

EC-Council

Exam Questions ECSAv10

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



NEW QUESTION 1

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

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

Answer: A

NEW QUESTION 2

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

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

Answer: D

NEW QUESTION 3

If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

- A. Parameter tampering Attack
- B. Sql injection attack
- C. Session Hijacking
- D. Cross-site request attack

Answer: D

NEW QUESTION 4

Harold is a security analyst who has just run the `rdisk /s` command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

- A. %systemroot%\LSA
- B. %systemroot%\repair
- C. %systemroot%\system32\drivers\etc
- D. %systemroot%\system32\LSA

Answer: B

NEW QUESTION 5

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 6

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 7

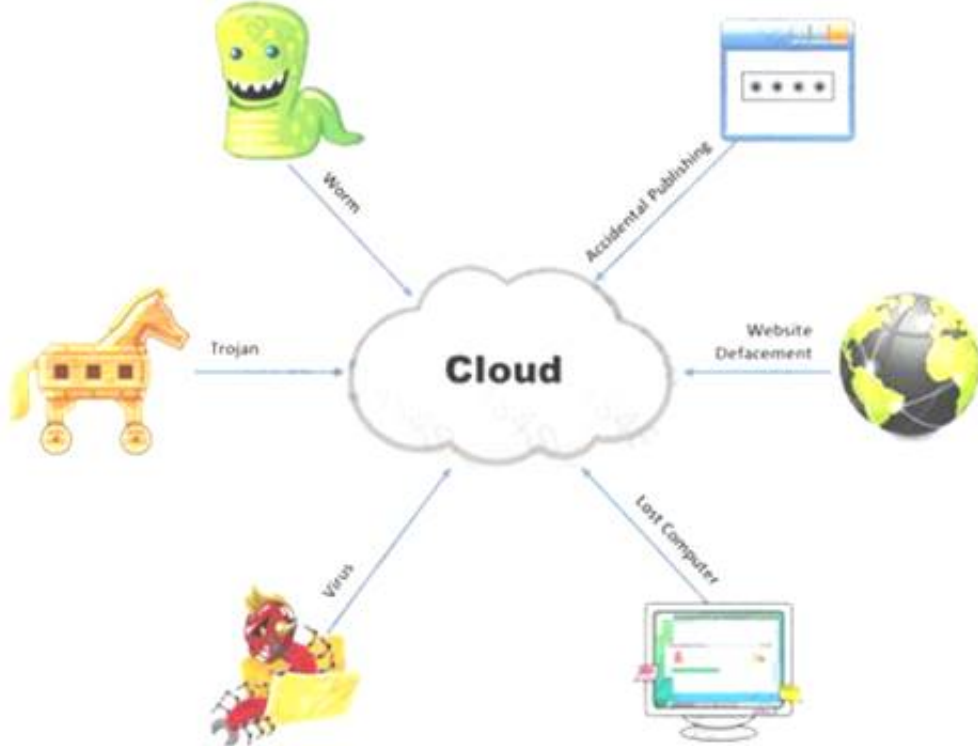
DMZ is a network designed to give the public access to the specific internal resources and you might want to do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories.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

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

Answer: A

NEW QUESTION 8

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 9

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 to 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 10

John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtrcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

- A. The SID of Hillary's network account
- B. The network shares that Hillary has permissions
- C. The SAM file from Hillary's computer
- D. Hillary's network username and password hash

