ECCouncil 412-79

EC-Council Certified Security Analyst (ECSA)

Version: 5.0

QUESTION NO: 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

Answer: A

Explanation:

SNMP Version 1 does not provide encryption, so the community strings are in the clear.

Known community strings, the default of Public and Private, are well known because these are the default community strings that come out of the box. By changing these values to different community string names, guessing the actual names will be difficult.

QUESTION NO: 2

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

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

Answer: A

Explanation:

1 – Physical

2 – Data Link

3 – Network

4 – Transport

5 – Session

6 – Presentation

7 - Application

QUESTION NO: 3

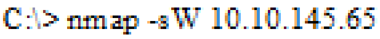
An "idle" system is also referred to as what?

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

Answer: A
Explanation:
In this case “idle” refers to a system that can be used as a go between for an idle scan. One workstation, sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system’s behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic. The ‘Idle” system is called a zombie.
The idle system is not a PC not being used because even a PC that is not in use could be generating network traffic. The issue is not whether a PC is in use, the issue is whether the PC is creating or processing network traffic.

QUESTION NO: 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

Answer: D
Explanation:
-sW Window scan: This advanced scan is very similar to
the ACK scan, except that it can sometimes detect
open ports as well as filtered/nonfiltered due to
an anomaly in the TCP window size reporting by some
operating systems. Systems vulnerable to this
include at least some versions of AIX, Amiga, BeOS,

BSDI, Cray, Tru64 UNIX, DG/UX, OpenVMS, Digital
UNIX, **FreeBSD**, HP-UX, OS/2, IRIX, MacOS, NetBSD,
OpenBSD, OpenStep, QNX, Rhapsody, SunOS 4.X,
Ultrix, VAX, and VxWorks. See the nmap-hackers
mailing list archive for a full list.

QUESTION NO: 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

Answer: D
Explanation:
In an idle scan, one workstation sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system's behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic

QUESTION NO: 6

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

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

Answer: D
Explanation:
48 bits is the size of a MAC address, and is layer 2
32 bits is the size of a IPV4 IP address, and is layer 3
16 bits is the size of an address for the TCP header and UDP header, and supports up to 65K ports

In each of these cases, the address size is the same for both a “source” and “destination” address.

QUESTION NO: 7

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
Explanation:
AXFR is a full DNS zone transfer, IXFR is an incremental DNS zone transfer.

QUESTION NO: 8

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

Explanation:

This indicates that Cross Site Scripting is possible. The proper acronym that is used is XSS and not CSS because CSS is already used in HTML for Cascading Style Sheets.

Web Bugs are usually a single pixel by single pixel within the HTML code.

SQL injection is usually performed by insertion of a quote character into a data field.

QUESTION NO: 9

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

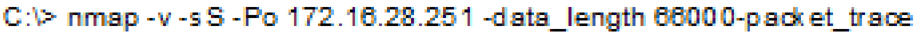
Answer: A

Explanation:

RestrictAnonymous is set by changing the registry key to 0 or 1 for Windows NT 4.0 or to 0, 1, or 2 for Windows 2000. These numbers correspond to the following settings:0 None. Rely on default permissions1 Do not allow enumeration of SAM accounts and names2 No access without explicit anonymous permissions

QUESTION NO: 10

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

Answer: A

Explanation:

-v (verbose) –sS (SYN scan) –Po (Ping Disable ICMP) target –data_length (option to control packet length) 66000 (size of packet) –packet_trace (Display nmap conversations during trace)

QUESTION NO: 11

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

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

Answer: D

Explanation:

QUESTION NO: 12

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

Explanation: Ettercap is the best answer as that tool makes extracting of username and password easier.

QUESTION NO: 13

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
Explanation:
Port 22 is the default port for SSH and is also used for sFTP. Since George wants traffic to and from the network, he needs the packets with either a source port of 22 (incoming) or dest port of 22 (outgoing)
Port 23 is the default port for Telnet.
sFTP uses TCP, not UDP

QUESTION NO: 14

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

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

Answer: D
Explanation:
The firewall has to keep track of outgoing sessions and only allow replies to those internally initiated sessions. This requires maintaining session state, and thus a stateful firewall.

