EC-Council

Exam Questions 312-50

Ethical Hacking and Countermeasures (CEHv6)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Topic 1)
Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

A. CHAT rooms
B. WHOIS database
C. News groups
D. Web sites
E. Search engines
F. Organization's own web site

Answer: ABCDEF

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

NEW QUESTION 2
- (Topic 1)
What does the term "Ethical Hacking" mean?

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

Answer: C

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

NEW QUESTION 3
- (Topic 1)
What is the essential difference between an 'Ethical Hacker' and a 'Cracker'?

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

Answer: C

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

NEW QUESTION 4
- (Topic 1)
ABC.com is legally liable for the content of email that is sent from its systems, regardless of whether the message was sent for private or business-related purpose. This could lead to prosecution for the sender and for the company's directors if, for example, outgoing email was found to contain material that was pornographic, racist or likely to incite someone to commit an act of terrorism.
You can always defend yourself by 'ignorance of the law' clause.

A. True
B. False

Answer: B

Explanation:
Ignorantia juris non excusat or Ignorantia legis neminem excusat (Latin for "ignorance of the law does not excuse" or "ignorance of the law excuses no one") is a public policy holding that a person who is unaware of a law may not escape liability for violating that law merely because he or she was unaware of its content; that is, persons have presumed knowledge of the law. Presumed knowledge of the law is the principle in jurisprudence that one is bound by a law even if one does not know of it. It has also been defined as the "prohibition of ignorance of the law".

NEW QUESTION 5
- (Topic 2)
Which of the following activities would not be considered passive footprinting?

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

Answer: C

Explanation:
Passive footprinting is a method in which the attacker never makes contact with the target. Scanning the targets IP addresses can be logged at the target and therefore contact has been made.

NEW QUESTION 6
- (Topic 2)
A Company security System Administrator is reviewing the network system log files. He notes the following:
? Network log files are at 5 MB at 12:00 noon.
? At 14:00 hours, the log files at 3 MB.
What should he assume has happened and what should he do about the situation?

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

Answer: B

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

NEW QUESTION 7
- (Topic 2)
You receive an email with the following message:
Hello Steve,
We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.
http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm
If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.
Sincerely, Technical Support
SuperEmailServices
From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:
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

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

NEW QUESTION 8
- (Topic 2)
To what does "message repudiation" refer to what concept in the realm of email security?

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

Answer: E

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

NEW QUESTION 9
- (Topic 2)
A very useful resource for passively gathering information about a target company is:

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

Answer: B

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

NEW QUESTION 10
- (Topic 2)
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.

NEW QUESTION 10
- (Topic 2)
System Administrators sometimes post questions to newsgroups when they run into technical challenges. As an ethical hacker, you could use the information in newsgroup posting to glean insight into the makeup of a target network. How would you search for these posting using Google search?

A. Search in Google using the key strings “the target company” and “newsgroups”
B. Search for the target company name at http://groups.google.com
C. Use NNTP websites to search for these postings
D. Search in Google using the key search strings “the target company” and “forums”

Answer: B

Explanation:
Using http://groups.google.com is the easiest way to access various newsgroups today. Before http://groups.google.com you had to use special NNTP clients or subscribe to some nntp to web services.

NEW QUESTION 12
- (Topic 2)
Your company trainee Sandra asks you which are the four existing Regional Internet Registry (RIR's)?

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

Answer: B

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

NEW QUESTION 14
- (Topic 2)
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.

NEW QUESTION 18
- (Topic 2)
Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?
(Note: The student is being tested on concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dumo.)

05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
.
.
.
05/20-17:06:58.685879 192.160.13.4:31337 -> 172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seg: 0XA1D95 Ack: 0x53 Win: 0x400
What is odd about this attack? (Choose the most appropriate statement)

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

Answer: B

Explanation:
Port 31337 is normally used by Back Orifice. Note that 31337 is hackers spelling of ‘elite’, meaning ‘elite hackers’.

NEW QUESTION 20
- (Topic 2)
You are footprinting the www.xsecurity.com domain using the Google Search Engine. You would like to determine what sites link to www.xsecurity .com at the first level of revelance.
Which of the following operator in Google search will you use to achieve this?

A. Link: www.xsecurity.com
B. serch?l:www.xsecurity.com
C. level1.www.security.com
D. pagerank:www.xsecurity.com

Answer: A

Explanation:
The query [link:] will list webpages that have links to the specified webpage. For instance, [link:www.google.com] will list webpages that have links pointing to the Google homepage. Note there can be no space between the "link:" and the web page url.

NEW QUESTION 23
- (Topic 3)
John has scanned the web server with NMAP. However, he could not gather enough information to help him identify the operating system running on the remote host
accurately.
What would you suggest to John to help identify the OS that is being used on the remote web server?

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

Answer: D

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

NEW QUESTION 28
- (Topic 3)
Which of the following is a patch management utility that scans one or more computers on your network and alerts you if you important Microsoft Security patches are missing. It then provides links that enable those missing patches to be downloaded and installed.

A. MBSA
B. BSSA
C. ASNB
D. PMUS

Answer: A

Explanation:
The Microsoft Baseline Security Analyzer (MBSA) is a tool put out by Microsoft to help analyze security problems in Microsoft Windows. It does this by scanning the system for security problems in Windows, Windows components such as the IIS web server application, Microsoft SQL Server, and Microsoft Office. One example of an issue might be that permissions for one of the directories in the wwwroot folder of IIS could be set at too low a level, allowing unwanted modification of files from outsiders.

NEW QUESTION 31
- (Topic 3)
You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of what protocols are being used. You need to discover as many different protocols as possible. Which kind of scan would you use to do this?

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

Answer: A

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

NEW QUESTION 36
- (Topic 3)
War dialing is a very old attack and depicted in movies that were made years ago. Why would a modem security tester consider using such an old technique?

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

Answer: B

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

NEW QUESTION 41
- (Topic 3)
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.

NEW QUESTION 42
- (Topic 3)
While reviewing the results of a scan run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
ystem Software
OS (tm) 4500 Software (C4500 ISM), Version 12.0(9), RELEASE SOFTWARE (fc1)
opyright (c) 1980-2000 0y cisco Systems Inc.
ompiled Tue 25-Jan-00 04:28 by bettyl
ystem sysObjectID 0 : OBJECT IDENTIFIER:
iso.org aud iltrelple  private.enterprises.cisco cotProdcisco4700
ystem.sysUpTime.0 : Timeticks  (150396017) 18 days, 2:26:20.17
ystem.sysContact.0 : DISPLAY STRING- (ascii):
ystem.sysName.0 : DISPLAY STRING- (ascii): somerroutername
ystem.sysLocation.0 : DISPLAY STRING- (ascii):
ystem.sysServices.0 : INTEGER: 6
ystem.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

What was used to obtain this output?

A. An SNMP Walk
B. Hping2 diagnosis
C. A Bo2K System query
D. Nmap protocol/port scan

Answer: A

Explanation:
The snmpwalk command is designed to perform a sequence of chained GETNEXT requests automatically, rather than having to issue the necessary snmpgetnext requests by hand. The command takes a single OID, and will display a list of all the results which lie within the subtree rooted on this OID.

NEW QUESTION 46
- (Topic 3)

```
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2006-09-25 00:01 EST
Host 192.168.0.0 seems to be a subnet broadcast address (returned 4 extra
ping ).
Host 192.168.0.1 appears to be up.
MAC Address: 00:12:17:31:4F:C4 (Cisco-Linksys)
Host 192.168.0.6 appears to be up.
MAC Address: 00:C0:4F:A1:25:4A (Dell Computer)
Host 192.168.0.10 appears to be up.
MAC Address: 00:B0:D0:FE:87:68 (Dell Computer)
Host 192.168.0.13 appears to be up.
MAC Address: 00:C0:4F:A1:25:89 (Dell Computer)
Host 192.168.0.100 appears to be up.
MAC Address: 00:C0:4F:A1:27:BF (Dell Computer)
Host 192.168.0.103 appears to be up.
MAC Address: 00:0D:88:66:FB:87 (D-Link)
Host 192.168.0.104 appears to be up.
Host 192.168.0.108 appears to be up.
MAC Address: 00:11:D8:90:D6:7F (Asustek Computer)
Host 192.168.0.255 seems to be a subnet broadcast address (returned 4 extra
pings).
Nmap run completed -- 256 IP addresses (8 hosts up) scanned in 4.390 seconds
```

Which of the following nmap command in Linux procedures the above output?

