EC-Council

Exam Questions 412-79v9

EC-Council Certified Security Analyst (ECSA) v9

NEW QUESTION 1
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 2
A framework for security analysis is composed of a set of instructions, assumptions, and limitations to analyze and solve security concerns and develop threat free applications. Which of the following frameworks helps an organization in the evaluation of the company's information security with that of the industrial standards?

A. Microsoft Internet Security Framework
B. Information System Security Assessment Framework
C. The IBM Security Framework
D. Nortell's Unified Security Framework

Answer: B

NEW QUESTION 3
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 4
Which one of the following 802.11 types uses either FHSS or DSSS for modulation?

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

Answer: D

NEW QUESTION 5
Which of the following is not the SQL injection attack character?

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

Answer: A

NEW QUESTION 6
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 7
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 8
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

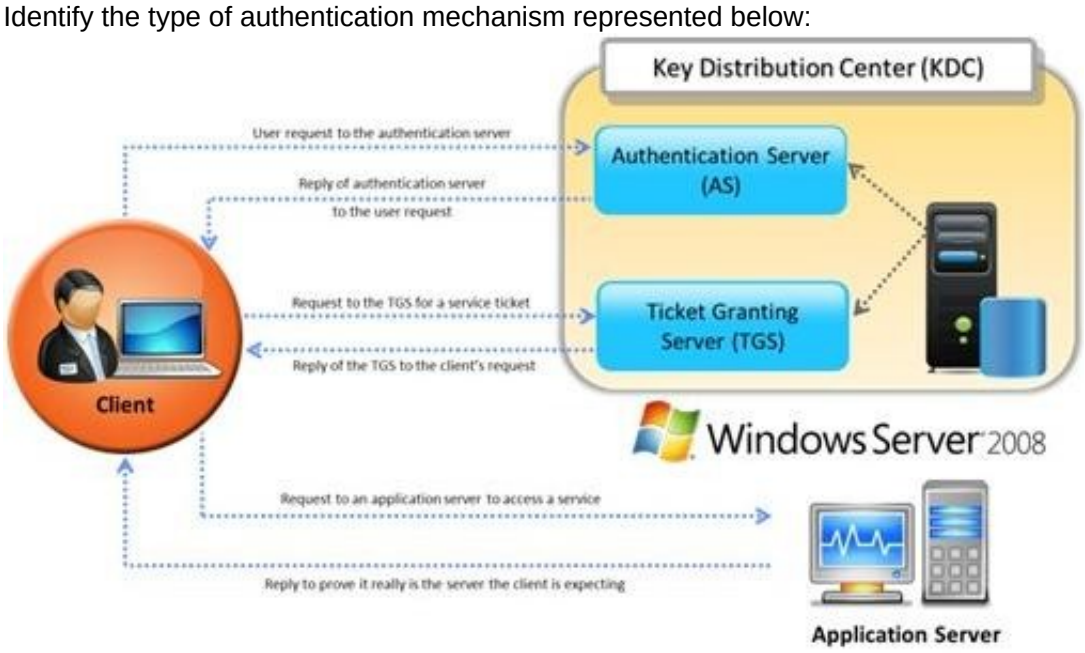
Answer: A

NEW QUESTION 9
Software firewalls work at which layer of the OSI model?

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

Answer: A

NEW QUESTION 10
Identify the type of authentication mechanism represented below:



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

Answer: D

Explanation:
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.
When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.
Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

NEW QUESTION 10
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

A. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?
B. 802.11b
C. 802.11g
D. 802.11-Legacy
E. 802.11n

Answer: A

NEW QUESTION 11
Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?

A. Anonymous Information Gathering
B. Private Information Gathering
C. Passive Information Gathering
D. Active Information Gathering

Answer: D

Explanation:
Reference: http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies.html

NEW QUESTION 13
Which of the following is NOT generally included in a quote for penetration testing services?

A. Type of testing carried out
B. Type of testers involved
C. Budget required
D. Expected timescale required to finish the project

Answer: B

NEW QUESTION 18
Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

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

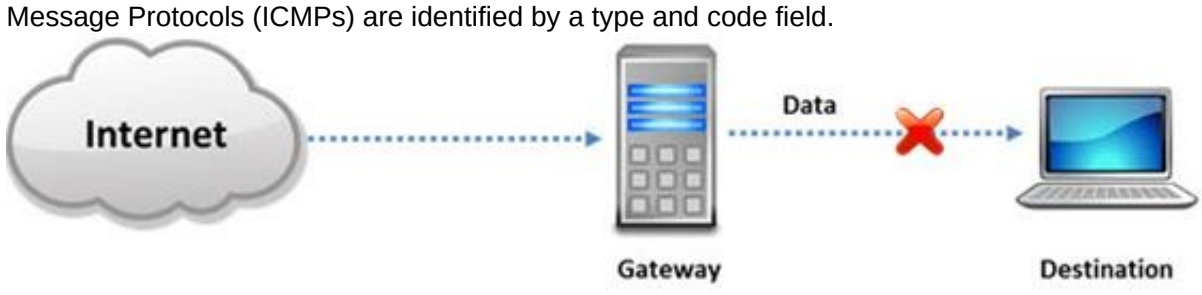
Answer: C

NEW QUESTION 23
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 28
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 29
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such

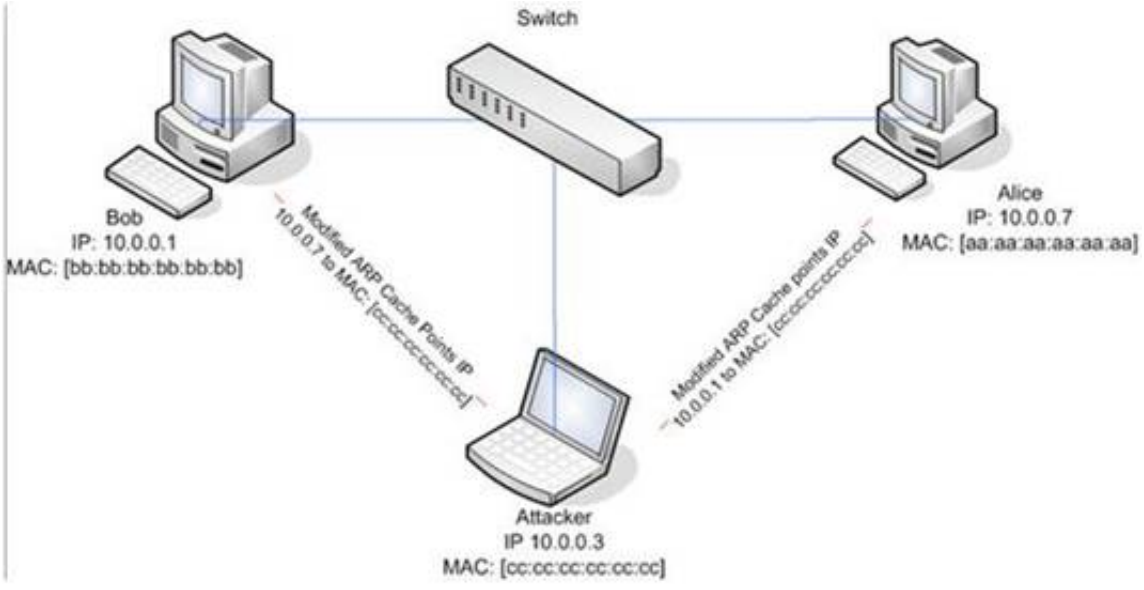
as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.
This attack takes advantage of the fact that many programmers rely on hidden 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 31
ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address
Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



