ECCouncil

Exam ECSAv8

EC-Council Certified Security Analyst (ECSA)

Version: 10.3

[Total Questions: 200]

Question No : 1

Which one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

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

Answer: C

Question No : 2

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?

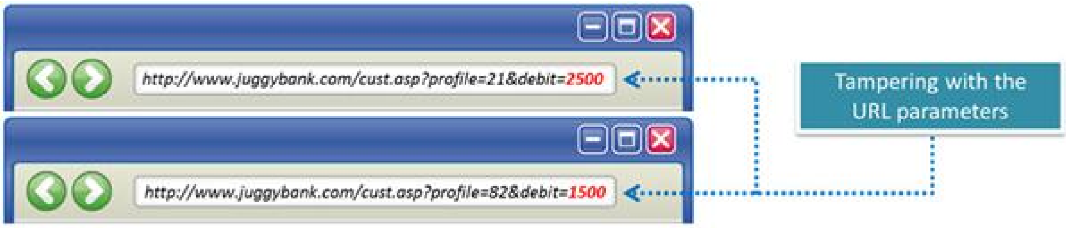
A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Answer: D

Question No : 3

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

Question No : 4

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

Question No : 5

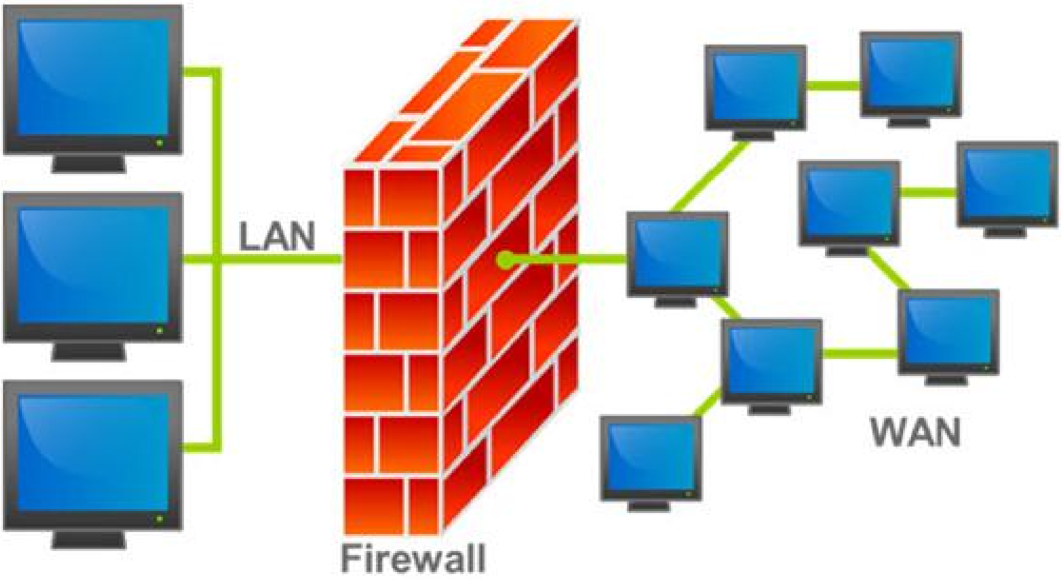
Metasploit framework in an open source platform for vulnerability research, development, and penetration testing. Which one of the following metasploit options is used to exploit multiple systems at once?

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

Answer: A

Question No : 6

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.



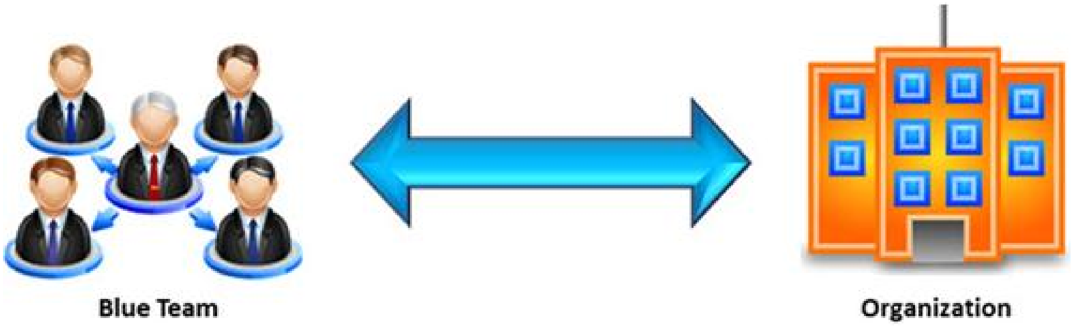
Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

A. Appliance based firewalls cannot be upgraded
B. Firewalls implemented on a hardware firewall are highly scalable
C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system
D. Operating system firewalls are highly configured

Answer: C

Question No : 7

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
Reference: https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/

Question No : 8

Which of the following will not handle routing protocols properly?

A. “Internet-router-firewall-net architecture”
B. “Internet-firewall-router-net architecture”
C. “Internet-firewall -net architecture”
D. “Internet-firewall/router(edge device)-net architecture”

Answer: B

Question No : 9

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

Question No : 10

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

Question No : 11

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
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based

assessment technology, second para)

Question No : 12

Which of the following password cracking techniques is used when the attacker has some information about the password?

A. Hybrid Attack
B. Dictionary Attack
C. Syllable Attack
D. Rule-based Attack

Answer: D

Reference:
http://202.154.59.182/mfile/files/Information%20System/Computer%20Forensics%3B%20Hard%20Disk%20and%20Operating%20Systems/CHAPTER%207%20Application%20Password%20Crackers.pdf (page 4, rule-based attack)

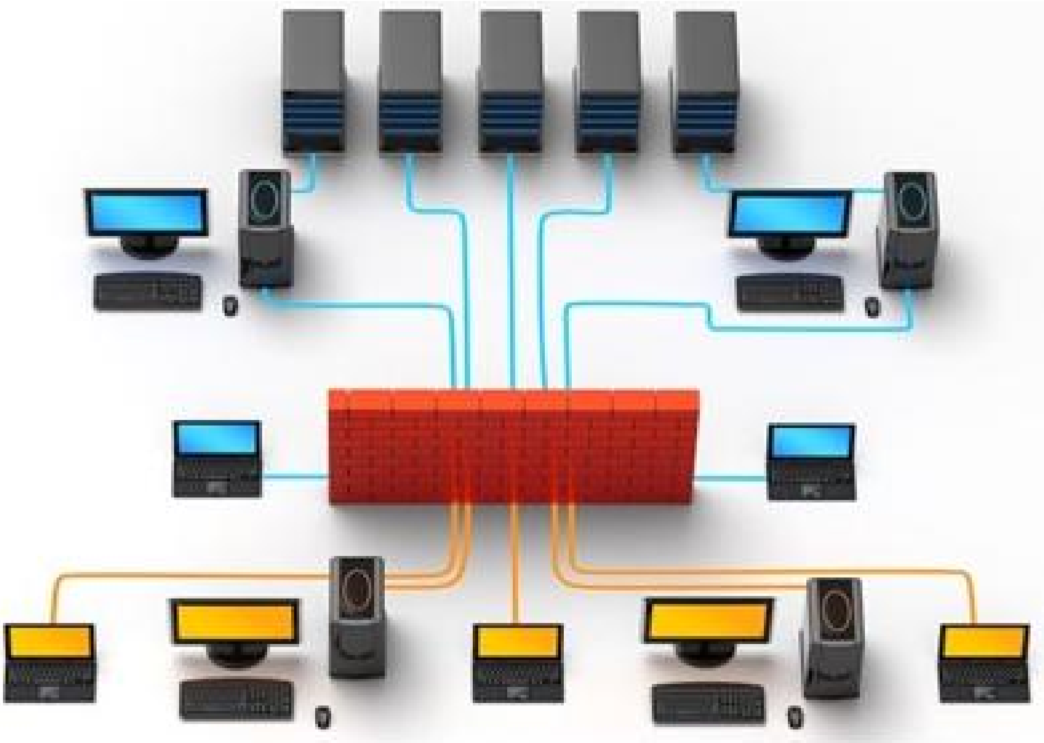
Question No : 13

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

Question No : 14

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

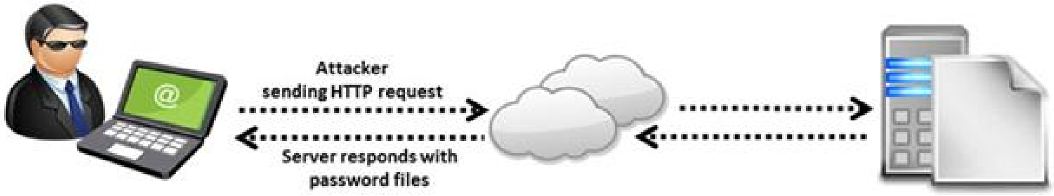
A. DNSSEC
B. Firewall
C. Packet filtering
D. IPSec

Answer: A
Reference: http://tools.ietf.org/html/draft-osterweil-dane-ipsec-01 (abstract, first para)

Question No : 15

A directory traversal (or path traversal) consists in exploiting insufficient security validation/sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs.

