Exam Questions 412-79v9

EC-Council Certified Security Analyst (ECSA) v9

https://www.2passeasy.com/dumps/412-79v9/

NEW QUESTION 1
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

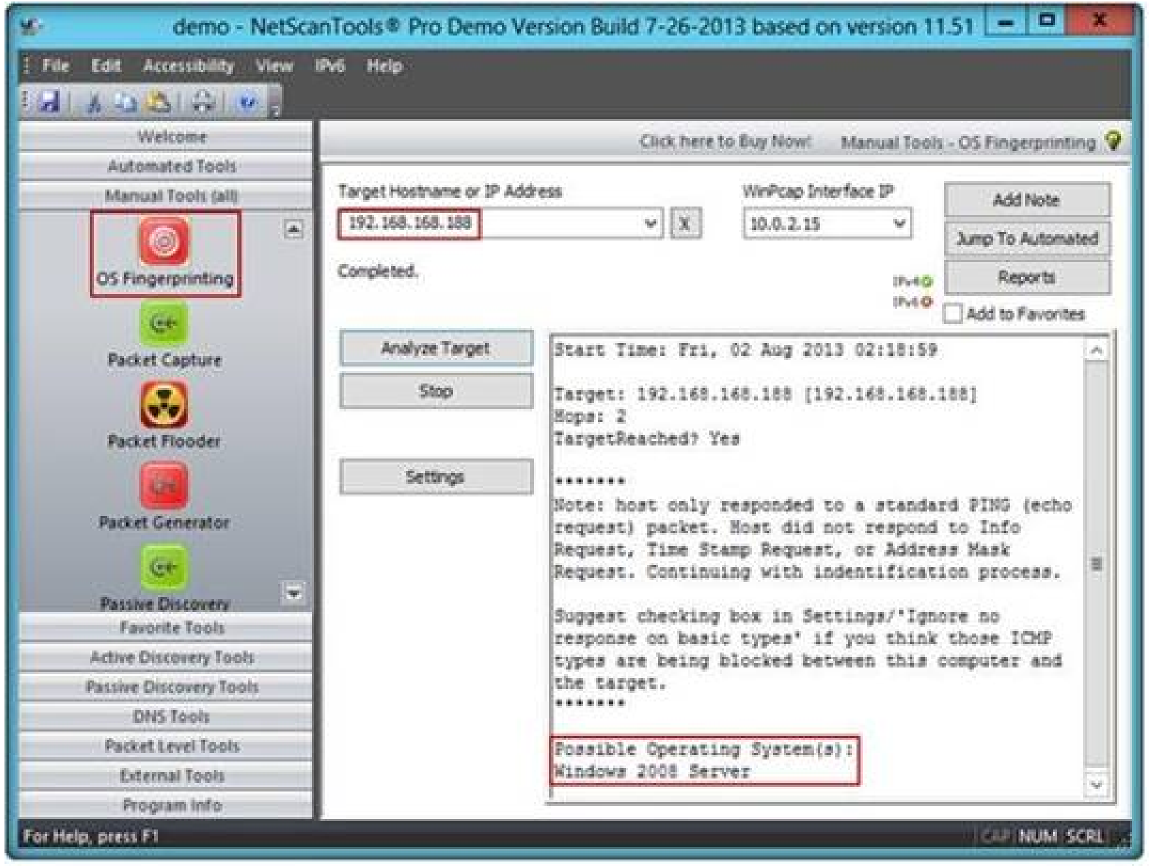
Answer: C

NEW QUESTION 2
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 3
A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



Target Hostname or IP Address: 192.168.168.188
WinPcap Interface IP: 10.0.2.15
Completed.

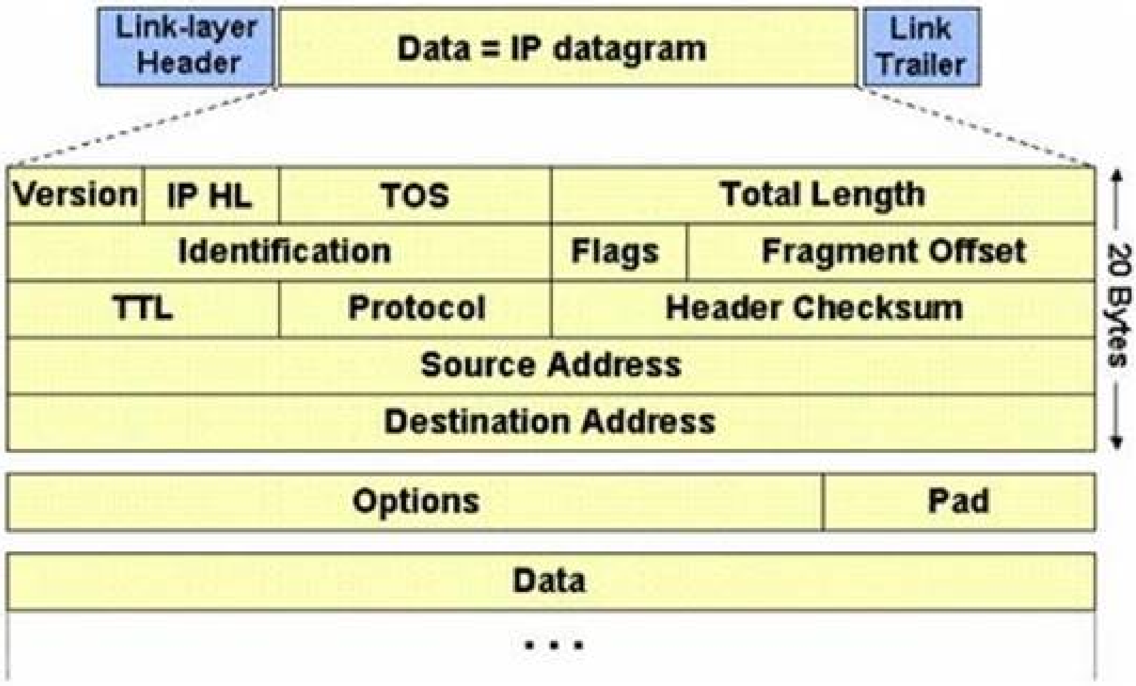
```
Start Time: Fri, 02 Aug 2013 02:18:59

Target: 192.168.168.188 [192.168.168.188]
Hops: 2
TargetReached? Yes

*******
Note: host only responded to a standard PING (echo
request) packet. Host did not respond to Info
Request, Time Stamp Request, or Address Mask
Request. Continuing with indentification process.

Suggest checking box in Settings/'Ignore no
response on basic types' if you think those ICMP
types are being blocked between this computer and
the target.
*******

Possible Operating System(s):
Windows 2008 Server
```

While performing ICMP scanning using Nmap tool, message received/type displays “3 – Destination Unreachable[5]” and code 3.
Which of the following is an appropriate description of this response?

A. Destination port unreachable
B. Destination host unavailable
C. Destination host unreachable
D. Destination protocol unreachable

Answer: A

NEW QUESTION 4
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

Explanation:
Reference: http://www.freesoft.org/CIE/Course/Section3/7.htm (fragment offset: 13 bits)

NEW QUESTION 5
Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

A. SYN Scan
B. TCP Connect Scan
C. XMAS Scan
D. Null Scan

Answer: A

NEW QUESTION 6
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 7
Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

A. Tcpdump
B. Capinfos
C. Tshark
D. Idl2wrs

Answer: B

NEW QUESTION 8
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 9
Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts
B. References
C. Research
D. Glossary

Answer: D

Explanation:
Refere' http://en.wikipedia.org/wiki/Glossary

NEW QUESTION 10
One of the steps in information gathering is to run searches on a company using complex keywords in Google.

terms appearing: anywhere in the page — Search for terms in the whole page, page title, or web address, links to the page you're looking for.

SafeSearch: Show most relevant results — Tell SafeSearch whether to filter sexually explicit content.

reading level: no reading level displayed — Find pages at one reading level or just view the level info.

file type: any format — Find pages in the format you prefer.

usage rights: not filtered by license — Find pages you are free to use yourself.

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

Explanation:
Reference: http://blog.hubspot.com/blog/tabid/6307/bid/1264/12-Quick-Tips-To-Search-Google-Like-An-Expert.aspx (specific document types)

NEW QUESTION 10
Which of the following protocol's traffic is captured by using the filter tcp.port==3389 in the Wireshark tool?