A. sudo nmap –sP 192.168.0.1/24
B. root nmap –sA 192.168.0.1/24
C. run nmap –TX 192.168.0.1/24
D. launch nmap –PP 192.168.0.1/24

Answer: A

Explanation:
This is an output from a ping scan. The option –sP will give you a ping scan of the 192.168.0.1/24 network.

NEW QUESTION 50
- (Topic 3)
Study the log below and identify the scan type.
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)
tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060) 4500
0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000

A. nmap -sR 192.168.1.10
B. nmap -sS 192.168.1.10
C. nmap -sV 192.168.1.10
D. nmap -sO -T 192.168.1.10

Answer: D

NEW QUESTION 52
- (Topic 3)
Destination unreachable administratively prohibited messages can inform the hacker to what?

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

Answer: D

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

NEW QUESTION 53
- (Topic 3)
Mark works as a contractor for the Department of Defense and is in charge of network security. He has spent the last month securing access to his network from

all possible entry points. He has segmented his network into several subnets and has installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Mark is fairly confident of his perimeter defense, but is still worried about programs like Hping2 that can get into a network through convert channels.
How should mark protect his network from an attacker using Hping2 to scan his internal network?

A. Blocking ICMP type 13 messages
B. Block All Incoming traffic on port 53
C. Block All outgoing traffic on port 53
D. Use stateful inspection on the firewalls

Answer: A

Explanation:
An ICMP type 13 message is an ICMP timestamp request and waits for an ICMP timestamp reply. The remote node is right to do, still it would not be necessary as it is optional and thus many ip stacks ignore such packets. Nevertheless, nmap again achived
to make its packets unique by setting the originating timestamp field in the packet to 0.

NEW QUESTION 54
- (Topic 3)
You are having problems while retrieving results after performing port scanning during internal testing. You verify that there are no security devices between you and the target system. When both stealth and connect scanning do not work, you decide to perform a NULL scan with NMAP. The first few systems scanned shows all ports open.
Which one of the following statements is probably true?

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

Answer: D

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

NEW QUESTION 56
- (Topic 3)
What are the four steps is used by nmap scanning?

A. DNS Lookup
B. ICMP Message
C. Ping
D. Reverse DNS lookup
E. TCP three way handshake
F. The Actual nmap scan

Answer: ACDF

Explanation:
Nmap performs four steps during a normal device scan. Some of these steps can be modified or disabled using options on the nmap command line.
? If a hostname is used as a remote device specification, nmap will perform a DNS lookup prior to the scan.
? Nmap pings the remote device. This refers to the nmap "ping" process, not (necessarily) a traditional ICMP echo request.
? If an IP address is specified as the remote device, nmap will perform a reverse DNS lookup in an effort to identify a name that might be associated with the IP address. This is the opposite process of what happens in step 1, where an IP address is found from a hostname specification.
? Nmap executes the scan. Once the scan is over, this four-step process is completed. Except for the actual scan process in step four, each of these steps can be disabled or prevented using different IP addressing or nmap options. The nmap process can be as "quiet" or as "loud" as necessary!

NEW QUESTION 59
- (Topic 3)
Which FTP transfer mode is required for FTP bounce attack?

A. Active Mode
B. Passive Mode
C. User Mode
D. Anonymous Mode

Answer: B

Explanation:
FTP bounce attack needs the server the support passive connections and the client program needs to use PORT command instead of the PASV command.

NEW QUESTION 64
- (Topic 3)
Gerald, the systems administrator for Hyped Enterprise, has just discovered that his network has been breached by an outside attacker. After performing routine maintenance on his servers, his discovers numerous remote tools were installed that no one claims to have knowledge of in his department.

Gerald logs onto the management console for his IDS and discovers an unknown IP address that scanned his network constantly for a week and was able to access his network through a high-level port that was not closed. Gerald traces the IP address he found in the IDS log to proxy server in Brazil.
Gerald calls the company that owns the proxy server and after searching through their logs, they trace the source to another proxy server in Switzerland. Gerald calls the company in Switzerland that owns the proxy server and after scanning through the logs again, they trace the source back to a proxy server in China.
What tool Geralds's attacker used to cover their tracks?

A. Tor
B. ISA
C. IAS
D. Cheops

Answer: A

Explanation:
Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. It provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy. Individuals can use it to keep remote Websites from tracking them and their family members. They can also use it to connect to resources such as news sites or instant messaging services that are blocked by their local Internet service providers (ISPs).

NEW QUESTION 65
- (Topic 3)
Which of the following systems would not respond correctly to an nmap XMAS scan?

A. Windows 2000 Server running IIS 5
B. Any Solaris version running SAMBA Server
C. Any version of IRIX
D. RedHat Linux 8.0 running Apache Web Server

Answer: A

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

NEW QUESTION 70
- (Topic 3)
Exhibit

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

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

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

Answer: B

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

NEW QUESTION 72
- (Topic 3)
Nathalie 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?

A. A FIN Scan
B. A Half Scan
C. A UDP Scan
D. The TCP Connect Scan

Answer: D

Explanation:
The connect() system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening,

connect() will succeed, otherwise the port isn't reachable. One strong advantage to this technique is that you don't need any special privileges. This is the fastest scanning method supported by nmap, and is available with the -t (TCP) option. The big downside is that this sort of scan is easily detectable and filterable.

NEW QUESTION 73
- (Topic 3)
What are the default passwords used by SNMP?(Choose two.)

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

Answer: CE

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.

NEW QUESTION 75
- (Topic 3)
An nmap command that includes the host specification of 202.176.56-57.* will scan ____ number of hosts.

A. 2
B. 256
C. 512
D. Over 10,000

Answer: C

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

NEW QUESTION 77
- (Topic 3)
Which of the following command line switch would you use for OS detection in Nmap?

A. -D
B. -O
C. -P
D. -X

Answer: B

Explanation:
OS DETECTION: -O: Enable OS detection (try 2nd generation w/fallback to 1st) -O2: Only use the new OS detection system (no fallback) -O1: Only use the old (1st generation) OS detection system --osscan-limit: Limit OS detection to promising targets -- osscan-guess: Guess OS more aggressively

NEW QUESTION 81
- (Topic 3)
You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different protocols as possible.
Which kind of scan would you use to achieve this? (Choose the best answer)

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

Answer: D

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

NEW QUESTION 85
- (Topic 3)
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: BD

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

NEW QUESTION 90
- (Topic 3)
While reviewing the result of scanning run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 · OBJECT IDENTIFIER:
.iso.org.dod.internet.private.enter rise:.cisco.catirod. cisco4700
system.sysUpTime.0 : Timeticks: (15639801/) 18 days, 2:26:20.17
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

Which among the following can be used to get this output?

A. A Bo2k system query.
B. nmap protocol scan
C. A sniffer
D. An SNMP walk

Answer: D

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

NEW QUESTION 95
- (Topic 3)
While performing ping scans into a target network you get a frantic call from the organization’s security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization’s IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.
C. Spoof the source IP address.
D. Only scan the Windows systems.

Answer: B

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

NEW QUESTION 99
- (Topic 3)
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: CDF

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

NEW QUESTION 101
- (Topic 3)
You have initiated an active operating system fingerprinting attempt with nmap against a target system:
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1
Starting nmap 3.28 (www.insecure.org/nmap/) at 2003-06-18 19:14 IDT Interesting ports on 10.0.0.1:
(The 1628 ports scanned but not shown below are in state: closed) Port State Service
21/tcp filtered ftp 22/tcp filtered ssh 25/tcp open smtp 80/tcp open http 135/tcp open loc-srv
139/tcp open netbios-ssn 389/tcp open LDAP 443/tcp open https 465/tcp open smtps 1029/tcp open ms-lsa 1433/tcp open ms-sql-s
2301/tcp open compaqdiag 5555/tcp open freeciv 5800/tcp open vnc-http 5900/tcp open vnc 6000/tcp filtered X11
Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE Nmap run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between different groups of Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.
What operating system is the target host running based on the open ports shown above?