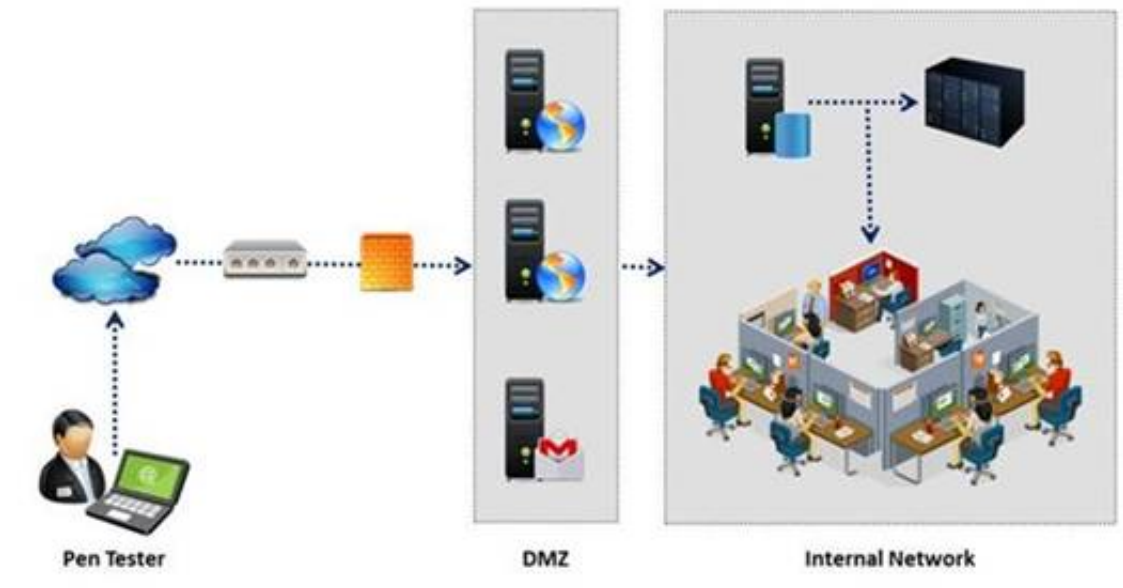
What type of attack would you launch after successfully deploying ARP spoofing?

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

Answer: D

Explanation:
http://en.wikipedia.org/wiki/ARP_spoofing

NEW QUESTION 33
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 35
During external penetration testing, which of the following techniques uses tools like Nmap to predict the sequence numbers generated by the targeted server and use this information to perform session hijacking techniques?

A. TCP Sequence Number Prediction
B. IPID State Number Prediction
C. TCP State Number Prediction
D. IPID Sequence Number Prediction

Answer: A

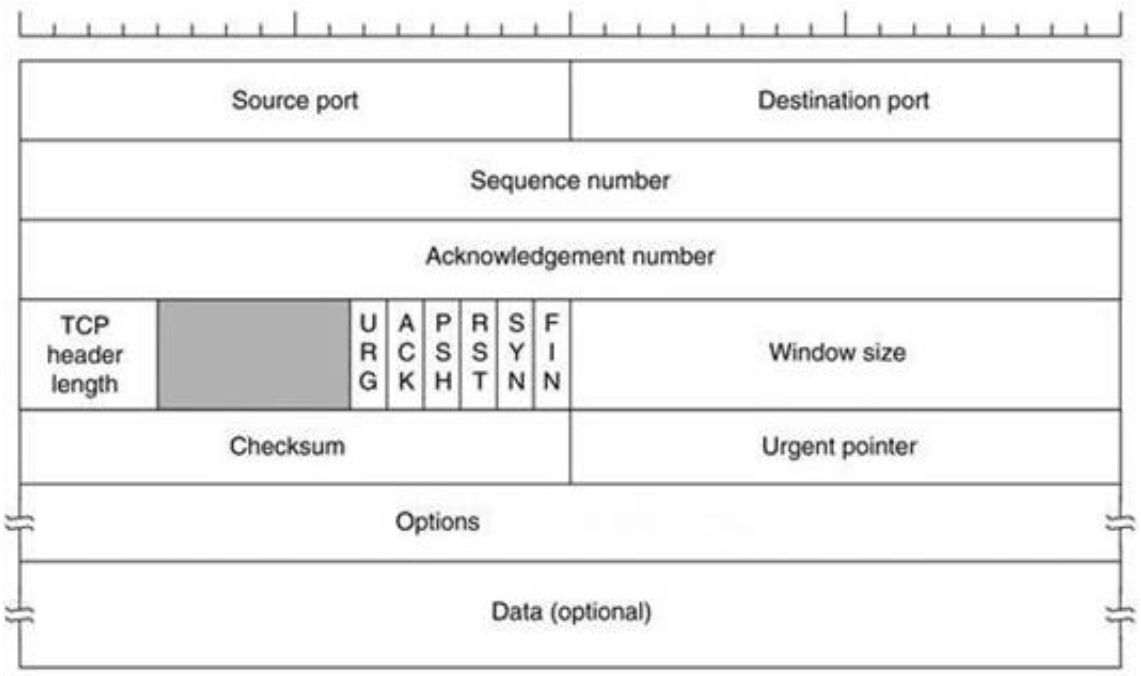
Explanation:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (p.43)

NEW QUESTION 40
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.(Select all that apply)

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

Answer: A

NEW QUESTION 44
Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment.
The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.
For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:



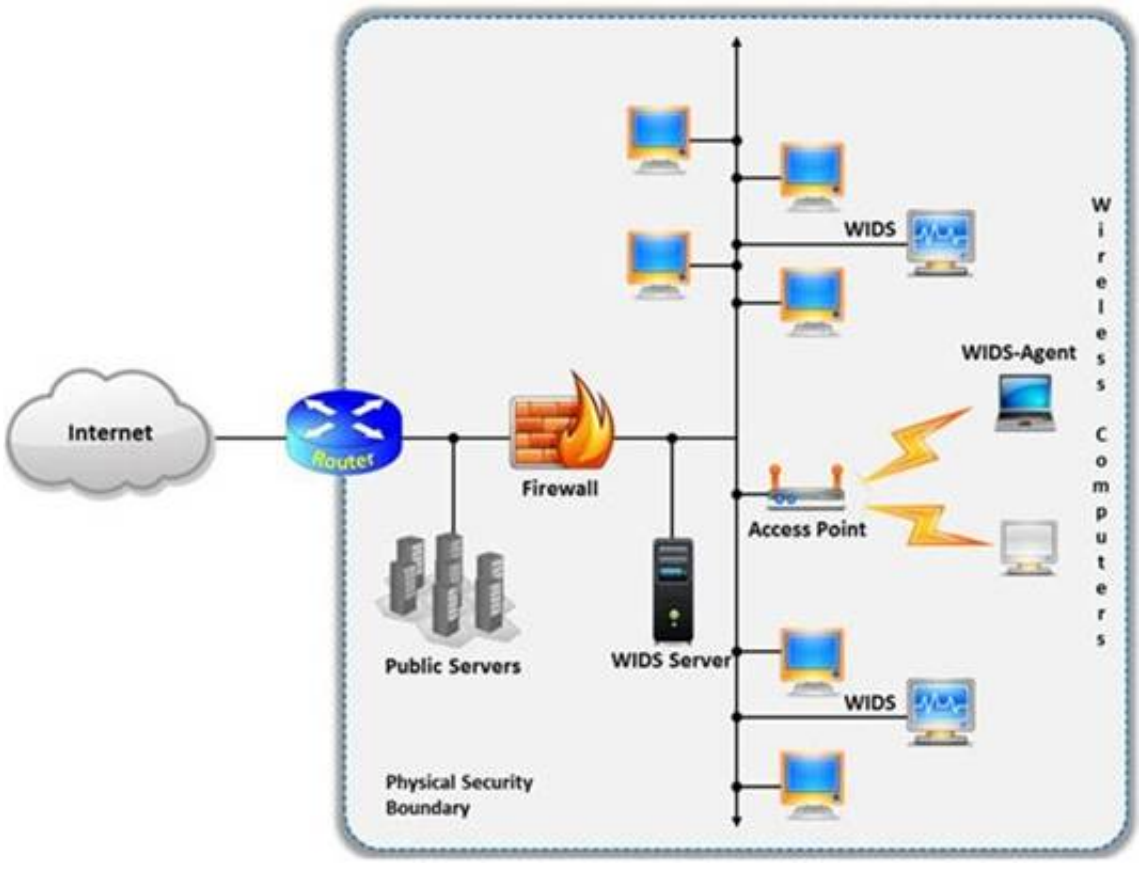
How many bits is a acknowledgement number?

A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits

Answer: B

Explanation:
Reference: http://en.wikipedia.org/wiki/Transmission_Control_Protocol (acknowledgement number)

NEW QUESTION 48
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

Explanation:
Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

NEW QUESTION 50
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 53
Which of the following is not a condition specified by Hamel and Prahalad (1990)?

A. Core competency should be aimed at protecting company interests
B. Core competency is hard for competitors to imitate
C. Core competency provides customer benefits
D. Core competency can be leveraged widely to many products and markets

Answer: A

Explanation:
Reference: http://www.studymode.com/essays/Hamel-Prahalad-Core-Competency- 1228370.html

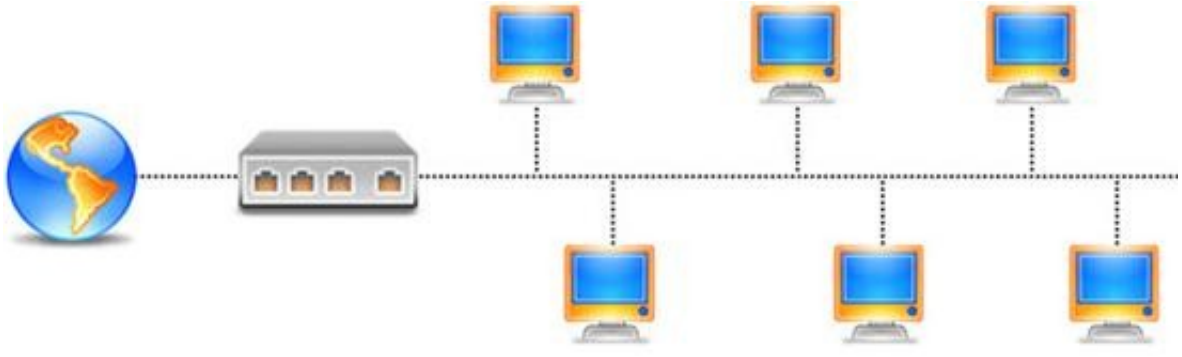
NEW QUESTION 54
John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

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

Answer: B

Explanation:
Reference: http://en.wikipedia.org/wiki/Hosts_(file) (location in the file system, see the table)

NEW QUESTION 58
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges.



Port numbers above 1024 are considered which one of the following?

A. Dynamically assigned port numbers
B. Statically assigned port numbers
C. Well-known port numbers
D. Unregistered port numbers

Answer: A

Explanation:
Reference: http://stackoverflow.com/questions/136709/what-port-number-should-i-use-when-testing-connections-in-my-local-intranet-in (see post 4)

NEW QUESTION 60
What is the maximum value of a “tinyint” field in most database systems?

A. 222
B. 224 or more
C. 240 or less
D. 225 or more

Answer: D

Explanation:
Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk-- R5r&sig=1hMOYByxt7ebRJ4UEjbpxMijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false