A. Reverse Gossip Transport Protocol (RGTP)
B. Real-time Transport Protocol (RTP)
C. Remote Desktop Protocol (RDP)
D. Session Initiation Protocol (SIP)

Answer: C

Explanation:

Reference: http://wiki.wireshark.org/RDP

NEW QUESTION 11
In the example of a /etc/passwd file below, what does the bold letter string indicate? nomad:HrLNrZ3VS3TF2:501:100: Simple Nomad:/home/nomad:/bin/bash

A. Maximum number of days the password is valid
B. Group number
C. GECOS information
D. User number

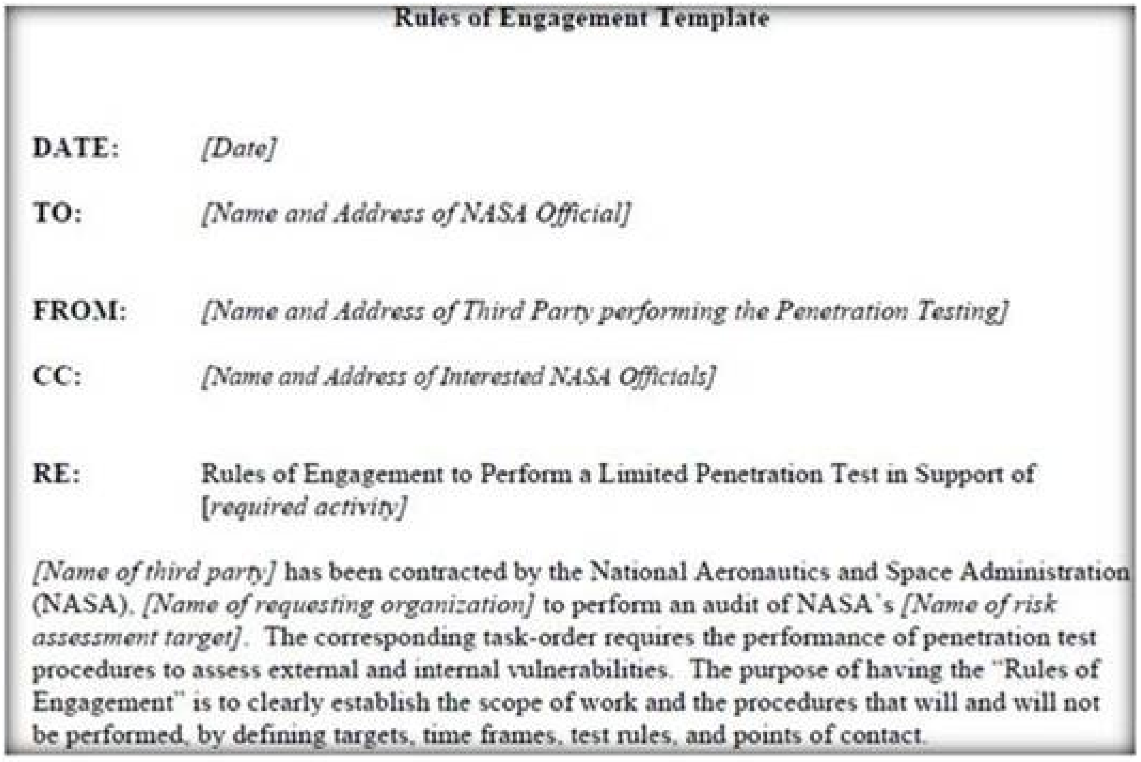
Answer: D

NEW QUESTION 13
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 17
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 21
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.

Confidential Information
Social Engineering
Access Details
Authorization Details

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 26
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 30
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 33
Software firewalls work at which layer of the OSI model?

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

Answer: A

NEW QUESTION 35
By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry
B. Netstat
C. Telnet
D. Tracert

Answer: A

Explanation:
Reference: http://support.microsoft.com/kb/832919

NEW QUESTION 36
During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Answer: D

NEW QUESTION 37
Which of the following scan option is able to identify the SSL services?

A. –sS
B. –sV
C. –sU
D. –sT

Answer: B

Explanation:
Reference: https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001) (blackbox test and example, second para)

NEW QUESTION 38
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 41
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

Explanation:
Reference: http://www.investopedia.com/terms/r/returnoninvestment.asp

NEW QUESTION 46
Which one of the following architectures has the drawback of internally considering the hosted services individually?

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

Answer: C

NEW QUESTION 47
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 52
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

Explanation:
Reference: http://luizfirmino.blogspot.com/2011_09_01_archive.html (see authorization attack)

NEW QUESTION 53
What threat categories should you use to prioritize vulnerabilities detected in the pen testing report?

A. 1, 2, 3, 4, 5
B. Low, medium, high, serious, critical
C. Urgent, dispute, action, zero, low
D. A, b, c, d, e

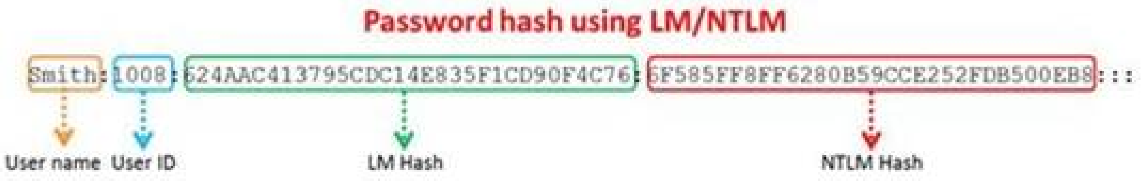
Answer: B

NEW QUESTION 58
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 61
Windows stores user passwords in the Security Accounts Manager database (SAM), or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.
NTLM and LM authentication protocols are used to securely store a user's password in the SAM database using different hashing methods.


Password hash using LM/NTLM
Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
User name
User ID
LM Hash
NTLM Hash

The SAM file in Windows Server 2008 is located in which of the following locations?

A. c:\windows\system32\config\SAM
B. c:\windows\system32\drivers\SAM
C. c:\windows\system32\Setup\SAM
D. c:\windows\system32\Boot\SAM

Answer: A

NEW QUESTION 62
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 64
An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is
developed from waveguide technology?

A. Leaky Wave Antennas
B. Aperture Antennas
C. Reflector Antenna
D. Directional Antenna

Answer: B

NEW QUESTION 66
From where can clues about the underlying application environment can be collected?

A. From the extension of the file
B. From executable file
C. From file types and directories
D. From source code

Answer: A

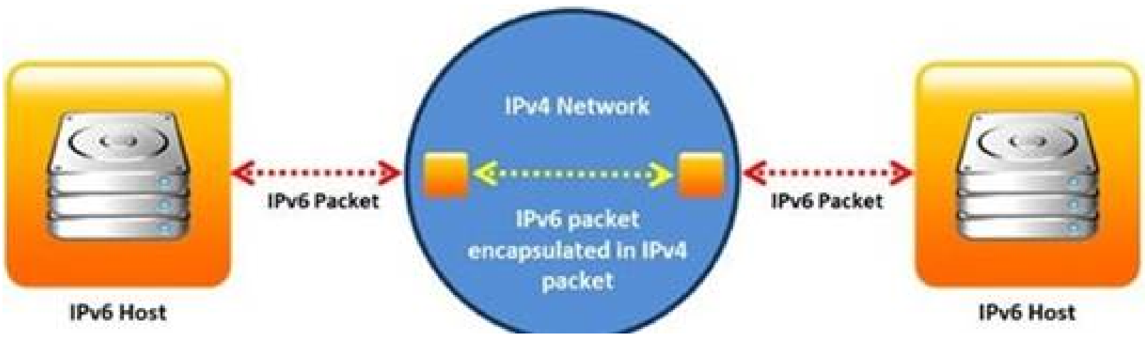
NEW QUESTION 70
Which of the following attacks does a hacker perform in order to obtain UDDI information
such as businessEntity, businesService, bindingTemplate, and tModel?