The goal of this attack is to order an application to access a computer file that is not intended to be accessible. This attack exploits a lack of security (the software is acting exactly as it is supposed to) as opposed to exploiting a bug in the code.


Attacker sending HTTP request
Server responds with password files

To perform a directory traversal attack, which sequence does a pen tester need to follow to manipulate variables of reference files?

A. dot-dot-slash (../) sequence
B. Denial-of-Service sequence
C. Brute force sequence
D. SQL Injection sequence

Answer: A
Reference:
https://www.cs.ucsb.edu/~vigna/publications/2010_doupe_cova_vigna_dimva10.pdf (pae 7, directory traversal)

Question No : 16

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

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

Answer: A

Question No : 17

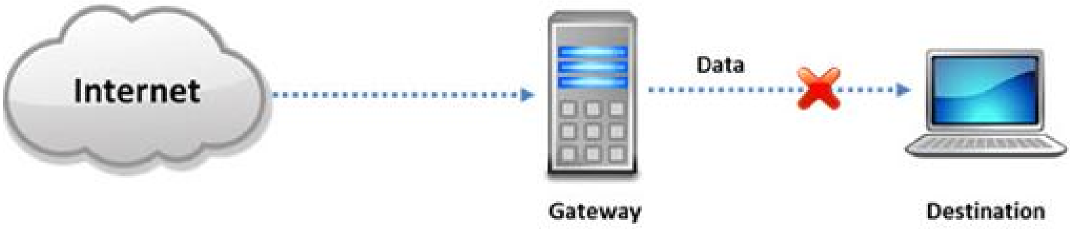
You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

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

Question No : 18

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



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

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

Answer: D

Question No : 19

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

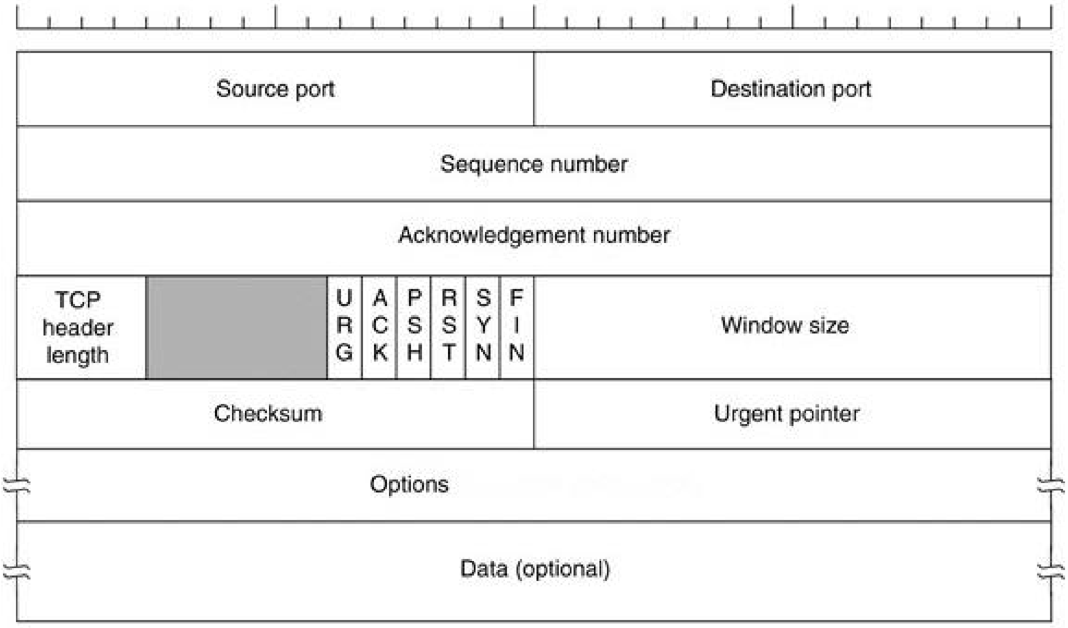
Question No : 20

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

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

Question No : 21

Which of the following is not the SQL injection attack character?

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

Answer: A

Question No : 22

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.

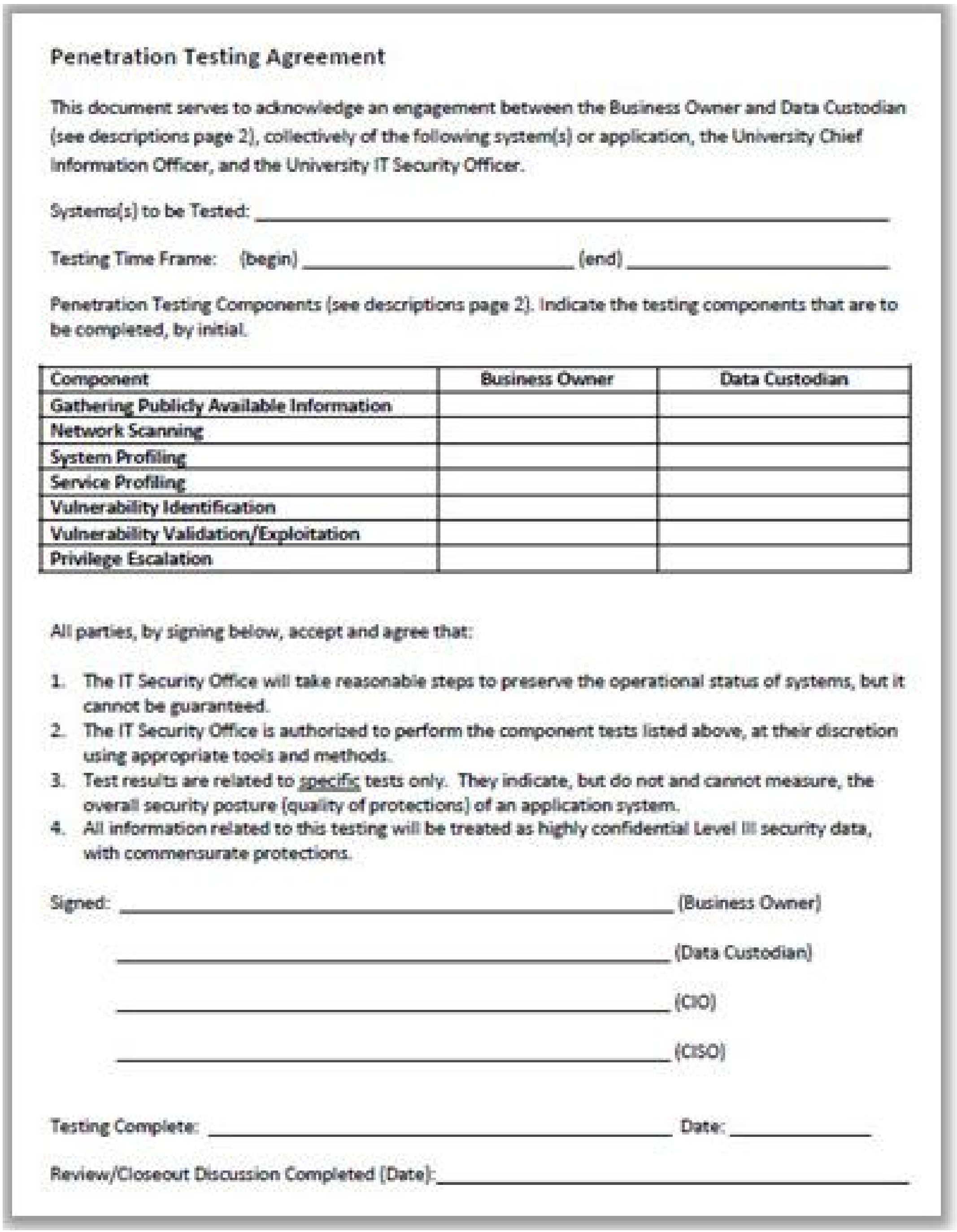
Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