NEW QUESTION 65
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

Explanation:
Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

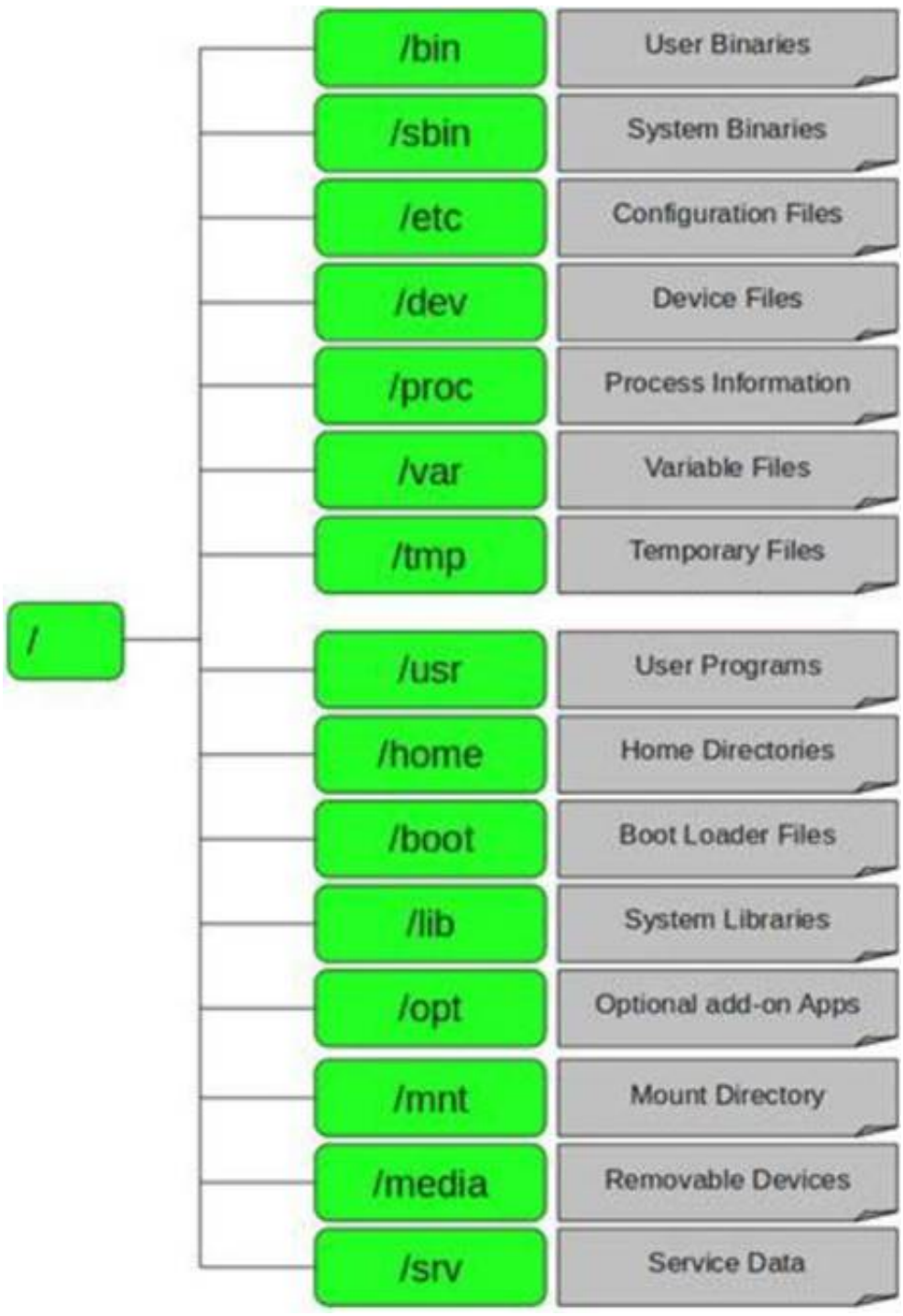
NEW QUESTION 69
Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above

Answer: A

Explanation:
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

NEW QUESTION 71
In Linux, /etc/shadow file stores the real password in encrypted format for user’s account with added properties associated with the user’s password.



In the example of a /etc/shadow file below, what does the bold letter string indicate?
Vivek: 1fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

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

Answer: B

Explanation:
Reference: http://www.cyberciti.biz/faq/understanding-etcshadow-file/ (bullet # 4)

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 80
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 84
Which one of the following is false about Wireshark? (Select all that apply)

A. Wireshark offers some options to analyze the WEP-decrypted data
B. It does not support decrypting the TKIP or CCMP packets
C. In order for Wireshark to decrypt the contents of the WEP-encrypted packets, it must be given the appropriate WEP key for the network

D. Packet Sniffer Mode

Answer: A

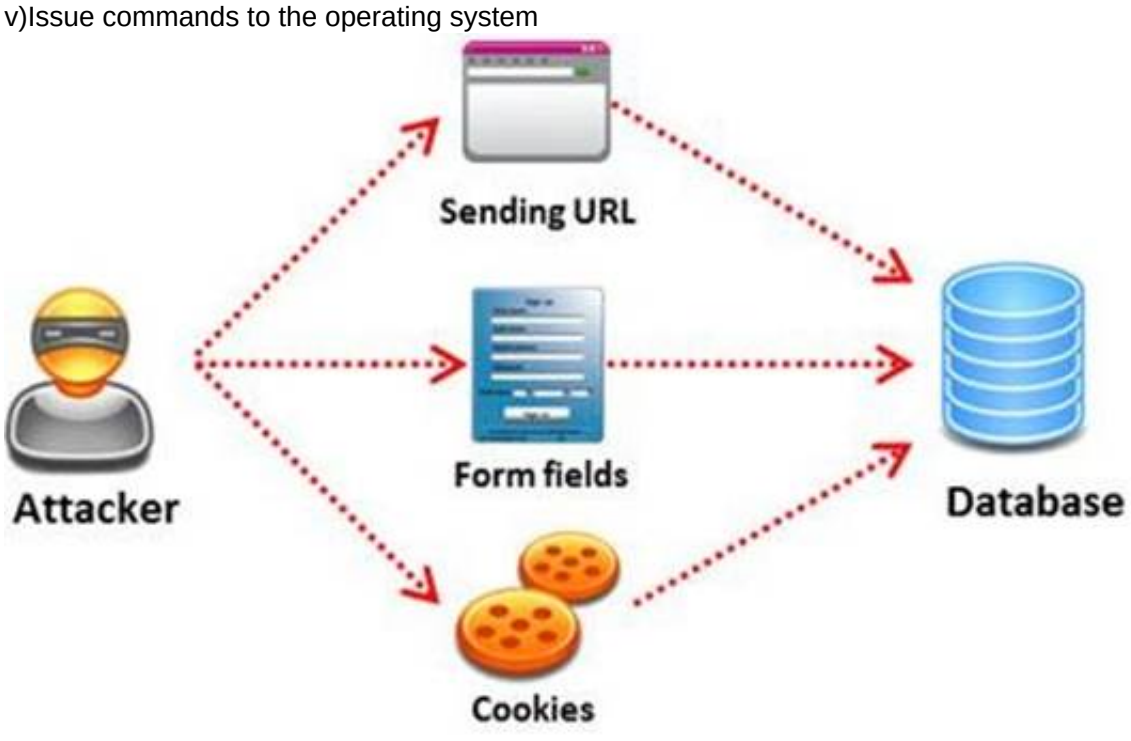
NEW QUESTION 85
The first and foremost step for a penetration test is information gathering. The main objective of this test is to gather information about the target system which can be used in a malicious manner to gain access to the target systems.