A. Windows XP
B. Windows 98 SE
C. Windows NT4 Server
D. Windows 2000 Server

Answer: D

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

NEW QUESTION 104
- (Topic 3)
Samantha has been actively scanning the client network for which she is doing a vulnerability assessment test. While doing a port scan she notices ports open in the 135 to 139 range. What protocol is most likely to be listening on those ports?

A. SMB
B. FTP
C. SAMBA
D. FINGER

Answer: A

Explanation:
Port 135 is for RPC and 136-139 is for NetBIOS traffic. SMB is an upper layer service that runs on top of the Session Service and the Datagram service of NetBIOS.

NEW QUESTION 106
- (Topic 3)
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 test 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
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: 63.226.81.13:4499 ->
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 63.226.81.13:1351 -> 172.16.1.107:11
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

NEW QUESTION 108
- (Topic 3)
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.

NEW QUESTION 110
- (Topic 3)
Because UDP is a connectionless protocol: (Select 2)

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

Answer: DE

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

NEW QUESTION 111
- (Topic 3)
Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log
B. ./snort -dev -l ./log
C. ./snort -dev -o ./log
D. ./snort -dev -p ./log

Answer: B

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

NEW QUESTION 112
- (Topic 3)
What does an ICMP (Code 13) message normally indicates?

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

Answer: C

Explanation:
CODE 13 and type 3 is destination unreachable due to communication administratively prohibited by filtering hence maybe they meant "code 13", therefore would be C).
Note:A - Type 3B - Type 4C - Type 3 Code 13D - Typ4 4

NEW QUESTION 117
- (Topic 3)
A distributed port scan operates by:

A. Blocking access to the scanning clients by the targeted host
B. Using denial-of-service software against a range of TCP ports
C. Blocking access to the targeted host by each of the distributed scanning clients
D. Having multiple computers each scan a small number of ports, then correlating the results

Answer: D

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

NEW QUESTION 119
- (Topic 3)
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: BE

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.

NEW QUESTION 120
- (Topic 3)
home/root # traceroute www.targetcorp.com <http://www.targetcorp.com> traceroute to www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18), 64 hops may, 40 byte packets
1 router.anon.com (192.13.212.254) 1.373 ms 1.123 ms 1.280 ms
2 192.13.133.121 (192.13.133.121) 3.680 ms 3.506 ms 4.583 ms
3 firewall.anon.com (192.13.192.17) 127.189 ms 257.404 ms 208.484 ms
4 anon-gw.anon.com (192.93.144.89) 471.68 ms 376.875 ms 228.286 ms
5 fe5-0.lin.isp.com (192.162.231.225) 2.961 ms 3.852 ms 2.974 ms
6 fe0-0.lon0.isp.com (192.162.231.234) 3.979 ms 3.243 ms 4.370 ms
7 192.13.133.5 (192.13.133.5) 11.454 ms 4.221 ms 3.333 ms
6 * * *
7 * * *
8 www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18) 5.392
ms 3.348 ms 3.199 ms
Use the traceroute results shown above to answer the following question:
The perimeter security at targetcorp.com does not permit ICMP TTL-expired packets out.

A. True
B. False

Answer: A

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

NEW QUESTION 123
- (Topic 3)
Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point.
Which of the following type of scans would be the most accurate and reliable option?

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

Answer: C

Explanation:
A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three- way handshake, and the port scanner immediately closes the connection. Otherwise an error code is returned.
Example of a three-way handshake followed by a reset: Source Destination Summary
---
[192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 SYN SEQ=3362197786 LEN=0 WIN=5840
[192.168.0.10] [192.168.0.8] TCP: D=49389 S=80 SYN ACK=3362197787 SEQ=58695210 LEN=0 WIN=65535
[192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 ACK=58695211 WIN<<2=5840 [192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 RST ACK=58695211 WIN<<2=5840

NEW QUESTION 126
- (Topic 3)
What ICMP message types are used by the ping command?

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

Answer: B

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

NEW QUESTION 129
- (Topic 3)
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.

NEW QUESTION 134
- (Topic 3)
Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

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

Answer: C

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

NEW QUESTION 136
- (Topic 3)
You are concerned that someone running PortSentry could block your scans, and you decide to slow your scans so that no one detects them. Which of the following commands will help you achieve this?

A. nmap -sS -PT -PI -O -T1 <ip address>
B. nmap -sO -PT -O -C5 <ip address>
C. nmap -sF -PT -PI -O <ip address>
D. nmap -sF -P0 -O <ip address>

Answer: A

Explanation:
-T[0-5]: Set timing template (higher is faster)

NEW QUESTION 138
- (Topic 3)
You are conducting an idlescan manually using HPING2. During the scanning process, you notice that almost every query increments the IPID- regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Which of he following options would be a possible reason?

A. Hping2 can’t be used for idlescanning
B. The Zombie you are using is not truly idle
C. These ports are actually open on the target system
D. A stateful inspection firewall is resetting your queries

Answer: B

Explanation:
If the IPID increments more than one value that means that there has been network traffic between the queries so the zombie is not idle.

NEW QUESTION 142
- (Topic 3)
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.

NEW QUESTION 145
- (Topic 4)
SNMP is a protocol used to query hosts, servers and devices about performance or health status data. Hackers have used this protocol for a long time to gather great amount of information about remote hosts. Which of the following features makes this possible?

A. It is susceptible to sniffing
B. It uses TCP as the underlying protocol
C. It is used by ALL devices on the market
D. It uses a community string sent as clear text

Answer: AD

Explanation:
SNMP uses UDP, not TCP, and even though many devices uses SNMP not ALL devices use it and it can be disabled on most of the devices that does use it. However SNMP is susceptible to sniffing and the community string (which can be said acts as a password) is sent in clear text.

NEW QUESTION 148
- (Topic 4)

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: BCE

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

NEW QUESTION 152
- (Topic 4)
SNMP is a connectionless protocol that uses UDP instead of TCP packets? (True or False)

A. True
B. False

Answer: A

Explanation:
TCP and UDP provide transport services. But UDP was preferred. This is due to TCP characteristics, it is a complicate protocol and it consume to many memory and CPU resources. Where as UDP is easy to build and run. Into devices (repeaters and modems) vendors have built simple version of IP and UDP.

NEW QUESTION 156
- (Topic 4)
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.

NEW QUESTION 157
- (Topic 4)
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: BC

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

NEW QUESTION 162
- (Topic 4)
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.

NEW QUESTION 167
- (Topic 4)
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.

NEW QUESTION 172
- (Topic 4)
Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for?
Select the best answers.

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

Answer: ABD

Explanation:
Explanations:
SNMPUtil is a SNMP enumeration utility that is a part of the Windows 2000 resource kit. With SNMPUtil, you can retrieve all sort of valuable information through SNMP. SNScan is a SNMP network scanner by Foundstone. It does SNMP scanning to find open SNMP ports. Solarwinds IP Network Browser is a SNMP enumeration tool with a graphical tree-view of the remote machine's SNMP data.

NEW QUESTION 177
- (Topic 4)
A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it?
Select the best answers.

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

Answer: ABD

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

NEW QUESTION 178
- (Topic 4)
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.

NEW QUESTION 181
- (Topic 4)
John is a keen administrator, and 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 are people who already attempt to compromise his newly renamed administrator account.
How is it possible for a remote attacker to decipher the name of the administrator account if it has been renamed?

A. The attacker used the user2sid program.
B. The attacker used the sid2user program.
C. The attacker used nmap with the –V switch.
D. The attacker guessed the new name.

Answer: B

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

NEW QUESTION 183
- (Topic 4)
Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139. What protocol is most likely to be listening on those ports?

