Vendor: EC-Council

Exam Code: EC0-479

Exam Name: EC-Council Certified Security Analyst(ECSA)

Version: Demo

QUESTION 1
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Change the default community string names
B. Block all internal MAC address from using SNMP
C. Block access to UDP port 171
D. Block access to TCP port 171

Correct Answer: A

QUESTION 2
At what layer of the OSI model do routers function on?

A. 3
B. 4
C. 5
D. 1

Correct Answer: A

QUESTION 3
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

Correct Answer: A

QUESTION 4
What operating system would respond to the following command?

```
C:\> nmap -sW 10.10.145.65
```

A. Mac OS X
B. Windows XP
C. Windows 95
D. FreeBSD

Correct Answer: D

QUESTION 5
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Windows computers will not respond to idle scans
B. Linux/Unix computers are constantly talking
C. Linux/Unix computers are easier to compromise
D. Windows computers are constantly talking

Correct Answer: D

QUESTION 6

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

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

Correct Answer: D

QUESTION 7
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Windows computers are constantly talking
B. Linux/Unix computers are constantly talking
C. Linux/Unix computers are easier to compromise
D. Windows computers will not respond to idle scans

Correct Answer: A

QUESTION 8
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

Correct Answer: D

QUESTION 9
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 CSS
C. Your website is not vulnerable
D. Your website is vulnerable to SQL injection

Correct Answer: B

QUESTION 10
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 RestrictAnonymous 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 Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

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

Correct Answer: A

QUESTION 11
What will the following command accomplish?

```
C:\> nmap -v -sS -Po 172.16.28.251 -data_length 66000-packet_trace
```

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle fragmented packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle under-sized packets

Correct Answer: A

QUESTION 12
What are the security risks of running a "repair" installation for Windows XP?

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

Correct Answer: D

QUESTION 13
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

Correct Answer: C

QUESTION 14
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

Correct Answer: C

QUESTION 15
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

Correct Answer: D

QUESTION 16
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. Oligomorhic
C. Polymorphic
D. Transmorphic

Correct Answer: A

QUESTION 17
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

Correct Answer: C

QUESTION 18
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 network

Correct Answer: C

QUESTION 19
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your

Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Simple Network Management Protocol
B. Broadcast System Protocol
C. Cisco Discovery Protocol
D. Border Gateway Protocol

Correct Answer: C

QUESTION 20
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud
B. There are no ways of performing a "stealthy" wireless scan
C. Nessus cannot perform wireless testing
D. Nessus is not a network scanner

Correct Answer: A

QUESTION 21
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

Correct Answer: B

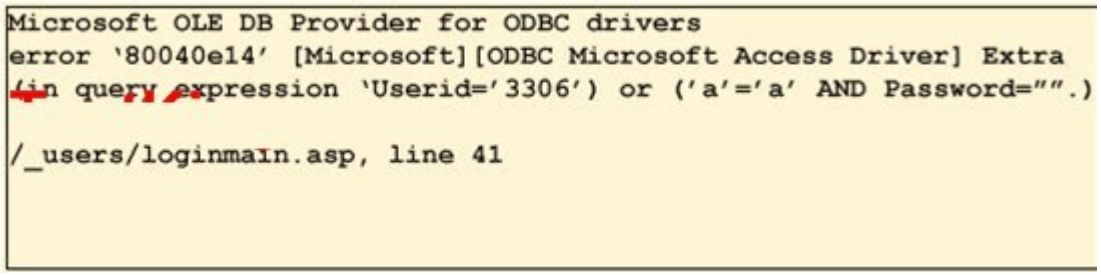
QUESTION 22
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

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

Correct Answer: C

QUESTION 23
To test your website for vulnerabilities, you type in a quotation mark (? for the username field. After you click Ok, you receive the following error message window:

What can you infer from this error window?
Exhibit:



A. SQL injection is not possible
B. SQL injection is possible
C. The user for line 3306 in the SQL database has a weak password
D. The quotation mark (? is a valid username

Correct Answer: B

QUESTION 24
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 footprinting against their Web servers. What tool should you use?