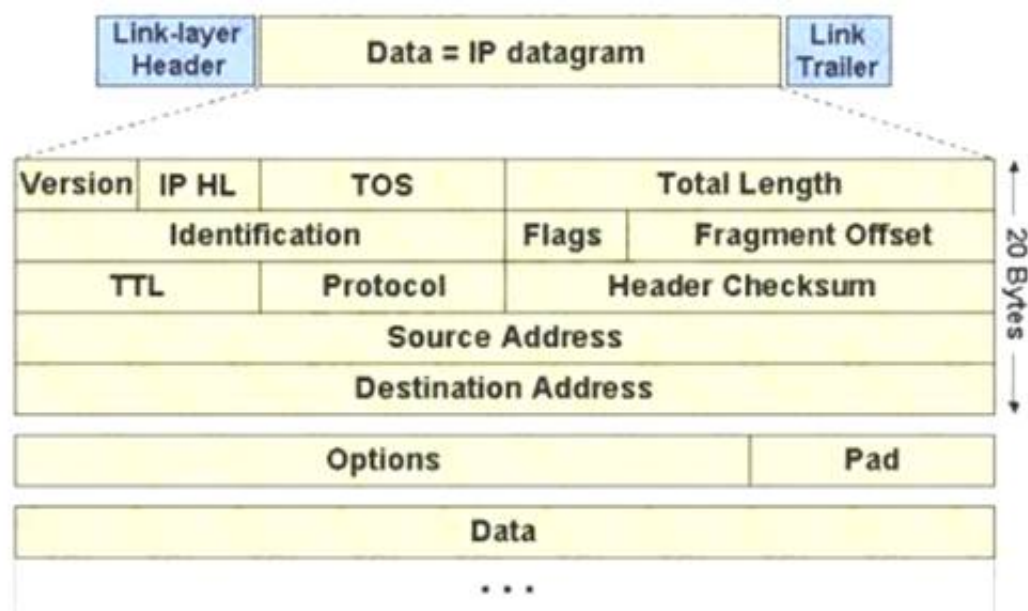
Answer: D

NEW QUESTION 10

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 14

Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword.

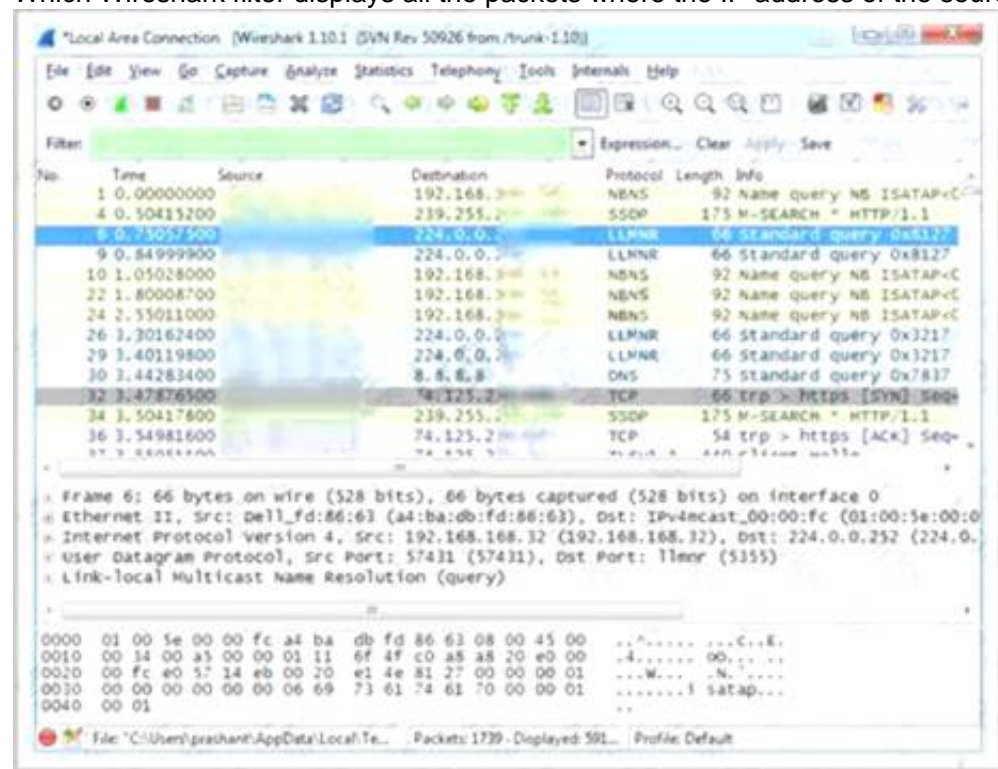
Which one of the following operator is used to define meta-variables?