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

Answer: A

Explanation:
Reference: http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web- Applications-pdf (page 99)

NEW QUESTION 75
Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation
B. Tunneling
C. Dual Stacks
D. Encapsulation

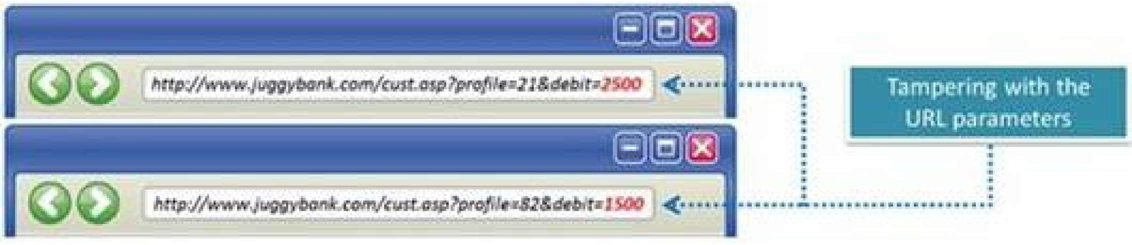
Answer: B

NEW QUESTION 80
Which one of the following acts related to the information security in the US fix the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

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

Answer: B

NEW QUESTION 82
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.


http://www.juggybank.com/cust.asp?profile=21&debit=2500
http://www.juggybank.com/cust.asp?profile=82&debit=1500
Tampering with the URL parameters

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 86
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 91
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James
testing against his network?

A. Smurf
B. Trinoo
C. Fraggle
D. SYN flood

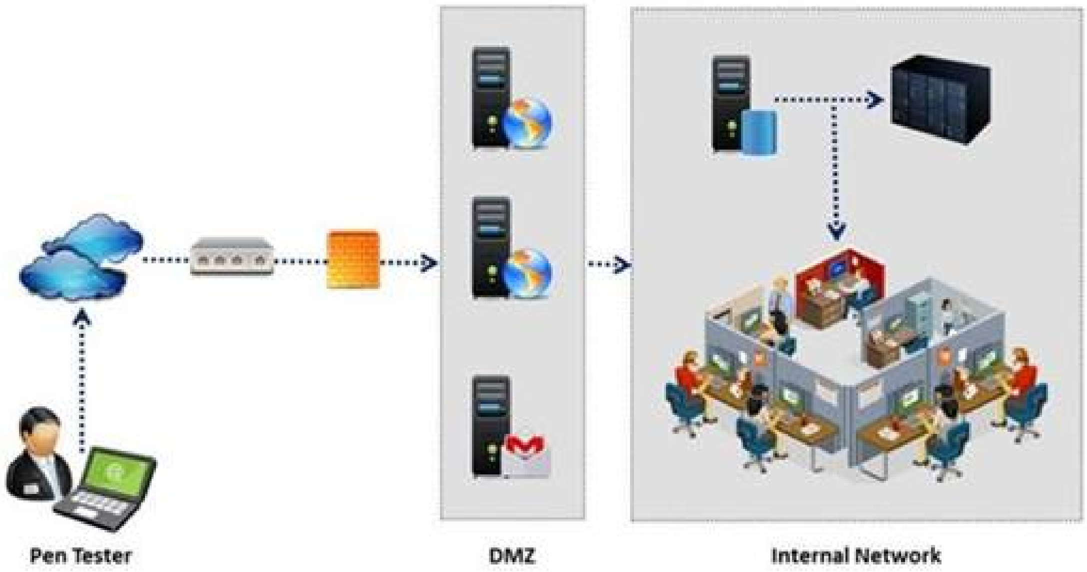
Answer: A

NEW QUESTION 93
Fuzz testing or fuzzing is a software/application testing technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.
Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs, and SQL injection.
Fuzzer helps to generate and submit a large number of inputs supplied to the application for testing it against the inputs. This will help us to identify the SQL inputs that generate malicious output.
Suppose a pen tester knows the underlying structure of the database used by the application (i.e., name, number of columns, etc.) that she is testing.
Which of the following fuzz testing she will perform where she can supply specific data to the application to discover vulnerabilities?

A. Clever Fuzz Testing
B. Dumb Fuzz Testing
C. Complete Fuzz Testing
D. Smart Fuzz Testing

Answer: D

NEW QUESTION 96
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 99
Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes.
Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

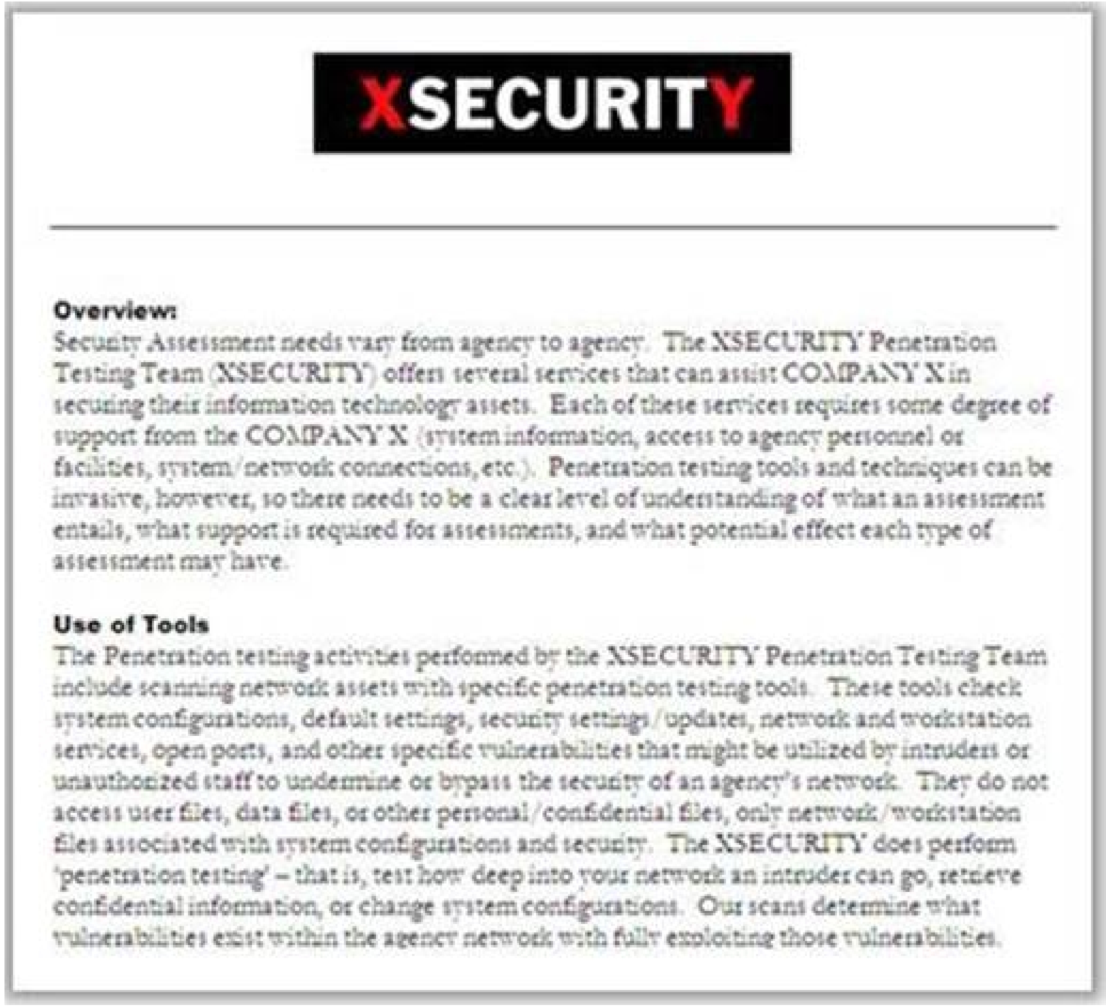
A. Packet Sniffer Mode
B. Packet Logger Mode
C. Network Intrusion Detection System Mode
D. Inline Mode

Answer: A

NEW QUESTION 101

Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.

Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.



