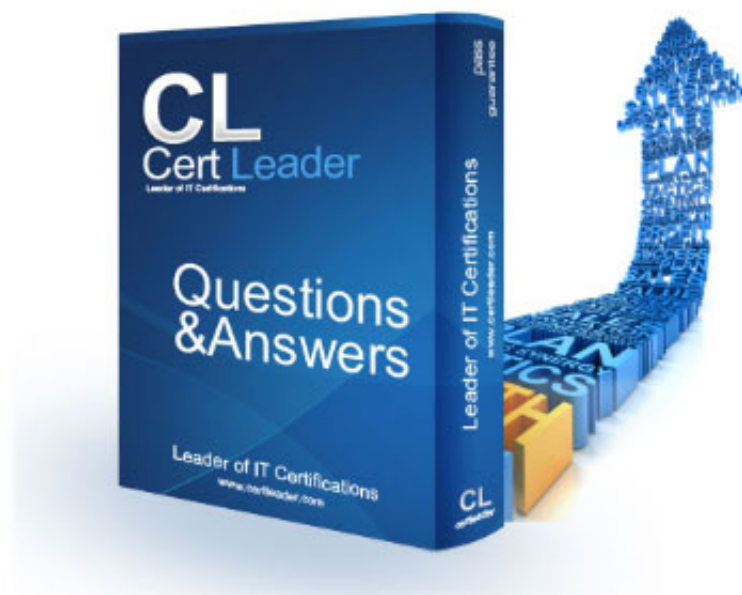


412-79v10 Dumps

EC-Council Certified Security Analyst (ECSA) V10

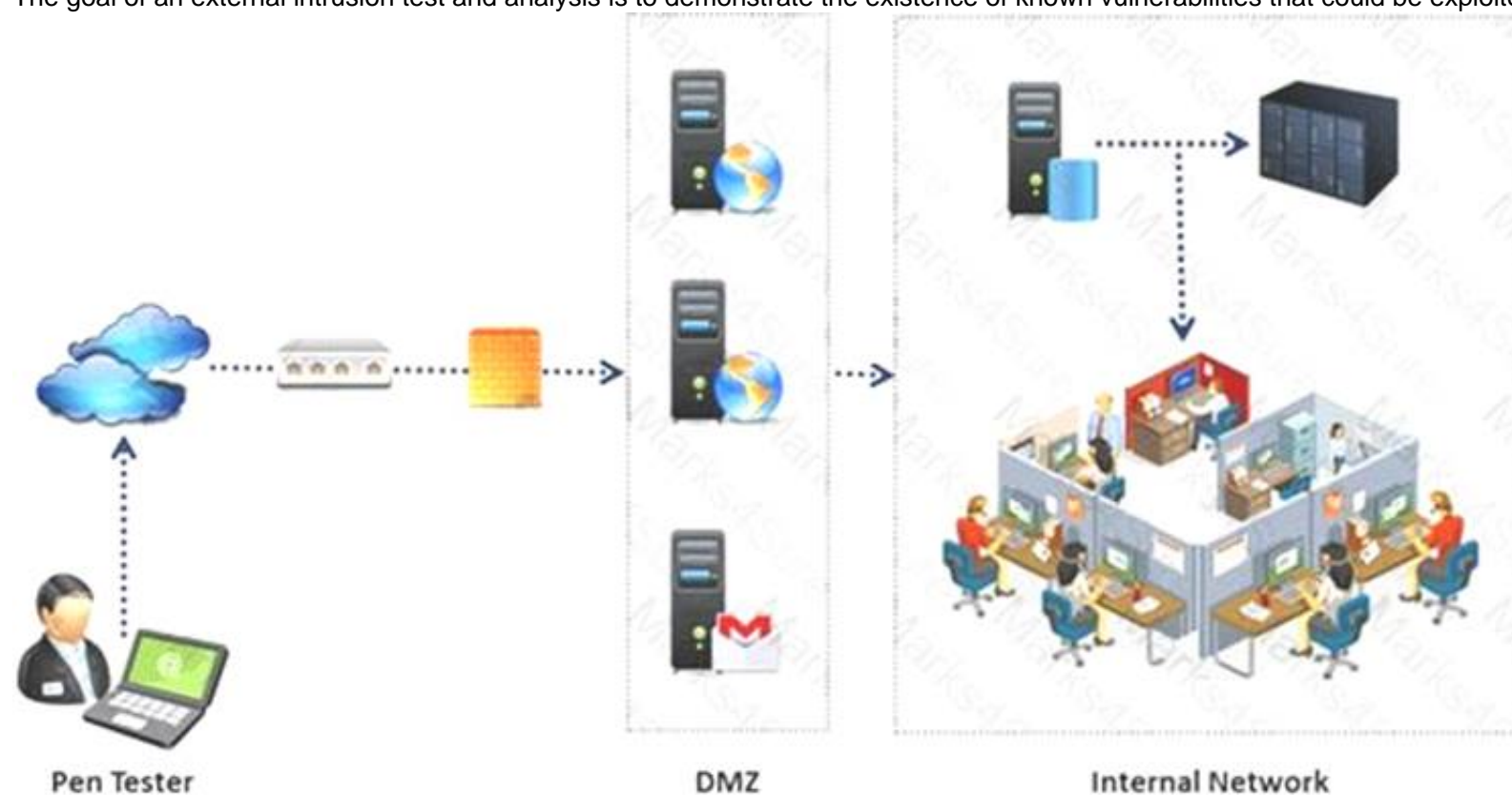
<https://www.certleader.com/412-79v10-dumps.html>



NEW QUESTION 1

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 2

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 3

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 4

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

`http://www.thetargetsite.com/scripts/../../../../../../../../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 5

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 6

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 7

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

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

Answer: B

NEW QUESTION 8

To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

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

Answer: C

NEW QUESTION 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

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet".

Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

- A. More RESET packets to the affected router to get it to power back up
- B. RESTART packets to the affected router to get it to power back up
- C. The change in the routing fabric to bypass the affected router
- D. STOP packets to all other routers warning of where the attack originated

Answer: C

NEW QUESTION 10

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 11

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 15

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG. What is Simon trying to accomplish here?

