EC-Council

Exam Questions ECSAv10

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

NEW QUESTION 1
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 2
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

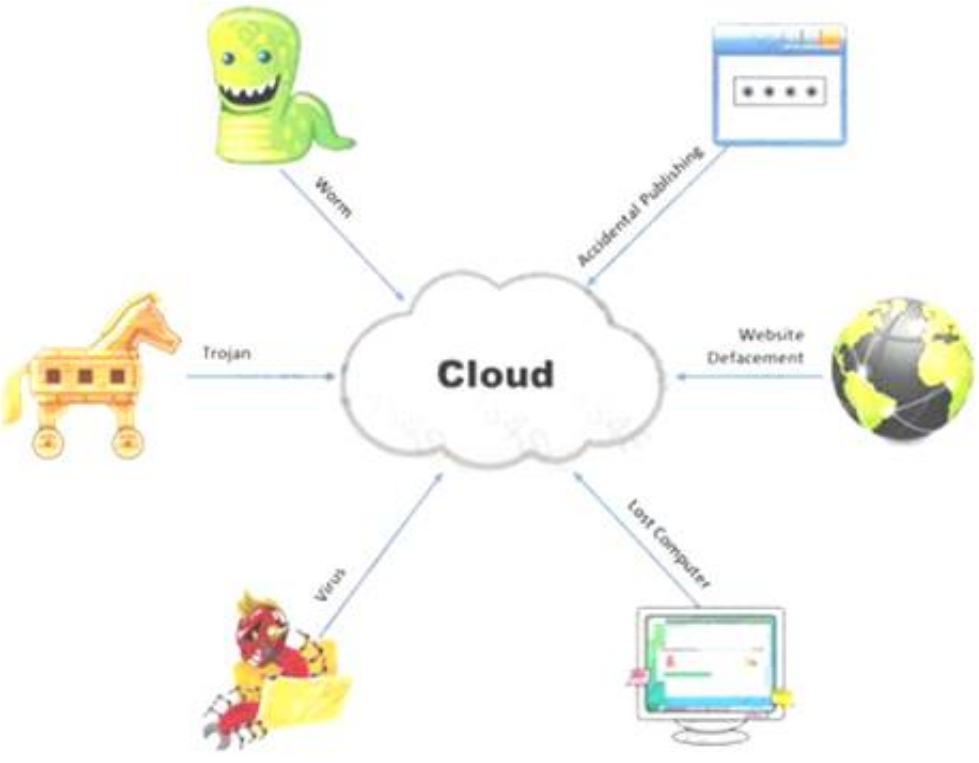
Answer: A

NEW QUESTION 3
Which one of the following acts makes reputational risk of poor security a reality because it requires public disclosure of any security breach that involves personal information if it is unencrypted or if it is reasonably believed that the information has been acquired by an unauthorized person?

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

Answer: A

NEW QUESTION 4
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 5
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

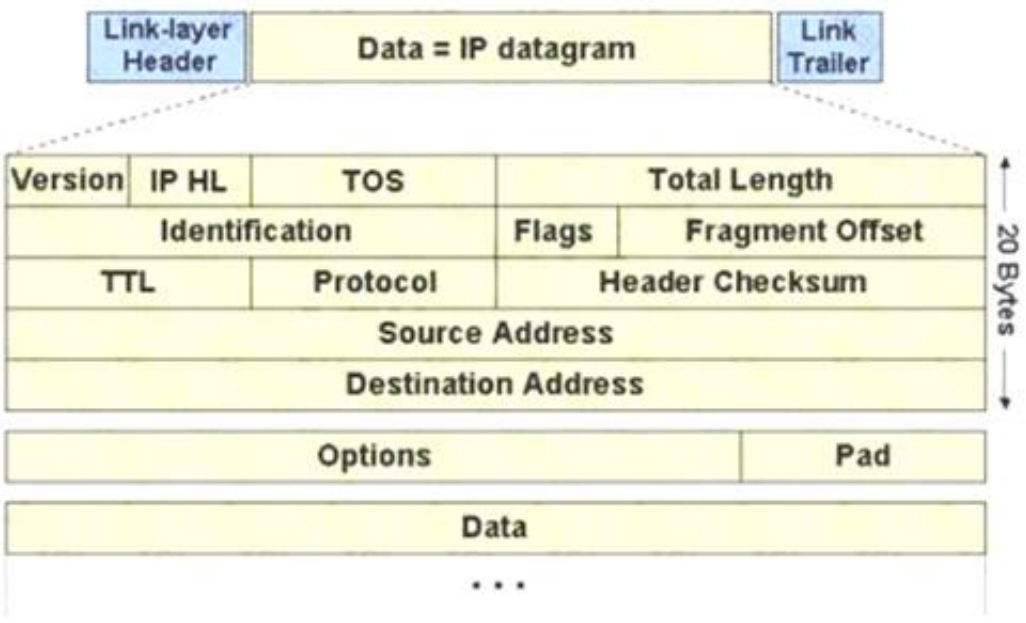
Answer: D

NEW QUESTION 6
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers.
Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal t monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. net port 22
B. udp port 22 and host 172.16.28.1/24
C. src port 22 and dst port 22
D. src port 23 and dst port 23

Answer: C

NEW QUESTION 7
The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.
The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.
IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.