XSECURITY

Overview:

Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools

The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement
B. Client fees agreement
C. Rules of engagement agreement
D. Confidentiality agreement

Answer: C

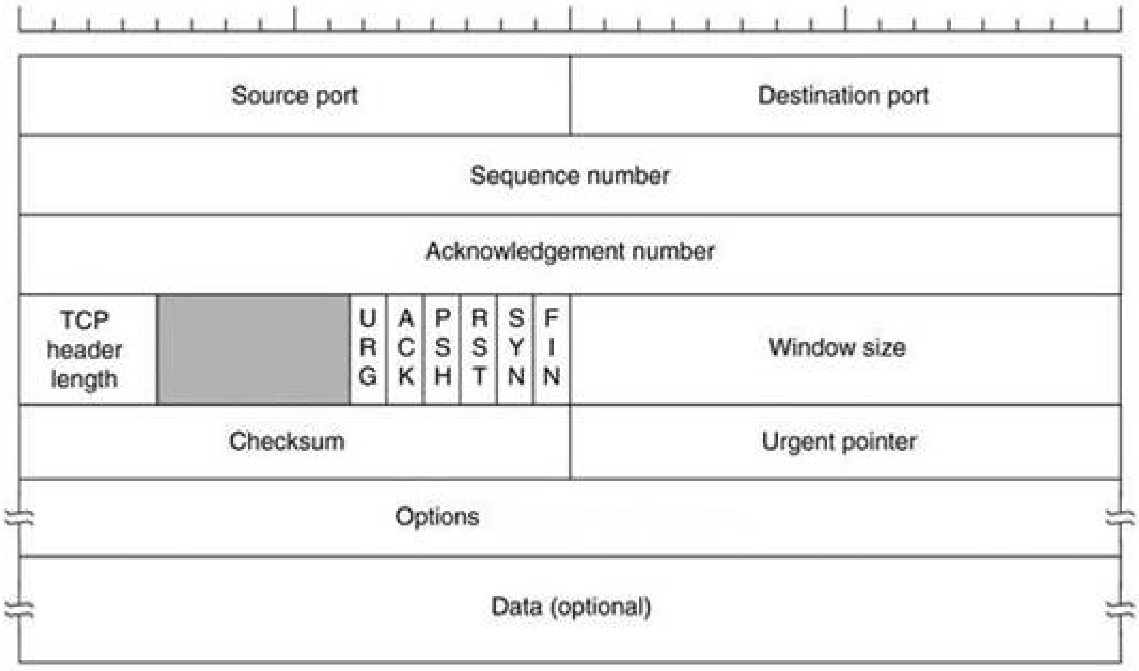
NEW QUESTION 104

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 108
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

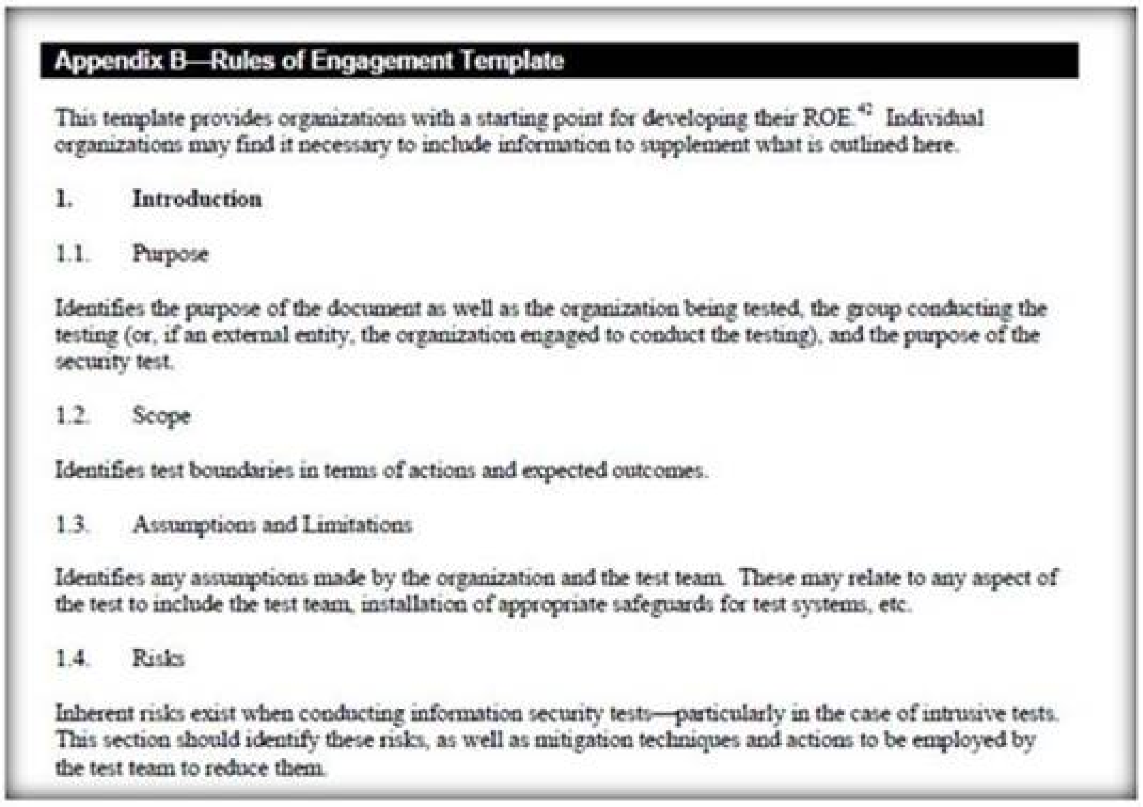
Explanation:
Reference: http://www.studymode.com/essays/Hamel-Prahalad-Core-Competency- 1228370.html

NEW QUESTION 112
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Answer: B

NEW QUESTION 115
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

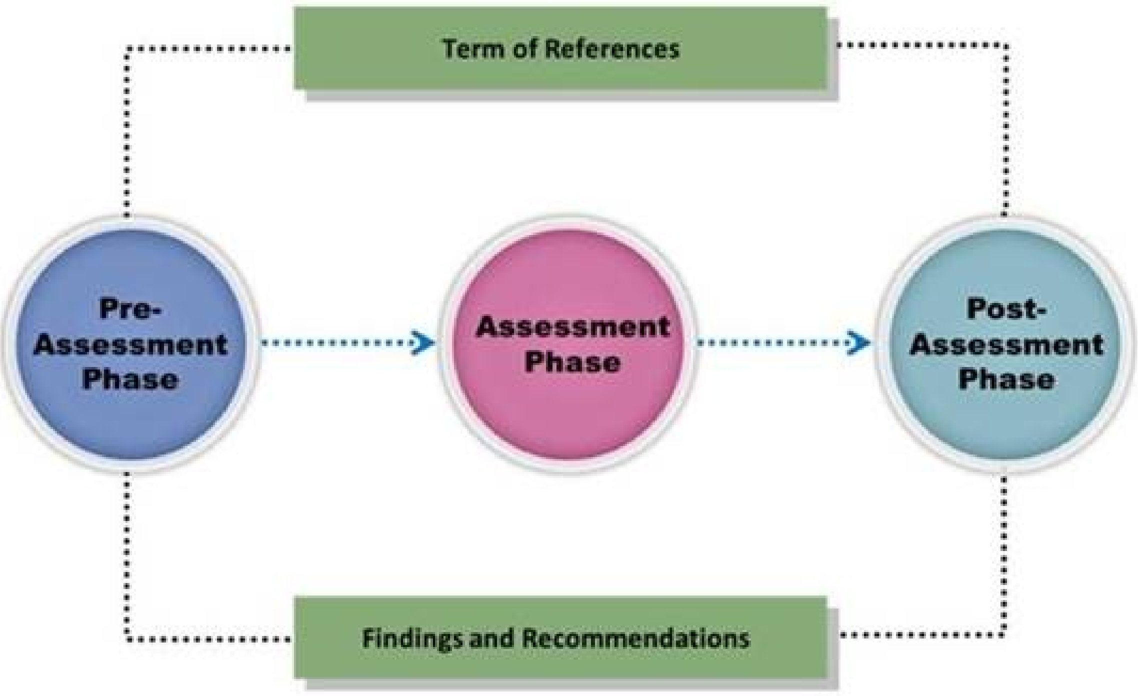
NEW QUESTION 120
This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

A. Blue team
B. Tiger team
C. Gorilla team
D. Lion team

Answer: B

NEW QUESTION 121
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



Term of References

Pre-Assessment Phase

Assessment Phase

Post-Assessment Phase

Findings and Recommendations

What does a vulnerability assessment identify?

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

Answer: B

NEW QUESTION 122
A firewall's decision to forward or reject traffic in network filtering is dependent upon which of the following?