QUESTION NO: 15

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

Answer: A
Explanation:

QUESTION NO: 16

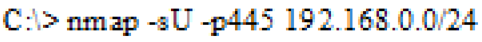
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions 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
Explanation:
When a router is taken offline, including this case where a denial of service disabled the router, the remaining routers will effectively remove the failed router from their tables and route traffic around that router – as if the router never existed.

QUESTION NO: 17

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

Answer: C
Explanation:
-sU is protocol UDP, -p445 is port 445
Although on a Windows system port 445 is used for access to file shares, called the Common Internet File System and is part of the SMB (server message block) mechanism, it is not really considered NetBIOS. Even if this was NetBIOS, the question could be confusing.
Option C is the best answer.

QUESTION NO: 18

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

Answer: C
Explanation:

QUESTION NO: 19

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

Answer: A
Explanation:

QUESTION NO: 20

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
Explanation:
A false negative is when something is there, but it is not found or reported. The vulnerability scan did not detect the vulnerability, so the vulnerability was actually there, but the scanner did not find it.
A false positive is reporting that something is there, but it is not. If the vulnerability scanner reported vulnerabilities that did not exist, then it would a false positive.
True Positives and True negatives occur when there are no reporting errors.

QUESTION NO: 21

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

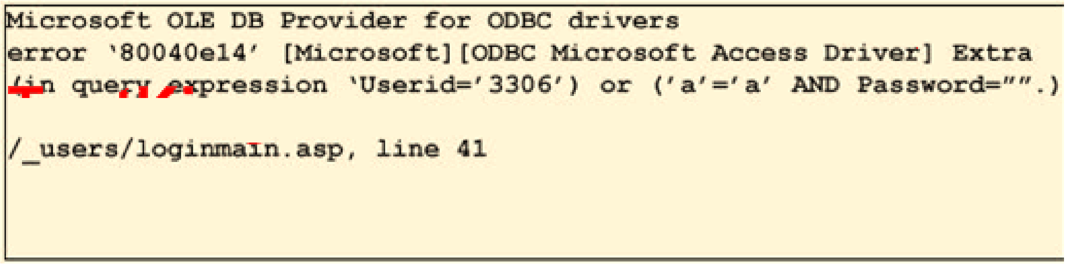
Explanation:

QUESTION NO: 22

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:



```
Microsoft OLE DB Provider for ODBC drivers
error '80040e14' [Microsoft][ODBC Microsoft Access Driver] Extra
(in query expression 'Userid='3306') or ('a'='a' AND Password="".)

/_users/loginmain.asp, line 41
```

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

Answer: B

Explanation:

QUESTION NO: 23

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

Answer: B

Explanation:

QUESTION NO: 24

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

Explanation:

QUESTION NO: 25

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

Answer: A

Explanation:

QUESTION NO: 26

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

Answer: D
Explanation:
Answer D is the best answer. Root privilege should be used for a service (daemon). If the service is compromised, then the attacker gains root privilege. The principle of least privilege should be followed and root should not be given to services or daemons.

QUESTION NO: 27

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

Answer: B
Explanation:

QUESTION NO: 28

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

A. Smurf scan
B. Tracert
C. Ping trace

D. ICMP ping sweep

Answer: D

Explanation:

Answer D is the best answer. ICMP Echo requests make up the PING function, and a scan to find hosts usually involves a PING Sweep.

QUESTION NO: 29

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

Answer: A

Explanation:

QUESTION NO: 30

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

Answer: D

Explanation:

QUESTION NO: 31

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

Explanation:

Answer B is the best answer. A mantrap is built with 2 set of doors, creating a trap between the 2 sets of doors. Only one set of doors can be unlocked at a time, one set of doors open, the person enters, those doors close and lock, and then the other set opens, allowing the person to pass through. A security guard, or camera, is used to make sure that only one person enters the mantrap at a time.

QUESTION NO: 32

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

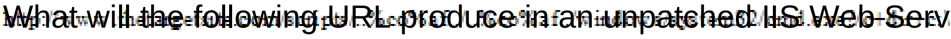
Answer: A

Explanation:

Answer A is the best answer. If the machine is “idle”, it will not be sending or receiving traffic.