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

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

Answer: C

NEW QUESTION 8
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 9
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

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

Answer: C

NEW QUESTION 10
What is the target host IP in the following command?
C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

A. Firewalk does not scan target hosts
B. 172.16.28.95
C. This command is using FIN packets, which cannot scan target hosts
D. 10.10.150.1

Answer: A

NEW QUESTION 10
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 12
One needs to run “Scan Server Configuration” tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured.
By default, the Nessus daemon listens to connections on which one of the following?

A. Localhost (127.0.0.1) and port 1241
B. Localhost (127.0.0.1) and port 1240
C. Localhost (127.0.0.1) and port 1246
D. Localhost (127.0.0.0) and port 1243

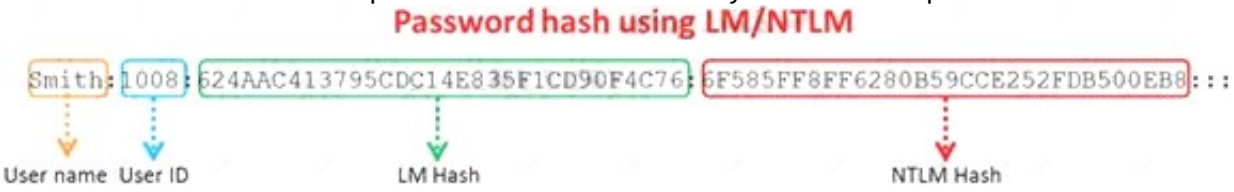
Answer: A

NEW QUESTION 15
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 16
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.



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: D

NEW QUESTION 21
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Answer: D

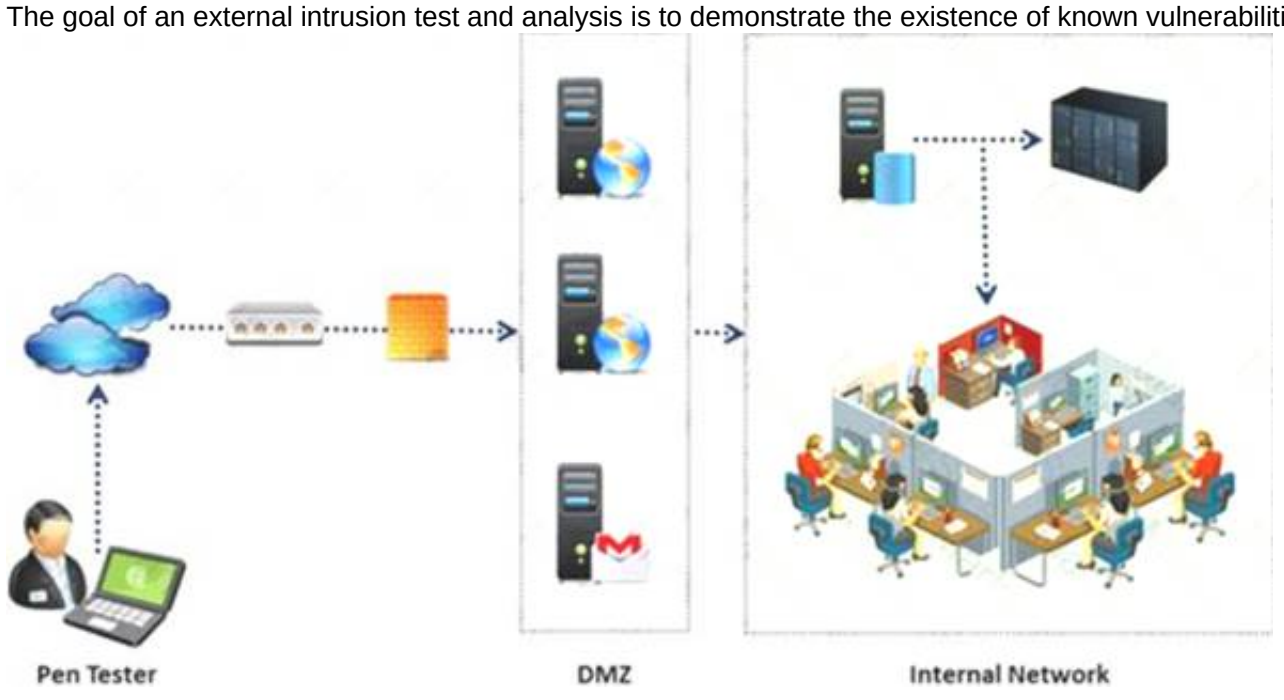
NEW QUESTION 24
Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

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

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

Answer: B

NEW QUESTION 29
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.



