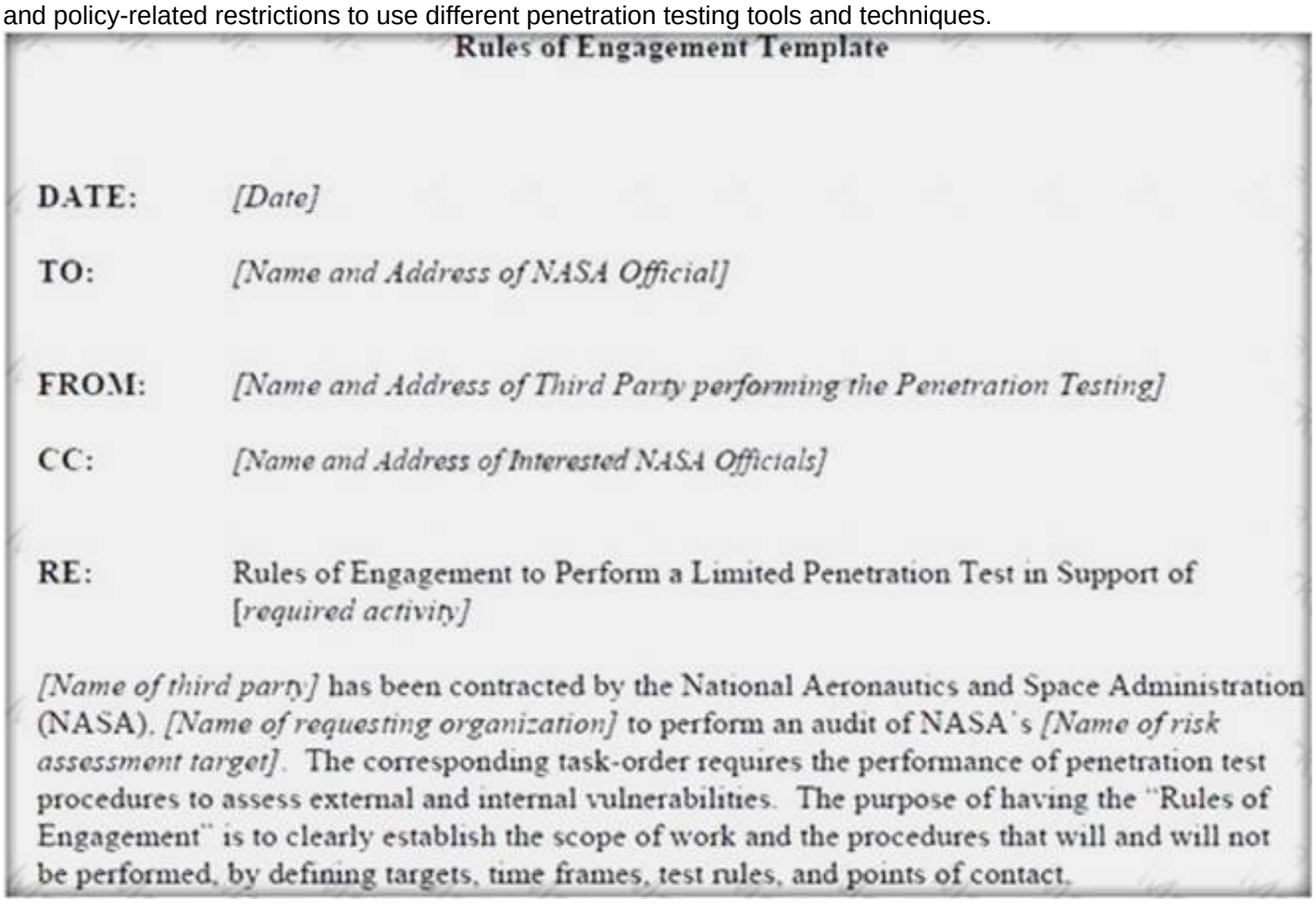
Answer: B

NEW QUESTION 90
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 93
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 96
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 98
DMZ is a network designed to give the public access to the specific internal resources and you might want to do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories.
Identify the attacks that fall under Passive attacks category.

A. Wardriving
B. Spoofing
C. Sniffing
D. Network Hijacking

Answer: A

NEW QUESTION 102
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 106
Which one of the following tools of trade is an automated, comprehensive penetration testing product for assessing the specific information security threats to an organization?

