EC-Council

Exam Questions 312-50

Ethical Hacking and Countermeasures (CEHv6)

NEW QUESTION 1
- (Topic 1)
What is "Hacktivism"?

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

Answer: A

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

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

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

Answer: C

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

NEW QUESTION 3
- (Topic 1)
Which of the following act in the united states specifically criminalizes the transmission of unsolicited commercial e-mail(SPAM) without an existing business relationship.

A. 2004 CANSPAM Act
B. 2003 SPAM Preventing Act
C. 2005 US-SPAM 1030 Act
D. 1990 Computer Misuse Act

Answer: A

Explanation:
The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. The law, which became effective January 1, 2004, covers email whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site. A "transactional or relationship message" – email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship – may not contain false or misleading routing information, but otherwise is exempt from most provisions of the CAN-SPAM Act.

NEW QUESTION 4
- (Topic 1)
What are the two basic types of attacks?(Choose two.

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

Answer: BD

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

NEW QUESTION 5
- (Topic 1)
ABC.com is legally liable for the content of email that is sent from its systems, regardless of whether the message was sent for private or business-related purpose. This could lead to prosecution for the sender and for the company’s directors if, for example, outgoing email was found to contain material that was pornographic, racist or likely to incite someone to commit an act of terrorism.
You can always defend yourself by ‘ignorance of the law’ clause.

A. True
B. False

Answer: B

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

NEW QUESTION 6
- (Topic 1)
The United Kingdom (UK) he passed a law that makes hacking into an unauthorized network a felony.
The law states:
Section1 of the Act refers to unauthorized access to computer material. This states that a person commits an offence if he causes a computer to perform any function with intent to secure unauthorized access to any program or data held in any computer. For a successful conviction under this part of the Act, the prosecution must prove that the access secured is unauthorized and that the suspect knew that this was the case. This section is designed to deal with common-or-graden hacking.
Section 2 of the deals with unauthorized access with intent to commit or facilitate the commission of further offences. An offence is committed under Section 2 if a Section 1 offence has been committed and there is the intention of committing or facilitating a further offense (any offence which attacks a custodial sentence of more than five years, not necessarily one covered but the Act). Even if it is not possible to prove the intent to commit the further offence, the Section 1 offence is still committed.
Section 3 Offences cover unauthorized modification of computer material, which generally means the creation and distribution of viruses. For conviction to succeed there must have been the intent to cause the modifications and knowledge that the modification had not been authorized
What is the law called?

A. Computer Misuse Act 1990
B. Computer incident Act 2000
C. Cyber Crime Law Act 2003
D. Cyber Space Crime Act 1995

Answer: A

Explanation:
Computer Misuse Act (1990) creates three criminal offences:
? Unauthorised access to computer material
? Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence
? Unauthorised modification of computer material

NEW QUESTION 7
- (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 8
- (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 9
- (Topic 2)
To what does “message repudiation” refer to what concept in the realm of email security?

A. Message repudiation means a user can validate which mail server or servers a message was passed through.

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

Answer: E

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

NEW QUESTION 10
- (Topic 2)
Bill has started to notice some slowness on his network when trying to update his company's website while trying to access the website from the Internet. Bill asks the help desk manager if he has received any calls about slowness from the end users, but the help desk manager says that he has not. Bill receives a number of calls from customers that can't access the company website and can't purchase anything online. Bill logs on to a couple of this routers and notices that the logs shows network traffic is at all time high. He also notices that almost all the traffic is originating from a specific address.
Bill decides to use Geotrace to find out where the suspect IP is originates from. The Geotrace utility runs a traceroute and finds that IP is coming from Panama. Bill knows that none of his customers are in Panama so he immediately thinks that his company is under a Denial of Service attack. Now Bill needs to find out more about the originating IP Address.
What Internet registry should Bill look in to find the IP Address?

A. LACNIC
B. ARIN
C. RIPELACNIC
D. APNIC

Answer: A

Explanation:
LACNIC is the Latin American and Caribbean Internet Addresses Registry that administers IP addresses, autonomous system numbers, reverse DNS, and other network resources for that region.

NEW QUESTION 10
- (Topic 2)
Network Administrator Patricia is doing an audit of the network. Below are some of her findings concerning DNS. Which of these would be a cause for alarm?
Select the best answer.