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 90
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

Explanation:
Reference: http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities

%20Using%20SQL.pdf

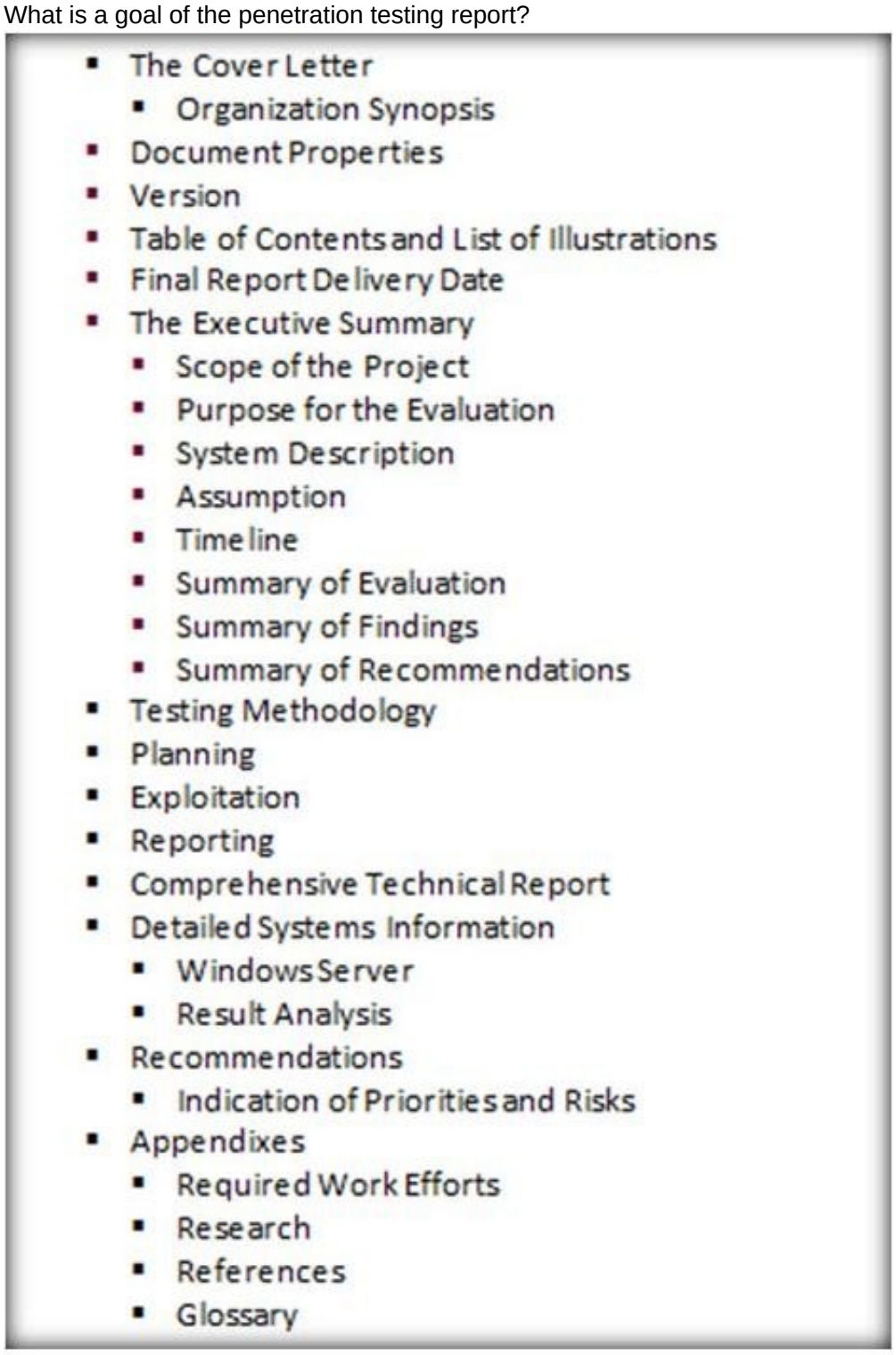
NEW QUESTION 93
HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

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

Explanation:
https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation%22+binary&source=bl&ots=pGMqass7ti&sig=rnIg1xZ78ScUvuIlTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgasrzgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false

NEW QUESTION 98
What is a goal of the penetration testing report?



A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.
B. The penetration testing report allows you to sleep better at night thinking your organization is protected
C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement securitycontrols and patch any flaws discovered during testing.
D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Answer: C

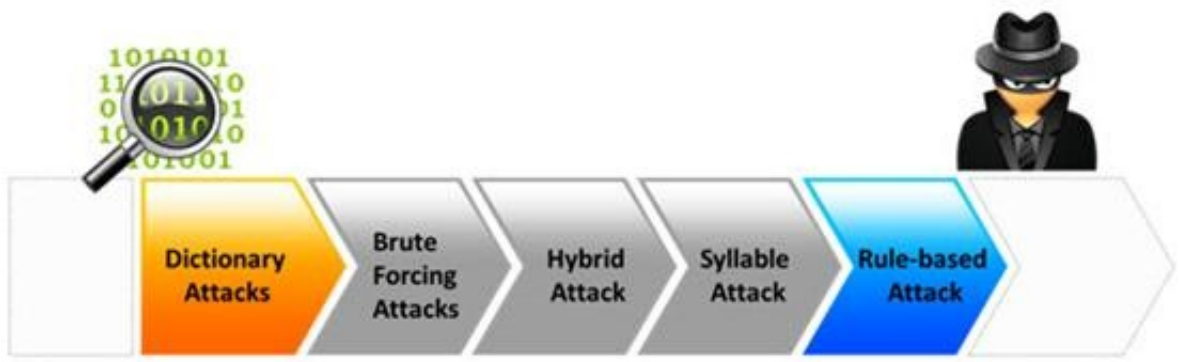
NEW QUESTION 103
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

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

Answer: D

Explanation:
Reference: http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA7- PA11&lpg=SA7-PA11&dq=vulnerability+assessment+tool+provides+security+to+the+IT+system+by+testing+for+vulnerabilities+in+the+applications+and+operation+system&source=bl&ots=SQCLHRnnjI&sig=HpenOheCU4GBOnkA4EurHCMfND4&hl=en&sa=X&ei=DqYfVJCLHMTnyQODn4C4Cw&ved=0CDQQ6AEwAw#v=onepage&q=vulnerability%20assessment%20tool%20provides%20security%20to%20the%20IT%20system%20by%20testing%20for%20vulnerabilities%20in%20the%20applications%20and%20operation%20system&f=false

NEW QUESTION 106
Passwords protect computer resources and files from unauthorized access by malicious users. Using passwords is the most capable and effective way to protect information and to increase the security level of a company.
Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system to gain unauthorized access to a system.



Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack
B. Rule-based attack
C. Hybrid attack
D. Dictionary attack

Answer: A

Explanation:
Reference: http://books.google.com.pk/books?id=m2qZNW4dcyIC&pg=PA237&lpg=PA237&dq=password+cracking+attacks+tries+every+combination+of+characters+until+the+password+is+broken&source=bl&ots=RKEUUo6LYj&sig=MPEfFBEpoO0yvOwMxYCoPQuqM5g&hl=en&sa=X&ei=ZdwdVJm3CoXSaPXsgPgM&ved=0CCEQ6AEwAQ#v=onepage&q=password%20cracking%20attacks%20tries%20every%20combination%20of%20characters%20until%20th e%20password%20is%20broken&f=false

NEW QUESTION 108
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

Explanation:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (page 71)

NEW QUESTION 113
Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test
B. Techniques for data exclusion from systems upon termination of the test
C. Details on how data should be transmitted during and after the test
D. Details on how organizational data is treated throughout and after the test

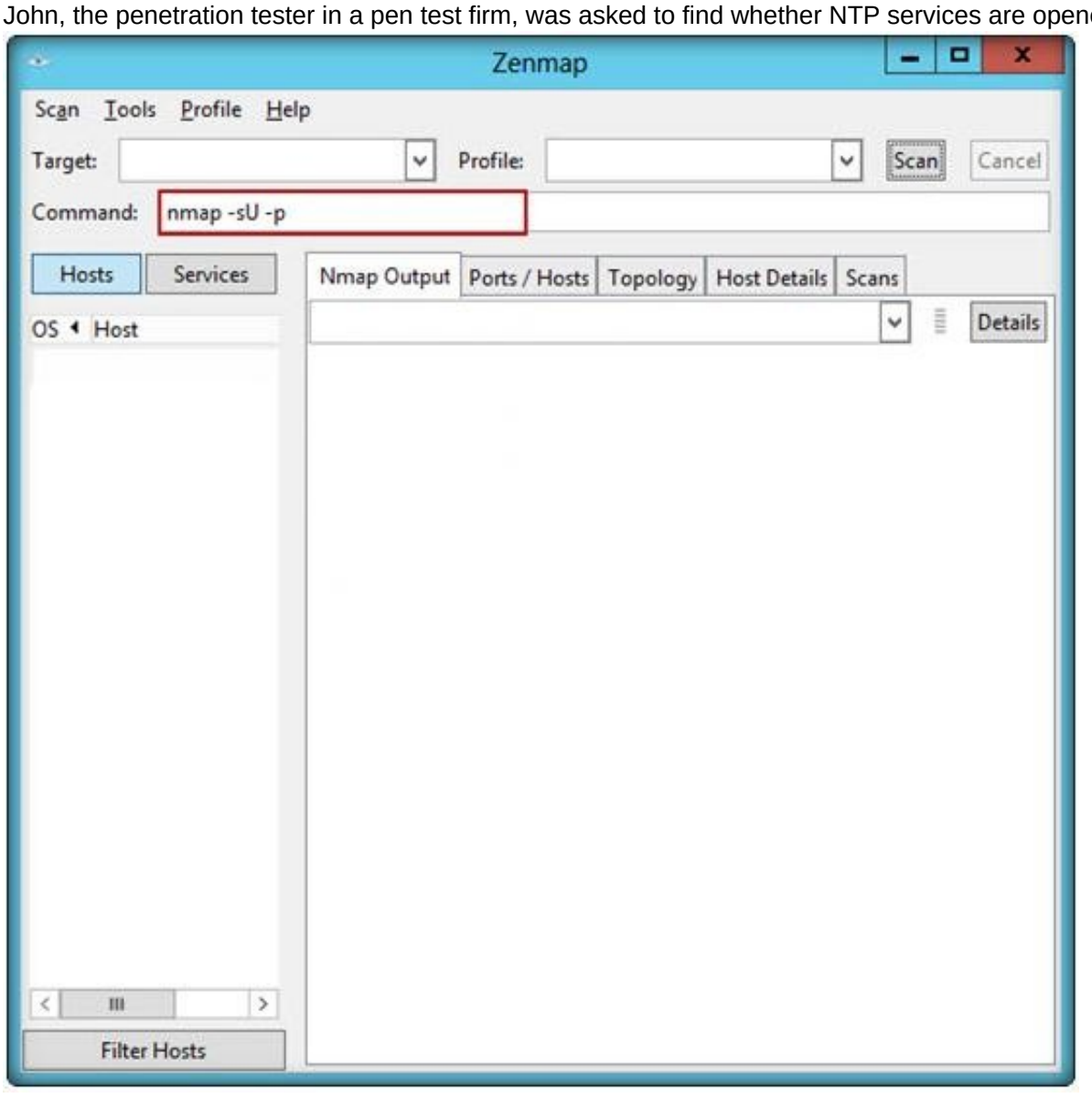
Answer: A

NEW QUESTION 114
A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing
B. Phishing
C. Insider Accomplice
D. Vishing

Answer: A

NEW QUESTION 117
John, the penetration tester in a pen test firm, was asked to find whether NTP services are opened on the target network (10.0.0.7) using Nmap tool.