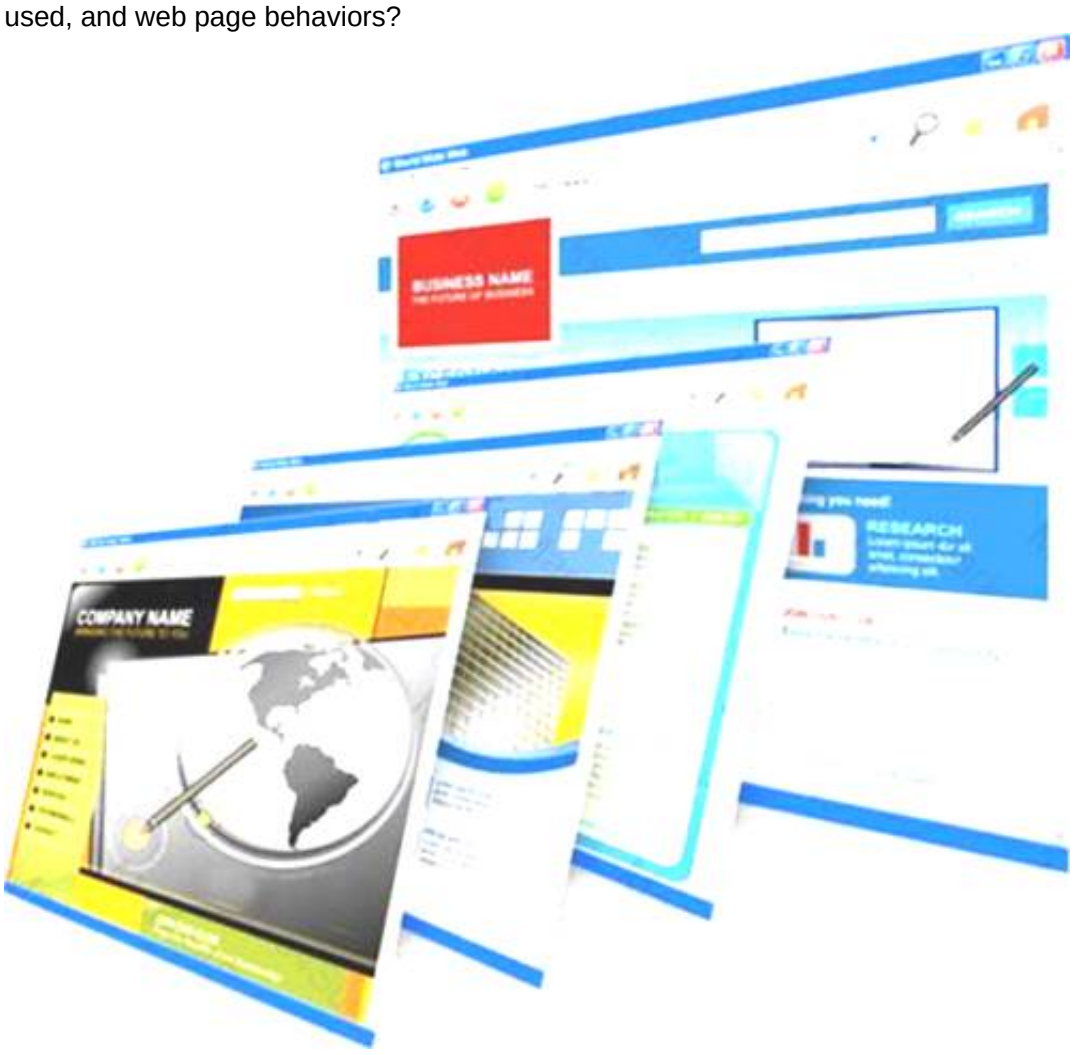
During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

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

Answer: B

NEW QUESTION 32
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption

used, and web page behaviors?



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

Answer: C

NEW QUESTION 33
The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

A. HIPAA
B. Sarbanes-Oxley 2002
C. Gramm-Leach-Bliley Act
D. California SB 1386a

Answer: C

NEW QUESTION 35
Identify the port numbers used by POP3 and POP3S protocols.

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

Answer: C

NEW QUESTION 37
One of the steps in information gathering is to run searches on a company using complex keywords in Google.

Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?

A. ROCHESTON fileformat:+ppt
B. ROCHESTON ppt:filestring
C. ROCHESTON filetype:ppt
D. ROCHESTON +ppt:filesearch

Answer: C

NEW QUESTION 40
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 44
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 48
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 49
Which of the following methods is used to perform server discovery?