A. Destination address
B. Port numbers
C. Source address
D. Protocol used

Answer: D

Explanation:
Reference: http://www.vicomsoft.com/learning-center/firewalls/ (what does a firewall do)

NEW QUESTION 123
Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

A. Invalid username or password

B. Account username was not found
C. Incorrect password
D. Username or password incorrect

Answer: C

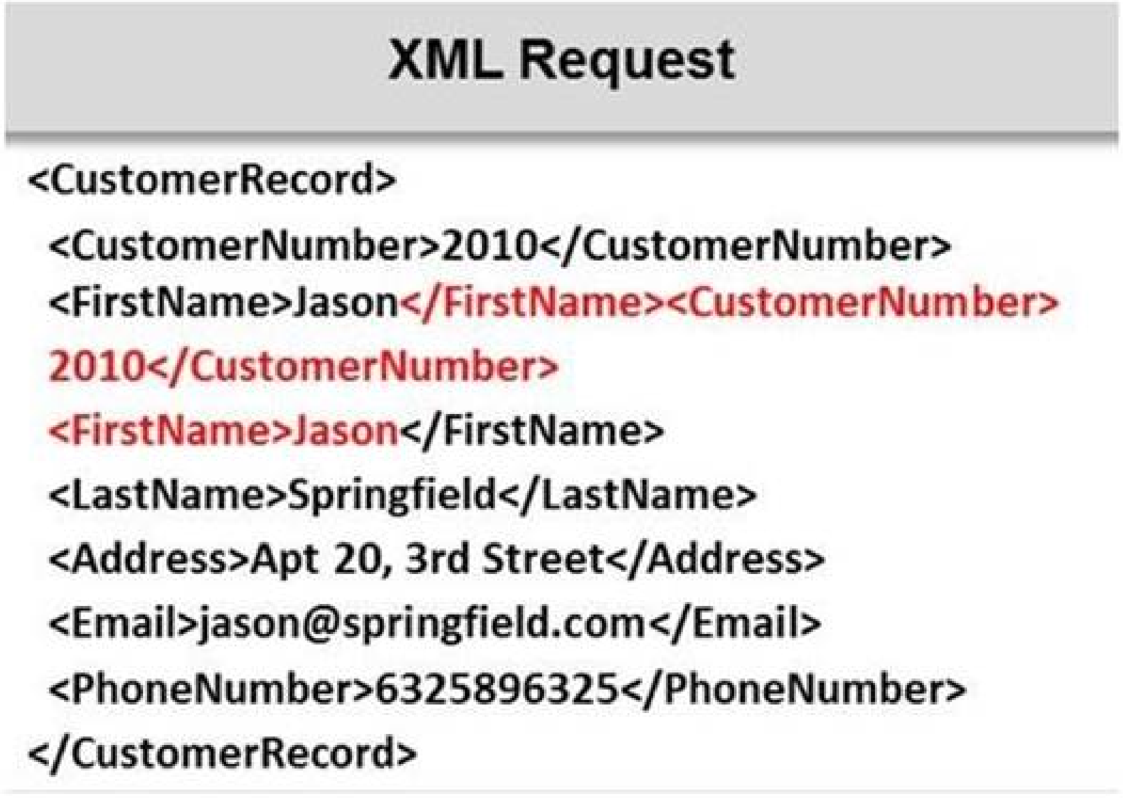
NEW QUESTION 126
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

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 131
Identify the injection attack represented in the diagram below:



XML Request

```
<CustomerRecord>
  <CustomerNumber>2010</CustomerNumber>
  <FirstName>Jason</FirstName><CustomerNumber>
  2010</CustomerNumber>
  <FirstName>Jason</FirstName>
  <LastName>Springfield</LastName>
  <Address>Apt 20, 3rd Street</Address>
  <Email>jason@springfield.com</Email>
  <PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

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

Answer: C

Explanation:
Reference: http://projects.webappsec.org/w/page/13247004/XML%20Injection

NEW QUESTION 136
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 139
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

Explanation:
Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

NEW QUESTION 142
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

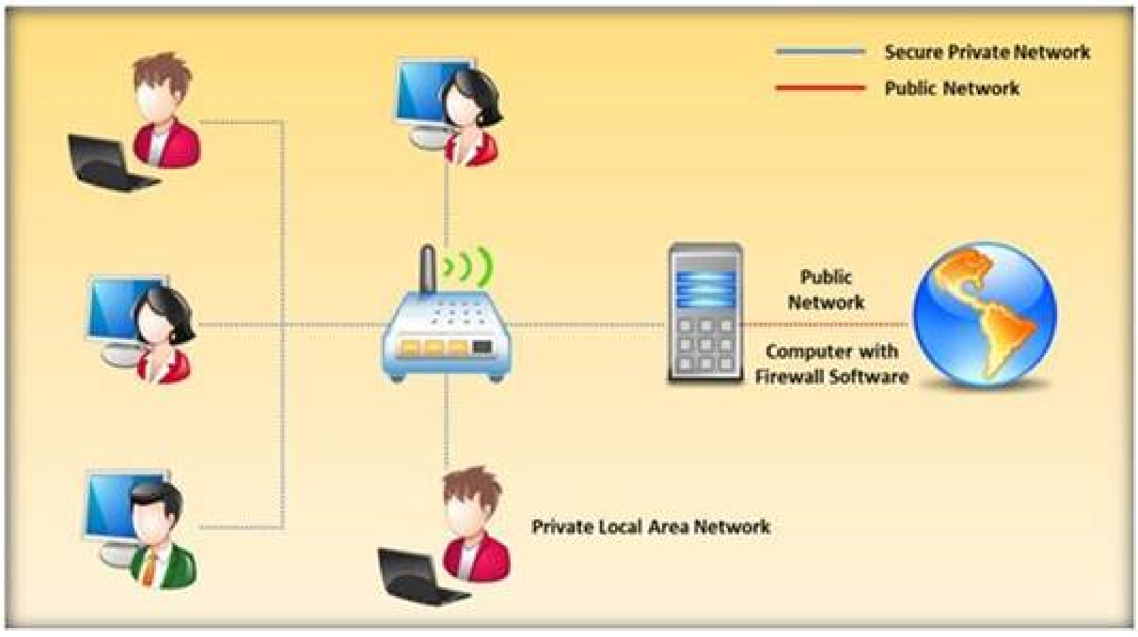
NEW QUESTION 145
Information gathering is performed to:
i) Collect basic information about the target company and its network
ii) Determine the operating system used, platforms running, web server versions, etc.
iii) Find vulnerabilities and exploits

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

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

Answer: D

NEW QUESTION 148
Packet filtering firewalls are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can: i)Drop the packet
ii) Forward it or send a message to the originator



At which level of the OSI model do the packet filtering firewalls work?

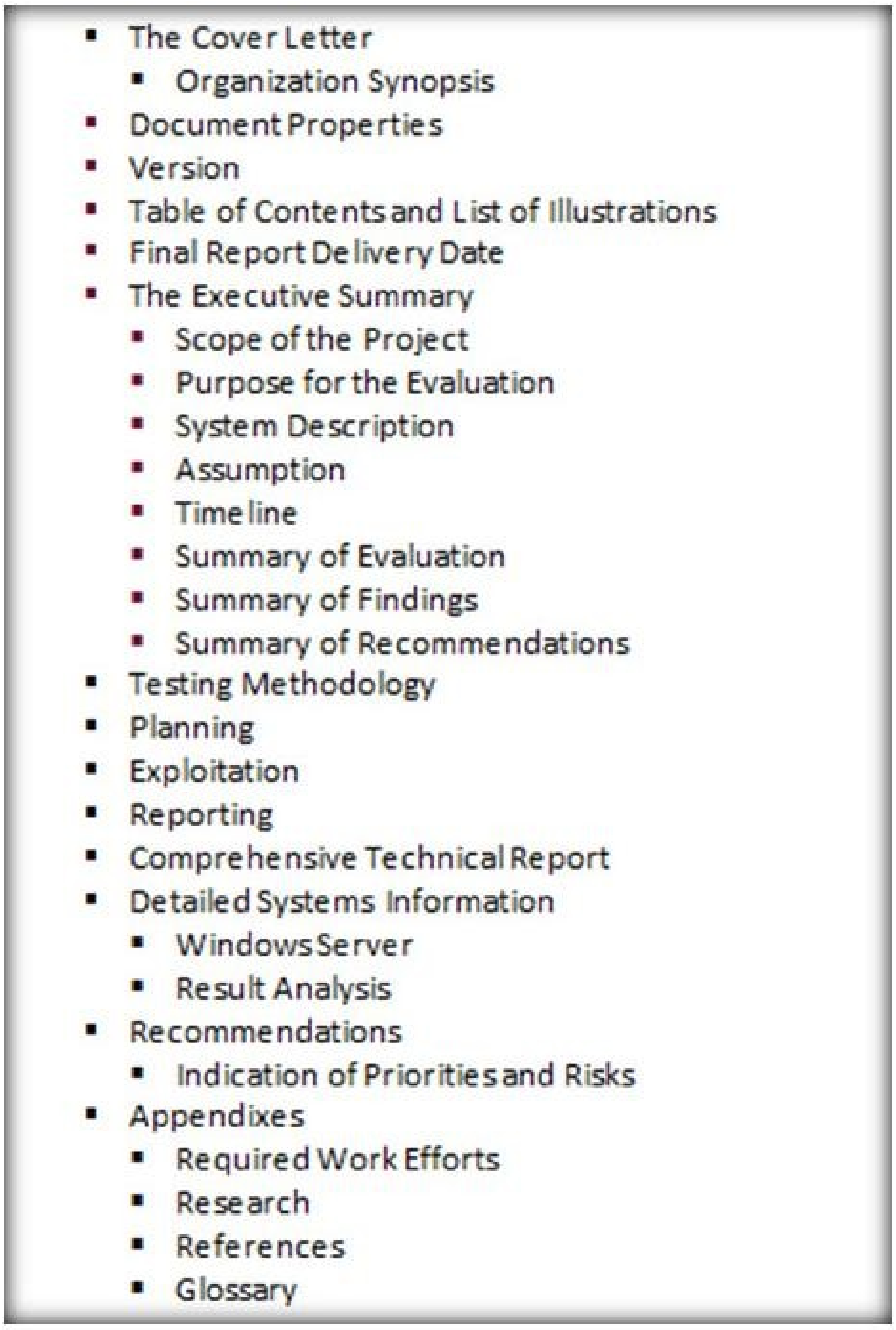
A. Application layer
B. Physical layer
C. Transport layer
D. Network layer

Answer: D

Explanation:

Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=At+which+level+of+the+OSI+model+do+the+packet+filtering+firewalls+work&source=bl&ots=zRrbcmY3pj&sig=I3vuS3VA7r-3VF8lC6xq_c_r31M&hl=en&sa=X&ei=wMcfVMetI8HPaNSRgPgD&ved=0CC8Q6AEwAg#v=onepage&q=At%20which%20level%20of%20the%20OSI%20model%20do%20the%20pa cket%20filtering%20firewalls%20work&f=false (packet filters)

NEW QUESTION 149
What is a goal of the penetration testing report?



- The Cover Letter
  - Organization Synopsis
- Document Properties
- Version
- Table of Contents and List of Illustrations
- Final Report Delivery Date
- The Executive Summary
  - Scope of the Project
  - Purpose for the Evaluation
  - System Description
  - Assumption
  - Time line
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Detailed Systems Information
  - Windows Server
  - Result Analysis
- Recommendations
  - Indication of Priorities and Risks
- Appendixes
  - Required Work Efforts
  - Research
  - References
  - Glossary

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 154
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 155
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 160
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

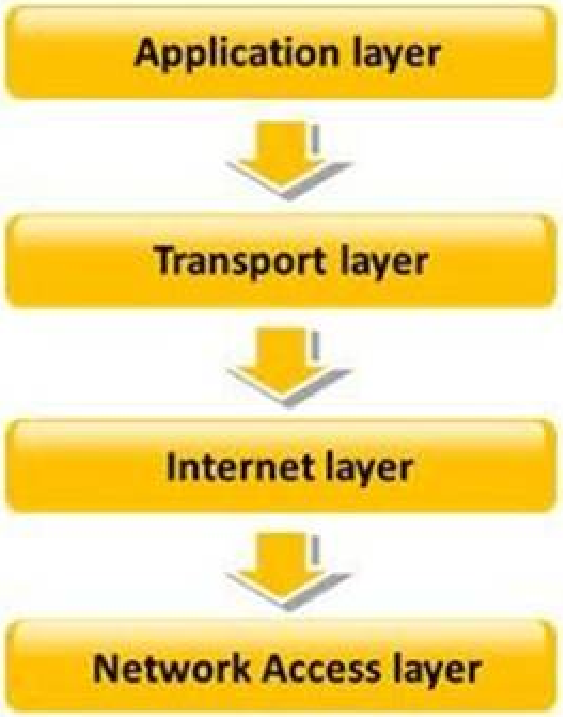
NEW QUESTION 162
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different 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 167
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-

to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer
B. Network Access layer
C. Internet layer
D. Application layer

Answer: C

NEW QUESTION 168