- A. "\$"
- B. "#"
- C. "*"
- D. "?"

Answer: A

NEW QUESTION 18

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



- 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

NEW QUESTION 23

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network.

How would you answer?

- A. IBM Methodology
- B. LPT Methodology

- C. Google Methodology
- D. Microsoft Methodology

Answer: B

NEW QUESTION 27

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 29

What are the scanning techniques that are used to bypass firewall rules and logging mechanisms and disguise themselves as usual network traffic?

- A. Connect Scanning Techniques
- B. SYN Scanning Techniques
- C. Stealth Scanning Techniques
- D. Port Scanning Techniques

Answer: C

NEW QUESTION 34

Which of the following is the objective of Gramm-Leach-Bliley Act?

- A. To ease the transfer of financial information between institutions and banks
- B. To protect the confidentiality, integrity, and availability of data
- C. To set a new or enhanced standards for all U.
- D. public company boards, management and public accounting firms
- E. To certify the accuracy of the reported financial statement

Answer: A

NEW QUESTION 38

An "idle" system is also referred to as what?

- A. Zombie
- B. PC not being used
- C. Bot
- D. PC not connected to the Internet

Answer: A

NEW QUESTION 41

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 45

A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card.

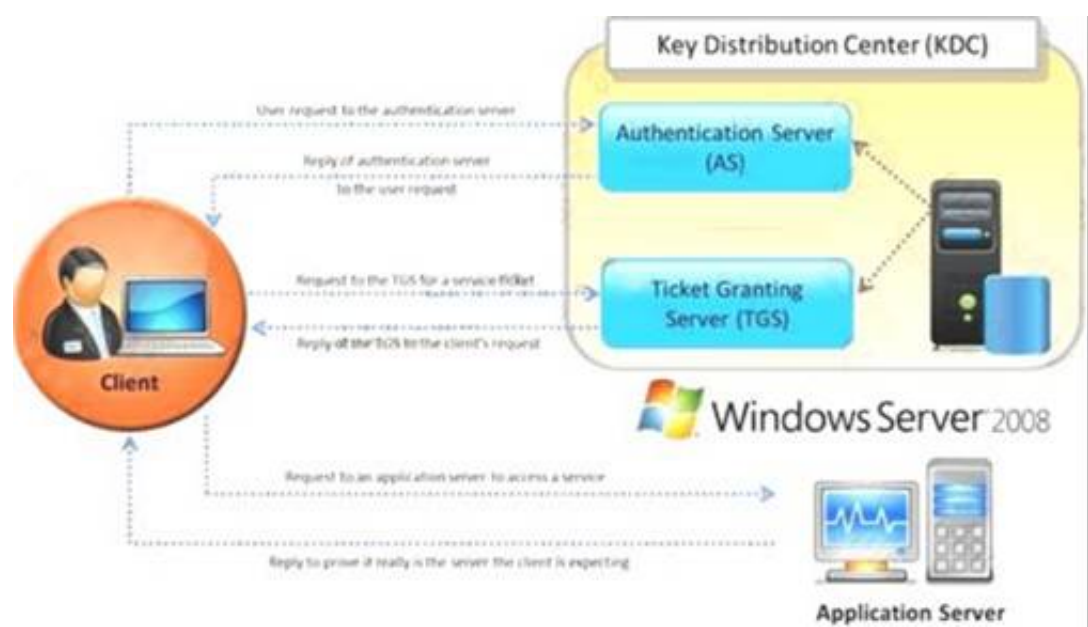
Which one of the following is well supported in most wireless applications?