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

Correct Answer: B

QUESTION 25
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

Correct Answer: B

QUESTION 26
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.ghttech.net
C. All sites that ghttech.net links to
D. All search engines that link to .net domains

Correct Answer: A

QUESTION 27
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. You cannot determine what privilege runs the daemon service
C. Root
D. Something other than root

Correct Answer: D

QUESTION 28
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Intruding into a honeypot is not illegal
B. Entrapment
C. Intruding into a DMZ is not illegal
D. Enticement

Correct Answer: B

QUESTION 29
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

Correct Answer: D

QUESTION 30
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Application-level proxy firewall
B. Data link layer firewall
C. Packet filtering firewall
D. Circuit-level proxy firewall

Correct Answer: A

QUESTION 31
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked
B. Only DNS traffic can be hijacked
C. Only FTP traffic can be hijacked
D. HTTP protocol does not maintain session

Correct Answer: D

QUESTION 32
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

Correct Answer: B

QUESTION 33
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

A. 31401
B. The zombie will not send a response
C. 31402
D. 31399

Correct Answer: A

QUESTION 34
What is the following command trying to accomplish?

```
C:\> nmap -sU -p445 192.168.0.0/24
```

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

Correct Answer: B

QUESTION 35
What will the following URL produce in an unpatched IIS Web Server?

```
http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\
```

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

Correct Answer: D

QUESTION 36
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

Correct Answer: A

QUESTION 37
A packet is sent to a router that does not have the packet destination address in its route table, how will

the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

Correct Answer: C

QUESTION 38
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 ombies? 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

Correct Answer: C

QUESTION 39
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

7+ years experience in Windows Server environment
5+ years experience in Exchange 2000/2003 environment
Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired,
MCSE, CEH preferred
No Unix/Linux Experience needed

What is this information posted on the job website considered?

A. Information vulnerability
B. Social engineering exploit
C. Trade secret
D. Competitive exploit

Correct Answer: A

QUESTION 40
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

Correct Answer: D

QUESTION 41
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 Lophtcrack 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

Correct Answer: D

QUESTION 42
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

Correct Answer: C

QUESTION 43
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

Correct Answer: A

QUESTION 44
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. Enumerate domain user accounts and built-in groups
B. Establish a remote connection to the Domain Controller
C. Poison the DNS records with false records
D. Enumerate MX and A records from DNS

Correct Answer: A

QUESTION 45
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. Perform a zone transfer
B. Perform DNS poisoning
C. Send DOS commands to crash the DNS servers
D. Enumerate all the users in the domain

Correct Answer: A

QUESTION 46
Why is it a good idea to perform a penetration test from the inside?

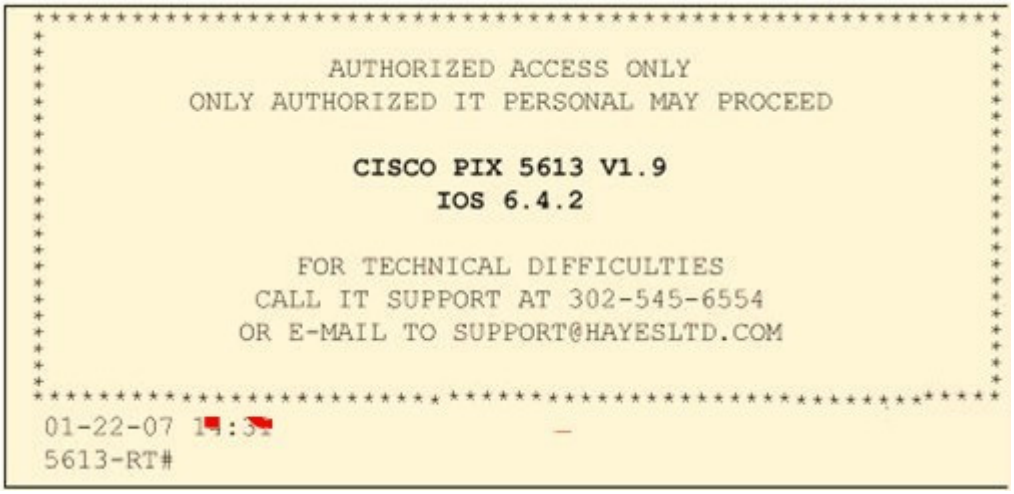
A. It is easier to hack from the inside
B. It is never a good idea to perform a penetration test from the inside
C. To attack a network from a hacker's perspective
D. Because 70% of attacks are from inside the organization

Correct Answer: D

QUESTION 47
Click on the Exhibit Button

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:



A. The banner should not state "only authorized IT personnel may proceed"
B. Remove any identifying numbers, names, or version information
C. The banner should include the Cisco tech support contact information as well
D. The banner should have more detail on the version numbers for the network equipment

Correct Answer: B

QUESTION 48
An "idle" system is also referred to as what?