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

Answer: D

Question No : 23

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: ____________

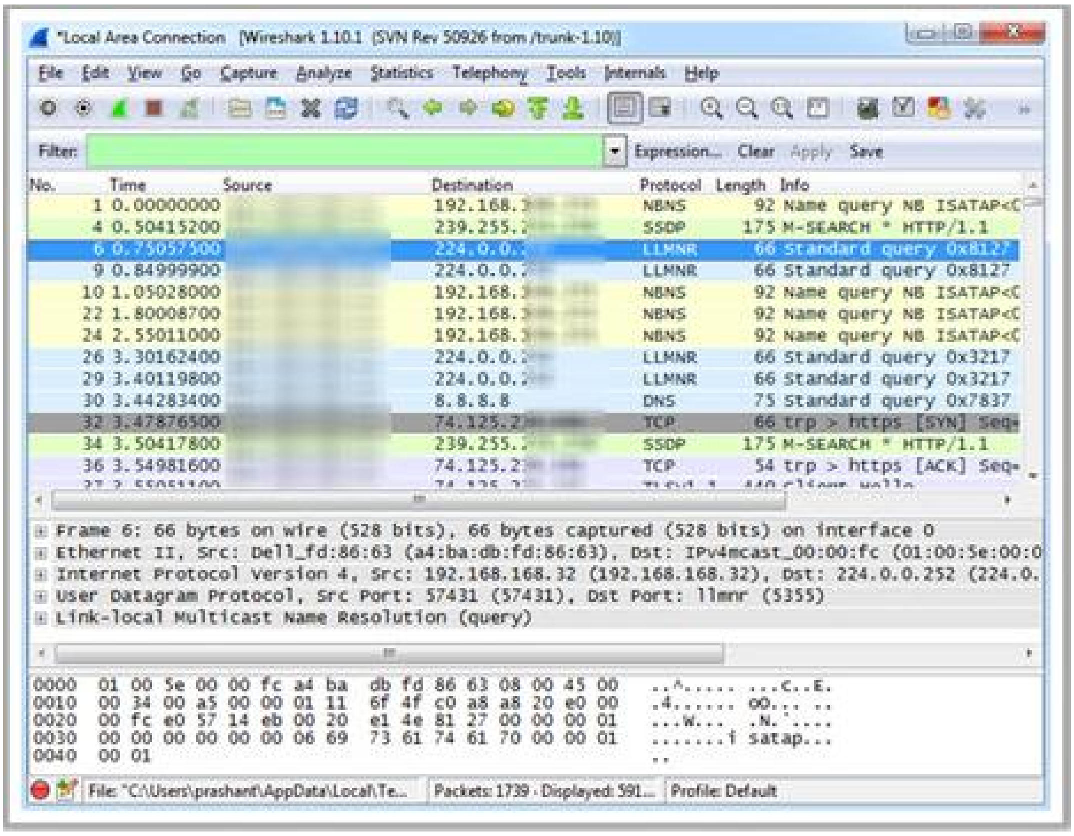
Review/Closeout Discussion Completed (Date): ______________________________

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

Question No : 24

Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



*Local Area Connection [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time         Source       Destination         Protocol Length Info
 1 0.00000000   [redacted]   192.168.[redacted]  NBNS       92 Name query NB ISATAP<C
 4 0.50415200   [redacted]   239.255.[redacted]  SSDP      175 M-SEARCH * HTTP/1.1
 6 0.75057500   [redacted]   224.0.0.[redacted]  LLMNR      66 Standard query 0x8127
 9 0.84999900   [redacted]   224.0.0.[redacted]  LLMNR      66 Standard query 0x8127
10 1.05028000   [redacted]   192.168.[redacted]  NBNS       92 Name query NB ISATAP<C
22 1.80008700   [redacted]   192.168.[redacted]  NBNS       92 Name query NB ISATAP<C
24 2.55011000   [redacted]   192.168.[redacted]  NBNS       92 Name query NB ISATAP<C
26 3.30162400   [redacted]   224.0.0.[redacted]  LLMNR      66 Standard query 0x3217
29 3.40119800   [redacted]   224.0.0.[redacted]  LLMNR      66 Standard query 0x3217
30 3.44283400   [redacted]   8.8.8.8             DNS        75 Standard query 0x7837
32 3.47876500   [redacted]   74.125.2[redacted]  TCP        66 trp > https [SYN] Seq=
34 3.50417800   [redacted]   239.255.[redacted]  SSDP      175 M-SEARCH * HTTP/1.1
36 3.54981600   [redacted]   74.125.2[redacted]  TCP        54 trp > https [ACK] Seq=

⊞ Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: Dell_fd:86:63 (a4:ba:db:fd:86:63), Dst: IPv4mcast_00:00:fc (01:00:5e:00:0
⊞ Internet Protocol Version 4, Src: 192.168.168.32 (192.168.168.32), Dst: 224.0.0.252 (224.0.
⊞ User Datagram Protocol, Src Port: 57431 (57431), Dst Port: llmnr (5355)
⊞ Link-local Multicast Name Resolution (query)