- A. Orinoco chipsets
- B. Prism II chipsets
- C. Atheros Chipset
- D. Cisco chipset

Answer: B

NEW QUESTION 49

Identify the type of authentication mechanism represented below:



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

Answer: D

NEW QUESTION 54

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

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

Answer: C

NEW QUESTION 55

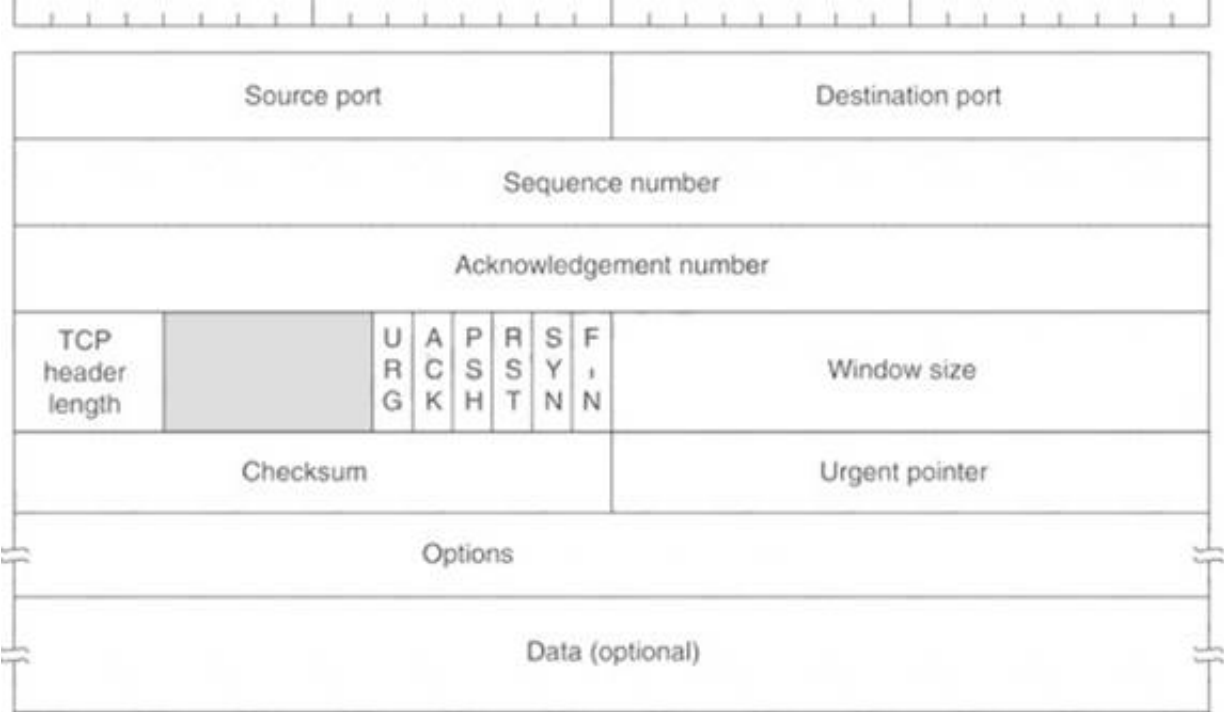
Identify the correct formula for Return on Investment (ROI).

- A. $ROI = ((Expected\ Returns - Cost\ of\ Investment) / Cost\ of\ Investment) * 100$
- B. $ROI = (Expected\ Returns + Cost\ of\ Investment) / Cost\ of\ Investment$
- C. $ROI = (Expected\ Returns\ Cost\ of\ Investment) / Cost\ of\ Investment$
- D. $ROI = ((Expected\ Returns + Cost\ of\ Investment) / Cost\ of\ Investment) * 100$

Answer: C

NEW QUESTION 59

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:



- A. 16 bits
- B. 32 bits

- C. 8 bits
- D. 24 bits

Answer: B

NEW QUESTION 62

Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

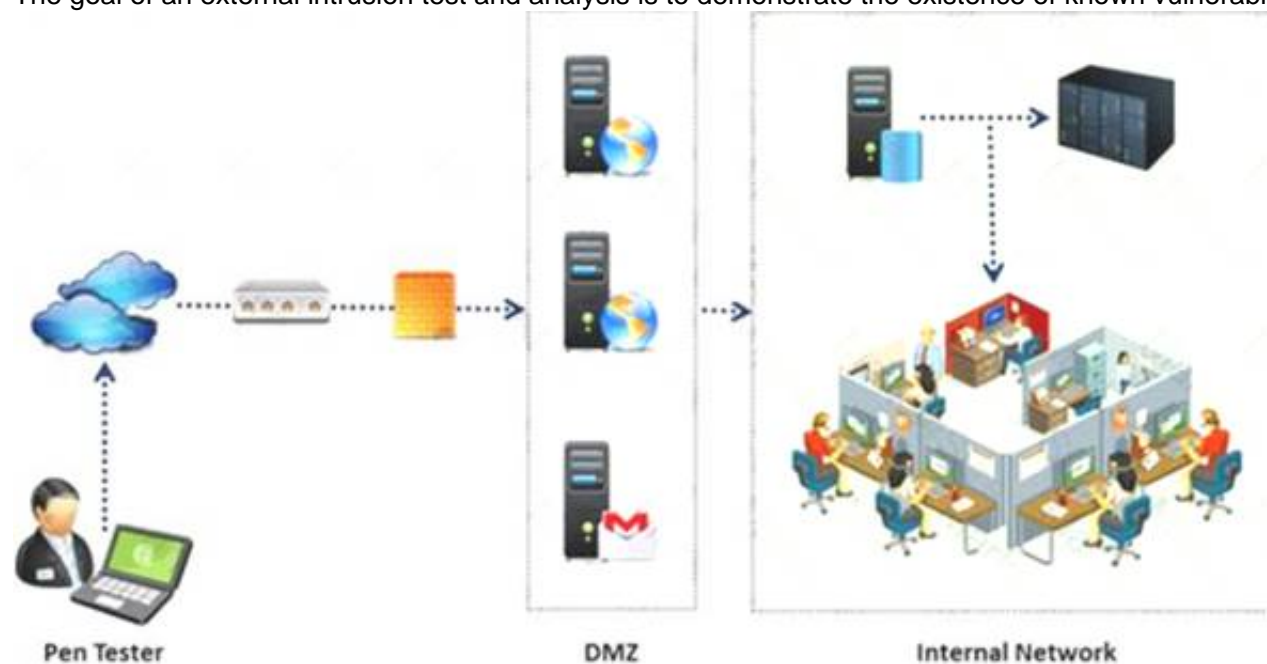
- A. Decreases consumed employee time and increases system uptime
- B. Increases detection and reaction time
- C. Increases response time
- D. Both Decreases consumed employee time and increases system uptime and Increases response time

Answer: A

NEW QUESTION 63

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 67

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

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

Answer: D

NEW QUESTION 69

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

- A. Testing to provide a more complete view of site security
- B. Testing focused on the servers, infrastructure, and the underlying software, including the target
- C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
- D. Testing performed from a number of network access points representing each logical and physical segment

Answer: B

NEW QUESTION 72

Which of the following will not handle routing protocols properly?

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

Answer: B

NEW QUESTION 76

The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the signal () function. Which one of the following functions is used as a program-specific signal and the handler for this calls the DropStats() function to output the current Snort statistics?

- A. SIGUSR1
- B. SIGTERM
- C. SIGINT
- D. SIGHUP

Answer: A

NEW QUESTION 78

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

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

Answer: C

NEW QUESTION 80

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

- A. True negatives
- B. False negatives
- C. False positives
- D. True positives

Answer: B

NEW QUESTION 82

You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable.

You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

- A. The firewall failed-open
- B. The firewall failed-bypass
- C. The firewall failed-closed
- D. The firewall ACL has been purged

Answer: A

NEW QUESTION 86

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

NEW QUESTION 88

How many possible sequence number combinations are there in TCP/IP protocol?