Logs are the record of the system and network activities. Syslog protocol is used for delivering log information across an IP network. Syslog messages can be sent via which one of the following?

A. UDP and TCP
B. TCP and SMTP
C. SMTP
D. UDP and SMTP

Answer: A

NEW QUESTION 169
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 174
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 178
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

Explanation:
Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

NEW QUESTION 183
John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

A. Penetration testing project plan
B. Penetration testing software project management plan
C. Penetration testing project scope report
D. Penetration testing schedule plan

Answer: A

Explanation:
Rfere http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approac h%20of%20the%20project&f=false

NEW QUESTION 184
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

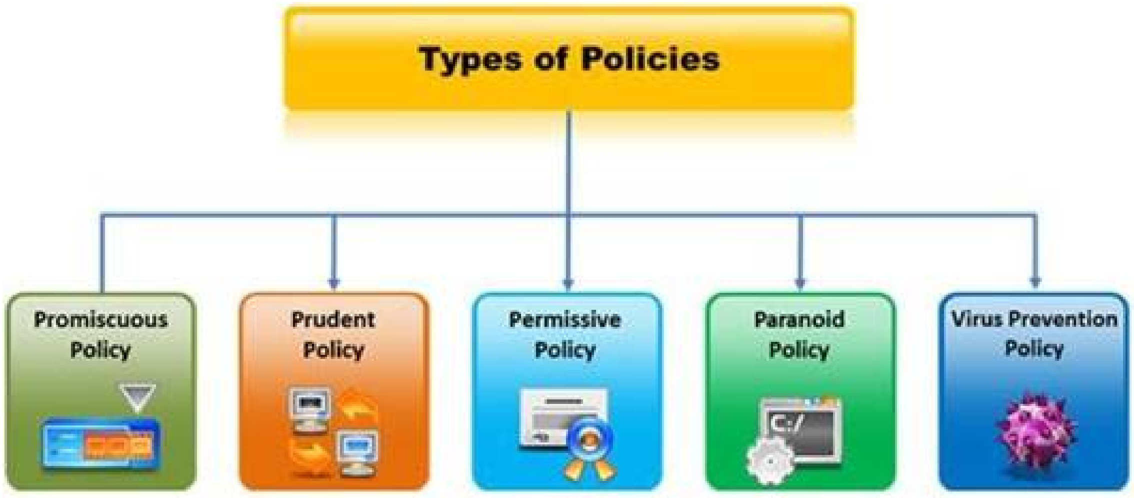
Answer: A

NEW QUESTION 187
How many bits is Source Port Number in TCP Header packet?

A. 48
B. 32
C. 64
D. 16

Answer: D

NEW QUESTION 190
Which type of security policy applies to the below configuration?
i)Provides maximum security while allowing known, but necessary, dangers ii)All services are blocked; nothing is allowed
iii) Safe and necessary services are enabled individually
iv) Non-essential services and procedures that cannot be made safe are NOT allowed v)Everything is logged



A. Paranoid Policy
B. Prudent Policy
C. Permissive Policy
D. Promiscuous Policy

Answer: B

NEW QUESTION 193
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 195
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 196
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls

Answer: D

Explanation:
Reference: http://www.vicomsoft.com/learning-center/firewalls/

NEW QUESTION 197
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 200
Identify the person who will lead the penetration-testing project and be the client point of contact.

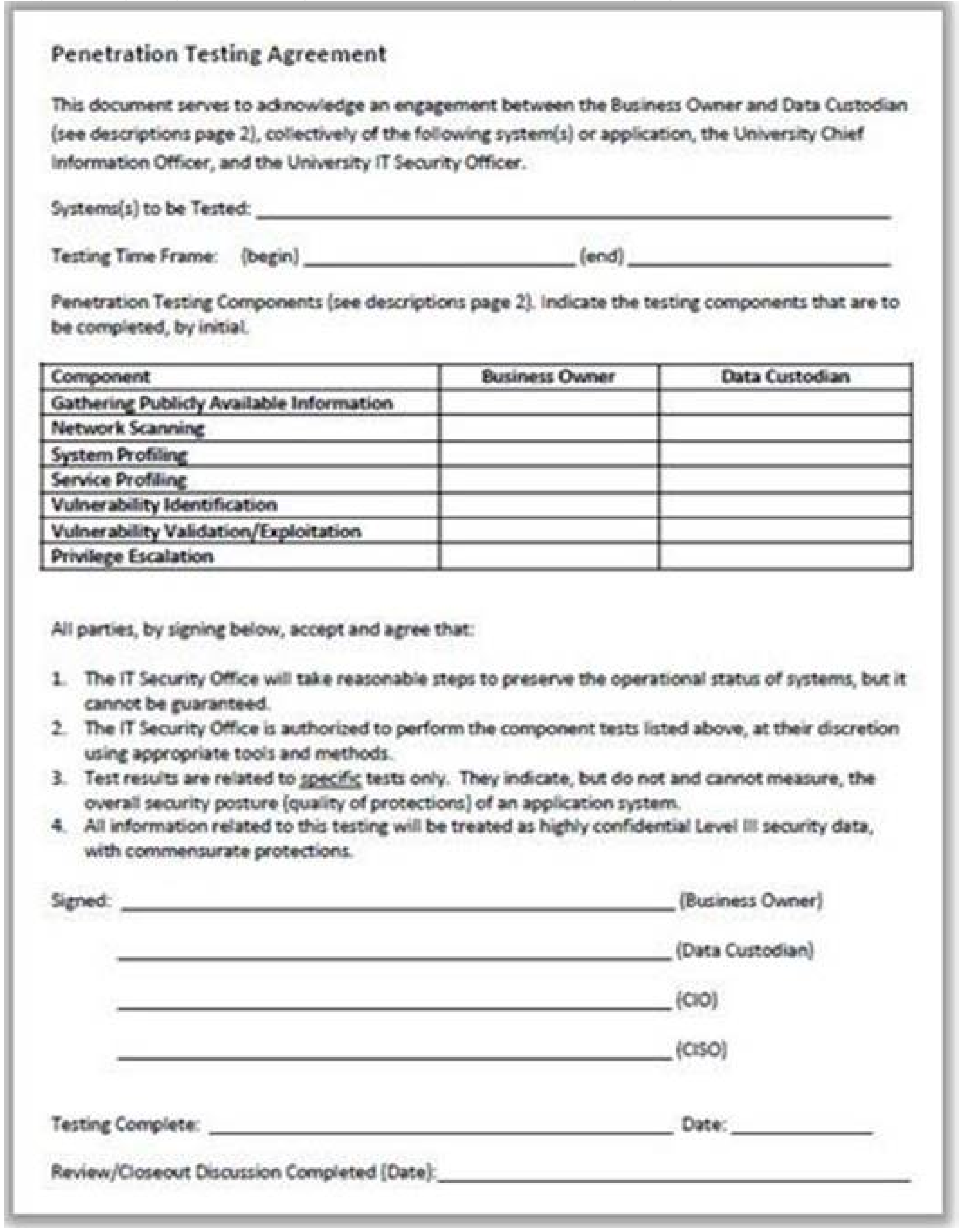
A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester

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 202
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)

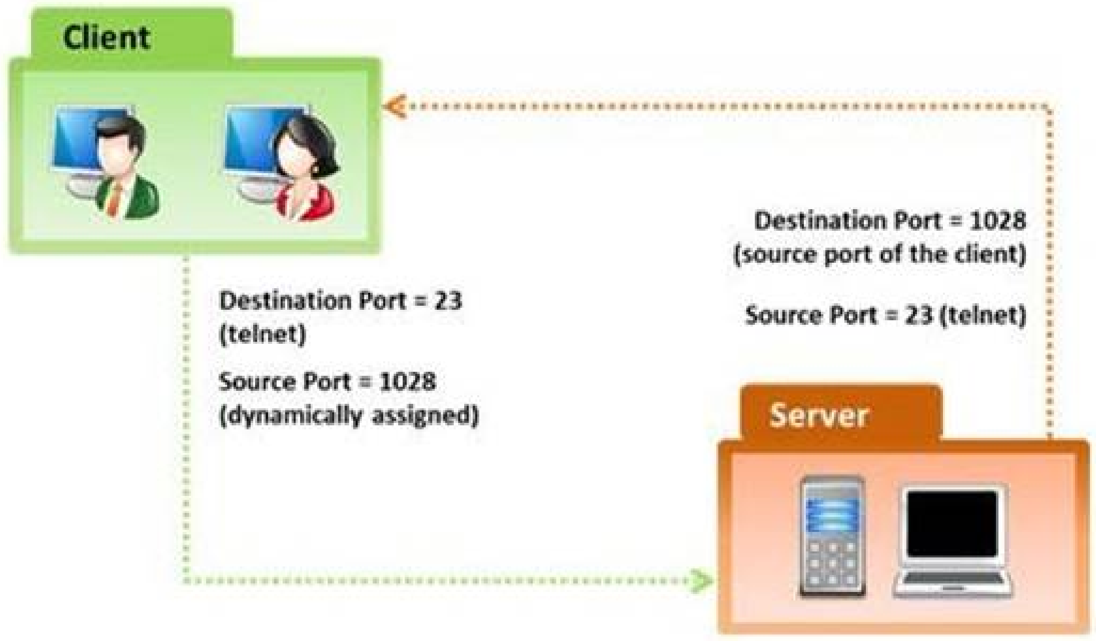
Testing Complete: ____________________ Date: ____________

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 204
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 208
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

Explanation:
Reference: http://www.sec.gov/rules/final/33-8238.htm (see background)

NEW QUESTION 210
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 212
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. The port numbers above 1024 are considered as which one of the following? (Select all that apply)

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

Answer: B

NEW QUESTION 217
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

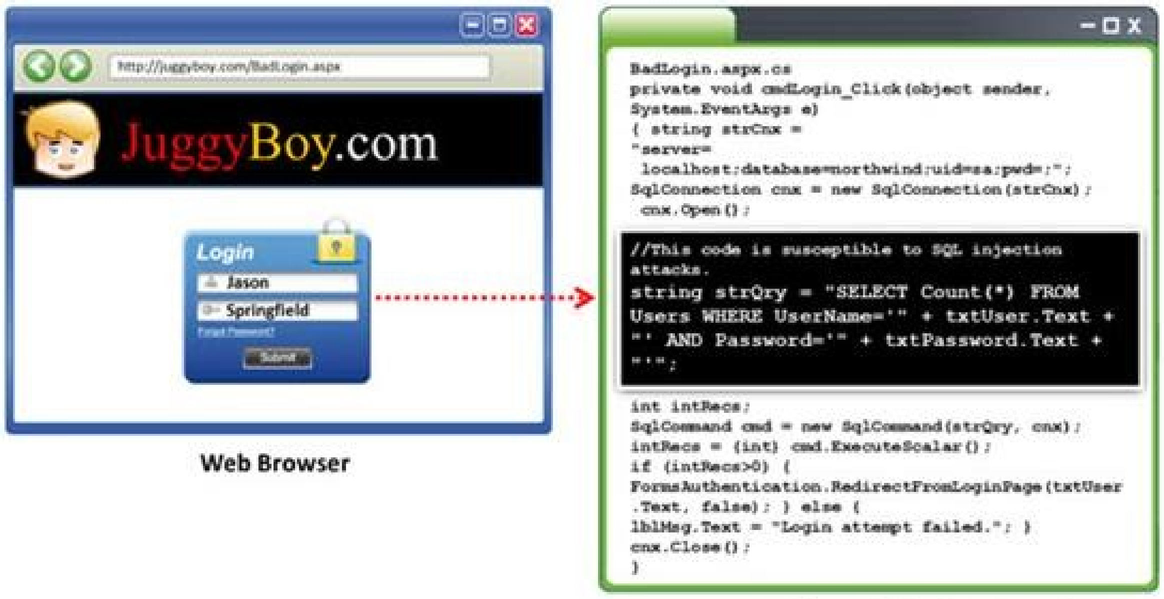
NEW QUESTION 222
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

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

Answer: B

Explanation:
Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

NEW QUESTION 226
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.