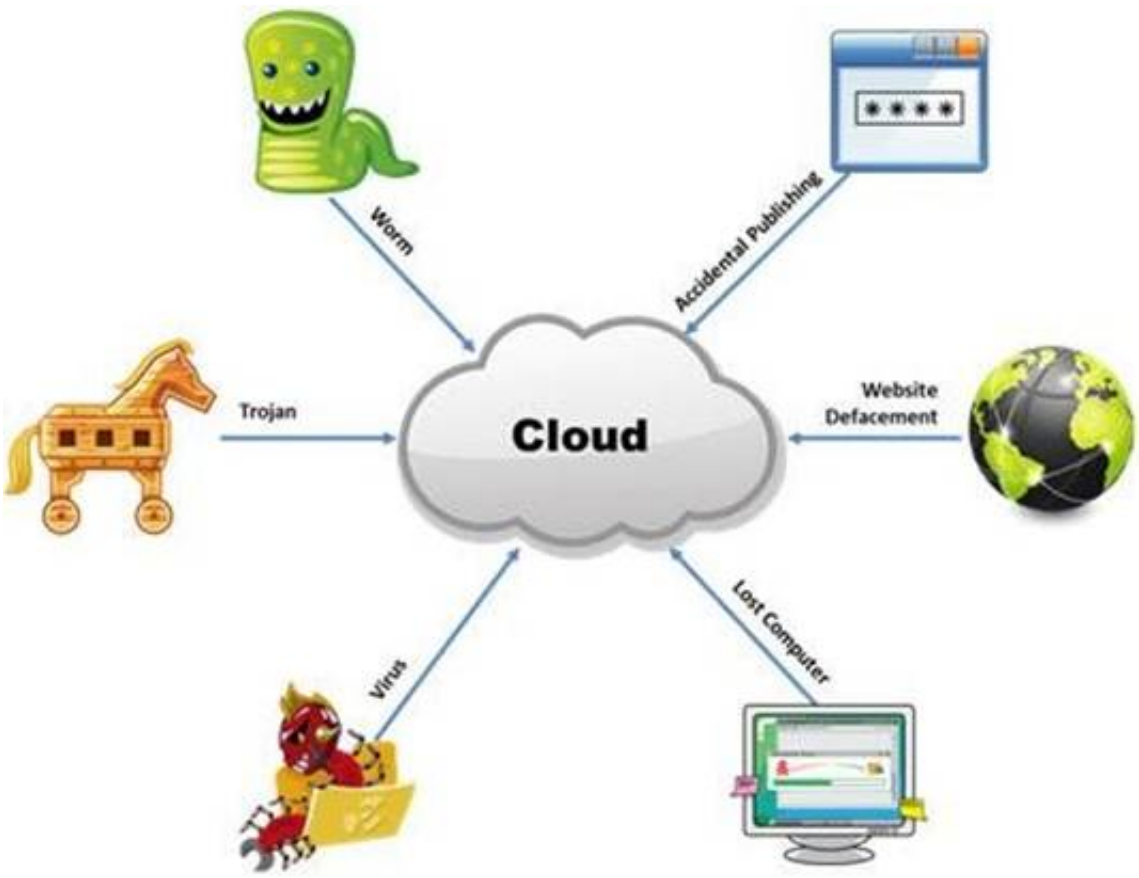


Which one of the following Nmap commands will he use to find it?

A. nmap -sU –p 389 10.0.0.7
B. nmap -sU –p 123 10.0.0.7
C. nmap -sU –p 161 10.0.0.7
D. nmap -sU –p 135 10.0.0.7

Answer: B

NEW QUESTION 119
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 120
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 a and c

Answer: A

Explanation:
Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection- systems (economic advantages, first para)

NEW QUESTION 125
Identify the data security measure which defines a principle or state that ensures that an action or transaction cannot be denied.

A. Availability
B. Integrity
C. Authorization
D. Non-Repudiation

Answer: D

Explanation:
Reference: http://en.wikipedia.org/wiki/Information_security (non-repudiation)

NEW QUESTION 126
Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Policy
B. Paranoid Policy
C. Promiscuous Policy
D. Prudent Policy

Answer: B

NEW QUESTION 131
Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Answer: C

Explanation:
Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction (page 15)

NEW QUESTION 136
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

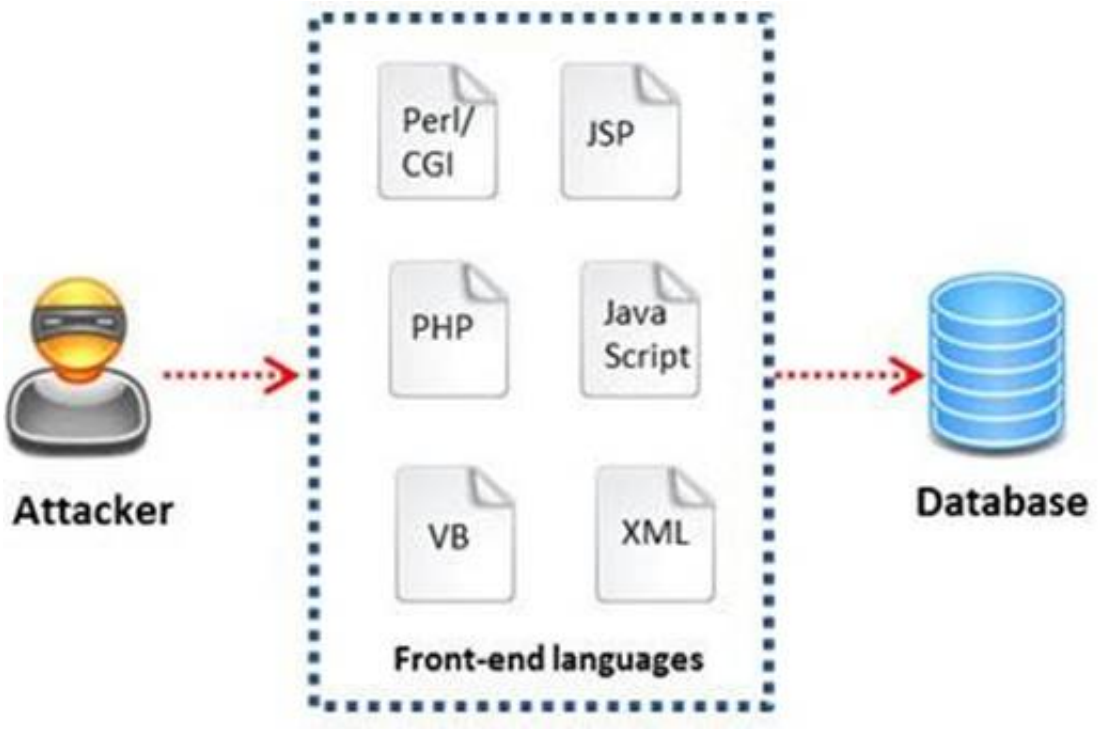
NEW QUESTION 141
Identify the port numbers used by POP3 and POP3S protocols.