- A. 320 billion
- B. 32 million
- C. 4 billion
- D. 1 billion

Answer: C

NEW QUESTION 93

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

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

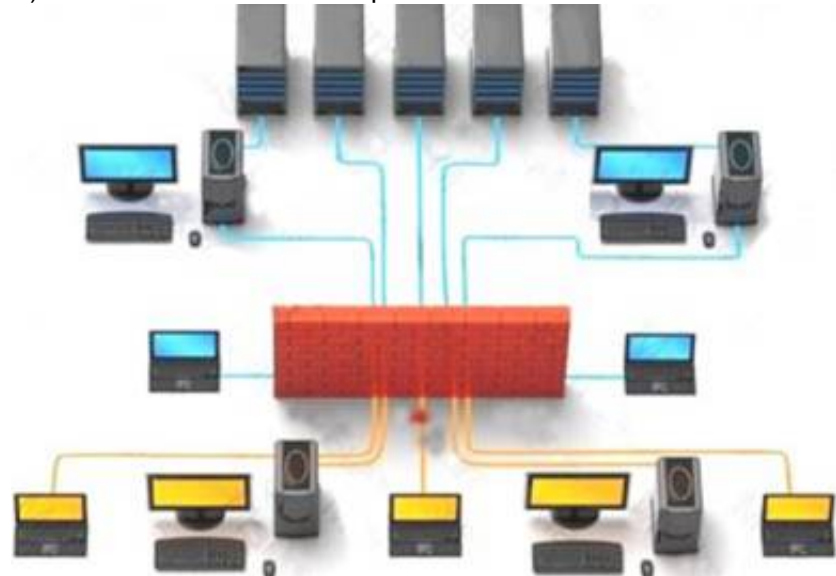
Answer:

B

NEW QUESTION 94

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 97

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 98

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 99

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 102

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 104

What does ICMP Type 3/Code 13 mean?

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

Answer: D

NEW QUESTION 109

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 110

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses.

You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

- A. Metamorphic
- B. Oligomorph
- C. Polymorphic
- D. Transmorphic

Answer: A

NEW QUESTION 111

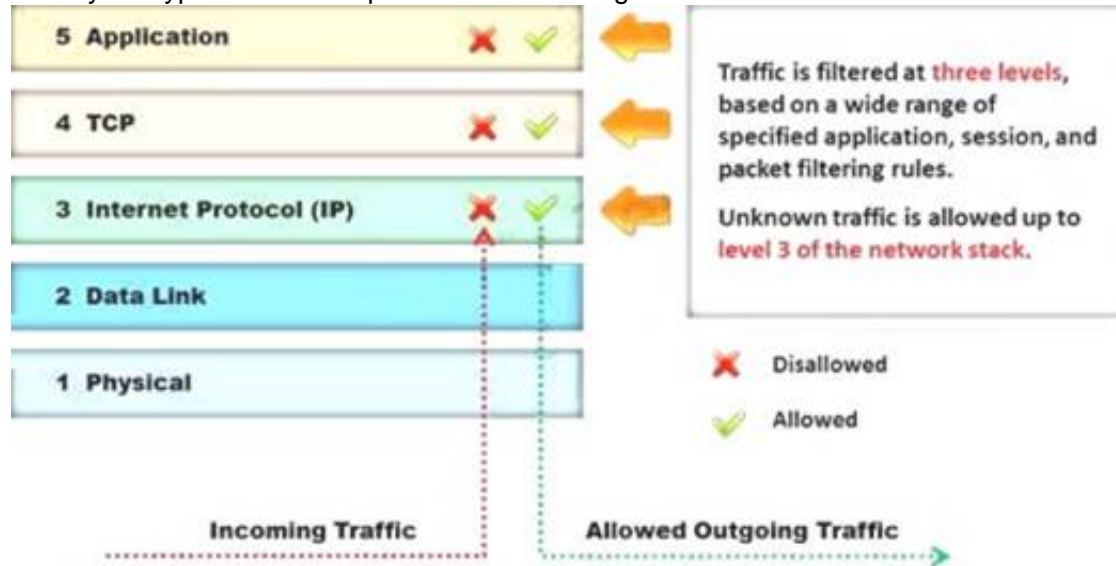
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

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

Answer: D

NEW QUESTION 116

Identify the type of firewall represented in the diagram below:



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

Answer: A

NEW QUESTION 118

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

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

Answer: D

NEW QUESTION 121

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 122

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.



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

NEW QUESTION 126

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

- A. Nmap
- B. Netcraft
- C. Ping sweep
- D. Dig

Answer: B

NEW QUESTION 127

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 129

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 132

Which of the following are the default ports used by NetBIOS service?