QUESTION NO: 33

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



[illegible]

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

Explanation:

Answer D is the best answer. This is an Windows IIS Directory Traversal Attack where the command is able to run programs out of the windows/system32 directory. In this case, cmd.exe which is the command prompt.

Answer C is incorrect, the SYSTEM32 subdirectory is where the cmd.exe program resides. The parameters to the command prompt follows the ? in the URL.

QUESTION NO: 34

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

Explanation:

QUESTION NO: 35

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 proper destination?

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

Answer: C

Explanation:

Answer C is the best answer. When a packet has to be forwarded, and there is no match in the routing table, the packet is sent to the default router. This is not just for routers, a host will have an internal routing table, and will act in the same manner.

QUESTION NO: 36

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
Explanation:
Answer C is the best answer. If zombies or bots are used, then this may be a special denial of service (DoS) called a distributed denial of service (DDoS). When the intent is to shut something down, the objective is usually denial of service.

QUESTION NO: 37

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

Answer: A
Explanation:
Answer A is the best answer. This job description leaks out too much information about the inside configuration of the data center, which can be used when launching an attack.

QUESTION NO: 38

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
Explanation:
Answer D is the best answer. If the port is actually open, it will not respond to a XMAS scan. This question doesn't ask what nmap will report, it just asks for the state of the port.

QUESTION NO: 39

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

Answer: D
Explanation:
Answer D is the best answer. Lophtcrack is a password cracking program used in the Windows environment. When in sniffer mode the program will catch credentials on the wire and crack the password. When Hillary clicks on the link, her network credentials are attached to the request to authenticate her. Lophtcrack will catch the network username and the password hash, and then can be used later to crack the hash and determine the cleartext password.

QUESTION NO: 40

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
Explanation:
Answer C is the beast answer. A firewall with stateful properties should not allow session initiation from outside the network. Any packet coming into the network should be in response to a packet that left. If the firewall makes such a decision by checking the ACK bit, such decision may be flawed when the firewall makes that decision only based on the ACK bit. What the firewall is doing is: If the ACK bit is on, then this message must be in response to a current session.

QUESTION NO: 41

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
Explanation:
Answer A is the best answer. Wireless frequencies for 802.11 are 2.5Ghz for B and G and 5.0Ghz for A. If 802.11 b or g are used, certain household appliances could conflict and interfere with the wireless network.
Answer B is incorrect, satellite TV runs at a higher band above 10 Ghz.

QUESTION NO: 42

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

Answer: A
Explanation:
Answer A is correct. Port 389 is the LDAP port, and Active Directory is built on LDAP. By accessing LDAP on a Domain Controller, you are trying to get the users, OU definitions, security groups, password hashes, and anything within Active Directory.
Answer B is incorrect. Although you are connecting to a service on the domain controller, this is not remote access to the domain controller.
Answer C and D are incorrect. Although when integrated DNS is used in an active directory configuration, and the zones would then be in LDAP, this is an exception.

QUESTION NO: 43

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

Answer: D
Explanation:
Answer A could have been a good answer; networks are typically less protected from the inside because of the trust of insiders.
Answer D is the best answer, because although the insiders are trusted more, the inside threat is

greater.

Answer B is incorrect.

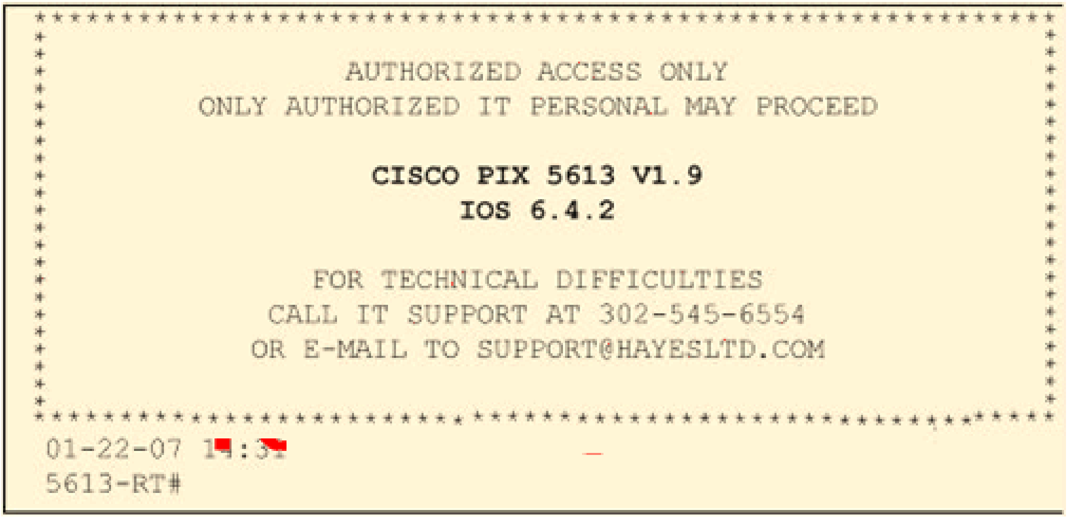
Answer C is incorrect, however, once a hacker does break in, the hacker is in the position of an insider and protection needs to be in place.