- A. Enumerate all the users in the domain
- B. Perform DNS poisoning
- C. Send DOS commands to crash the DNS servers
- D. Perform a zone transfer

Answer: D

NEW QUESTION 16

Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents	
1 The Cover Letter.....	2
1.1 Document Properties.....	3
1.2 Version.....	3
1.3 Table of Contents and List of Illustrations.....	4
1.4 Final Report Delivery Date.....	4
2 The Executive Summary.....	5
2.1 Scope of the Project.....	5
2.2 Purpose for the Evaluation.....	6
2.3 System Description.....	6
2.4 Assumption.....	7
2.5 Timeline.....	8
2.6 Summary of Evaluation.....	9
2.7 Summary of Findings.....	10
2.8 Summary of Recommendations.....	11
2.9 Testing Methodology.....	12
2.10 Planning.....	14
2.11 Exploitation.....	14
2.12 Reporting.....	15
3 Comprehensive Technical Report.....	16
3.1 Detailed SYSTEMS Information.....	17
3.2 Windows server.....	18
4 Result Analysis.....	19
5 Recommendations.....	20
6 Appendixes.....	21
6.1 Required Work Efforts.....	22
6.2 Research.....	24
6.3 References.....	24
6.4 Glossary.....	25

- A. Client-Side Test Report
- B. Activity Report
- C. Host Report
- D. Vulnerability Report

Answer: A

NEW QUESTION 17

Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

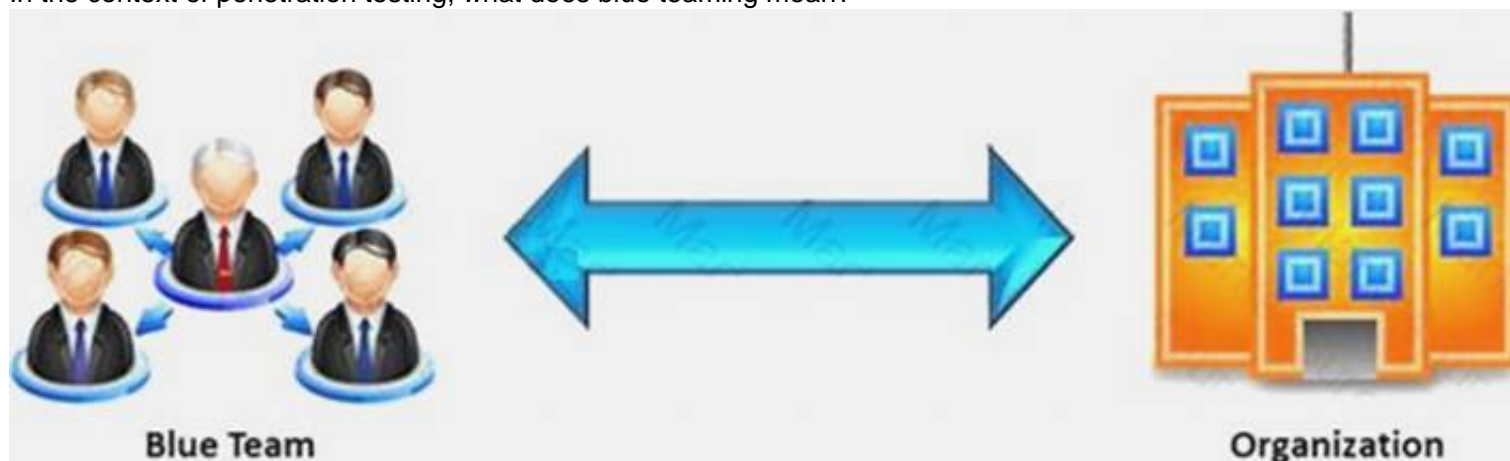
```
include <stdio.h>
#include <string.h>
int main(int argc, char *argv[])
{
char buffer[10]; if (argc < 2)
{
fprintf(stderr, "USAGE: %s string\n", argv[0]); return 1;
}
strcpy(buffer, argv[1]); return 0;
}
```

- A. Buffer overflow
- B. Format string bug
- C. Kernal injection
- D. SQL injection

Answer: A

NEW QUESTION 19

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 20

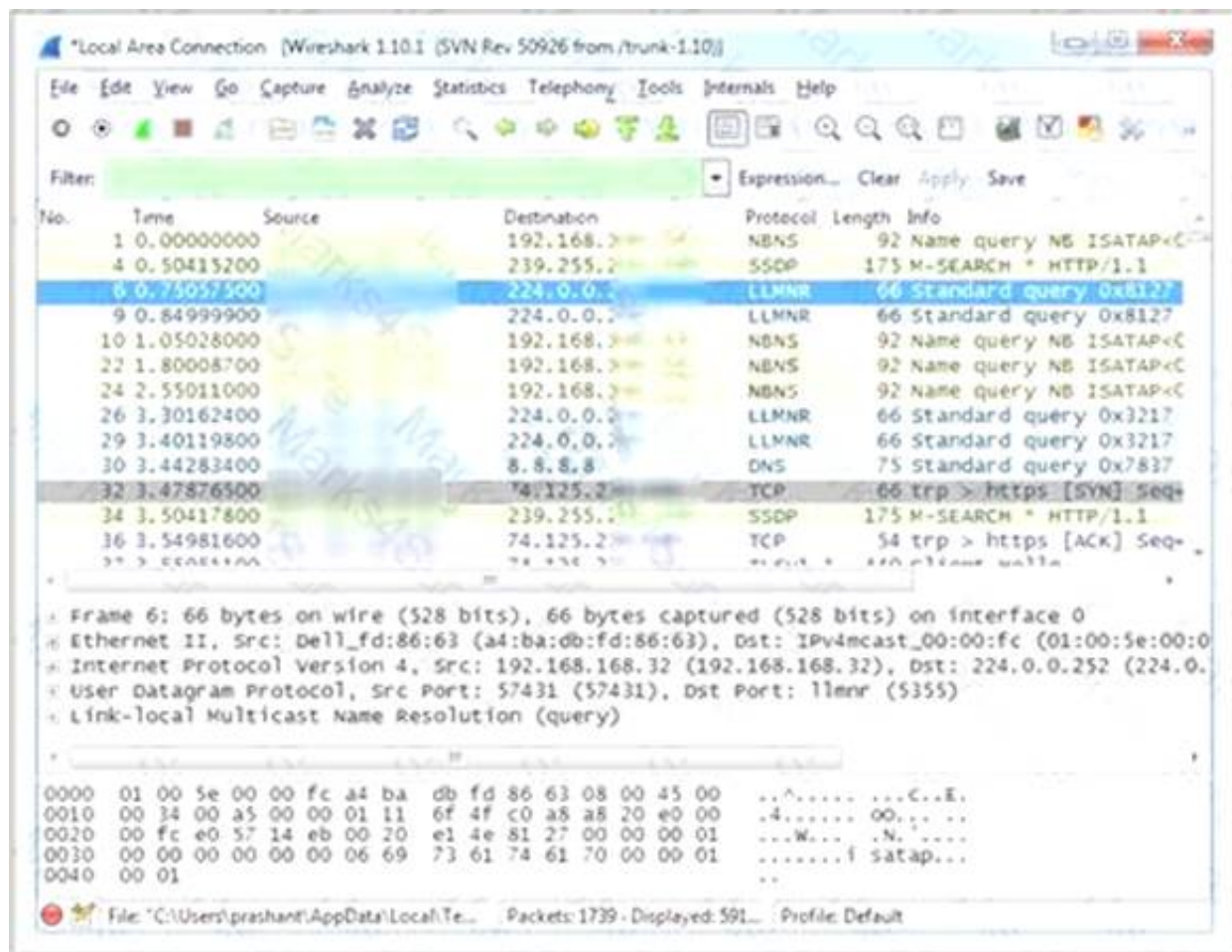
Identify the policy that defines the standards for the organizational network connectivity and security standards for computers that are connected in the organizational network.