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

Correct Answer: D

QUESTION 49
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. False negatives
B. True positives
C. True negatives
D. False positives

Correct Answer: A

QUESTION 50
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

Correct Answer: C

QUESTION 51
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. Enumerate domain user accounts and built-in groups
D. Establish a remote connection to the Domain Controller

Correct Answer: C

QUESTION 52
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. intitle:"exchange server"
B. outlook:"search"
C. locate:"logon page"
D. allinurl:"exchange/logon.asp"

Correct Answer: D

QUESTION 53
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable BGP
B. Disable BGP
C. Enable direct broadcasts
D. Disable direct broadcasts

Correct Answer: D

QUESTION 54
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

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

Correct Answer: C

QUESTION 55
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

Correct Answer: A

QUESTION 56
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

Correct Answer: A

QUESTION 57
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

Correct Answer: C

QUESTION 58
Software firewalls work at which layer of the OSI model?

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

Correct Answer: A

QUESTION 59
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 1386

Correct Answer: C

QUESTION 60
What does ICMP Type 3/Code 13 mean?

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

Correct Answer: D

QUESTION 61
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 lage 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

Correct Answer: C

QUESTION 62
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

Correct Answer: B

QUESTION 63
How many possible sequence number combinations are there in TCP/IP protocol?

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

Correct Answer: C

QUESTION 64
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. src port 22 and dst port 22
B. src port 23 and dst port 23
C. net port 22
D. udp port 22 and host 172.16.28.1/24

Correct Answer: A

QUESTION 65
Software firewalls work at which layer of the OSI model?

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

Correct Answer: D

QUESTION 66
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

Correct Answer: A

QUESTION 67
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. Ping trace
B. Tracert
C. Smurf scan
D. ICMP ping sweep

Correct Answer: D

QUESTION 68
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk sets all packets with a TTL of zero
B. Firewalk cannot pass through Cisco firewalls
C. Firewalk sets all packets with a TTL of one
D. Firewalk cannot be detected by network sniffers

Correct Answer: C

QUESTION 69
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. NIPS
B. Passive IDS
C. Progressive IDS
D. Active IDS

Correct Answer: D

QUESTION 70
As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The employees network usernames and passwords
B. The MAC address of the employees?computers
C. The IP address of the employees computers
D. Bank account numbers and the corresponding routing numbers

Correct Answer: A

QUESTION 71
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. You cannot determine what privilege runs the daemon service
B. Guest
C. Root
D. Something other than root

Correct Answer: D

QUESTION 72
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. Enable tunneling feature on the switch
B. Trick the switch into thinking it already has a session with Terri's computer
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Poison the switch's MAC address table by flooding it with ACK bits

Correct Answer: B

QUESTION 73
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

Correct Answer: A

QUESTION 74
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

Correct Answer: A

QUESTION 75
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Fuzzing
B. Tailgating
C. Man trap attack
D. Backtrapping

Correct Answer: B

QUESTION 76
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 Lophtcrack 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 SAM file from Hillary computer
B. Hillary network username and password hash
C. The SID of Hillary network account
D. The network shares that Hillary has permissions

Correct Answer: B

QUESTION 77
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

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

Correct Answer: D

QUESTION 78
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. NIPS
B. Passive IDS
C. Progressive IDS
D. Active IDS

Correct Answer: D

QUESTION 79
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's 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 footprinting against their Web servers. What tool should you use?

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

Correct Answer: B

QUESTION 80
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

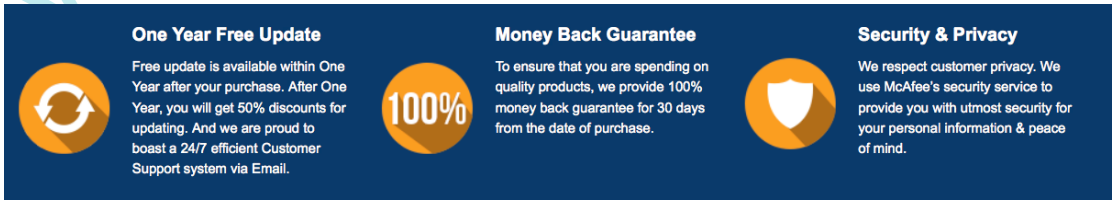
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.