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

Answer: B

NEW QUESTION 54
Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing
B. Double Blind Testing
C. Announced Testing
D. Blind Testing

Answer: B

NEW QUESTION 59
Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

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

Answer: B

NEW QUESTION 60
Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement
B. Rules of Behavior Agreement
C. Liability Insurance
D. Non-Disclosure Agreement

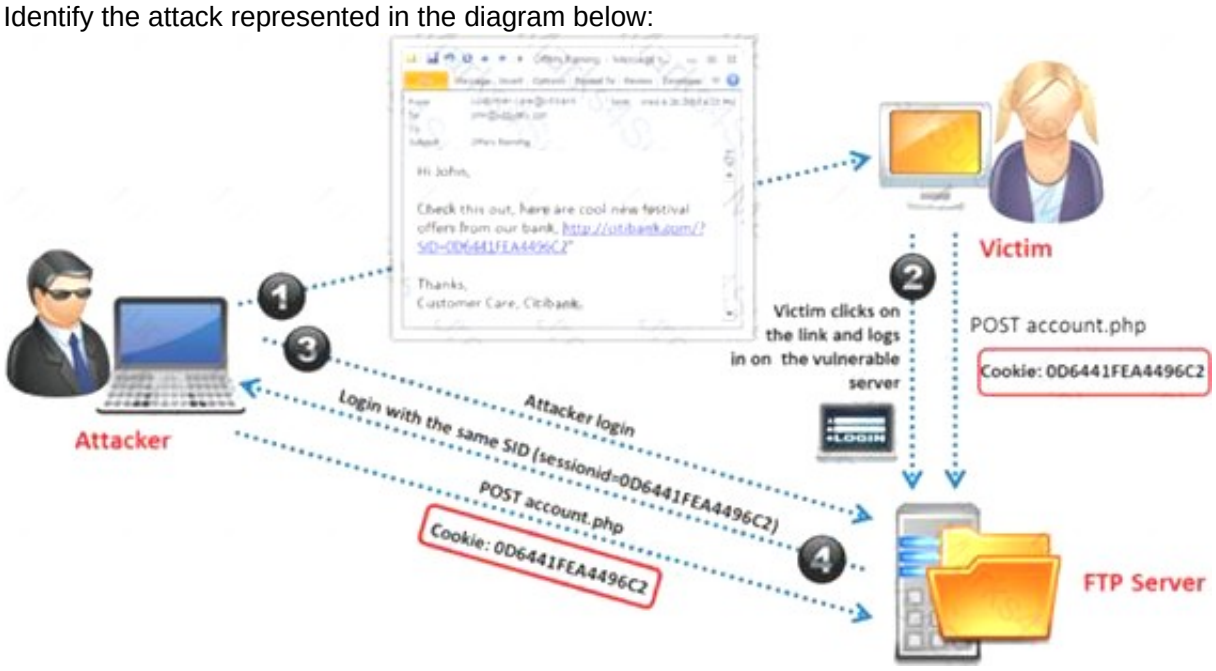
Answer: D

NEW QUESTION 61
Which of the following defines the details of services to be provided for the client's organization and the list of services required for performing the test in the organization?

A. Draft
B. Report
C. Requirement list
D. Quotation

Answer: D

NEW QUESTION 64
Identify the attack represented in the diagram below:



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

Answer: B

NEW QUESTION 67
What does ICMP Type 3/Code 13 mean?

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

Answer: D

NEW QUESTION 70
A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase
B. Pre-attack phase and attack phase
C. Attack phase
D. Pre-attack phase

Answer: D

NEW QUESTION 73
In Linux, what is the smallest possible shellcode?

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

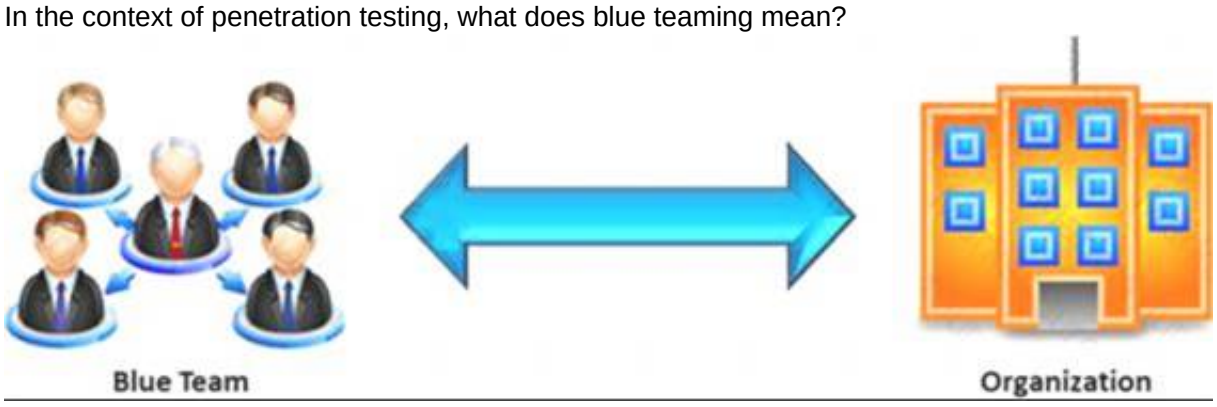
Answer: D

NEW QUESTION 75
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

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

Answer: D

NEW QUESTION 76
In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization's IT staff
B. It is the most expensive and most widely used
C. It may be conducted with or without warning
D. A penetration test performed without the knowledge of the organization's IT staff but with permission from upper management