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

Answer: C

NEW QUESTION 21

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 26

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 28

DNS information records provide important data about:

- A. Phone and Fax Numbers
- B. Location and Type of Servers
- C. Agents Providing Service to Company Staff
- D. New Customer

Answer: B

NEW QUESTION 30

Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

- A. Special-Access Policy
- B. User Identification and Password Policy
- C. Personal Computer Acceptable Use Policy
- D. User-Account Policy

Answer: B

NEW QUESTION 35

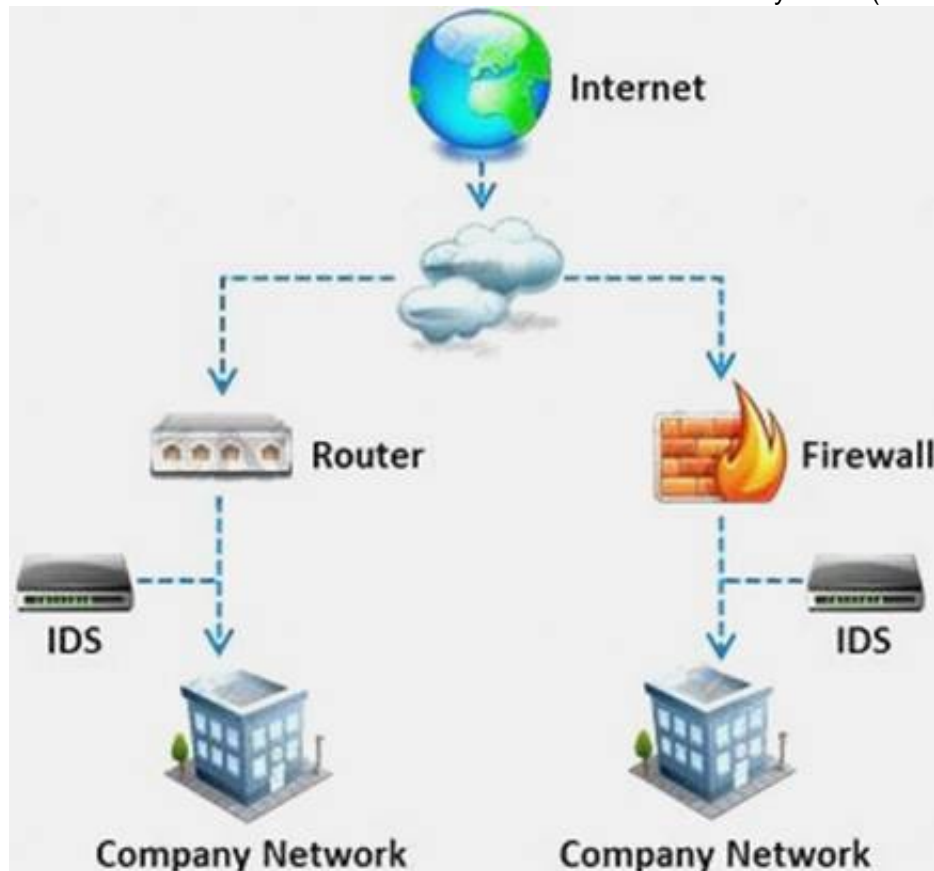
Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?

- A. AES
- B. DES (ECB mode)
- C. MD5
- D. RC5

Answer: C

NEW QUESTION 38

What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



- A. NIDS are usually a more expensive solution to implement compared to HIDS.
- B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
- C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.
- D. HIDS requires less administration and training compared to NIDS.

Answer: C

NEW QUESTION 41

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 45

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 49

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 53

Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most people say 'Wireless' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and G. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

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

Answer: A

NEW QUESTION 54

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 55

What are the 6 core concepts in IT security?