A. Sunbelt Network Security Inspector (SNSI)
B. CORE Impact
C. Canvas
D. Microsoft Baseline Security Analyzer (MBSA)

Answer: C

NEW QUESTION 109
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 114
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 119
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 122
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 125
What are the scanning techniques that are used to bypass firewall rules and logging mechanisms and disguise themselves as usual network traffic?

A. Connect Scanning Techniques

B. SYN Scanning Techniques
C. Stealth Scanning Techniques
D. Port Scanning Techniques

Answer: C

NEW QUESTION 128
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 129
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

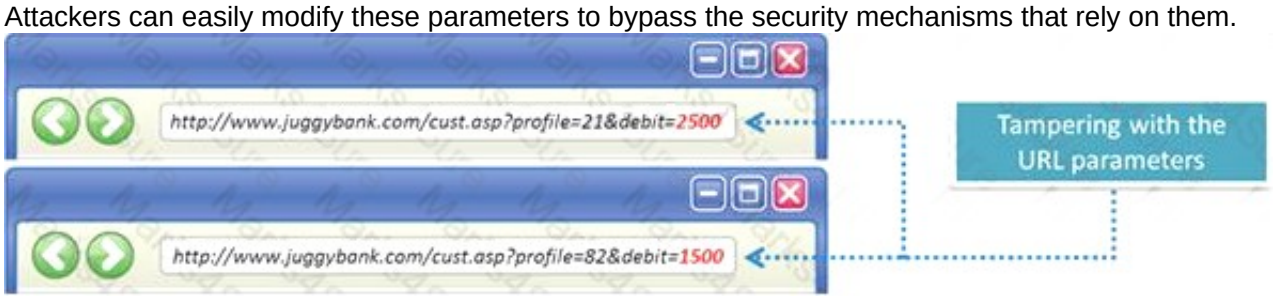
Answer: B

NEW QUESTION 132
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 135
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 139
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 142
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 145
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 149
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 150
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 154
Identify the port numbers used by POP3 and POP3S protocols.

A. 113 and 981
B. 111 and 982
C. 110 and 995
D. 109 and 973

Answer: C

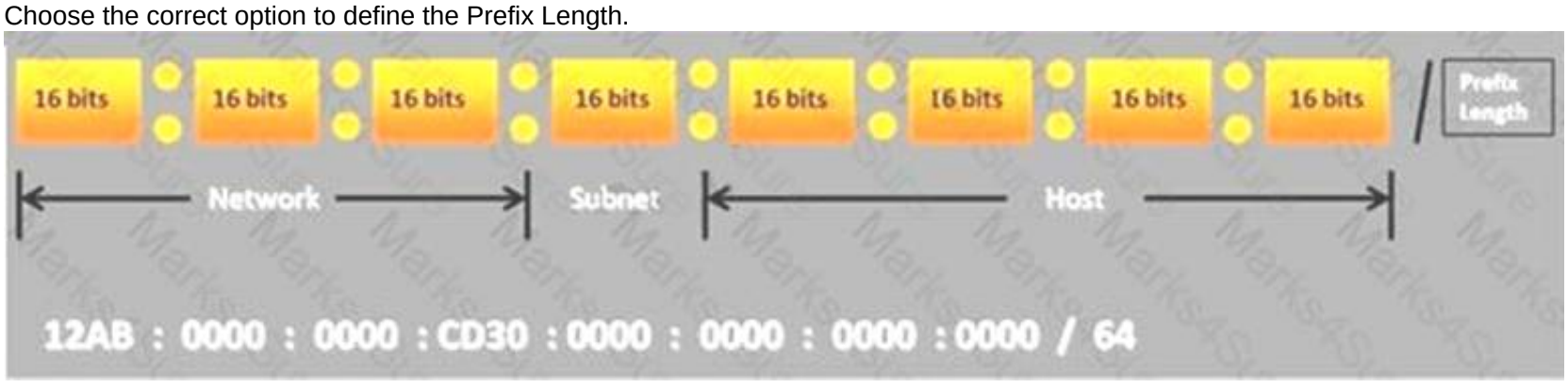
NEW QUESTION 156
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