0000  01 00 5e 00 00 fc a4 ba  db fd 86 63 08 00 45 00   ..^..... ...c..E.
0010  00 34 00 a5 00 00 01 11  6f 4f c0 a8 a8 20 e0 00   .4...... oO... ..
0020  00 fc e0 57 14 eb 00 20  e1 4e 81 27 00 00 00 01   ...W...  .N.'....
0030  00 00 00 00 00 00 06 69  73 61 74 61 70 00 00 01   .......i satap...
0040  00 01                                              ..
```

File: "C:\Users\prashant\AppData\Local\Te... | Packets: 1739 · Displayed: 591... | Profile: Default

A. ip.dst==10.0.0.7
B. ip.port==10.0.0.7
C. ip.src==10.0.0.7
D. ip.dstport==10.0.0.7

Answer: C

Question No : 25

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?

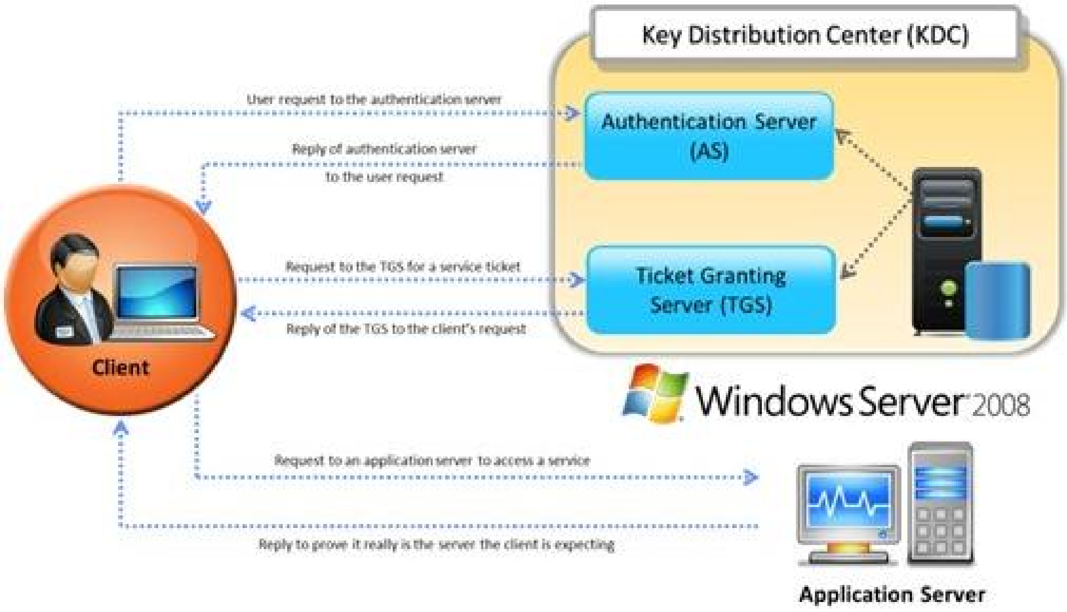
A. Localhost (127.0.0.1) and port 1241
B. Localhost (127.0.0.1) and port 1240

C. Localhost (127.0.0.1) and port 1246
D. Localhost (127.0.0.0) and port 1243

Answer: A

Question No : 26

Identify the type of authentication mechanism represented below:


Key Distribution Center (KDC)
User request to the authentication server
Authentication Server (AS)
Reply of authentication server to the user request
Request to the TGS for a service ticket
Ticket Granting Server (TGS)
Reply of the TGS to the client's request
Client
Windows Server 2008
Request to an application server to access a service
Reply to prove it really is the server the client is expecting
Application Server

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

Answer: D

Explanation:

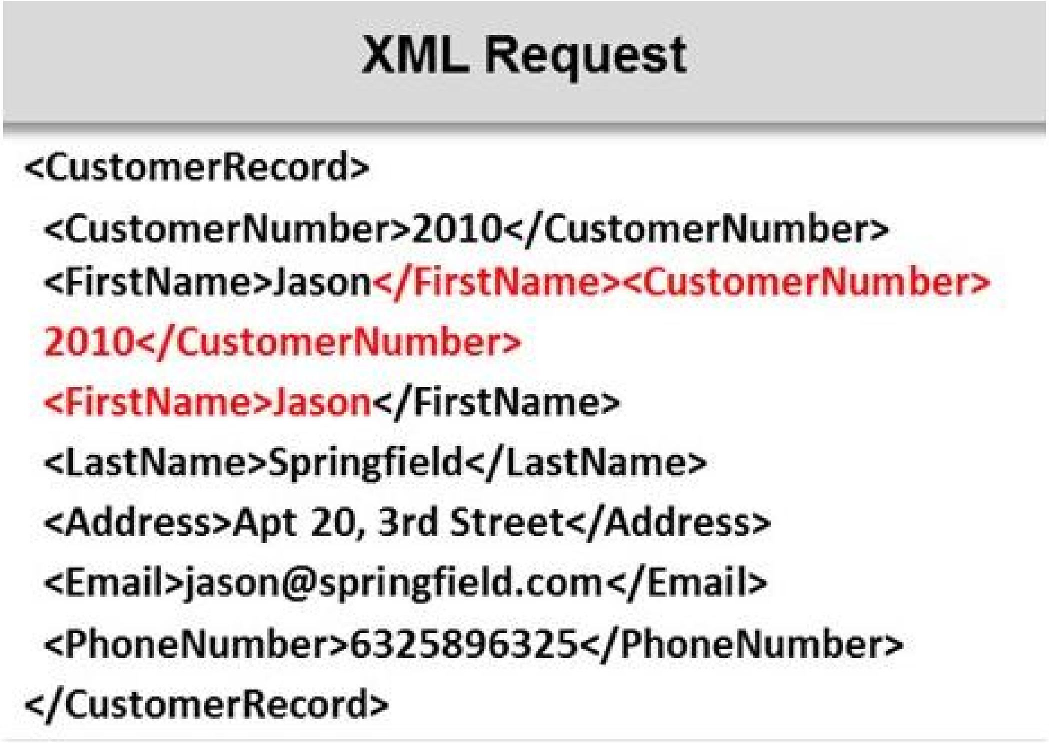
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

Question No : 27

Identify the injection attack represented in the diagram below:



XML Request

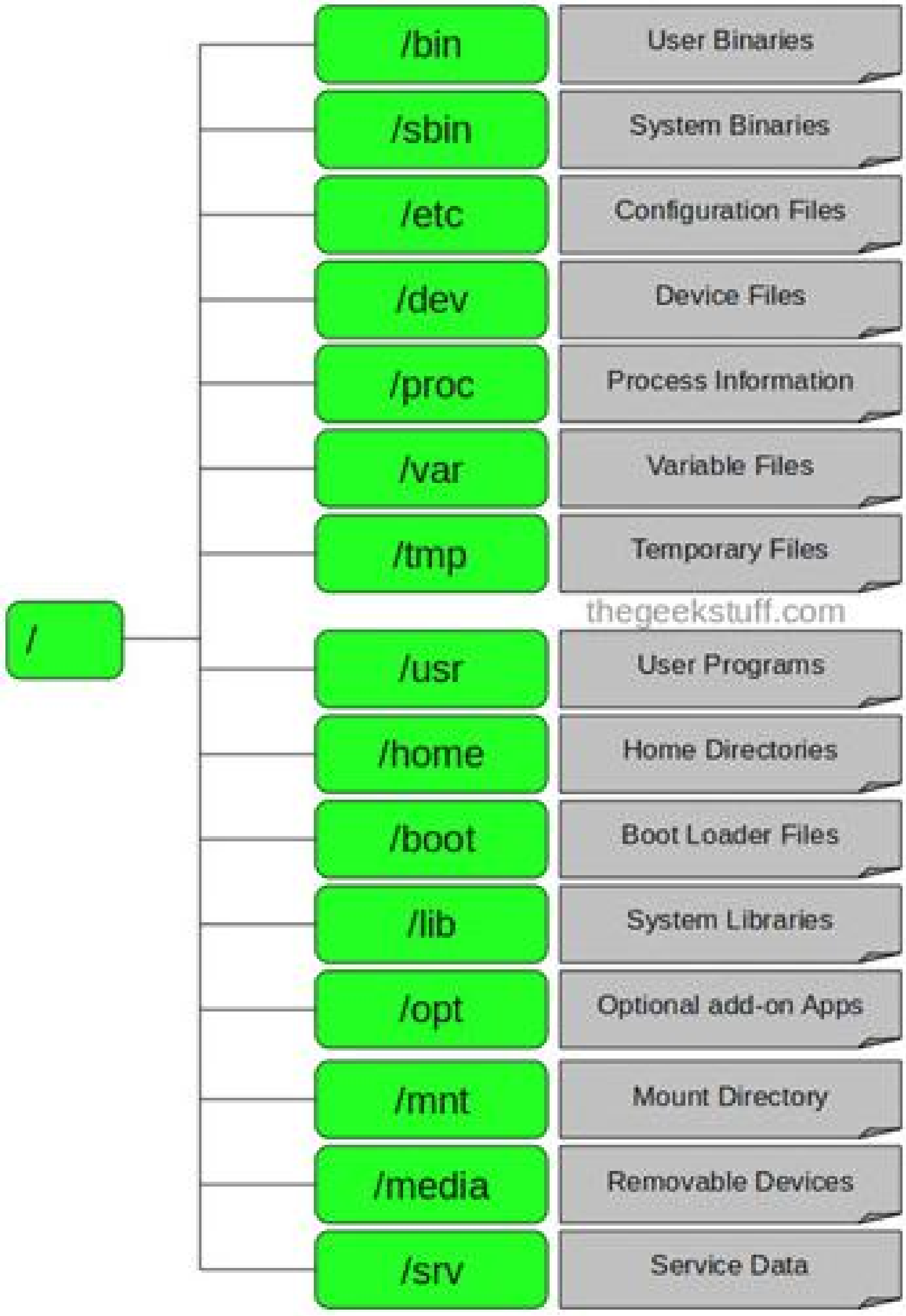
```
<CustomerRecord>
  <CustomerNumber>2010</CustomerNumber>
  <FirstName>Jason</FirstName><CustomerNumber>
  2010</CustomerNumber>
  <FirstName>Jason</FirstName>
  <LastName>Springfield</LastName>
  <Address>Apt 20, 3rd Street</Address>
  <Email>jason@springfield.com</Email>
  <PhoneNumber>6325896325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

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

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

Question No : 28

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



In the example of a /etc/shadow file below, what does the bold letter string indicate?