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

Answer: B

NEW QUESTION 59

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 63

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 66

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

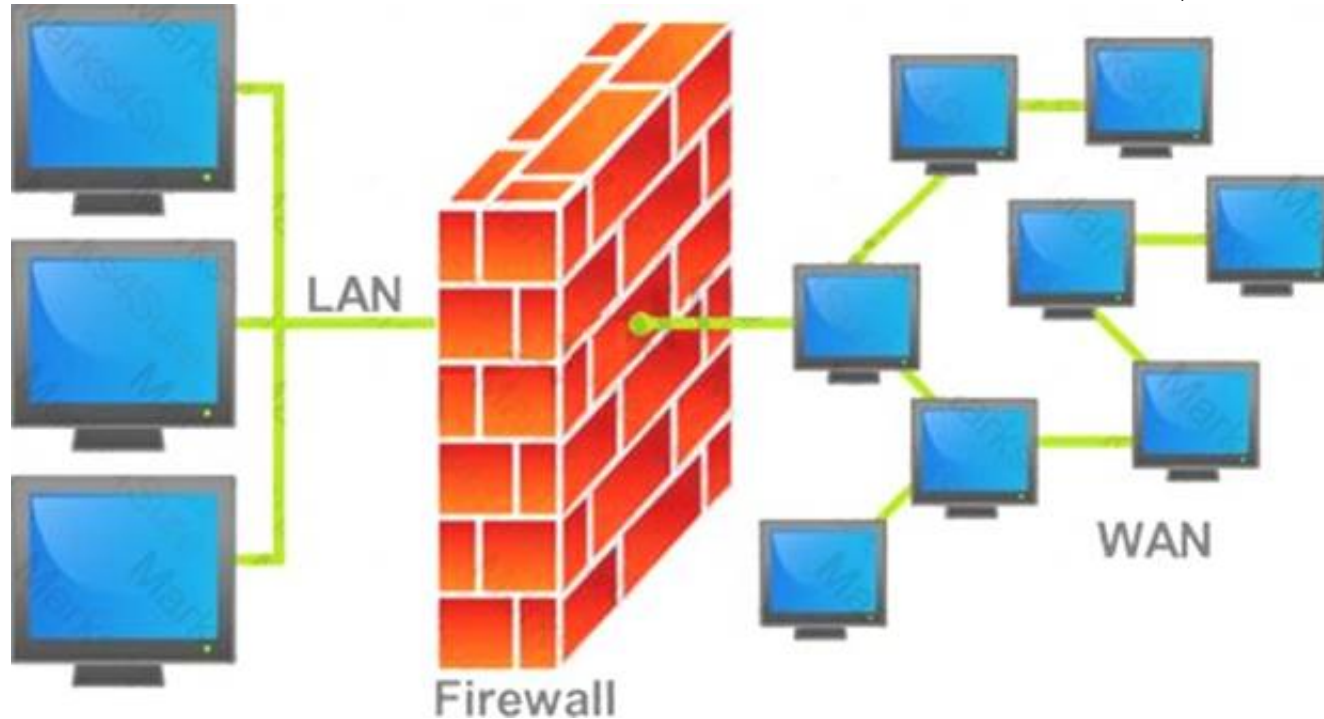
Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

- A. ./snort -dvr packet.log icmp
- B. ./snort -dev -l ./log
- C. ./snort -dv -r packet.log
- D. ./snort -l ./log -b

Answer: C

NEW QUESTION 72

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.



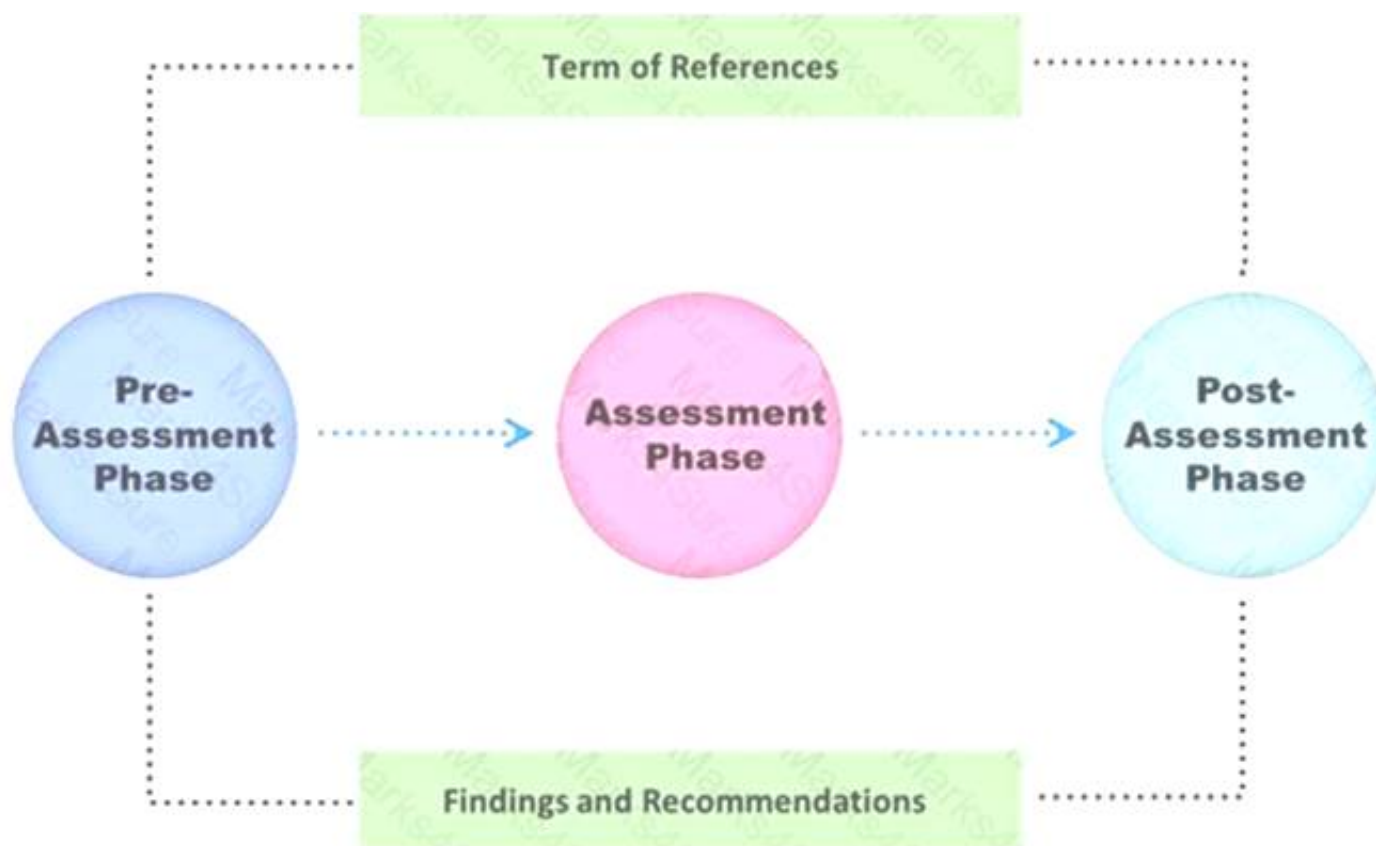
Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

- 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: A

NEW QUESTION 76

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



What does a vulnerability assessment identify?

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

Answer: B

NEW QUESTION 80

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\$GteyHdicpGOffXX40w#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

NEW QUESTION 81

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

link:www.ghttech.net

What will this search produce?

- A. All sites that link to ghttech.net
- B. Sites that contain the code: link:www.ghntech.net
- C. All sites that ghttech.net links to
- D. All search engines that link to .net domains

Answer: A

NEW QUESTION 85

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 89

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 94

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 96

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 98

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 101

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 106

Which one of the following log analysis tools is used for analyzing the server's log files?