- A. A.-135, 136, 139, 445B.134, 135, 136, 137C.137, 138, 139, 140D.133, 134, 139, 142

Answer: A

NEW QUESTION 133

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 137

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 140

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

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

Answer: C

NEW QUESTION 143

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 146

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 148

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 153

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

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

Answer: D

NEW QUESTION 156

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

NEW QUESTION 160

A framework for security analysis is composed of a set of instructions, assumptions, and limitations to analyze and solve security concerns and develop threat free applications.

Which of the following frameworks helps an organization in the evaluation of the company's information security with that of the industrial standards?

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

Answer: B

NEW QUESTION 164

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

```
<script>alert("This is a test.")</script>
```

When you type this and click on search, you receive a pop-up window that says: "This is a test."

What is the result of this test?

- A. Your website is vulnerable to web bugs
- B. Your website is vulnerable to XSS
- C. Your website is not vulnerable
- D. Your website is vulnerable to SQL injection

Answer: B

NEW QUESTION 168

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code.

While searching through the code, you come across something abnormal:

```
<img  
src=http://coolwebsearch.com/ads/pixel.news.com width=1 height=1 border=0  
>
```

What have you found?

- A. Trojan.downloader
- B. Blind bug
- C. Web bug
- D. CGI code

Answer: C

NEW QUESTION 173

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 176

What will the following URL produce in an unpatched IIS Web Server?

<http://www.thetargetsite.com/scripts/../../../../%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 177

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

- A. Service account passwords in plain text
- B. Cached password hashes for the past 20 users
- C. IAS account names and passwords
- D. Local store PKI Kerberos certificates

Answer: A

NEW QUESTION 182

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

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

Answer: D

NEW QUESTION 183

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes. Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.

What can a pen tester do to detect input sanitization issues?

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

Answer: D

NEW QUESTION 184

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

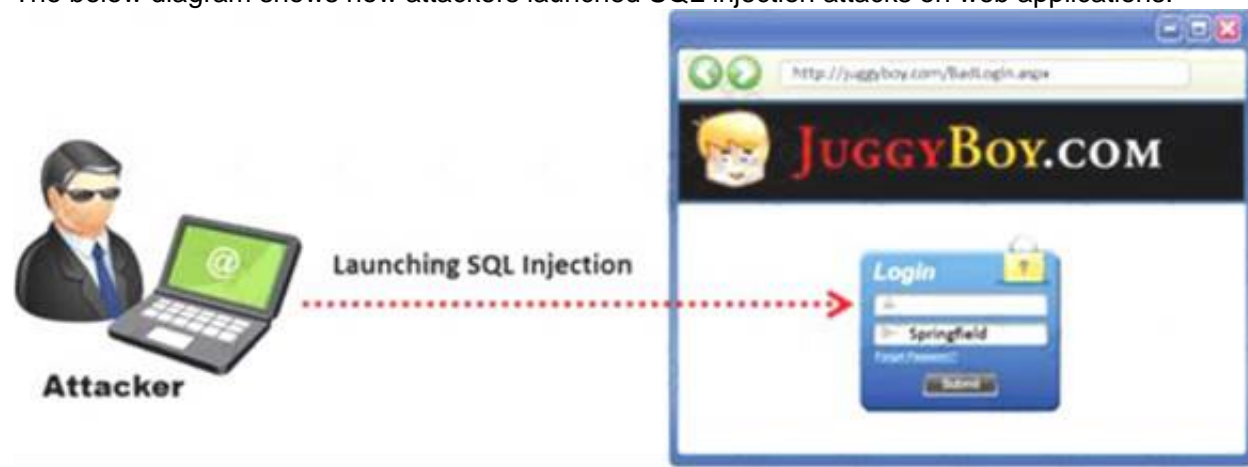
- A. Microsoft Baseline Security Analyzer (MBSA)
- B. CORE Impact
- C. Canvas
- D. Network Security Analysis Tool (NSAT)