Vivek: $1$fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

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

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

Question No : 29

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

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

Answer: B

Question No : 30

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

Question No : 31

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

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

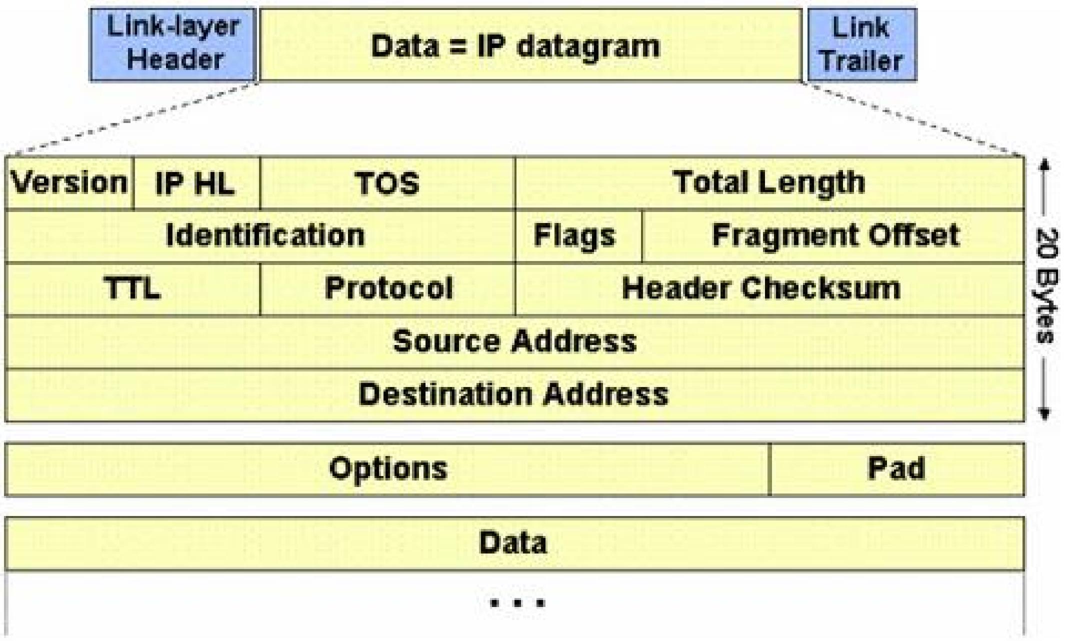
Answer: A

Question No : 32

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

Question No : 33

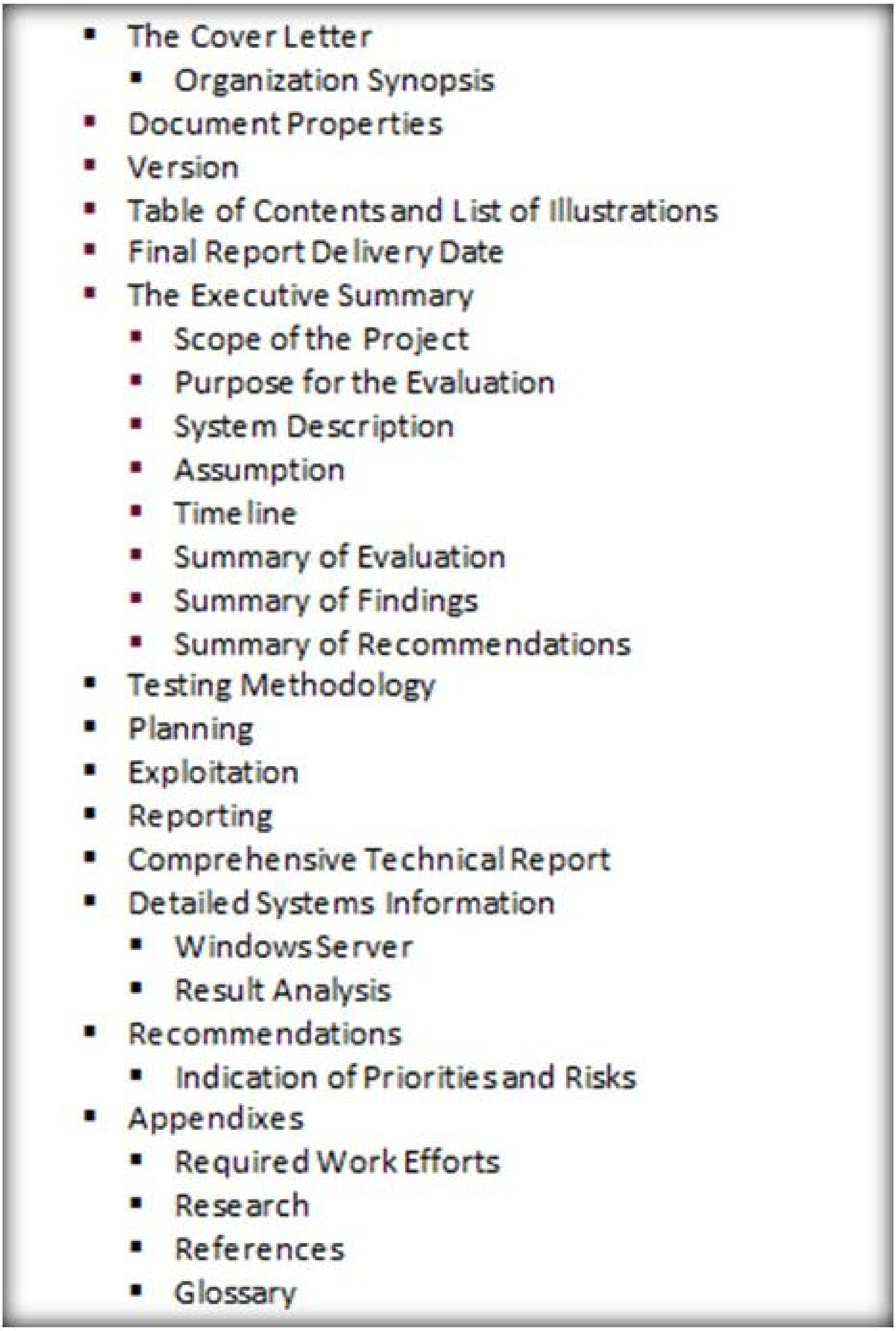
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port21

Answer: C

Question No : 34

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
  - Timeline
  - 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 security

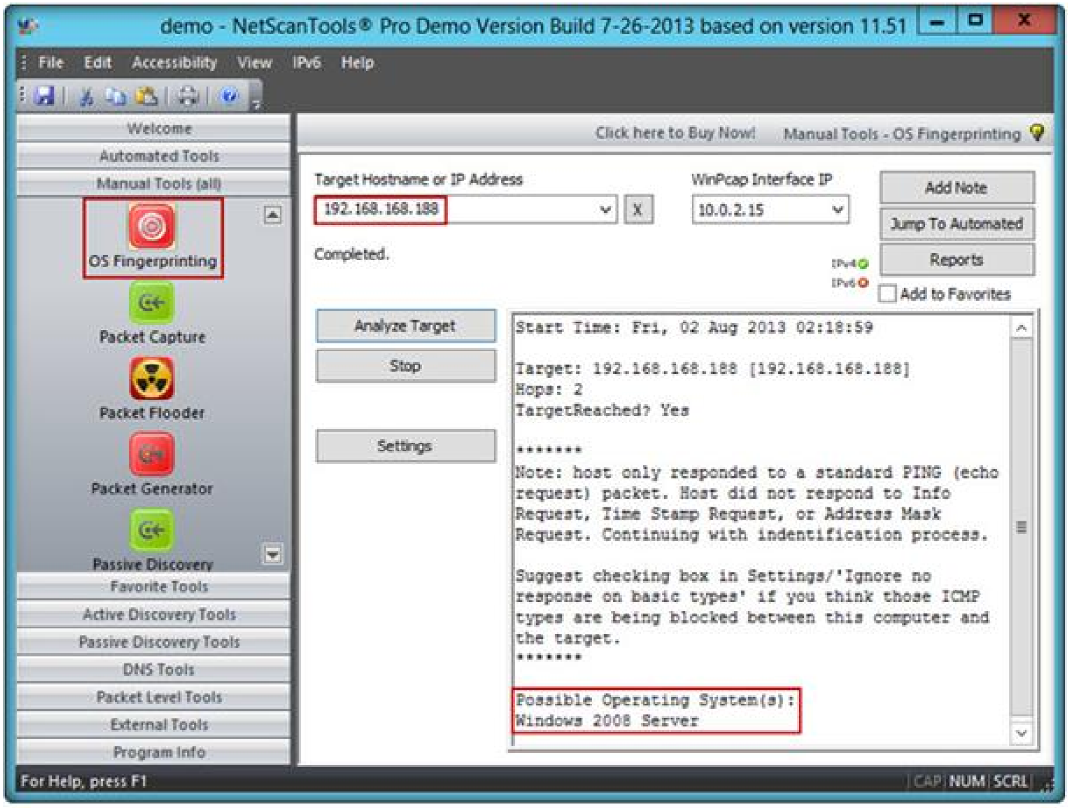
controls and patch any flaws discovered during testing.

D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Answer: C

Question No : 35

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

Question No : 36

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

Question No : 37

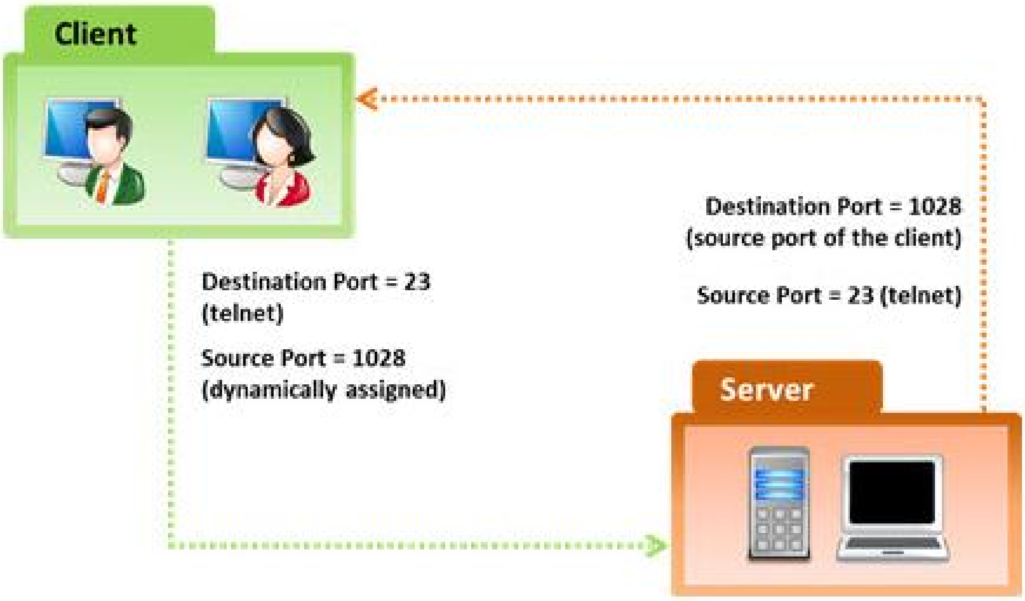
The framework primarily designed to fulfill a methodical and organized way of addressing five threat classes to network and that can be used to access, plan, manage, and maintain secure computers and communication networks is:

A. Nortells Unified Security Framework
B. The IBM Security Framework
C. Bell Labs Network Security Framework
D. Microsoft Internet Security Framework

Answer: C

Question No : 38

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

Question No : 39

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

Question No : 40

John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

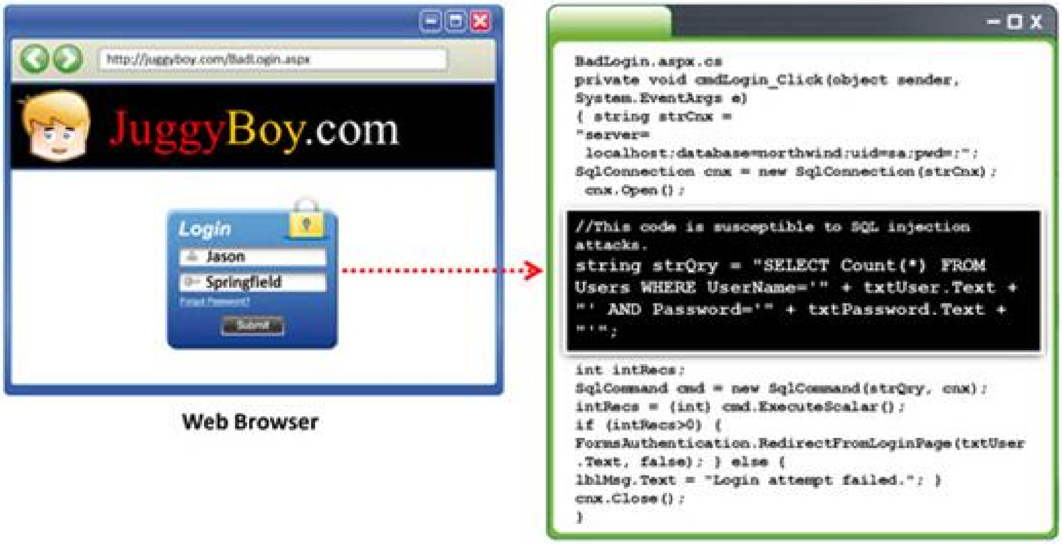
Which of the following factors does he need to consider while preparing the pen testing pricing report?