```
BadLogin.aspx.cs
private void cmdLogin_Click(object sender,
System.EventArgs e)
{ string strCnx =
"server=
 localhost;database=northwind;uid=sa;pwd=;";
SqlConnection cnx = new SqlConnection(strCnx);
 cnx.Open();
//This code is susceptible to SQL injection
attacks.
string strQry = "SELECT Count(*) FROM
Users WHERE UserName='" + txtUser.Text +
"' AND Password='" + txtPassword.Text +
"'";
int intRecs;
SqlCommand cmd = new SqlCommand(strQry, cnx);
intRecs = (int) cmd.ExecuteScalar();
if (intRecs>0) {
FormsAuthentication.RedirectFromLoginPage(txtUser
.Text, false); } else {
lblMsg.Text = "Login attempt failed."; }
cnx.Close();
}
```

Web Browser

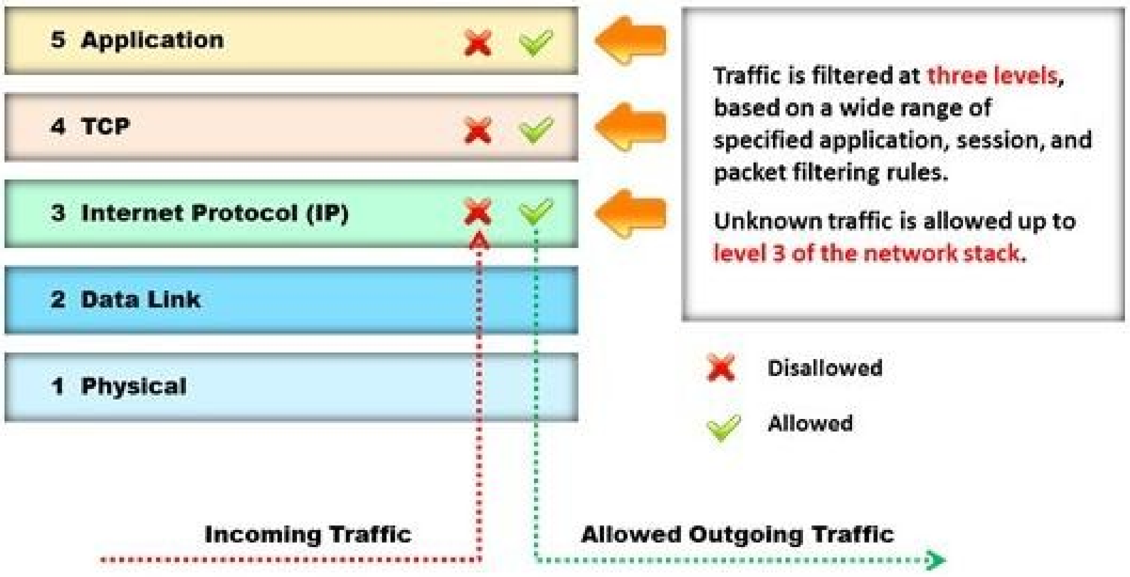
Server Side Code (BadLogin.aspx)

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 227
Identify the type of firewall represented in the diagram below:



Traffic is filtered at three levels, based on a wide range of specified application, session, and packet filtering rules.

Unknown traffic is allowed up to level 3 of the network stack.

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

Answer: A

Explanation:
Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

NEW QUESTION 231
Which of the following attacks is an offline attack?

A. Pre-Computed Hashes
B. Hash Injection Attack
C. Password Guessing
D. Dumpster Diving

Answer: A

Explanation:
Reference: http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html

NEW QUESTION 234
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 235
What are the 6 core concepts in IT security?

A. Server management, website domains, firewalls, IDS, IPS, and auditing
B. Authentication, authorization, confidentiality, integrity, availability, and non-repudiation
C. Passwords, logins, access controls, restricted domains, configurations, and tunnels
D. Biometrics, cloud security, social engineering, DoS attack, viruses, and Trojans

Answer: B

NEW QUESTION 240
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

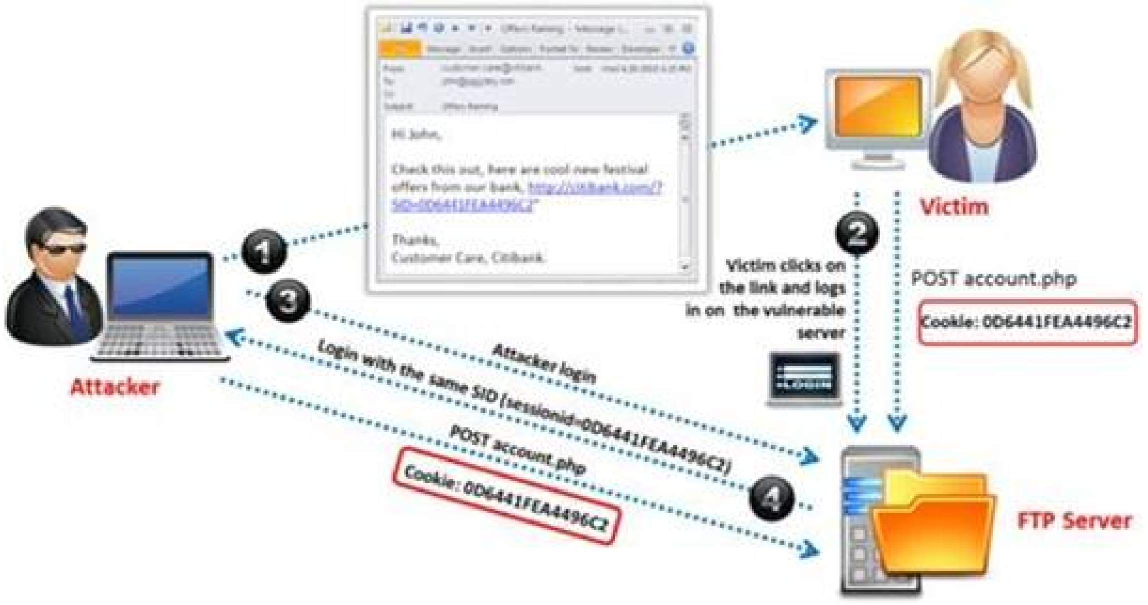
NEW QUESTION 244
Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?

A. Microsoft Baseline Security Analyzer (MBSA)
B. CORE Impact
C. Canvas

D. Network Security Analysis Tool (NSAT)

Answer: C

NEW QUESTION 246
Identify the attack represented in the diagram below:


Hi John,
Check this out, here are cool new festival offers from our bank, http://citiBank.com/?SID=0D6441FEA4496C2"
Thanks,
Customer Care, Citibank.
Victim
2
Victim clicks on the link and logs in on the vulnerable server
POST account.php
Cookie: 0D6441FEA4496C2
1
3
Attacker
Attacker login
Login with the same SID (sessionid=0D6441FEA4496C2)
POST account.php
Cookie: 0D6441FEA4496C2
4
FTP Server

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

Answer: B

Explanation:
Reference: http://en.wikipedia.org/wiki/Session_hijacking

NEW QUESTION 248
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 253
What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of ‘in-depth ethical hacking’
B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
C. Vulnerability testing is more expensive than penetration testing
D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Answer: A

NEW QUESTION 254
Which one of the following components of standard Solaris Syslog is a UNIX command that is used to add single-line entries to the system log?

A. “Logger”
B. ”/etc/syslog.conf”
C. “Syslogd”
D. “Syslogd.conf”

Answer: A

NEW QUESTION 257
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 261
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 264
Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

```
type="color" default="#204063" value="#204063">
<Variable name="blo        cription="Blog Title Color"
type="color"  ult="#eef6fe  e="#eef6fe">
<Variable nam        ription="Blog Description Color"
type="c  stTitleColor" descr  eef6fe">
<Variable n  default="#477fba" val  Post Title Color"
type=        77fba">
<Variable n  lateHeader BUG" descr  "Date Header Color"
type=  default="#8facc8" valu  acc8">
<Variable n  debarHeaderColor" d  on="Sidebar Title Color"
type=        809fbd">
<Variable n  fault="#809fbd" v  ="Link Color"
type=  inkColor" d  ="#4386ce">
        description="Visited Link Color"
        2462a5" value="#2462a5">
        Color" description="Sidebar Link Color"
        599be2" value="#599be2">
        edLinkColor"
        Visited Link Color"
        #3372b6" value="#3372b6">
```

Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

A. Web Penetration Testing
B. Functionality Testing
C. Authorization Testing
D. Source Code Review

Answer: D

NEW QUESTION 265
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 266
......