- A. Performance Analysis of Logs tool
- B. Network Sniffer Interface Test tool
- C. Ka Log Analyzer tool
- D. Event Log Tracker tool

Answer: C

NEW QUESTION 108

Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

- A. Threat-Assessment Phase
- B. Pre-Assessment Phase
- C. Assessment Phase
- D. Post-Assessment Phase

Answer: B

NEW QUESTION 113

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 117

Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

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

Answer: A

NEW QUESTION 121

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. Aircsnort
- B. Aircrack
- C. Aircpwn
- D. WEPCrack

Answer: C

NEW QUESTION 122

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 123

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 127

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
```

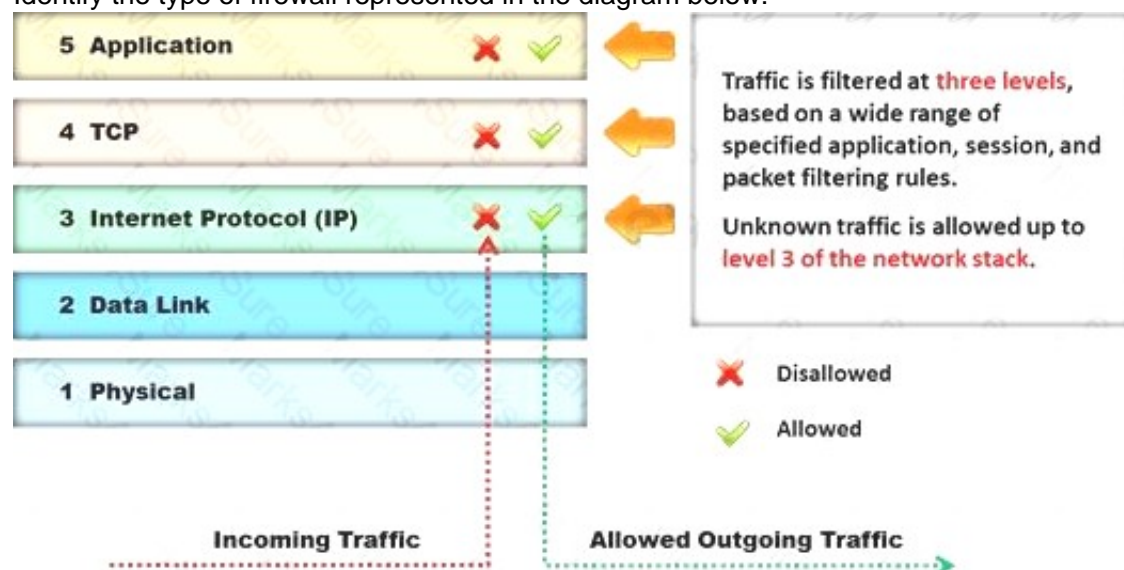
>
What have you found?

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

Answer: C

NEW QUESTION 130

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 134

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 138

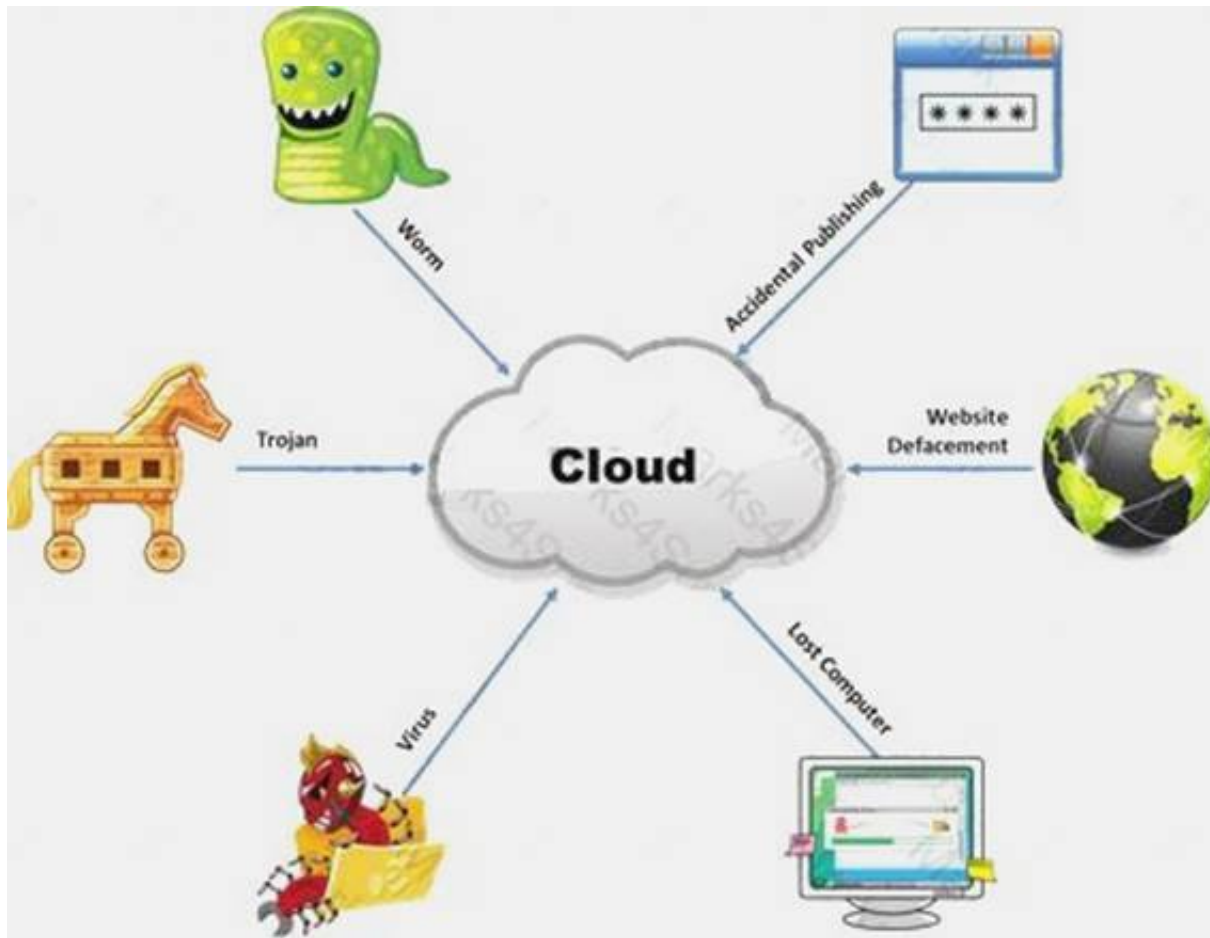
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

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

Answer: D

NEW QUESTION 139

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 141

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 146

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 151

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 153

A Demilitarized Zone (DMZ) is a computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization.

Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

- A. Lightweight Directory Access Protocol (LDAP)
- B. Simple Network Management Protocol (SNMP)
- C. Telnet
- D. Secure Shell (SSH)

Answer: D

NEW QUESTION 156

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 158

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 161

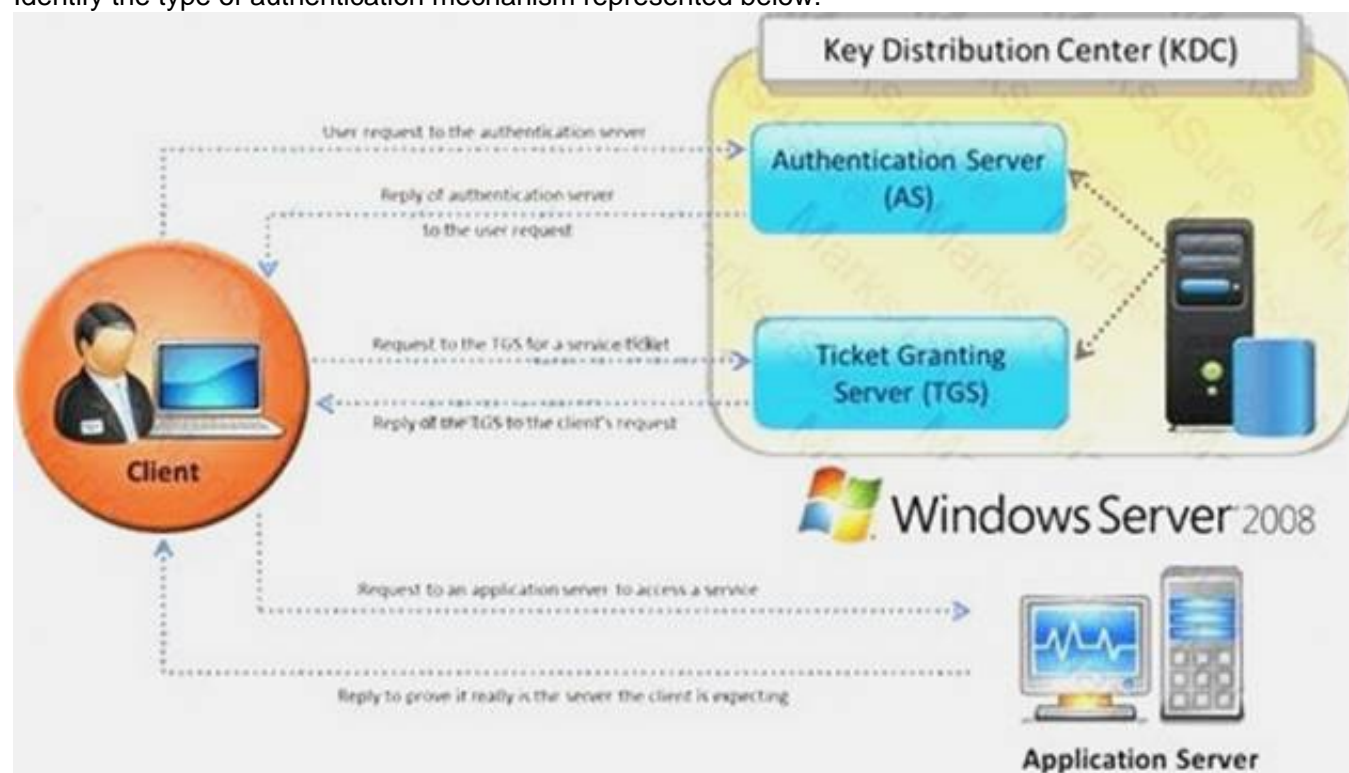
You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into 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 166

Identify the type of authentication mechanism represented below:



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

Answer: D

NEW QUESTION 171

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 174

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 178

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 180

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 182

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 184

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 187

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 191

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 195

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 197

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

- A. Analyzing, categorizing and prioritizing resources
- B. Evaluating the existing perimeter and internal security
- C. Checking for a written security policy
- D. Analyzing the use of existing management and control architecture

Answer: C

NEW QUESTION 199

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

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