A. Number of employees in the client organization
B. Complete structure of the organization
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Answer: C

Question No : 41

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?

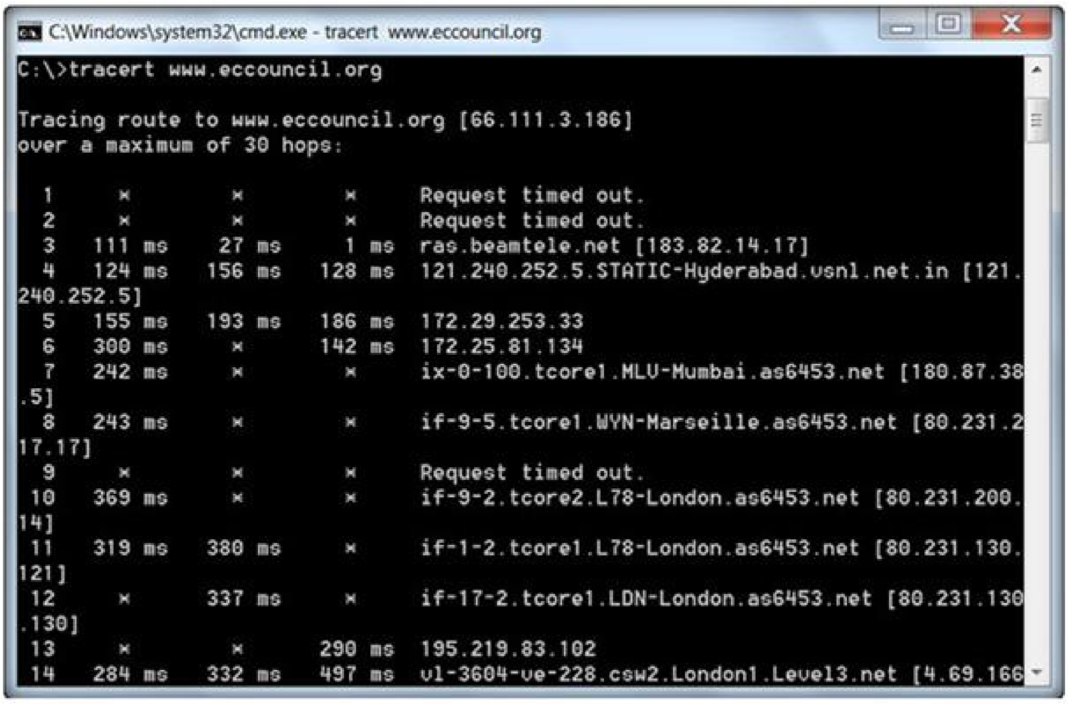
A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Answer: D

Question No : 42

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.

The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



```
C:\>tracert www.eccouncil.org

Tracing route to www.eccouncil.org [66.111.3.186]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3   111 ms    27 ms     1 ms  ras.beamtele.net [183.82.14.17]
  4   124 ms   156 ms   128 ms  121.240.252.5.STATIC-Hyderabad.vsnl.net.in [121.
240.252.5]
  5   155 ms   193 ms   186 ms  172.29.253.33
  6   300 ms     *      142 ms  172.25.81.134
  7   242 ms     *        *     ix-0-100.tcore1.MLV-Mumbai.as6453.net [180.87.38
.5]
  8   243 ms     *        *     if-9-5.tcore1.WYN-Marseille.as6453.net [80.231.2
17.17]
  9     *        *        *     Request timed out.
 10   369 ms     *        *     if-9-2.tcore2.L78-London.as6453.net [80.231.200.
14]
 11   319 ms   380 ms     *     if-1-2.tcore1.L78-London.as6453.net [80.231.130.
121]
 12     *      337 ms     *     if-17-2.tcore1.LDN-London.as6453.net [80.231.130
.130]
 13     *        *      290 ms  195.219.83.102
 14   284 ms   332 ms   497 ms  vl-3604-ve-228.csw2.London1.Level3.net [4.69.166
```

During routing, each router reduces packets' TTL value by

A. 3
B. 1
C. 4
D. 2

Answer: B
Reference: http://www.packetu.com/2009/10/09/traceroute-through-the-asa/

Question No : 43

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

Question No : 44

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

Question No : 45

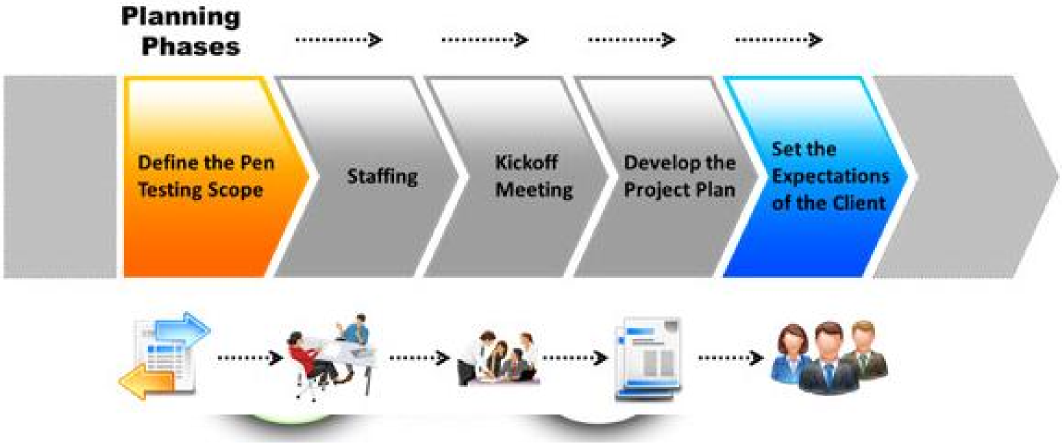
An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

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

Answer: B

Question No : 46

The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client’s operating environment, threat perception, security and compliance requirements, ROE, and budget. Various components need to be considered for testing while developing the scope of the project.


Planning Phases
Define the Pen Testing Scope
Staffing
Kickoff Meeting
Develop the Project Plan
Set the Expectations of the Client

Which of the following is NOT a pen testing component to be tested?

A. System Software Security
B. Intrusion Detection
C. Outside Accomplices
D. Inside Accomplices

Answer: C

Question No : 47

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

A. –sS
B. –sV
C. –sU
D. –sT

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

Question No : 48

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

Question No : 49

Identify the policy that defines the standards for the organizational network connectivity and security standards for computers that are connected in the organizational network.

A. Information-Protection Policy
B. Special-Access Policy
C. Remote-Access Policy
D. Acceptable-Use Policy

Answer: C

Question No : 50

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

Question No : 51

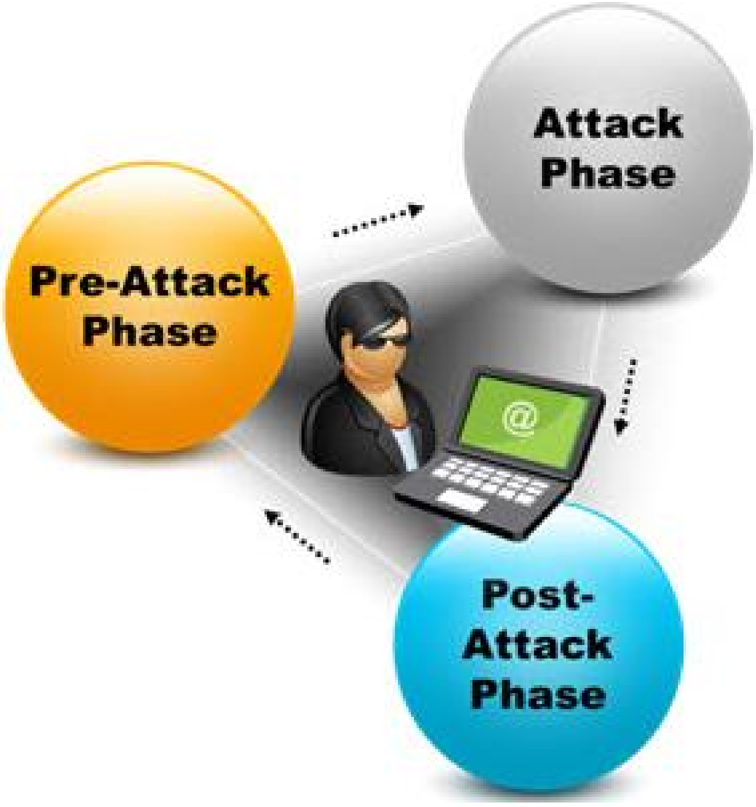
Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