QUESTION NO: 44

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 clients about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:



```
************************************************************
*                                                          *
*                 AUTHORIZED ACCESS ONLY                   *
*         ONLY AUTHORIZED IT PERSONAL MAY PROCEED          *
*                                                          *
*                  CISCO PIX 5613 V1.9                     *
*                       IOS 6.4.2                          *
*                                                          *
*               FOR TECHNICAL DIFFICULTIES                 *
*             CALL IT SUPPORT AT 302-545-6554              *
*           OR E-MAIL TO SUPPORT@HAYESLTD.COM              *
*                                                          *
************************************************************
 01-22-07 1[redacted]:3[redacted]
 5613-RT#
```

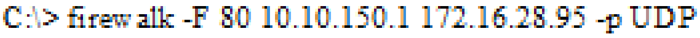
A. The banner should not state "only authorized IT personnel may proceed"
B. Remove any identifying numbers, names, or version information
C. The banner should include the Cisco tech support contact information as well
D. The banner should have more detail on the version numbers for the network equipment

Answer: B
Explanation:
Answer B is correct. The banner should only have a legal warning. Any identification, including the company name, location, e-mail address, and the make, model and OS version information, should not be on a warning banner. This information can be used by an attacker to identify the

device, identify potential vulnerabilities, and provide information for social engineering. Some organizations will strip the information for perimeter equipment and still provide detailed information for inside the network.

QUESTION NO: 45

What is the target host IP in the following command?



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

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

Answer: A
Explanation:
Firewalk does not have a “-F” option. Firewalk is only used to determine which ports on the IP forwarding device are enabled. It is not used for scanning targets on the other side of the IP forwarding device.

QUESTION NO: 46

In Linux, what is the smallest possible shellcode?

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

Answer: D
Explanation:

QUESTION NO: 47

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
Explanation:
Answer C is correct. This is a web bug, which is a one pixel by a 1 pixel area on the web page. Each time the web page is launched, this URL is accessed and a entry will appear in the web server log at coolwebsearch.com.

QUESTION NO: 48

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?

A. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
B. Passwords of 14 characters or less are broken up into two 7-character hashes
C. The passwords that were cracked are local accounts on the Domain Controller
D. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network

Answer: B
Explanation:
Answer A is incorrect. Active Directory uses LDAP for storage of user accounts and passwords, and the SAM database on the Domain Controllers are not used. Although this question does not

directly indicate AD, the use of GPO implies use of AD. In an AD environment, all non-domain controllers will have use a SAM database for local accounts.
Answer B is the best choice. The SAM database was pulled from a standalone server, not a domain controller. That server would have an active and used SAM database for local accounts on that server. The passwords were determined by breaking the LM (LAN Manager) hashes, which breaks the password into two 7 character pieces. If the policy was to force 15 character passwords, then the LM Hashes would not be used.
Answer C is wrong. Domain Controllers in AD do not have local accounts.
Answer D is not really correct. There may be an assumption that the GPO was not forced to immediately replicate, but since it is a small bank, depending on how small, there could be a few domain controllers. The real answer here, based on Answer D would be: “it depends”. Either way, there is too much speculation on the replication time of the GPO.

Here is a note, not mentioned: Unless you check the box to force a password change on next logon, the fact that the GPO was set to at least 14 character passwords does not force the password to be changed. When the user attempts to change the password, then the GPO will force the password to be 14 characters, it doesn’t actually force the user to change an existing password. This is a misconception that setting options take effect immediately, when they don’t.