Answer: A

NEW QUESTION 81
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

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

D. HTML Configuration Arbitrary Administrative Access Vulnerability

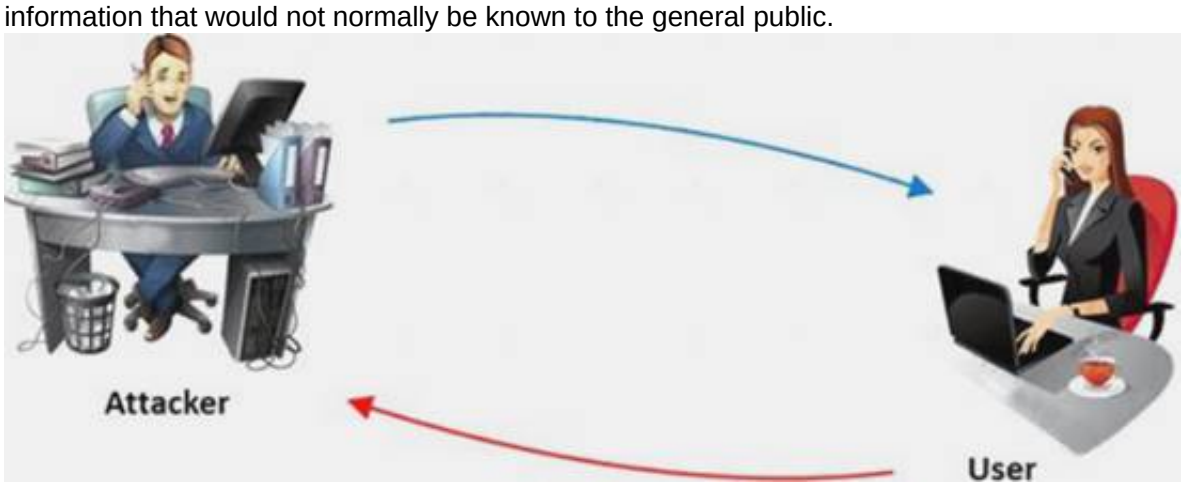
Answer: C

NEW QUESTION 82
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

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

Answer: D

NEW QUESTION 87
The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing
B. Spoofing
C. Tapping
D. Vishing

Answer: D

NEW QUESTION 89
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 93
Metasploit framework in an open source platform for vulnerability research, development, and penetration testing. Which one of the following metasploit options is used to exploit multiple systems at once?

A. NinjaDontKill
B. NinjaHost
C. RandomNops
D. EnablePython

Answer: A

NEW QUESTION 97
SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. A successful SQL injection attack can:
i) Read sensitive data from the database
iii) Modify database data (insert/update/delete)
iii) Execute administration operations on the database (such as shutdown the DBMS)
iV) Recover the content of a given file existing on the DBMS file system or write files into the file system
v) Issue commands to the operating system

Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.
In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing
B. Function Testing
C. Dynamic Testing
D. Static Testing

Answer: D

NEW QUESTION 98
You are assisting a Department of Defense contract company to become compliant with the stringent
security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers.
What type of firewall must you implement to abide by this policy?

A. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Statefull firewall

Answer: D

NEW QUESTION 103
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address.
Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. A switched network will not respond to packets sent to the broadcast address
B. Only IBM AS/400 will reply to this scan
C. Only Unix and Unix-like systems will reply to this scan
D. Only Windows systems will reply to this scan

Answer: C

NEW QUESTION 108
Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

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

Answer: B

NEW QUESTION 110
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 112
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Avoid cross talk
B. Avoid over-saturation of wireless signals
C. So that the access points will work on different frequencies

D. Multiple access points can be set up on the same channel without any issues

Answer: A

NEW QUESTION 117
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London.
After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

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

Answer: C

NEW QUESTION 119
War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks.
Which one of the following is a Linux based program that exploits the weak IV (Initialization Vector) problem documented with static WEP?

A. Airsnort
B. Aircrack
C. WEPCrack
D. Airpwn

Answer: A

NEW QUESTION 120
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 125
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.