Answer: A

NEW QUESTION 202

The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc.

Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations.

Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.



What is the best way to protect web applications from parameter tampering attacks?

- A. Validating some parameters of the web application
- B. Minimizing the allowable length of parameters
- C. Using an easily guessable hashing algorithm
- D. Applying effective input field filtering parameters

Answer: D

NEW QUESTION 206

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

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

Answer: A

NEW QUESTION 208

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 209

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 214

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 215

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 216

Identify the framework that comprises of five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement:

- A. Information System Security Assessment Framework (ISSAF)
- B. Microsoft Internet Security Framework
- C. Nortells Unified Security Framework
- D. Federal Information Technology Security Assessment Framework

Answer: D

NEW QUESTION 221

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

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

Answer: A

NEW QUESTION 223

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

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

Answer: A

NEW QUESTION 228

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

- A. Poison the DNS records with false records
- B. Enumerate MX and A records from DNS
- C. Establish a remote connection to the Domain Controller
- D. Enumerate domain user accounts and built-in groups

Answer: D

NEW QUESTION 232

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 236

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 240

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

`http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--`

`http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--`

`http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--`

`http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—`

What is the table name?

- A. CTS
- B. QRT
- C. EMP
- D. ABC

Answer: C

NEW QUESTION 242

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 247

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 251

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

- A. Filtered
- B. Stealth
- C. Closed
- D. Open

Answer: D

NEW QUESTION 255

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 257

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 259

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 263

Identify the injection attack represented in the diagram below:

XML Request

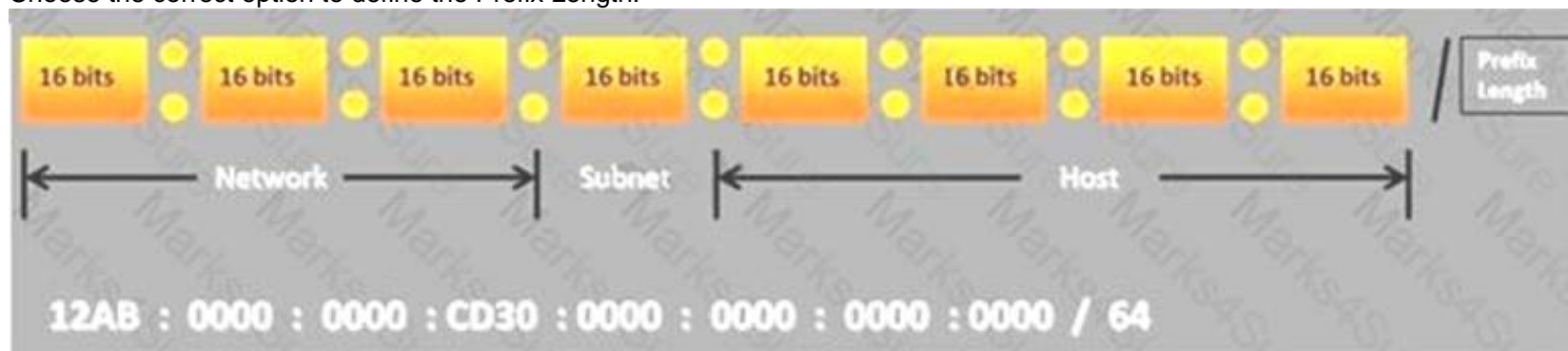
```
<CustomerRecord>
  <CustomerNumber>2010</CustomerNumber>
  <FirstName>Jason</FirstName><CustomerNumber>
2010</CustomerNumber>
  <FirstName>Jason</FirstName>
  <LastName>Springfield</LastName>
  <Address>Apt 20, 3rd Street</Address>
  <Email>jason@springfield.com</Email>
  <PhoneNumber>6325896325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