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

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

Answer: A

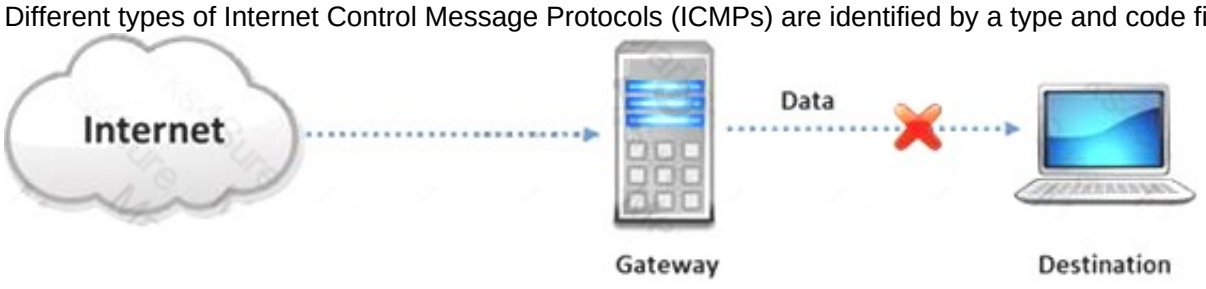
NEW QUESTION 159
Choose the correct option to define the Prefix Length.



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 160
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 164
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 168
In Linux, what is the smallest possible shellcode?

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

Answer: D

NEW QUESTION 173
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 174
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 176
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 180
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 184
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 188
What is the following command trying to accomplish?

```
C:\> nmap -sU -p445 192.168.0.0/24
```

A. Verify that NETBIOS is running for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that UDP port 445 is open for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 networks