Another consideration is that this server where the SAM was pulled was called a standalone server. The difference between a standalone and member server is that the standalone is not a member of the domain, where the member server is a member of the domain – just not a domain controller. The use of the term standalone, if used properly, meant that the standalone server was not joined to the domain, and the GPO would never be applied to the server.

This question does have issues the way written.

QUESTION NO: 49

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"

Answer: D

Explanation:

QUESTION NO: 50

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

Answer: D
Explanation:

QUESTION NO: 51

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

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

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

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

Answer: C
Explanation:

QUESTION NO: 52

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
Explanation:
Answer A is the correct answer. The internal buffer is defined as a character string of 10 characters. A character string is passed as an argument. If the character string passed to the subroutine is longer than 10 characters, the buffer will overflow and parts of the stack will be overwritten.

QUESTION NO: 53

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

Explanation:

Answer A is the correct answer. CVE (Common Vulnerabilities and Exposures) is a dictionary of publically known vulnerabilities and exposure maintained by Mitre.

QUESTION NO: 54

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

Explanation:

QUESTION NO: 55

Software firewalls work at which layer of the OSI model?

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

Answer: A

Explanation:

QUESTION NO: 56

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

Answer: C

Explanation:

Answer A is incorrect, HIPAA is to protect medical information

Answer B is incorrect, SOX is to insure the integrity of financial records of publically traded companies

Answer D is incorrect. Although SB 1386 may provide some of these protections, it only applies to business operating within California or any business holding and processing the data of a California citizen.

Answer C is the correct answer. As part of expanding the financial markets that Insurance Companies and Banks could enter, GLBA also adds privacy protection for consumers.

QUESTION NO: 57

What does ICMP Type 3/Code 13 mean?

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

Answer: D

Explanation:

Answer A is incorrect, this would be a ICMP Type 3/Code 1

Answer B is incorrect, this would be a ICMP Type 3/Code 3

Answer C is incorrect, this would be a ICMP Type 3/CodeCm

Answer D is correct. This is a destination unreachable message. When passing through a router that filters packets, code 13 is used to indicate that the packet was Administratively Blocked.

QUESTION NO: 58

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
Explanation:
Answer D is incorrect. Windows implements the feature specified in the RFC that allows a silent discard of an IMCP packet addressed to a broadcast or multicast address.

QUESTION NO: 59

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
Explanation:
Answer B is the best answer. Encrypting File System (EFS) is a Microsoft file system that is encrypted. It is really NTFS, with encryption enabled. It is not enough to just encrypt using EFS, removal of the keys is required from the workstation, because should they be extracted, then the EFS can be compromised.
Answer C may be incorrect. There is always an issue of reusing acronyms. DFS could mean

Distributed File System, used in Windows, and is not encrypted. Then there is Deniable File System, which is an encrypted file system.

Answer D is incorrect. IPS is usually Intrusion Protection Systems, not a file system encryption method.

QUESTION NO: 60

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

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

Answer: C

Explanation:

Answer C is the correct answer. The sequence number for TCP protocol is a 32 bit unsigned number which is 4,294,967,295. UDP and ICMP does not use sequence numbers, so this is TCP protocol – not TCP/IP which is used to include the entire suite of IP components.

QUESTION NO: 61

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are not considered safe by Sarbanes-Oxley
C. PDF passwords are converted to clear text when sent through E-mail
D. When sent through E-mail, PDF passwords are stripped from the document completely

Answer: A

Explanation:

Answer A is the best choice. Although maybe not easily cracked, they can be brute forced. If the PDF version was produced by an earlier version of Acrobat, removal of the password is easy and fact using PDF password removal type tools.

Answer C and D are wrong; the passwords are not converted to clear text or stripped.

QUESTION NO: 62

What will the following command produce on a website login page?

```
SELECT email, passwd, login_id, full_name
 FROM members
WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'
```

A. Inserts the Error! Reference source not found. email address into the members table
B. Retrieves the password for the first user in the members table
C. Deletes the entire members table
D. This command will not produce anything since the syntax is incorrect

Answer: C
Explanation:

QUESTION NO: 63

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
Explanation:
Based on the question, none of these seem correct. This is name-dropping and comes under the

principal of Authority. “After hearing the name of the CEO” indicates a response to Authority, you don’t want to make the boss mad.