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

Answer: C

NEW QUESTION 268

Choose the correct option to define the Prefix Length.



- A. Prefix Length = Subnet + Host portions
- B. Prefix Length = Network + Host portions
- C. Prefix Length = Network + Subnet portions
- D. Prefix Length = Network + Subnet + Host portions

Answer: C

NEW QUESTION 269

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



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

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

Answer: D

NEW QUESTION 271

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

- A. Circuit level firewalls

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

Answer: D

NEW QUESTION 275

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 279

External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.



Which of the following types of penetration testing is performed with no prior knowledge of the site?

- A. Blue box testing
- B. White box testing
- C. Grey box testing
- D. Black box testing

Answer: D

NEW QUESTION 281

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

- A. IPSEC does not work with packet filtering firewalls
- B. NAT does not work with IPSEC
- C. NAT does not work with statefull firewalls
- D. Statefull firewalls do not work with packet filtering firewalls

Answer: B

NEW QUESTION 284

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 287

In Linux, what is the smallest possible shellcode?

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

Answer: D

NEW QUESTION 289

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

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

Answer: D

NEW QUESTION 291

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



Which of the following information gathering terminologies refers to gathering information through social engineering on-site visits, face-to-face interviews, and direct questionnaires?

- A. Active Information Gathering
- B. Pseudonymous Information Gathering
- C. Anonymous Information Gathering
- D. Open Source or Passive Information Gathering

Answer: A

NEW QUESTION 294

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 297

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 300

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies.

A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces.

What could have prevented this information from being stolen from the laptops?

- A. SDW Encryption
- B. EFS Encryption
- C. DFS Encryption

D. IPS Encryption

Answer: B

NEW QUESTION 301

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 303

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the Restrict Anonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server.

Using User info tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

- A. Restrict Anonymous must be set to "2" for complete security
- B. Restrict Anonymous must be set to "3" for complete security
- C. There is no way to always prevent an anonymous null session from establishing
- D. Restrict Anonymous must be set to "10" for complete security

Answer: A

NEW QUESTION 308

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 312

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 313

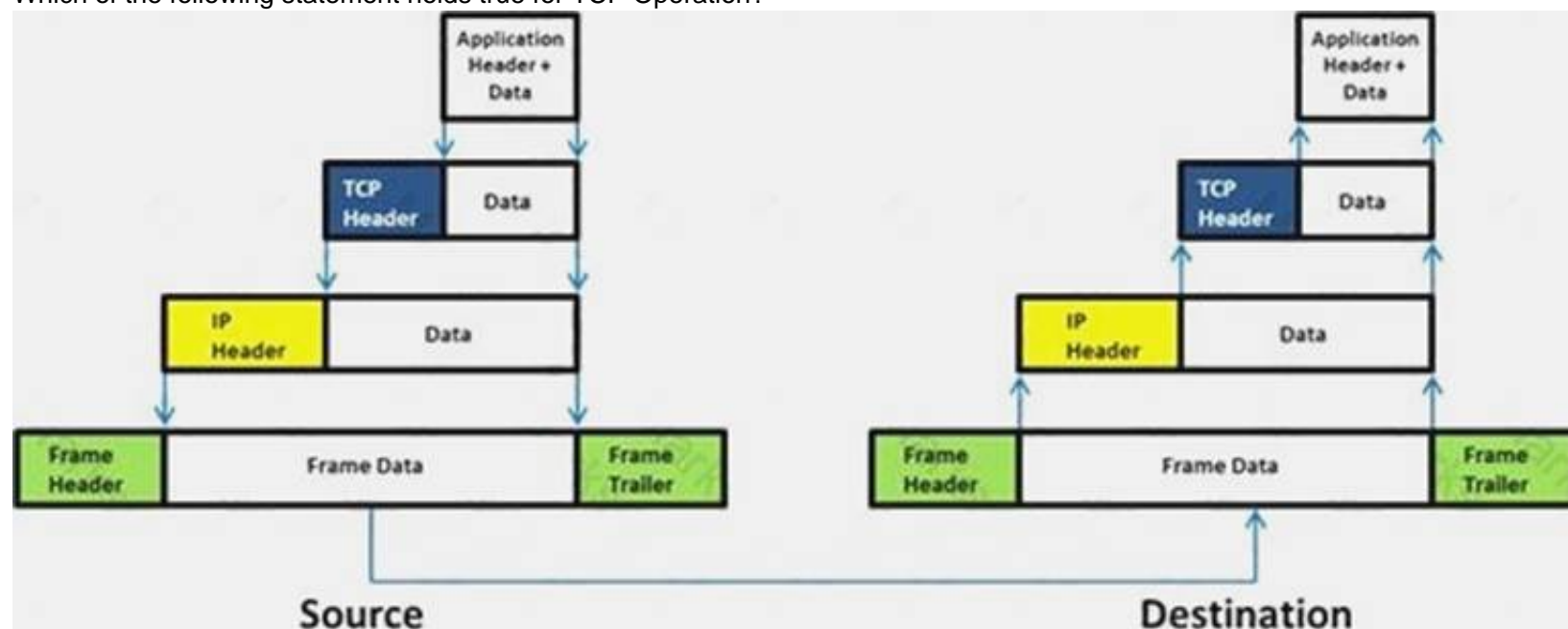
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five 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 318