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

Answer: D

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

NEW QUESTION 188
- (Topic 4)
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

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

NEW QUESTION 193
- (Topic 4)
Exhibit:

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 ID:53476 DF F
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./....../....../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, */*..Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 t-Lalla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encodi
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A ng: Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```

Study the following log extract and identify the attack.

A. Hexcode Attack
B. Cross Site Scripting
C. Multiple Domain Traversal Attack
D. Unicode Directory Traversal Attack

Answer: D

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

NEW QUESTION 197
- (Topic 4)
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool “SIDExtractor”. Here is the output of the SIDs:
s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang s-1-5-21-1125394485-807628933-54978560-555Micah
From the above list identify the user account with System Administrator privileges.

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

Answer: F

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

NEW QUESTION 201
- (Topic 4)
What does FIN in TCP flag define?

A. Used to close a TCP connection
B. Used to abort a TCP connection abruptly
C. Used to indicate the beginning of a TCP connection
D. Used to acknowledge receipt of a previous packet or transmission

Answer: A

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

NEW QUESTION 206
- (Topic 4)
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.

NEW QUESTION 210
- (Topic 4)
Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two.
What would you call this attack?

A. Interceptor
B. Man-in-the-middle
C. ARP Proxy
D. Poisoning Attack

Answer: B

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

NEW QUESTION 211
- (Topic 4)
Which DNS resource record can indicate how long any "DNS poisoning" could last?

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

Answer: B

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

NEW QUESTION 212
- (Topic 4)
What port number is used by LDAP protocol?

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

Answer: B

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

NEW QUESTION 217
- (Topic 4)
Jonathan being a keen administrator has followed all of the best practices he could find on securing his Windows Server. He renamed the Administrator account to a new name that can’t be easily guessed but there remain people who attempt to
compromise his newly renamed administrator account. How can a remote attacker decipher the name of the administrator account if it has been renamed?

A. The attacker guessed the new name
B. The attacker used the user2sid program
C. The attacker used to sid2user program
D. The attacker used NMAP with the V option

Answer: C

Explanation:
User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine Sid2user.exe can then be used to retrieve the names of all the user accounts and more. These utilities do not exploit a bug but call the functions LookupAccountName and LookupAccountSid respectively. What

is more these can be called against a remote machine without providing logon credentials save those needed for a null session connection.

NEW QUESTION 221
- (Topic 4)
Which of the following statements about a zone transfer correct?(Choose three.

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

Answer: ACE

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.

NEW QUESTION 224
- (Topic 5)
_____ is the process of converting something from one representation to the simplest form. It deals with the way in which systems convert data from one form to another.

A. Canonicalization
B. Character Mapping
C. Character Encoding
D. UCS transformation formats

Answer: A

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

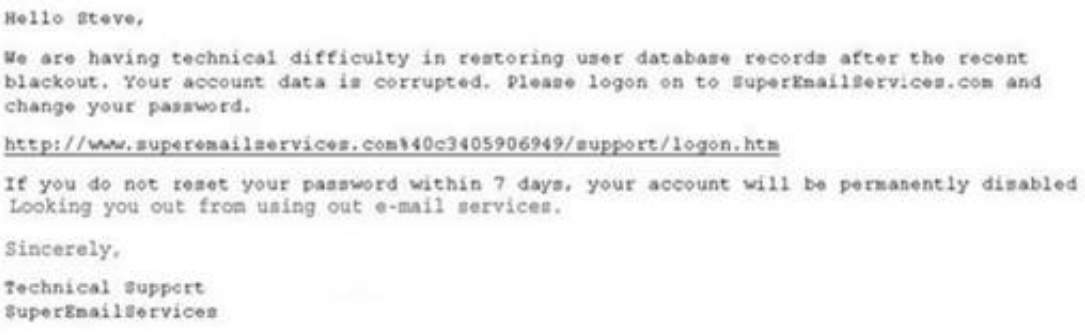
NEW QUESTION 225
- (Topic 5)
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored? (Choose the best answer)

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

Answer: C

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

NEW QUESTION 226
- (Topic 5)
Exhibit


Hello Steve,

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

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

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

Sincerely,

Technical Support
SuperEmailServices

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

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

Answer: C

Explanation:
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)

NEW QUESTION 231
- (Topic 5)
Which of the following is an attack in which a secret value like a hash is captured and then reused at a later time to gain access to a system without ever decrypting or decoding the hash.

A. Replay Attacks
B. Brute Force Attacks
C. Cryptography Attacks
D. John the Ripper Attacks

Answer: A

Explanation:
A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

NEW QUESTION 236
- (Topic 5)
An attacker runs netcat tool to transfer a secret file between two hosts.
Machine A: netcat -l -p 1234 < secretfile Machine B: netcat 192.168.3.4 > 1234
He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt the information before transmitting onto the wire?

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

Answer: D

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

NEW QUESTION 240
- (Topic 5)
Which of the following is the primary objective of a rootkit?

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

Answer: C

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

NEW QUESTION 242
- (Topic 5)
Password cracking programs reverse the hashing process to recover passwords.(True/False.

A. True
B. False

Answer: B

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

NEW QUESTION 246
- (Topic 5)
When discussing passwords, what is considered a brute force attack?

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

Answer: A

Explanation:

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

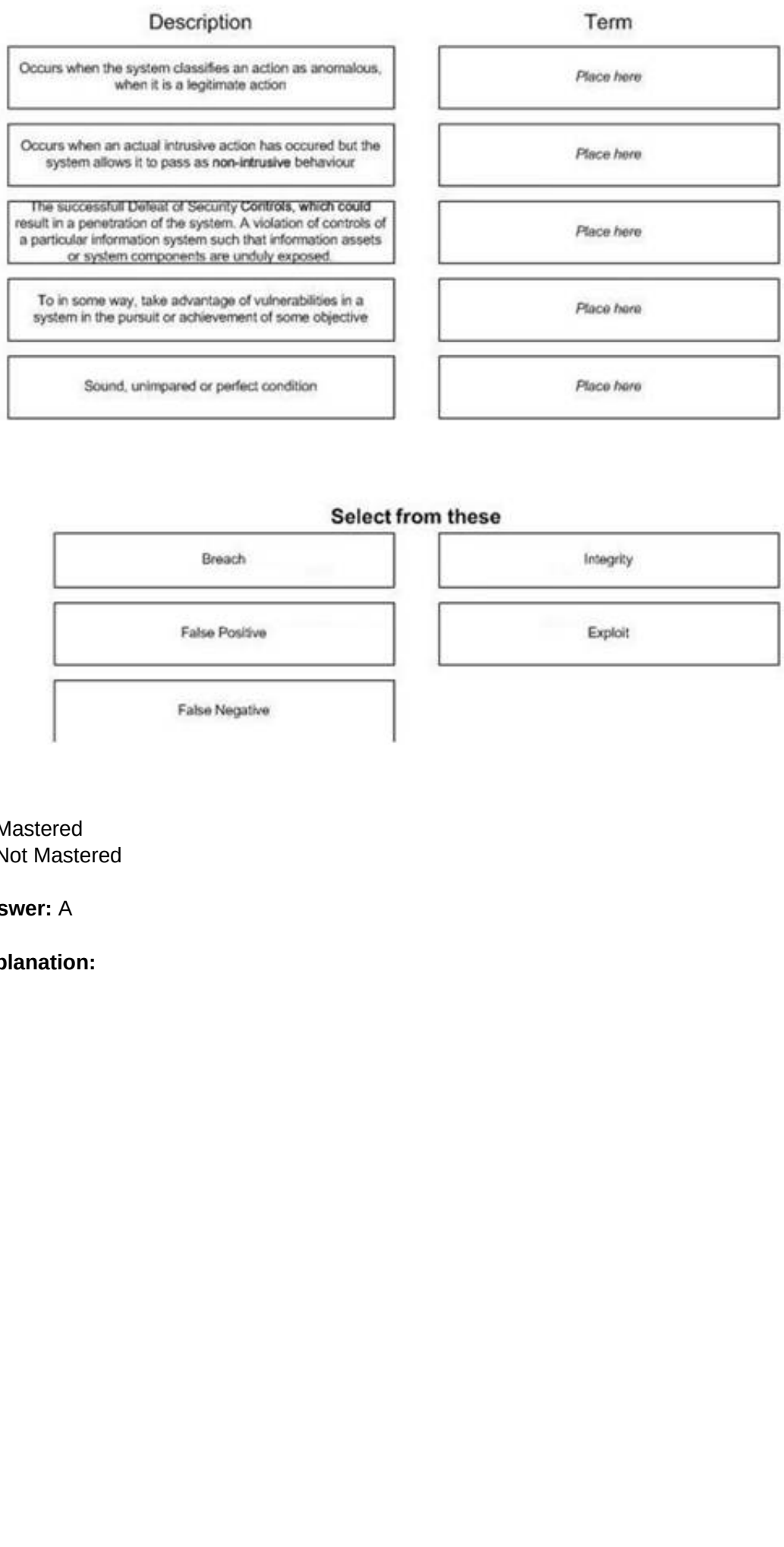
NEW QUESTION 247
- (Topic 5)
A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging in.
What do you think is the most likely reason behind this?