QUESTION NO: 64

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 160
C. 161
D. 163

Answer: A,C
Explanation:
SNMP uses two UDP ports, 161 & 162. The SNMP agent listens on UDP port 161. The agent may send traps and other alerts out via UDP 162.

QUESTION NO: 65

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

Answer: C
Explanation:
Answer C is the best answer, but might not be completely true. It would be true if the machine running firewalk was on the direct subnet connected to the firewall. Otherwise the father away firewalk is from the firewall, the higher the TTL. Remember, that once the firewall has been reached, then the TTL will be +1, and is never raised above that. The TTL needs to be just enough to pierce the firewall to determine if the port is actually open. A sniffer immediately after the firewall, with no additional hops, will pick up the firewalk traffic, but any hops between the firewall

and the sniffer will not reach the sniffer because the maximum TTL will only get the packet to the other side of the firewall, and no further.

QUESTION NO: 66

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

Answer: D
Explanation:

QUESTION NO: 67

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

Answer: C
Explanation:
Answer A is not correct. In order for this to actually work, since you are asking the employee to CREATE an account, is the assumption that the user will create an account using the same Username and Password that is used as their network username and password. [it is very likely that some or a lot of users will actually create their account on the survey site using their current network credentials – one less password to remember]
Answer B is not correct. In order for this to work, there cannot be a router between the user and the survey site. If there is a router, then the MAC address that will be captured will be the last hop prior to reaching the survey site.
Answer C is the best answer. Assuming that spoofing is not used, for example the use of a proxy server, the web server logs should show all the IP addresses. This requires assumptions, i.e. the

survey web site is within the corporate intranet. If the traffic has to leave the firewall, and if NATing is in effect, then the addresses will be changed and the collected IP addresses can not be traced back to the user.
Answer D is incorrect. Not unless the survey web site collects that information. The composition of the survey is not provided.

Whether answer A (the original answer) or answer C are the best really depends on the underlying assumptions for this question. Answer A relies on human behavior, Answer C relies on network topology. Both are not specified and both rely on speculation.

QUESTION NO: 68

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
Explanation:
The LPT – Licensed Penetrator Tester

QUESTION NO: 69

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

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

Answer: A
Explanation:

QUESTION NO: 70

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
Explanation:
The firewall can fail Open or Closed.
If the firewall fails closed, then nothing passes.
If the firewall fails open, then everything passes.
Think of a door – it is either open or closed, and the firewall is the door.
Answer A is the best answer.

QUESTION NO: 71

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

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

Answer: A
Explanation:
Answer B is incorrect, and is probably listed as a distracter. BGP is a protocol that routers use, but here it is spelled wrong.
Answer C is incorrect. ATM is a data link (layer 2) layer of communications. Note that routers run on layer 3.
Answer D is incorrect. UDP is a transport (layer 4) layer protocol, used above the router level for communications.

Answer A is the best answer, OSPF is a routing protocol. Also not listed, would be BGP and RIP as example of other protocols that routers utilize.

QUESTION NO: 72

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

Answer: B

Explanation:

Answer B is the best answer. Tailgating, or also called piggybacking, is when one person follows another in to a secure area, and both get in on the same credentials.

Answer C is wrong, although a man trap is a device that is used to prevent tailgating.

QUESTION NO: 73

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

Explanation:

The rdisk command creates a backup of the SAM file in the repair directory. Once the copy is made, it still has to be retrieved.

QUESTION NO: 74

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

Answer: D

Explanation:

Answer A is wrong, Fraggle sends UDP traffic to broadcast addresses to create a denial of service, this attack does not use ICMP.
Answer C is wrong, Trinoo uses a UDF flood attack from a botnet type of army. This is actually a distributed denial of service DDoS attack, but does not use ICMP.
Answer B is wrong, a SYN flood send TCP SYN commands to a host to absorb resources. It is a Denial of Service attack, but does not use ICMP.
Answer D is the best choice, in this attack ICMP echo commands are passed to broadcast addresses to create a denial of service. This is the only attack listed that uses ICMP.