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

Answer: C

NEW QUESTION 129
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

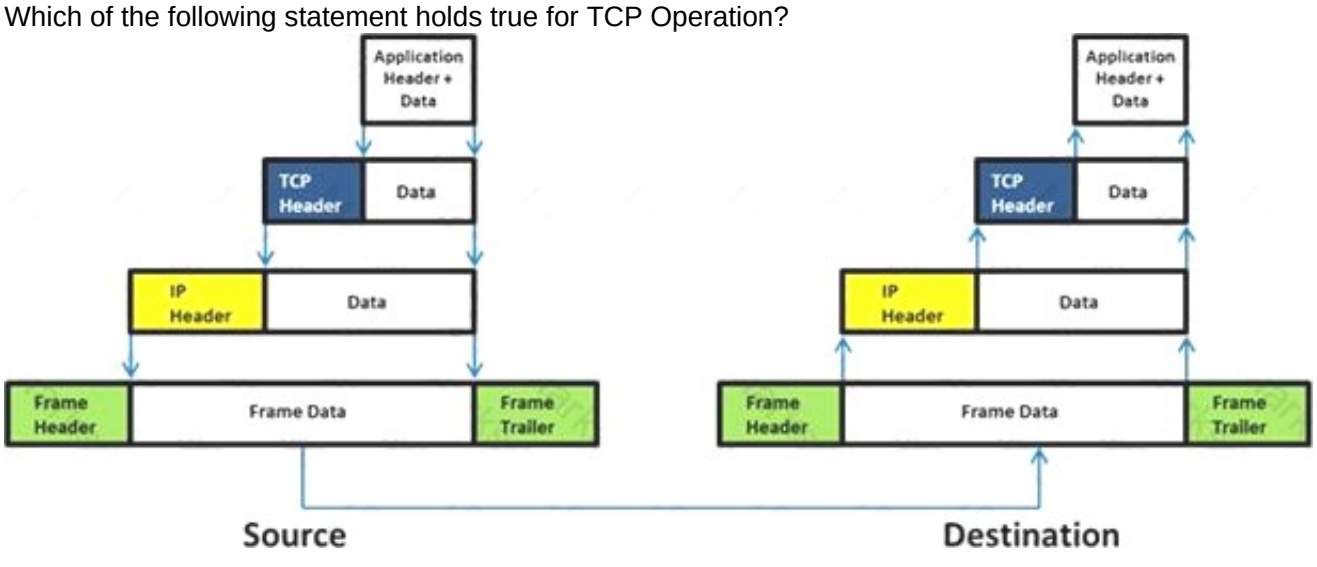
Answer: C

NEW QUESTION 130
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 133
Which of the following statement holds true for TCP Operation?



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

Answer: D

NEW QUESTION 135
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs.
He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. CVE
B. IANA
C. RIPE
D. APIPA

Answer: A

NEW QUESTION 138
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 143
What will the following URL produce in an unpatched IIS Web Server?
http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

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

Answer: D

NEW QUESTION 147
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 149
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)

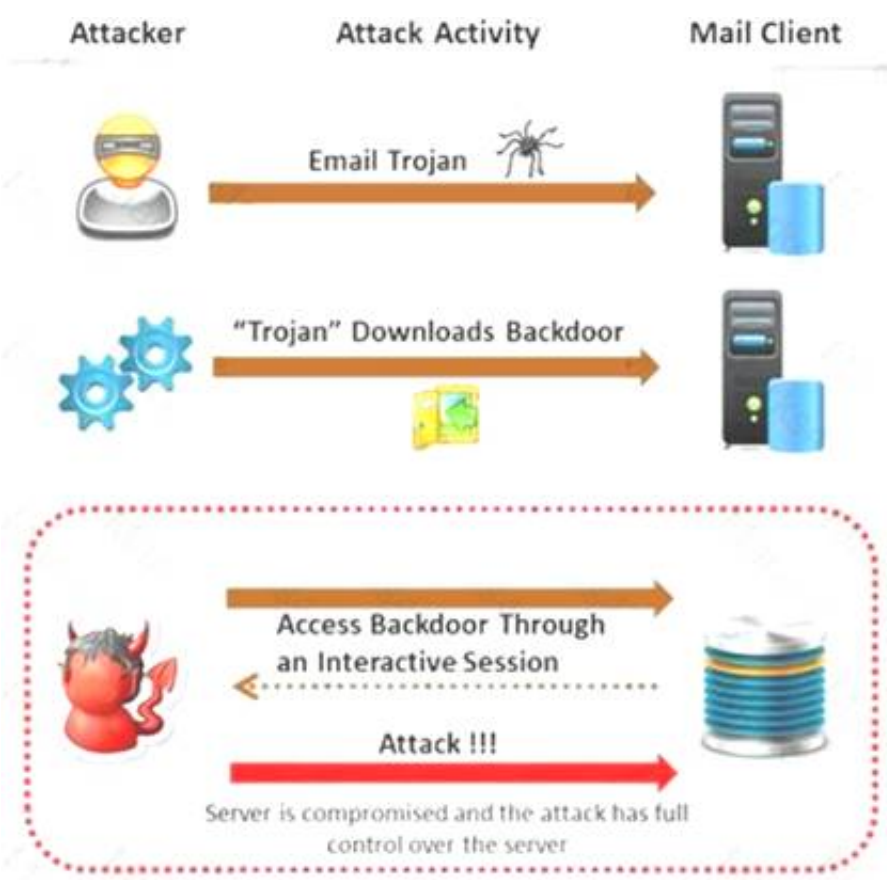
Answer: A

NEW QUESTION 150
NTP protocol is used to synchronize the system clocks of computers with a remote time server or time source over a network. Which one of the following ports is used by NTP as its transport layer?