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

Answer: B

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

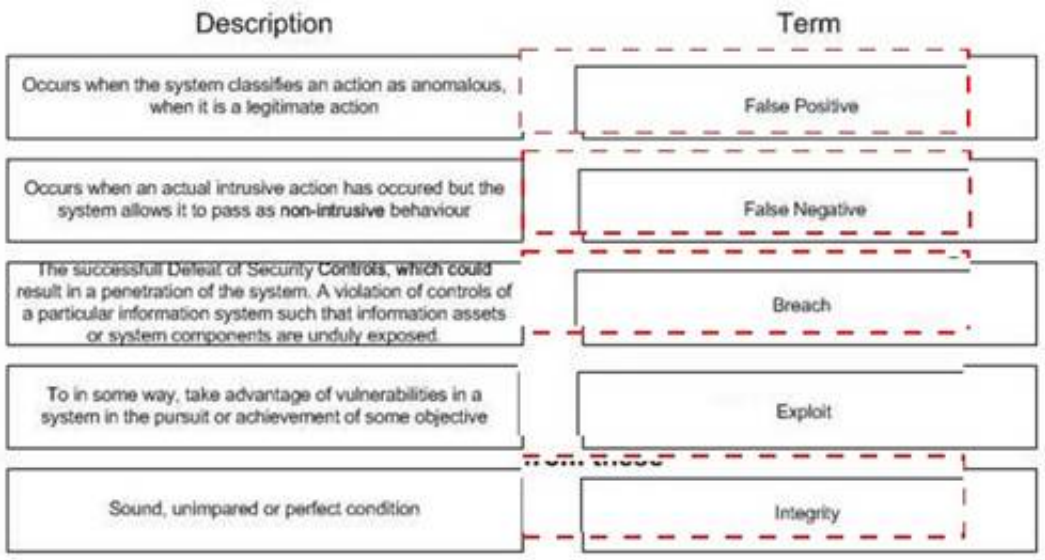
NEW QUESTION 250
DRAG DROP - (Topic 5)
Drag the term to match with it's description
Exhibit:

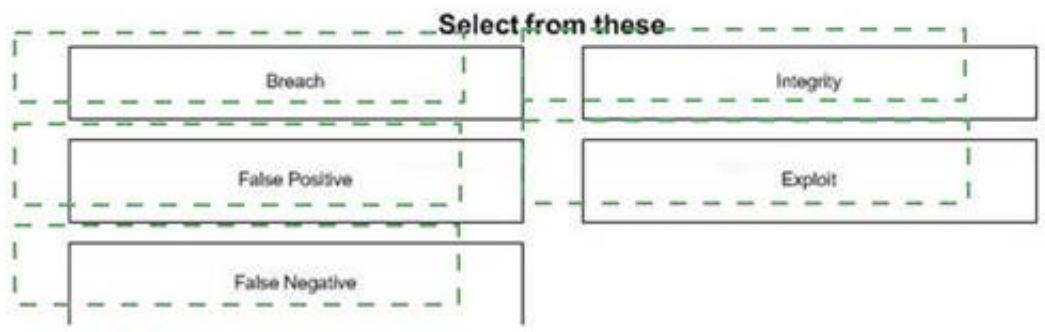


A. Mastered
B. Not Mastered

Answer: A

Explanation:





NEW QUESTION 252
- (Topic 5)
You are the IT Manager of a large legal firm in California. Your firm represents many important clients whose names always must remain anonymous to the public. Your boss, Mr. Smith is always concerned about client information being leaked or revealed to the pres or public. You have just finished a complete security overhaul of your information system including an updated IPS, new firewall, email encryption and employee security awareness training. Unfortunately, many of your firm's clients do not trust technology to completely secure their information, so couriers routinely have to travel back and forth to and from the office with sensitive information.
Your boss has charged you with figuring out how to secure the information the couriers must transport. You propose that the data be transferred using burned CD's or USB flash drives. You initially think of encrypting the files, but decide against that method for fear the encryption keys could eventually be broken.
What software application could you use to hide the data on the CD's and USB flash drives?

A. Snow
B. File Snuff
C. File Sneaker
D. EFS

Answer: A

Explanation:
The Snow software developed by Matthew Kwan will insert extra spaces at the end of each line. Three bits are encoded in each line by adding between 0 and 7 spaces that are ignored by most display programs including web browsers.

NEW QUESTION 255
- (Topic 5)
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

A. Block port 25 at the firewall.
B. Shut off the SMTP service on the server.
C. Force all connections to use a username and password.
D. Switch from Windows Exchange to UNIX Sendmail.
E. None of the above.

Answer: E

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

NEW QUESTION 257
- (Topic 5)
John Beetlesman, the hacker has successfully compromised the Linux System of Agent Telecommunications, Inc's WebServer running Apache. He has downloaded sensitive documents and database files off the machine.
Upon performing various tasks, Beetlesman finally runs the following command on the Linux box before disconnecting.
for ((i=0;i<1;i++));do
?dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done
What exactly is John trying to do?

A. He is making a bit stream copy of the entire hard disk for later download
B. He is deleting log files to remove his trace
C. He is wiping the contents of the hard disk with zeros
D. He is infecting the hard disk with random virus strings

Answer: C

Explanation:
dd copies an input file to an output file with optional conversions. –if is input file, -of is output file. /dev/zero is a special file that provides as many null characters (ASCII NULL, 0x00; not ASCII character "digit zero", "0", 0x30) as are read from it. /dev/hda is the hard drive.

NEW QUESTION 259
- (Topic 5)
What file system vulnerability does the following command take advantage of? type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

A. HFS
B. ADS
C. NTFS
D. Backdoor access

Answer: B

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

NEW QUESTION 262
- (Topic 5)
You are the security administrator for a large online auction company based out of Los Angeles. After getting your ENSA CERTIFICATION last year, you have steadily been fortifying your network’s security including training OS hardening and network security. One of the last things you just changed for security reasons was to modify all the built-in administrator accounts on the local computers of PCs and in Active Directory. After through testing you found and no services or programs were affected by the name changes.
Your company undergoes an outside security audit by a consulting company and they said that even through all the administrator account names were changed, the accounts could still be used by a clever hacker to gain unauthorized access. You argue with the auditors and say that is not possible, so they use a tool and show you how easy it is to utilize the administrator account even though its name was changed.
What tool did the auditors use?

A. sid2user
B. User2sid
C. GetAcct
D. Fingerprint

Answer: A

Explanation:
User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine Sid2user.exe can then be used to retrieve the names of all the user accounts and more.

NEW QUESTION 266
- (Topic 5)
Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

A. Snow
B. Gif-It-Up
C. NiceText
D. Image Hide

Answer: A

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

NEW QUESTION 271
- (Topic 5)
You are a Administrator of Windows server. You want to find the port number for POP3. What file would you find the information in and where?
Select the best answer.