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

Answer: B
Reference: http://books.google.com.pk/books?id=QWQRSTnkFsQC&pg=SA4-PA5&lpg=SA4-PA5&dq=attributes+has+a+LM+and+NTLMv1+value+as+64bit+%2B+64bit+%2B+64bit+and+NTLMv2+value+as+128+bits&source=bl&ots=wJPR32BaF6&sig=YEt9LNfQAbm2M-c6obVggKCkQ2s&hl=en&sa=X&ei=scMfVMfdC8u7ygP4xYGQDg&ved=0CCkQ6AEwAg#v=onepage&q=attributes%20has%20a%20LM%20and%20NTLMv1%20value%20as%2064bit%20%2B%2064bit%20%2B%2064bit%20and%20NTLMv2%20value%20as%20128%20bits&f=false (see Table 4-1)

Question No : 52

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

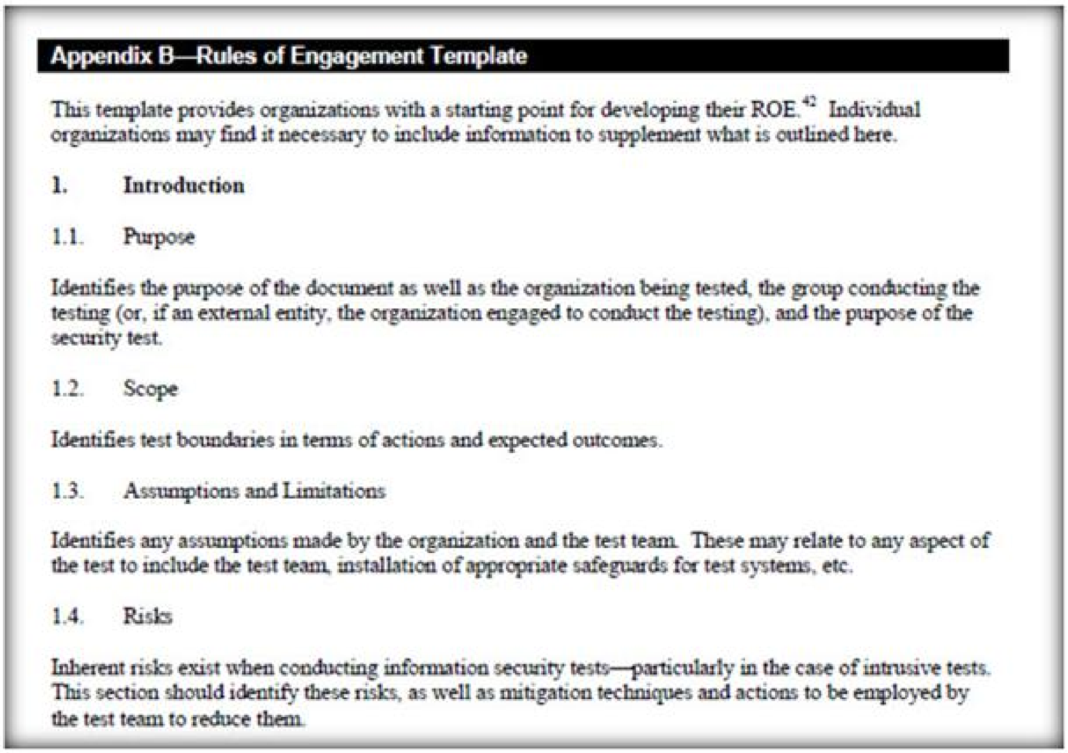
Answer: D

Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf?sequence=1 (page 28, first para)

Question No : 53

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

Question No : 54

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

Question No : 55

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

Question No : 56

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

Question No : 57

A security policy is a document or set of documents that describes, at a high level, the security controls that will be implemented by the company. Which one of the following policies forbids everything and restricts usage of company computers, whether it is system usage or network usage?

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

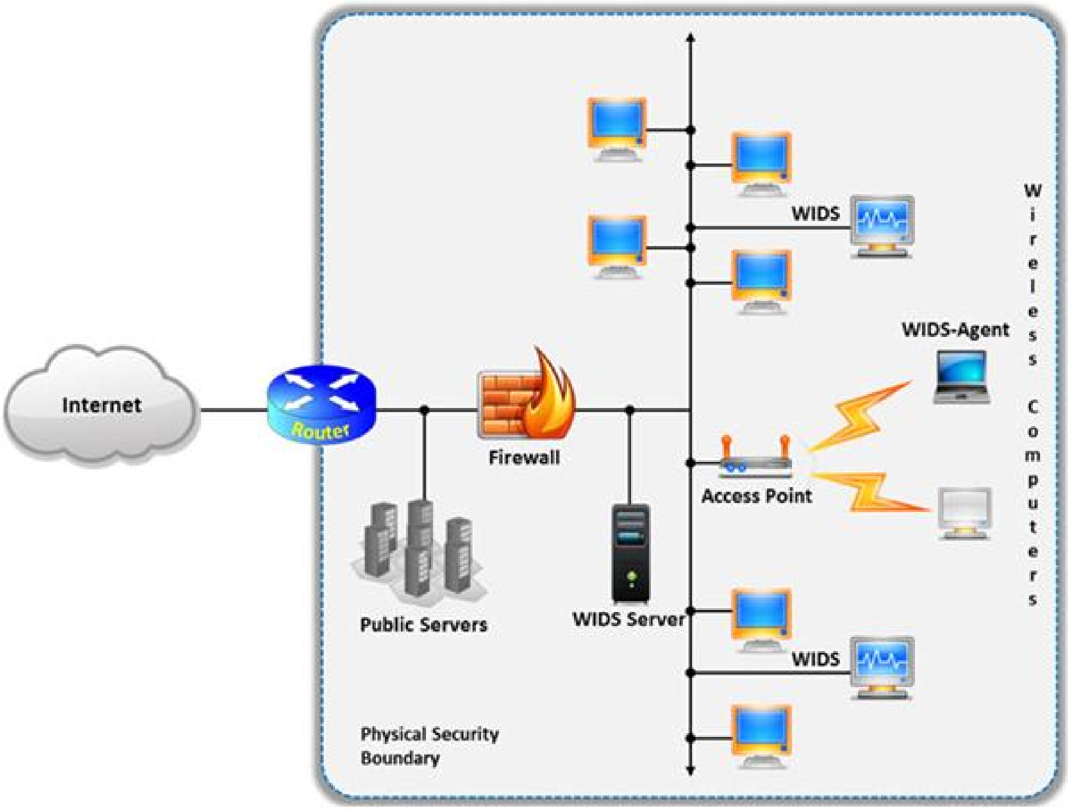
Answer: A

Question No : 58

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected.

Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



A. Social engineering
B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Answer: D

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

Question No : 59

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

Microsoft Exams List

70-246 Dump PDF VCE	70-485 Dump PDF VCE	70-742 Dump PDF VCE	98-366 Dump PDF VCE
70-247 Dump PDF VCE	70-486 Dump PDF VCE	70-743 Dump PDF VCE	98-367 Dump PDF VCE
70-331 Dump PDF VCE	70-487 Dump PDF VCE	70-744 Dump PDF VCE	98-368 Dump PDF VCE
70-332 Dump PDF VCE	70-488 Dump PDF VCE	70-761 Dump PDF VCE	98-369 Dump PDF VCE
70-333 Dump PDF VCE	70-489 Dump PDF VCE	70-762 Dump PDF VCE	98-372 Dump PDF VCE
70-334 Dump PDF VCE	70-490 Dump PDF VCE	70-765 Dump PDF VCE	98-373 Dump PDF VCE
70-339 Dump PDF VCE	70-491 Dump PDF VCE	70-768 Dump PDF VCE	98-374 Dump PDF VCE
70-341 Dump PDF VCE	70-492 Dump PDF VCE	70-980 Dump PDF VCE	98-375 Dump PDF VCE
70-342 Dump PDF VCE	70-494 Dump PDF VCE	70-981 Dump PDF VCE	98-379 Dump PDF VCE
70-345 Dump PDF VCE	70-496 Dump PDF VCE	70-982 Dump PDF VCE	MB2-700 Dump PDF VCE
70-346 Dump PDF VCE	70-497 Dump PDF VCE	74-343 Dump PDF VCE	MB2-701 Dump PDF VCE
70-347 Dump PDF VCE	70-498 Dump PDF VCE	74-344 Dump PDF VCE	MB2-702 Dump PDF VCE
70-348 Dump PDF VCE	70-499 Dump PDF VCE	74-409 Dump PDF VCE	MB2-703 Dump PDF VCE
70-354 Dump PDF VCE	70-517 Dump PDF VCE	74-678 Dump PDF VCE	MB2-704 Dump PDF VCE
70-383 Dump PDF VCE	70-532 Dump PDF VCE	74-697 Dump PDF VCE	MB2-707 Dump PDF VCE
70-384 Dump PDF VCE	70-533 Dump PDF VCE	77-420 Dump PDF VCE	MB2-710 Dump PDF VCE
70-385 Dump PDF VCE	70-534 Dump PDF VCE	77-427 Dump PDF VCE	MB2-711 Dump PDF VCE
70-410 Dump PDF VCE	70-640 Dump PDF VCE	77-600 Dump PDF VCE	MB2-712 Dump PDF VCE
70-411 Dump PDF VCE	70-642 Dump PDF VCE	77-601 Dump PDF VCE	MB2-713 Dump PDF VCE
70-412 Dump PDF VCE	70-646 Dump PDF VCE	77-602 Dump PDF VCE	MB2-714 Dump PDF VCE
70-413 Dump PDF VCE	70-673 Dump PDF VCE	77-603 Dump PDF VCE	MB2-715 Dump PDF VCE
70-414 Dump PDF VCE	70-680 Dump PDF VCE	77-604 Dump PDF VCE	MB2-716 Dump PDF VCE
70-417 Dump PDF VCE	70-681 Dump PDF VCE	77-605 Dump PDF VCE	MB2-717 Dump PDF VCE
70-461 Dump PDF VCE	70-682 Dump PDF VCE	77-881 Dump PDF VCE	MB2-718 Dump PDF VCE
70-462 Dump PDF VCE	70-684 Dump PDF VCE	77-882 Dump PDF VCE	MB5-705 Dump PDF VCE
70-463 Dump PDF VCE	70-685 Dump PDF VCE	77-883 Dump PDF VCE	MB6-700 Dump PDF VCE
70-464 Dump PDF VCE	70-686 Dump PDF VCE	77-884 Dump PDF VCE	MB6-701 Dump PDF VCE
70-465 Dump PDF VCE	70-687 Dump PDF VCE	77-885 Dump PDF VCE	MB6-702 Dump PDF VCE
70-466 Dump PDF VCE	70-688 Dump PDF VCE	77-886 Dump PDF VCE	MB6-703 Dump PDF VCE
70-467 Dump PDF VCE	70-689 Dump PDF VCE	77-887 Dump PDF VCE	MB6-704 Dump PDF VCE
70-469 Dump PDF VCE	70-692 Dump PDF VCE	77-888 Dump PDF VCE	MB6-705 Dump PDF VCE
70-470 Dump PDF VCE	70-695 Dump PDF VCE	77-891 Dump PDF VCE	MB6-884 Dump PDF VCE
70-473 Dump PDF VCE	70-696 Dump PDF VCE	98-349 Dump PDF VCE	MB6-885 Dump PDF VCE
70-480 Dump PDF VCE	70-697 Dump PDF VCE	98-361 Dump PDF VCE	MB6-886 Dump PDF VCE
70-481 Dump PDF VCE	70-698 Dump PDF VCE	98-362 Dump PDF VCE	MB6-889 Dump PDF VCE
70-482 Dump PDF VCE	70-734 Dump PDF VCE	98-363 Dump PDF VCE	MB6-890 Dump PDF VCE
70-483 Dump PDF VCE	70-740 Dump PDF VCE	98-364 Dump PDF VCE	MB6-892 Dump PDF VCE
70-484 Dump PDF VCE	70-741 Dump PDF VCE	98-365 Dump PDF VCE	MB6-893 Dump PDF VCE

Cisco Exams List

010-151 Dump PDF VCE	350-018 Dump PDF VCE	642-737 Dump PDF VCE	650-667 Dump PDF VCE
100-105 Dump PDF VCE	352-001 Dump PDF VCE	642-742 Dump PDF VCE	650-669 Dump PDF VCE
200-001 Dump PDF VCE	400-051 Dump PDF VCE	642-883 Dump PDF VCE	650-752 Dump PDF VCE
200-105 Dump PDF VCE	400-101 Dump PDF VCE	642-885 Dump PDF VCE	650-756 Dump PDF VCE
200-120 Dump PDF VCE	400-151 Dump PDF VCE	642-887 Dump PDF VCE	650-968 Dump PDF VCE
200-125 Dump PDF VCE	400-201 Dump PDF VCE	642-889 Dump PDF VCE	700-001 Dump PDF VCE
200-150 Dump PDF VCE	400-251 Dump PDF VCE	642-980 Dump PDF VCE	700-037 Dump PDF VCE
200-155 Dump PDF VCE	400-351 Dump PDF VCE	642-996 Dump PDF VCE	700-038 Dump PDF VCE
200-310 Dump PDF VCE	500-006 Dump PDF VCE	642-997 Dump PDF VCE	700-039 Dump PDF VCE
200-355 Dump PDF VCE	500-007 Dump PDF VCE	642-998 Dump PDF VCE	700-101 Dump PDF VCE
200-401 Dump PDF VCE	500-051 Dump PDF VCE	642-999 Dump PDF VCE	700-104 Dump PDF VCE
200-601 Dump PDF VCE	500-052 Dump PDF VCE	644-066 Dump PDF VCE	700-201 Dump PDF VCE
210-060 Dump PDF VCE	500-170 Dump PDF VCE	644-068 Dump PDF VCE	700-205 Dump PDF VCE
210-065 Dump PDF VCE	500-201 Dump PDF VCE	644-906 Dump PDF VCE	700-260 Dump PDF VCE
210-250 Dump PDF VCE	500-202 Dump PDF VCE	646-048 Dump PDF VCE	700-270 Dump PDF VCE
210-255 Dump PDF VCE	500-254 Dump PDF VCE	646-365 Dump PDF VCE	700-280 Dump PDF VCE
210-260 Dump PDF VCE	500-258 Dump PDF VCE	646-580 Dump PDF VCE	700-281 Dump PDF VCE
210-451 Dump PDF VCE	500-260 Dump PDF VCE	646-671 Dump PDF VCE	700-295 Dump PDF VCE
210-455 Dump PDF VCE	500-265 Dump PDF VCE	646-985 Dump PDF VCE	700-501 Dump PDF VCE
300-070 Dump PDF VCE	500-275 Dump PDF VCE	648-232 Dump PDF VCE	700-505 Dump PDF VCE
300-075 Dump PDF VCE	500-280 Dump PDF VCE	648-238 Dump PDF VCE	700-601 Dump PDF VCE
300-080 Dump PDF VCE	500-285 Dump PDF VCE	648-244 Dump PDF VCE	700-602 Dump PDF VCE
300-085 Dump PDF VCE	500-290 Dump PDF VCE	648-247 Dump PDF VCE	700-603 Dump PDF VCE
300-101 Dump PDF VCE	500-801 Dump PDF VCE	648-375 Dump PDF VCE	700-701 Dump PDF VCE
300-115 Dump PDF VCE	600-199 Dump PDF VCE	648-385 Dump PDF VCE	700-702 Dump PDF VCE
300-135 Dump PDF VCE	600-210 Dump PDF VCE	650-032 Dump PDF VCE	700-703 Dump PDF VCE
300-160 Dump PDF VCE	600-211 Dump PDF VCE	650-042 Dump PDF VCE	700-801 Dump PDF VCE
300-165 Dump PDF VCE	600-212 Dump PDF VCE	650-059 Dump PDF VCE	700-802 Dump PDF VCE
300-180 Dump PDF VCE	600-455 Dump PDF VCE	650-082 Dump PDF VCE	700-803 Dump PDF VCE
300-206 Dump PDF VCE	600-460 Dump PDF VCE	650-127 Dump PDF VCE	810-403 Dump PDF VCE
300-207 Dump PDF VCE	600-501 Dump PDF VCE	650-128 Dump PDF VCE	820-424 Dump PDF VCE
300-208 Dump PDF VCE	600-502 Dump PDF VCE	650-148 Dump PDF VCE	840-425 Dump PDF VCE
300-209 Dump PDF VCE	600-503 Dump PDF VCE	650-159 Dump PDF VCE	
300-210 Dump PDF VCE	600-504 Dump PDF VCE	650-281 Dump PDF VCE	
300-320 Dump PDF VCE	640-692 Dump PDF VCE	650-393 Dump PDF VCE	
300-360 Dump PDF VCE	640-875 Dump PDF VCE	650-472 Dump PDF VCE	
300-365 Dump PDF VCE	640-878 Dump PDF VCE	650-474 Dump PDF VCE	
300-370 Dump PDF VCE	640-911 Dump PDF VCE	650-575 Dump PDF VCE	
300-375 Dump PDF VCE	640-916 Dump PDF VCE	650-621 Dump PDF VCE	
300-465 Dump PDF VCE	642-035 Dump PDF VCE	650-663 Dump PDF VCE	
300-470 Dump PDF VCE	642-732 Dump PDF VCE	650-665 Dump PDF VCE	
300-475 Dump PDF VCE	642-747 Dump PDF VCE	650-754 Dump PDF VCE	