A. TCP port 152
B. UDP port 177
C. UDP port 123
D. TCP port 113

Answer: C

NEW QUESTION 155
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.



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

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

Answer: D

NEW QUESTION 159
How many bits is Source Port Number in TCP Header packet?

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

Answer: D

NEW QUESTION 161
What is a good security method to prevent unauthorized users from "tailgating"?

A. Electronic key systems
B. Man trap
C. Pick-resistant locks
D. Electronic combination locks

Answer: B

NEW QUESTION 164
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 165
Mason is footprinting an organization to gather competitive intelligence. He visits the company's website for contact information and telephone numbers but does not find any. He knows the entire staff directory was listed on their website 12 months. How can he find the directory?

A. Visit Google’s search engine and view the cached copy
B. Crawl and download the entire website using the Surfoffline tool and save them to his computer
C. Visit the company's partners’ and customers' website for this information
D. Use Way Back Machine in Archive.org web site to retrieve the Internet archive

Answer: D

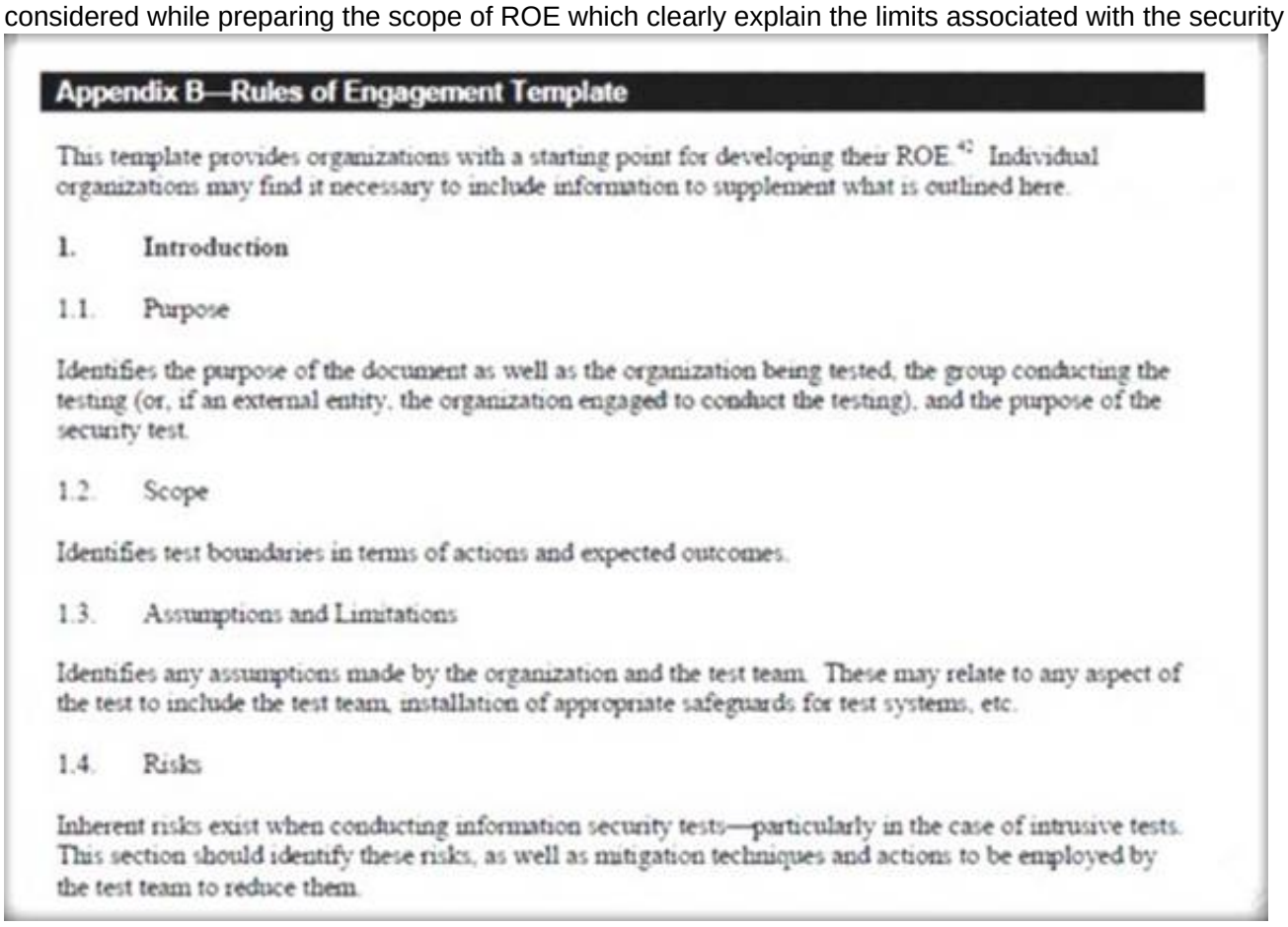
NEW QUESTION 167
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a

browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Answer: A

NEW QUESTION 169
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 173
What is the following command trying to accomplish?
C:\> nmap -sU -p445 192.168.0.0/24