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

Answer: C

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

NEW QUESTION 275
- (Topic 5)
What hacking attack is challenge/response authentication used to prevent?

A. Replay attacks
B. Scanning attacks
C. Session hijacking attacks
D. Password cracking attacks

Answer: A

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

NEW QUESTION 280
- (Topic 5)
You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption.
What encryption algorithm will you be decrypting?

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

Answer: B

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

NEW QUESTION 285
- (Topic 5)
Which of the following are well know password-cracking programs?(Choose all that apply.

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

Answer: AE

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

NEW QUESTION 287
- (Topic 5)
How would you describe an attack where an attacker attempts to deliver the payload over multiple packets over long periods of time with the purpose of defeating simple pattern matching in IDS systems without session reconstruction? A characteristic of this attack would be a continuous stream of small packets.

A. Session Splicing
B. Session Stealing
C. Session Hijacking
D. Session Fragmentation

Answer: A

NEW QUESTION 290
- (Topic 5)
What is GINA?

A. Gateway Interface Network Application
B. GUI Installed Network Application CLASS
C. Global Internet National Authority (G-USA)
D. Graphical Identification and Authentication DLL

Answer: D

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

NEW QUESTION 294
- (Topic 5)
Attackers can potentially intercept and modify unsigned SMB packets, modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after a legitimate authentication and gain unauthorized access to data. Which of the following is NOT a means that can be used to minimize or protect against such an attack?

A. Timestamps
B. SMB Signing
C. File permissions
D. Sequence numbers monitoring

Answer: ABD

NEW QUESTION 295
- (Topic 5)
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

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

Answer: C

Explanation:
All are DDOS tools.

NEW QUESTION 297
- (Topic 5)
This kind of password cracking method uses word lists in combination with numbers and special characters:

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

Answer: A

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

NEW QUESTION 299
- (Topic 5)
Which of the following LM hashes represent a password of less than 8 characters? (Select 2)

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

Answer: BE

Explanation:
Notice the last 8 characters are the same

NEW QUESTION 301
- (Topic 5)
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 clients hosts and servers.

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

Answer: A

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

NEW QUESTION 304
- (Topic 5)
You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assesments to protect the company's network. During one of your

periodic checks to see how well policy is being observed by the employees, you discover an employee has attached a modem to his telephone line and workstation. He has used this modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

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

Answer: D

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

NEW QUESTION 306
- (Topic 5)
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Covert keylogger
B. Stealth keylogger
C. Software keylogger
D. Hardware keylogger

Answer: D

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

NEW QUESTION 310
- (Topic 5)
In the context of Windows Security, what is a 'null' user?

A. A user that has no skills
B. An account that has been suspended by the admin
C. A pseudo account that has no username and password
D. A pseudo account that was created for security administration purpose

Answer: C

Explanation:
NULL sessions take advantage of "features" in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Using these NULL connections allows you to gather the following information from the host:* List of users and groups * List of machines * List of shares * Users and host SID' (Security Identifiers)
NULL sessions exist in windows networking to allow: * Trusted domains to enumerate resources * Computers outside the domain to authenticate and enumerate users * The SYSTEM account to authenticate and enumerate resources
NetBIOS NULL sessions are enabled by default in Windows NT and 2000. Windows XP and 2003 will allow anonymous enumeration of shares, but not SAM accounts.

NEW QUESTION 312
- (Topic 5)
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 asking - Windows 2000/XP keeps users passwords not "apparently", but as hashes, i.e. actually as "check sum" of the passwords. Let's go into the passwords keeping at large. The most interesting structure of the complex SAM-file building is so called V-block. It's size is 32 bytes and it includes hashes of the password for the local entering: NT Hash of 16-byte length, and hash used during the authentication of access to the common resources of other computers LanMan Hash, or simply LM Hash, of the same 16-byte length. Algorithms of the formation of these hashes are following:
NT Hash formation:
? User password is being generated to the Unicode-line.
? Hash is being generated based on this line using MD4 algorithm.
? 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:
? User password is being shifted to capitals and added by nulls up to 14-byte length.
? 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.
? Then LM Hash is being additionally encoded the same way as it had been done in the NT Hash formation algorithm step 3.

NEW QUESTION 313
- (Topic 6)

What is a Trojan Horse?

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

Answer: B

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

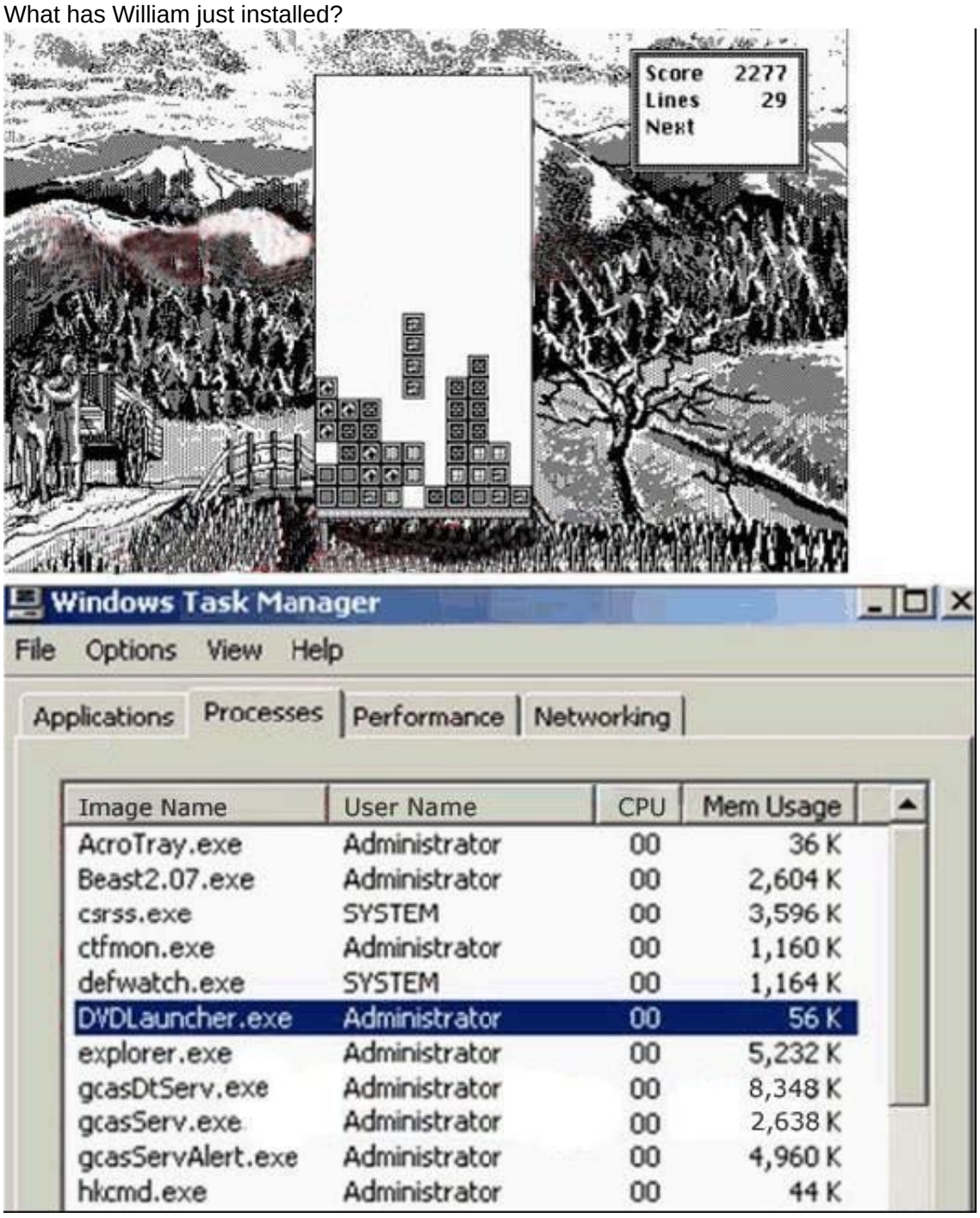
NEW QUESTION 318
- (Topic 6)
Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?