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

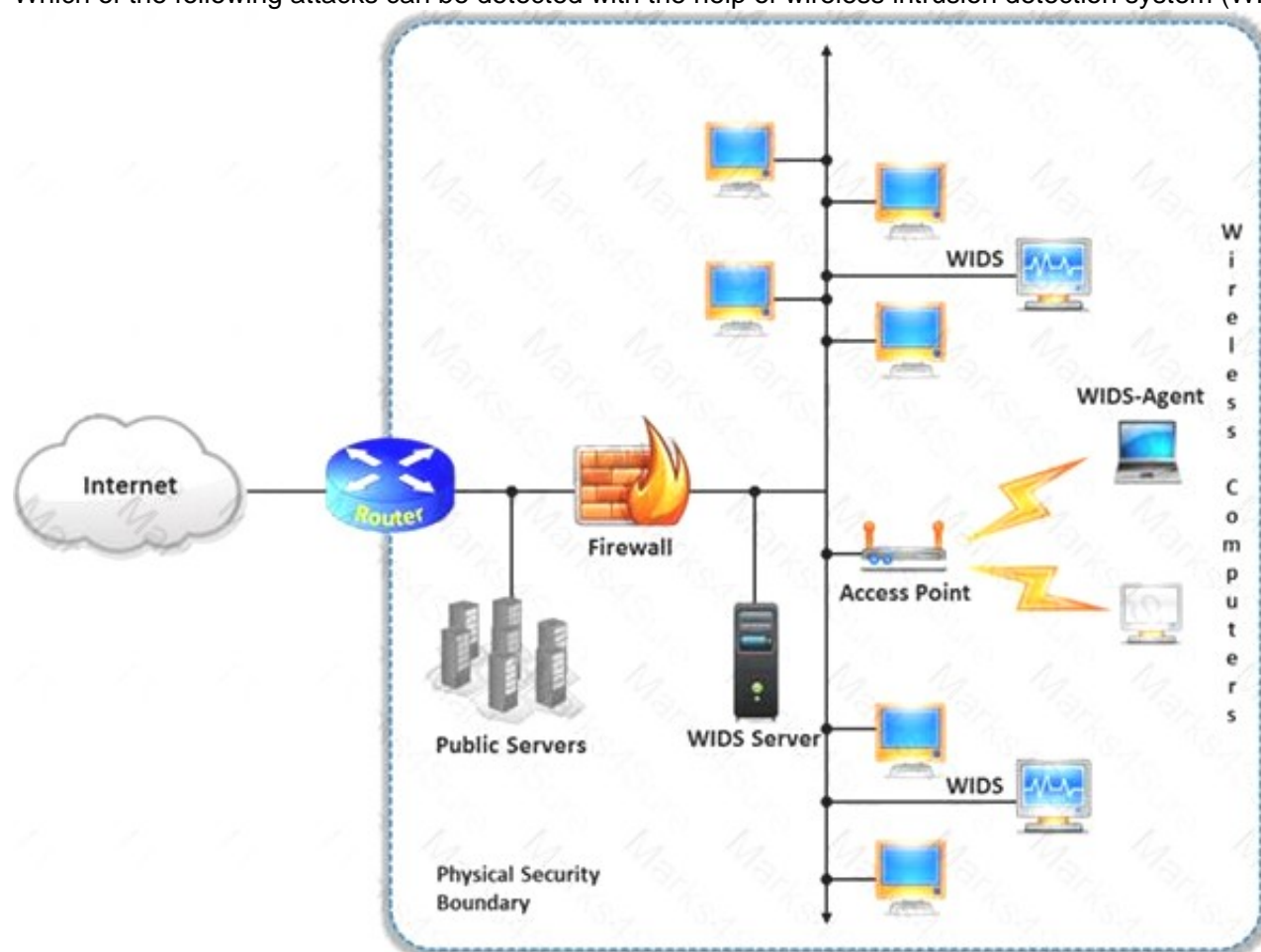
Answer: D

NEW QUESTION 319

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 320

Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

- A. Using session hijacking
- B. Using proxy servers
- C. Using authentication
- D. Using encryption

Answer: B

NEW QUESTION 324

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 325

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 326

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 330

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 331

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 335

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 340

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 342

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 344

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

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

Answer: A

NEW QUESTION 346

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 350

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted.

Which one of the following scanned timing options in NMAP's scan is useful across slow WAN links or to hide the scan?

- A. Paranoid
- B. Sneaky
- C. Polite
- D. Normal

Answer: C

NEW QUESTION 351

What is the target host IP in the following command?

```
C:\> firewall -F 80 10.10.150.1 172.16.28.95 -p UDP
```

- A. Firewall 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 353

Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

- A. Wireshark: Capinfos
- B. Wireshark: Tcpdump
- C. Wireshark: Text2pcap
- D. Wireshark: Dumpcap

Answer: D

NEW QUESTION 356

Output modules allow Snort to be much more flexible in the formatting and presentation of output to its users. Snort has 9 output plug-ins that push out data in different formats. Which one of the following output plug-ins allows alert data to be written in a format easily importable to a database?

- A. unified
- B. csv
- C. alert_unixsock
- D. alert_fast

Answer: B

NEW QUESTION 361

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa.

She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for.

What principal of social engineering did Julia use?

- A. Reciprocation
- B. Friendship/Liking
- C. Social Validation
- D. Scarcity

Answer: A

NEW QUESTION 363

Why is a legal agreement important to have before launching a penetration test?

Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

- A. Guarantees your consultant fees
- B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
- C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
- D. It is important to ensure that the target organization has implemented mandatory security policies

Answer: C

NEW QUESTION 364

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 367

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

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

Answer: B

NEW QUESTION 368

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 373

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 374

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 412-79v10 Exam with Our Prep Materials Via below:

<https://www.certleader.com/412-79v10-dumps.html>