Answer: C

NEW QUESTION 189
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

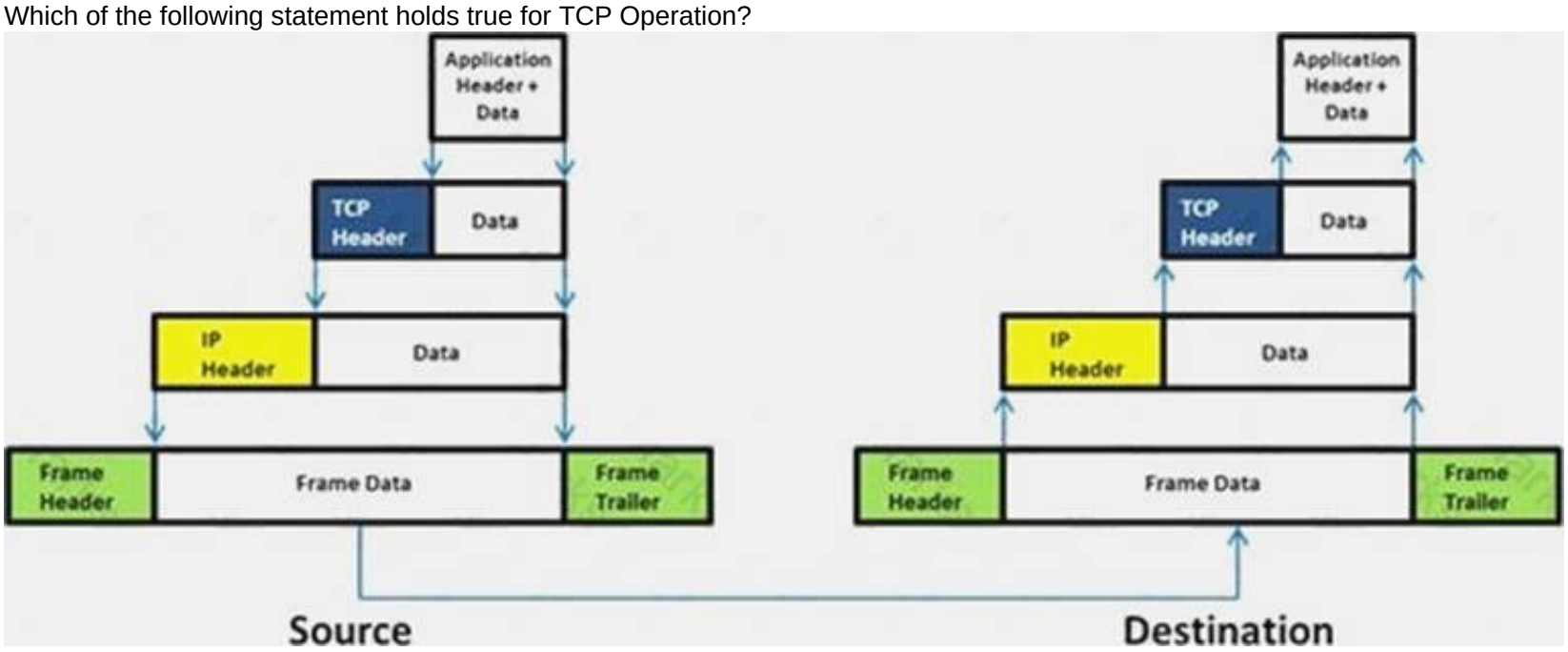
Answer: C

NEW QUESTION 192
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

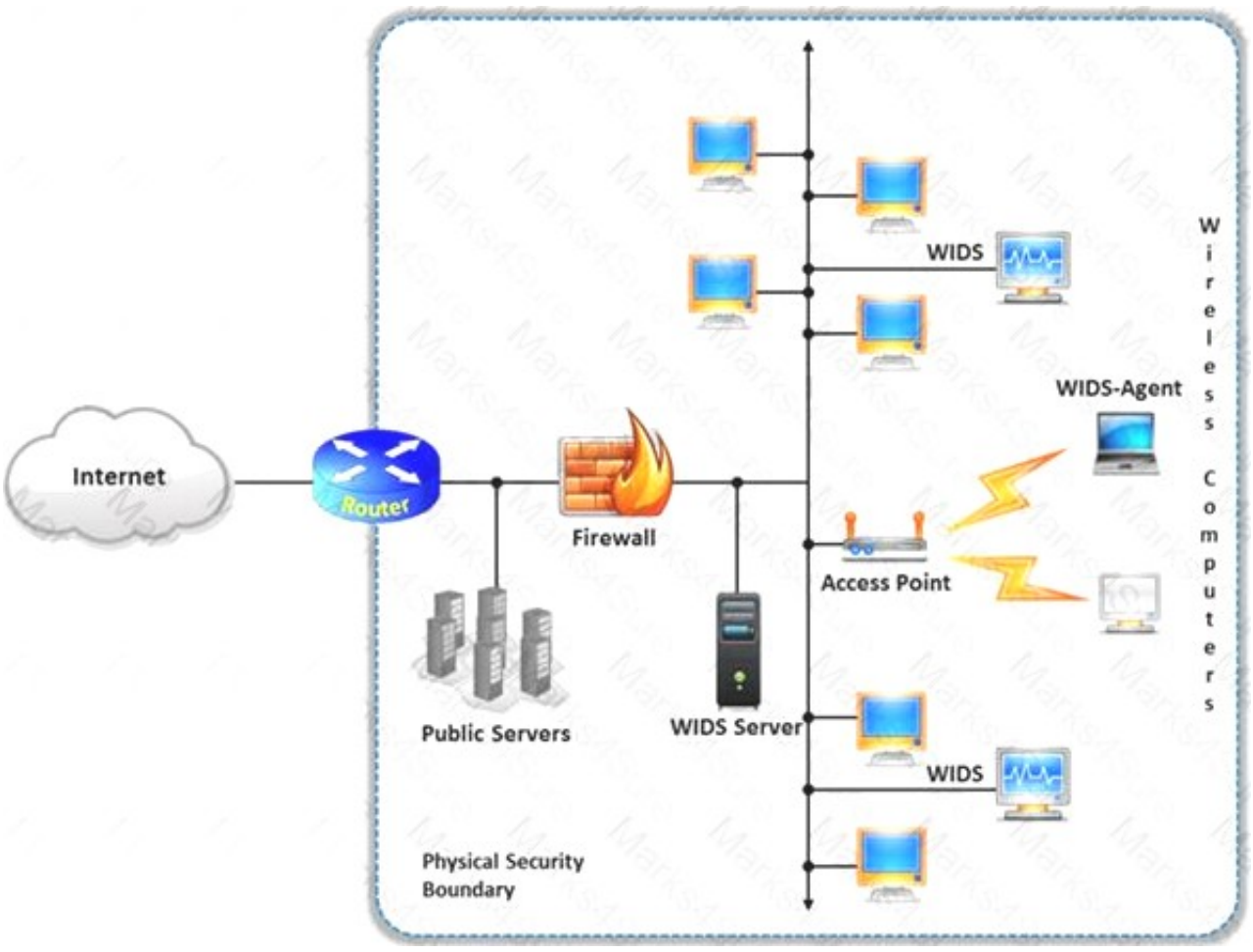
NEW QUESTION 195
Which of the following statement holds true for TCP Operation?