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

Answer: DE

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

NEW QUESTION 322
- (Topic 6)
William has received a Tetris game from someone in his computer programming class through email. William does not really know the person who sent the game very well, but decides to install the game anyway because he really likes Tetris.
After William installs the game, he plays it for a couple of hours. The next day, William plays the Tetris game again and notices that his machines have begun to slow down. He brings up his Task Manager and sees the following programs running (see Screenshot):
What has William just installed?



A. Remote Access Trojan (RAT)
B. Zombie Zapper (ZoZ)

C. Bot IRC Tunnel (BIT)
D. Root Digger (RD)

Answer: A

Explanation:
RATs are malicious programs that run invisibly on host PCs and permit an intruder remote access and control. On a basic level, many RATs mimic the functionality of legitimate remote control programs such as Symantec's pcAnywhere but are designed specifically for stealth installation and operation. Intruders usually hide these Trojan horses in games and other small programs that unsuspecting users then execute on their PCs.
Typically, exploited users either download and execute the malicious programs or are tricked into clicking rogue email attachments.

NEW QUESTION 327
- (Topic 6)
Which definition below best describes a covert channel?

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

Answer: A

Explanation:
A covert channel is a hidden communication channel not intended for information transfer at all. Redundancy can often be used to communicate in a covert way. There are several ways that hidden communication can be set up.

NEW QUESTION 331
- (Topic 6)
A file integrity program such as Tripwire protects against Trojan horse attacks by:

A. Automatically deleting Trojan horse programs
B. Rejecting packets generated by Trojan horse programs
C. Using programming hooks to inform the kernel of Trojan horse behavior
D. Helping you catch unexpected changes to a system utility file that might indicate it had been replaced by a Trojan horse

Answer: D

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

NEW QUESTION 336
- (Topic 6)
John wants to try a new hacking tool on his Linux System. As the application comes from a site in his untrusted zone, John wants to ensure that the downloaded tool has not been Trojaned. Which of the following options would indicate the best course of action for John?

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

Answer: C

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

NEW QUESTION 337
- (Topic 6)
Exhibit: * Missing*
Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

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

Answer: D

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

NEW QUESTION 340
- (Topic 6)
You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run

netstat
command to look for open ports and you notice a strange port 6666 open. What is the next step you would do?

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

Answer: D

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

NEW QUESTION 342
- (Topic 7)
Windump is a 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. PCAP
B. NTPCAP
C. LibPCAP
D. WinPCAP

Answer: D

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

NEW QUESTION 347
- (Topic 7)
Which tool/utility can help you extract the application layer data from each TCP connection from a log file into separate files?

A. Snort
B. argus
C. TCPflow
D. Tcpdump

Answer: C

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

NEW QUESTION 348
- (Topic 7)
What port number is used by Kerberos protocol?

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

Answer: B

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

NEW QUESTION 353
- (Topic 7)
Bob is conducting a password assessment for one of his clients. Bob suspects that password policies are not in place and weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weakness and key loggers. What are the means that Bob can use to get password from his client hosts and servers?

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

Answer: A

Explanation:
All loggers will work as long as he has physical access to the computers.

NEW QUESTION 357
- (Topic 7)
What does the following command in "Ettercap" do? ettercap –NCLzs –quiet

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

Answer: C

Explanation:
-L specifies that logging will be done to a binary file and –s tells us it is running in script mode.

NEW QUESTION 358
- (Topic 7)
A POP3 client contacts the POP3 server:

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

Answer: B

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

NEW QUESTION 363
- (Topic 7)
How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS's on a network?

A. Covert Channel
B. Crafted Channel
C. Bounce Channel
D. Deceptive Channel

Answer: A

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

NEW QUESTION 364
- (Topic 7)
Samantha was hired to perform an internal security test of company. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing.
Which of the following techniques can she use to gather information from the switched network or to disable some of the traffic isolation features of the switch? (Choose two)

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

Answer: BD

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

NEW QUESTION 366
- (Topic 7)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco Router’s access-list as below:

```
p address 192.168.1.1 255.255.255.0
p nat inside
alf-duplex
!
router rip
etwork 192.168.1.0
!
ip nat inside source list 102 interface Ethernet0/0 overload
no ip http server
ip classless
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 102 permit ip any any
!
snmp-server community public RO
snmp-server community private RW 1
snmp-server enable traps tty
!
line con 0
ogging synchronous
ogin
line aux 0
line vty 0 4
assword secret
ogin
```

You are tried to conduct security testing on their network. You successfully brute- force for SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection.
You want to retrieve the Cisco Configuration from the router. How would you proceed?

A. Send a customized SNMP set request with spoofed source IP Address in the range- 192.168.1.0
B. Run a network sniffer and capture the returned traffic with the configuration file from the router
C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
D. Use the Cisco's TFTP default password to connect and download the configuration file

Answer: AB

Explanation:
SNMP is allowed only by access-list 1. Therefore you need to spoof a 192.168.1.0/24 address and then sniff the reply from the gateway.

NEW QUESTION 367
- (Topic 7)
Which of the following display filters will you enable in Ethereal to view the three- way handshake for a connection from host 192.168.0.1?

A. ip == 192.168.0.1 and tcp.syn
B. ip.addr = 192.168.0.1 and syn = 1
C. ip.addr==192.168.0.1 and tcp.flags.syn
D. ip.equals 192.168.0.1 and syn.equals on

Answer: C

NEW QUESTION 371
- (Topic 8)
What happens during a SYN flood attack?

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

Answer: A

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

NEW QUESTION 375
- (Topic 8)
Peter has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the External Gateway interface. Further inspection reveals they are not responses from internal hosts request but simply responses coming from the Internet. What could be the likely cause of this?

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

Answer: C

Explanation:
An attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks with forged source address pointing to the target (victim) of the attack. All the systems on these networks reply to the victim with ICMP echo replies. This rapidly exhausts the bandwidth available to the target.

NEW QUESTION 376
- (Topic 8)
The evil hacker, is purposely sending fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes. From the information given, what type of attack is attempting to perform?

A. Syn flood
B. Smurf
C. Ping of death
D. Fraggle

Answer: C

Explanation:
Reference: http://insecure.org/sploits/ping-o-death.html

NEW QUESTION 378
- (Topic 8)
When working with Windows systems, what is the RID of the true administrator account?

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

Answer: A

Explanation:
The built-in administrator account always has a RID of 500.

NEW QUESTION 382
- (Topic 8)
Henry is an attacker and wants to gain control of a system and use it to flood a target system with requests, so as to prevent legitimate users from gaining access. What type of attack is Henry using?

A. Henry is executing commands or viewing data outside the intended target path
B. Henry is using a denial of service attack which is a valid threat used by an attacker
C. Henry is taking advantage of an incorrect configuration that leads to access with higher- than-expected privilege
D. Henry uses poorly designed input validation routines to create or alter commands to gain access to unintended data or execute commands

Answer: B

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

NEW QUESTION 385
- (Topic 8)
When working with Windows systems, what is the RID of the true administrator account?

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

Answer: A

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

NEW QUESTION 387
- (Topic 8)
Global deployment of RFC 2827 would help mitigate what classification of attack?