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

Answer: C

NEW QUESTION 174
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)

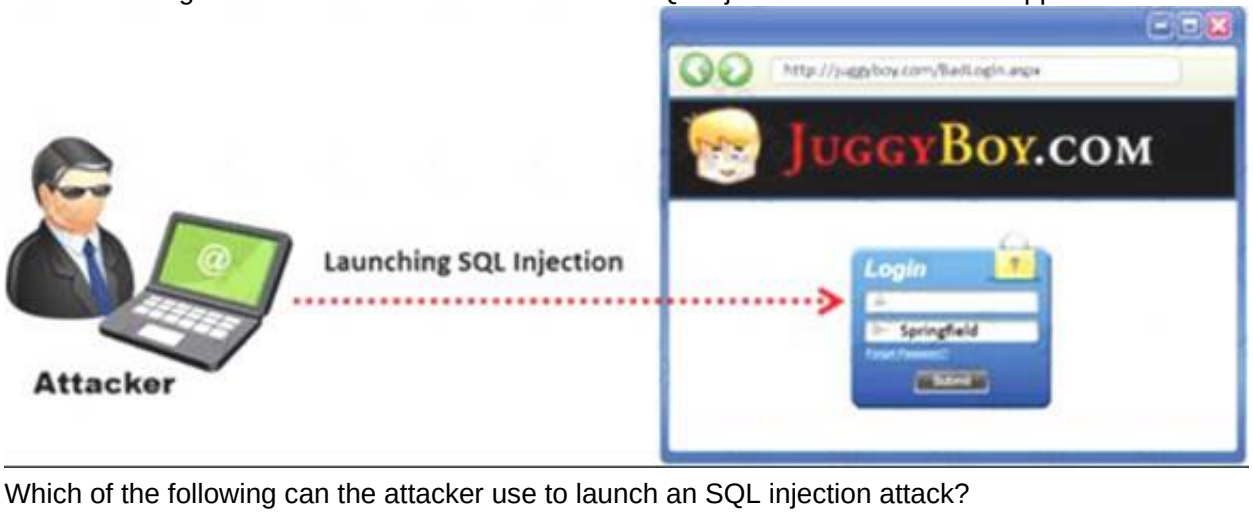
Answer: C

NEW QUESTION 178
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

NEW QUESTION 183
SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type.
This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database.
The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

A. Blah' "2=2 –"
B. Blah' and 2=2 -
C. Blah' and 1=1 -
D. Blah' or 1=1 -

Answer: D

NEW QUESTION 188
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 192
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

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

Answer: C

NEW QUESTION 194
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast.
On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently.
What could be Tyler issue with his home wireless network?

A. 2.4 Ghz Cordless phones
B. Satellite television
C. CB radio
D. Computers on his wired network

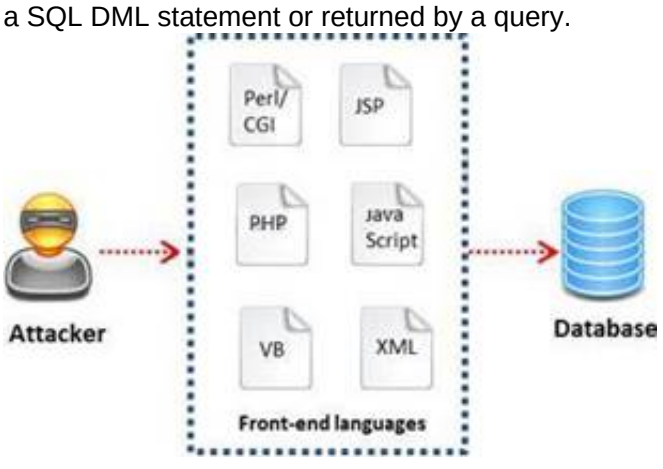
Answer: A

NEW QUESTION 198
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 201
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 204
HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

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

Answer: D

NEW QUESTION 206
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 210
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 213
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies.
In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks
B. Service Level Configuration Attacks
C. Inside Attacks
D. URL Tampering Attacks

Answer: A

NEW QUESTION 218
What are the security risks of running a "repair" installation for Windows XP?

A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. Pressing Shift+F10 gives the user administrative rights

Answer: D

NEW QUESTION 222
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

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

D. Tree-based Assessment

Answer: A

NEW QUESTION 225

.....

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

ECSAv10 Practice Exam Features:

* ECSAv10 Questions and Answers Updated Frequently

* ECSAv10 Practice Questions Verified by Expert Senior Certified Staff

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

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