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 200
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 203
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 205
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 207
Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Po
B. Paranoid Policy

C. Promiscuous Policy
D. Prudent Policy

Answer: B

NEW QUESTION 208
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

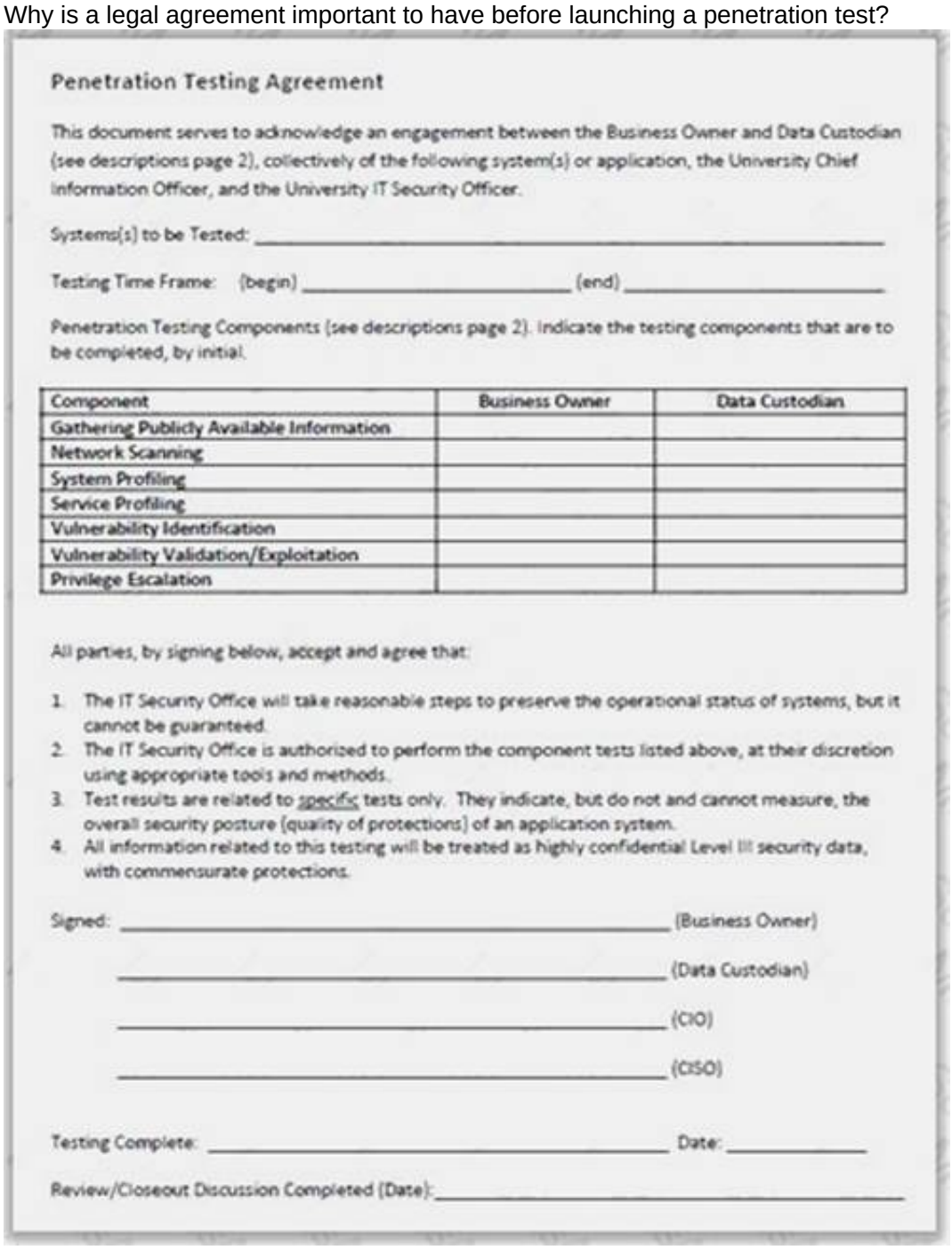
Answer: C

NEW QUESTION 210
Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

A. Wireshark: Capinfos
B. Wireshark: Tcpdump
C. Wireshark: Text2pcap
D. Wireshark: Dumpcap

Answer: D

NEW QUESTION 215
Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

System(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)
_____ (Data Custodian)
_____ (CIO)
_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees
B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
D. It is important to ensure that the target organization has implemented mandatory security policies

Answer: C

NEW QUESTION 219
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Answer: B

NEW QUESTION 220
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 224
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
B. Examine Server Side Includes (SSI)
C. Examine Hidden Fields
D. Examine E-commerce and Payment Gateways Handled by the Web Server

Answer: C

NEW QUESTION 229
What operating system would respond to the following command?

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

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

Answer: D

NEW QUESTION 233
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 234
.....

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