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

Answer: C

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

NEW QUESTION 389
- (Topic 8)
Steven, a security analyst for XYZ associates, is analyzing packets captured by Ethereal on a Linux Server inside his network when the server starts to slow down tremendously. Steven examines the following Ethereal captures:

File Edit Capture Display Tools

No.	Time	Source	Destination	Protocol
79	18.641058	172.18.0.2	172.18.255.255	NBNS
80	18.902646	172.18.0.2	172.18.255.255	NBNS
81	19.097138	cisco_c4:40:41	Spanning-tree-(for-br	STP
82	19.299265	172.18.0.3	127.0.0.1	ICMP
83	19.319210	172.18.0.2	172.18.255.255	NBNS
84	19.573854	172.18.0.2	172.18.255.255	NBNS
85	19.624918	172.18.0.2	172.18.255.255	BROWSE
86	19.744655	172.18.0.2	172.18.255.255	NBNS
87	19.786917	cisco_c4:40:41	Spanning-tree-(for-br	STP
88	19.978174	172.18.0.3	127.0.0.1	ICMP
89	19.988595	172.18.0.2	172.18.255.255	NBNS
90	20.103432	172.18.0.2	172.18.255.255	NBNS
91	20.225561	cisco_c4:40:41	Spanning-tree-(for-br	STP
92	20.292238	172.18.0.2	172.18.255.255	NBNS
93	20.496416	172.18.0.3	127.0.0.1	ICMP
94	20.509504	172.18.0.2	172.18.255.255	NBNS
95	20.762120	172.18.0.2	172.18.255.255	NBNS
96	20.812541	cisco_c4:40:41	Spanning-tree-(for-br	STP
97	21.033806	172.18.0.2	172.18.255.255	NBNS

A. Smurf Attack
B. ARP Spoofing
C. Ping of Death
D. SYN Flood

Answer: A

Explanation:
A perpetrator is sending a large amount of ICMP echo (ping) traffic to IP broadcast addresses, all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding.

NEW QUESTION 390
- (Topic 8)
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: AB

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

NEW QUESTION 393
- (Topic 8)
A denial of Service (DoS) attack works on the following principle:

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

Answer: D

Explanation:
Denial-of-service (often abbreviated as DoS) is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an Internet service,

such as a web site. This can be done by exercising a software bug that causes the software running the service to fail (such as the “Ping of Death” attack against Windows NT systems), sending enough data to consume all available network bandwidth (as in the May, 2001 attacks against Gibson Research), or sending data in such a way as to consume a particular resource needed by the service.

NEW QUESTION 394
- (Topic 8)
A Buffer Overflow attack involves:

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

Answer: D

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

NEW QUESTION 397
- (Topic 8)
Eve decides to get her hands dirty and tries out a Denial of Service attack that is relatively new to her. This time she envisages using a different kind of method to attack Brownies Inc. Eve tries to forge the packets and uses the broadcast address. She launches an attack similar to that of fraggle. What is the technique that Eve used in the case above?

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

Answer: A

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

NEW QUESTION 401
- (Topic 8)
You have been called to investigate a sudden increase in network traffic at company. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do you think was the most likely cause behind this sudden increase in traffic?

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

Answer: A

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

NEW QUESTION 405
- (Topic 8)
Smurf is a simple attack based on IP spoofing and broadcasts. A single packet (such as an ICMP Echo Request) is sent as a directed broadcast to a subnet on the Internet. All the machines on that subnet respond to this broadcast. By spoofing the source IP Address of the packet, all the responses will get sent to the spoofed IP Address. Thus, a hacker can often flood a victim with hundreds of responses for every request the hacker sends out.
Who are the primary victims of these attacks on the Internet today?

A. IRC servers are the primary victim to smurf attacks
B. IDS devices are the primary victim to smurf attacks
C. Mail Servers are the primary victim to smurf attacks
D. SPAM filters are the primary victim to surf attacks

Answer: A

Explanation:
IRC servers are the primary victim to smurf attacks. Script-kiddies run programs that scan the Internet looking for "amplifiers" (i.e. subnets that will respond). They compile lists of these amplifiers and exchange them with their friends. Thus, when a victim is flooded with responses, they will appear to come from all over the Internet. On IRCs, hackers will use bots (automated programs) that connect to IRC servers and collect IP addresses. The bots then send the forged packets to the amplifiers to inundate the victim.

NEW QUESTION 407
- (Topic 8)
Which one of the following instigates a SYN flood attack?

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

Answer: B

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

NEW QUESTION 411
- (Topic 8)
Hackers usually control Bots through:

A. IRC Channel
B. MSN Messenger
C. Trojan Client Software
D. Yahoo Chat
E. GoogleTalk

Answer: A

Explanation:
Most of the bots out today has a function to connect to a predetermined IRC channel in order to get orders.

NEW QUESTION 412
- (Topic 8)
How does a denial-of-service attack work?

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

Answer: C

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

NEW QUESTION 414
- (Topic 8)
What do you call a system where users need to remember only one username and password, and be authenticated for multiple services?

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

Answer: C

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

NEW QUESTION 415
- (Topic 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.

NEW QUESTION 419

- (Topic 9)
Which of these are phases of a reverse social engineering attack? Select the best answers.

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

Answer: ABD

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

NEW QUESTION 424
- (Topic 9)
A majority of attacks come from insiders, people who have direct access to a company's computer system as part of their job function or a business relationship. Who is considered an insider?

A. The CEO of the company because he has access to all of the computer systems
B. A government agency since they know the company computer system strengths and weaknesses
C. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants
D. A competitor to the company because they can directly benefit from the publicity generated by making such an attack

Answer: C

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

NEW QUESTION 425
- (Topic 9)
Your boss at ABC.com asks you what are the three stages of Reverse Social Engineering.

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

Answer: A

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

NEW QUESTION 430
- (Topic 9)
Study the following e-mail message. When the link in the message is clicked, it will take you to an address like: http://hacker.xsecurity.com/in.htm. Note that hacker.xsecurity.com is not an official SuperShopper site!
What attack is depicted in the below e-mail? Dear SuperShopper valued member,
Due to concerns, for the safety and integrity of the SuperShopper community we have issued this warning message. It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports.
If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service.
However, failure to update your records will result to your account cancellation. This notification expires within 24 hours.
Once you have updated your account records your SuperShopper will not be interrupted and will continue as normal.
Please follow the link below and renew your account information. https://www.supershopper.com/cgi-bin/webscr?cmd=update-run SuperShopper Technical Support http://www.supershopper.com

A. Phishing attack
B. E-mail spoofing
C. social engineering
D. Man in the middle attack

Answer: A

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

NEW QUESTION 433
- (Topic 9)
What is the most common vehicle for social engineering attacks?

A. Phone
B. Email
C. In person

D. P2P Networks

Answer: A

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

NEW QUESTION 434
- (Topic 9)
Dave has been assigned to test the network security of Acme Corp. The test was announced to the employees. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a sand clock to mark the progress of the test. Dave successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access. How was security compromised and how did the firewall respond?

A. The attack did not fall through as the firewall blocked the traffic
B. The attack was social engineering and the firewall did not detect it
C. The attack was deception and security was not directly compromised
D. Security was not compromised as the webpage was hosted internally

Answer: B

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

NEW QUESTION 438
- (Topic 9)
Why is Social Engineering considered attractive by hackers and also adopted by experts in the field?

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

Answer: C

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

NEW QUESTION 443
- (Topic 10)
What is the key advantage of Session Hijacking?

A. It can be easily done and does not require sophisticated skills.
B. You can take advantage of an authenticated connection.
C. You can successfully predict the sequence number generation.
D. You cannot be traced in case the hijack is detected.

Answer: B

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

NEW QUESTION 446
- (Topic 10)
Which of the following attacks takes best advantage of an existing authenticated connection

A. Spoofing
B. Session Hijacking
C. Password Sniffing
D. Password Guessing

Answer: B

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

NEW QUESTION 450
- (Topic 10)
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
F. Hunt is used for password cracking

Answer: D

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

NEW QUESTION 455
- (Topic 10)
After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledge (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen and then opens a second connection from a forget IP address. The attack doesn't see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP Address is used for authentication, the attacker can use the one-side communication to break into the server. What attacks can you successfully launch against a server using the above technique?

A. Session Hijacking attacks
B. Denial of Service attacks
C. Web Page defacement attacks
D. IP Spoofing Attacks

Answer: A

Explanation:
The term Session Hijacking refers to the exploitation of a valid computer session - sometimes also called a session key - to gain unauthorised access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

NEW QUESTION 460
.....

Relate Links

100% Pass Your 312-50 Exam with Exambible Prep Materials

https://www.exambible.com/312-50-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/