Answer: C

NEW QUESTION 186

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 189

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

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 195

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 200

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

NEW QUESTION 202

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

- A. Smurf scan

- B. Tracert
- C. Ping trace
- D. ICMP ping sweep

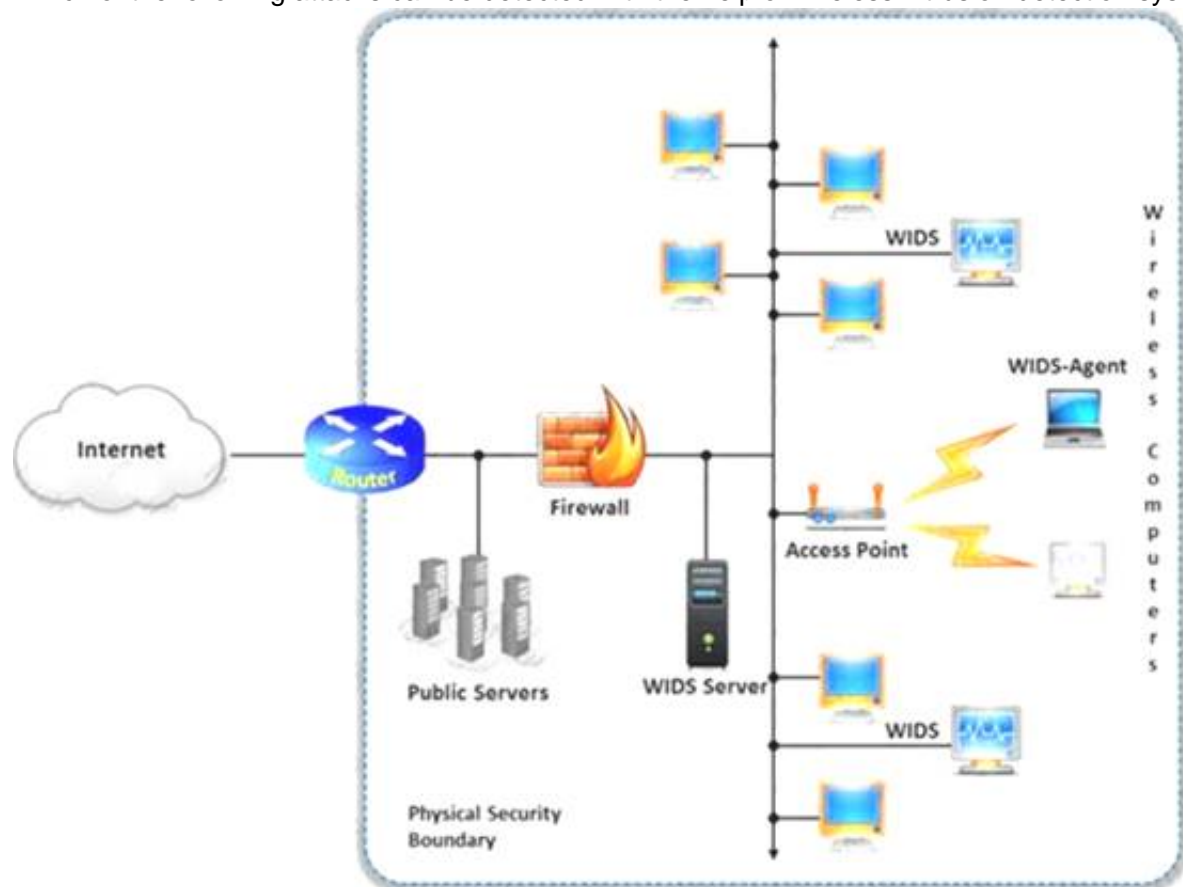
Answer: D

NEW QUESTION 204

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools.

The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

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



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

Answer: D

NEW QUESTION 205

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs.

The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

- A. Pattern matching
- B. Statistical-based anomaly detection
- C. Real-time anomaly detection
- D. Signature-based anomaly detection

Answer: C

NEW QUESTION 207

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 208

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 209

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The ECSAv10 Practice Test Here](#)