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

Answer: C

Explanation:
Reference: https://publib.boulder.ibm.com/infocenter/wsmashin/v1r1/index.jsp?topic=/com.ibm.websph ere.sMash.doc/using/zero.mail/MailStoreConfiguration.html

NEW QUESTION 143
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'#

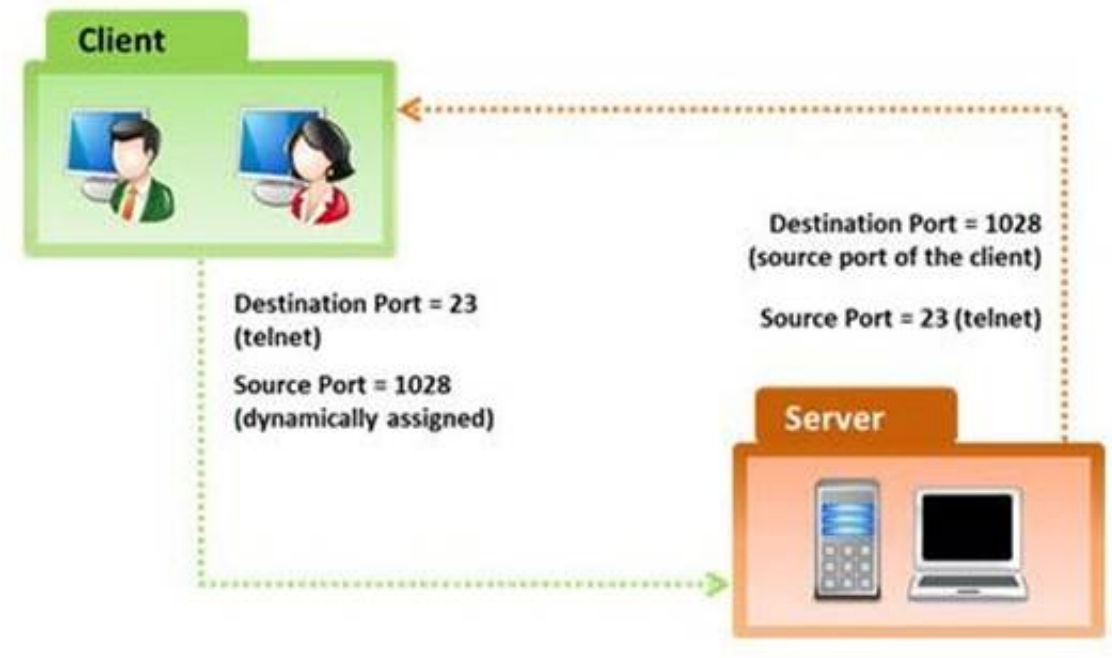
Answer: C

NEW QUESTION 148
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John’s email address.

A. Call his wife and ask for his personal email account
B. Call a receptionist and ask for John Stevens' personal email account
C. Search in Google for his personal email ID
D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Answer: D

NEW QUESTION 152
In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows
B. Windowing
C. Positive Acknowledgment with Retransmission (PAR)
D. Synchronization

Answer: C

Explanation:
Reference: http://condor.depaul.edu/jkristof/technotes/tcp.html (1.1.3 Reliability)

NEW QUESTION 153
In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique
B. IDS evasion technique
C. UDP evasion technique
D. TTL evasion technique

Answer: D

Explanation:
Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)

NEW QUESTION 154
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 157
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

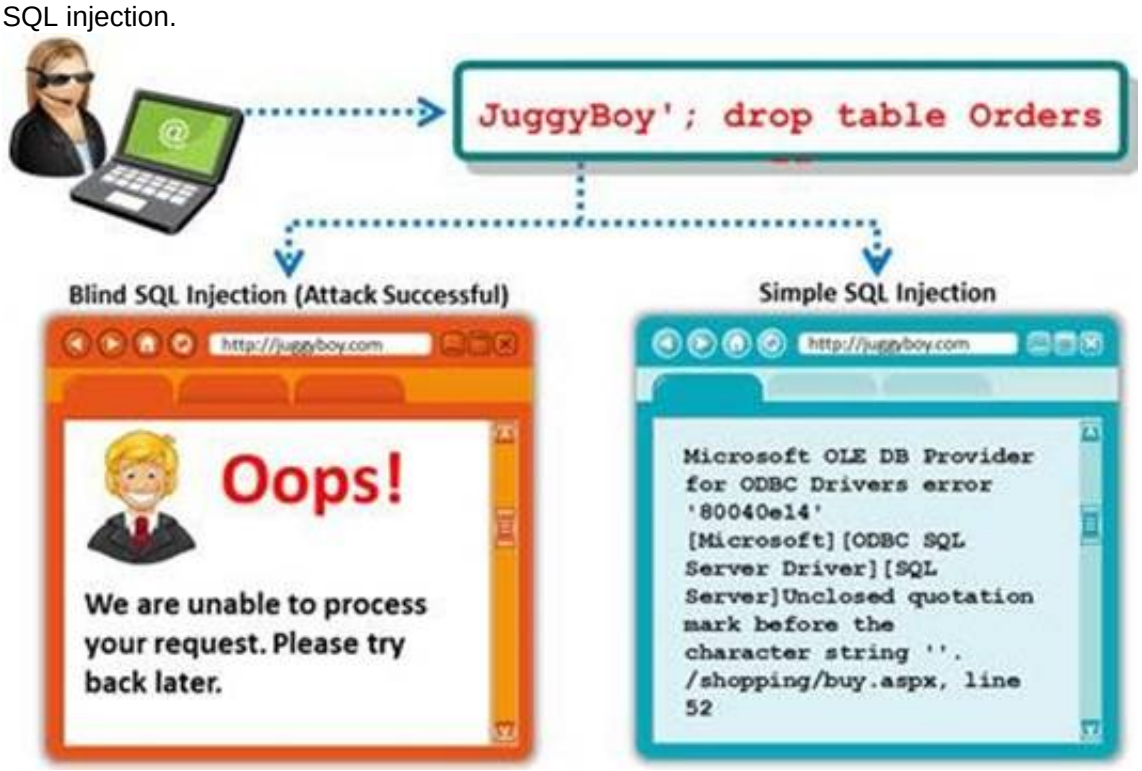
Explanation:
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

NEW QUESTION 160
Which one of the following log analysis tools is a Cisco Router Log Format log analyzer and it parses logs, imports them into a SQL database (or its own built-in database), aggregates them, and generates the dynamically filtered reports, all through a web interface?

A. Event Log Tracker
B. Sawmill
C. Syslog Manager
D. Event Log Explorer

Answer: B

NEW QUESTION 162
A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.
A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--
What is the database name?

A. WXYZ
B. PQRS
C. EFGH
D. ABCD

Answer: D

Explanation:
Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to 2051)

NEW QUESTION 167
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 wherethe user input is used as part of a SQL identifier without any input sanitization

Answer: D

NEW QUESTION 169
Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named “Access Point Detection”. This plug- in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting
B. HTTP fingerprinting
C. FTP fingerprinting
D. SNMP fingerprinting

Answer: C

NEW QUESTION 174
What information can be collected by dumpster diving?

A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above

Answer: A

Explanation:
Reference: http://www.spamlaws.com/dumpster-diving.html

NEW QUESTION 176
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 178
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 180
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

412-79v9 Practice Exam Features:

* 412-79v9 Questions and Answers Updated Frequently

* 412-79v9 Practice Questions Verified by Expert Senior Certified Staff

* 412-79v9 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 412-79v9 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year