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

Answer: A

Explanation:

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

NEW QUESTION 15
- (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 20
- (Topic 2)
You are footprinting the www.xsecurity.com domain using the Google Search Engine. You would like to determine what sites link to www.xsecurity .com at the first level of revelance.
Which of the following operator in Google search will you use to achieve this?

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

Answer: A

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

NEW QUESTION 21
- (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 26
- (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 27
- (Topic 3)
Which of the following is a patch management utility that scans one or more computers on your network and alerts you if you important Microsoft Security patches are missing. It then provides links that enable those missing patches to be downloaded and installed.

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

Answer: A

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

NEW QUESTION 29
- (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 31
- (Topic 3)
War dialing is a very old attack and depicted in movies that were made years ago. Why would a modem security tester consider using such an old technique?

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

Answer: B

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

NEW QUESTION 35
- (Topic 3)
What is the disadvantage of an automated vulnerability assessment tool?

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

Answer: E

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

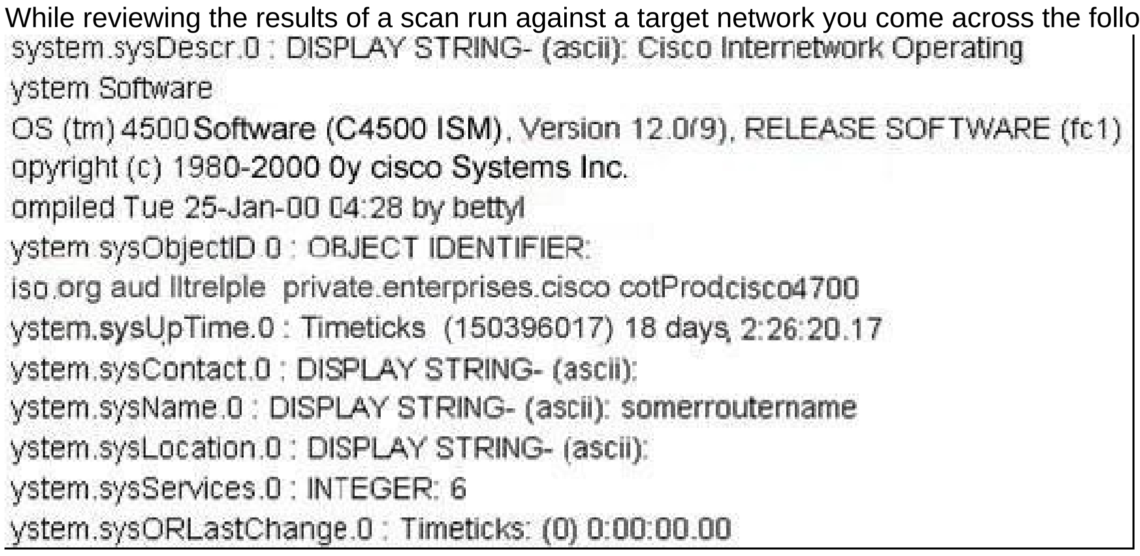
NEW QUESTION 36
- (Topic 3)
____ is one of the programs used to wardial.

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

Answer: E

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

NEW QUESTION 40
- (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 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 49
- (Topic 3)
Mark works as a contractor for the Department of Defense and is in charge of network security. He has spent the last month securing access to his network from all possible entry points. He has segmented his network into several subnets and has installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Mark is fairly confident of his perimeter defense, but is still worried about programs like Hping2 that can get into a network through convert channels.
How should mark protect his network from an attacker using Hping2 to scan his internal network?

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

Answer: A

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

NEW QUESTION 50
- (Topic 3)
What port scanning method is the most reliable but also the most detectable?

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

Answer: B

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

NEW QUESTION 53
- (Topic 3)
Which Type of scan sends a packets with no flags set ? Select the Answer

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

Answer: B

Explanation:
The types of port connections supported are:
? TCP Full Connect. This mode makes a full connection to the target's TCP ports and can save any data or banners returned from the target. This mode is the most accurate for determining TCP services, but it is also easily recognized by Intrusion Detection Systems (IDS).
? UDP ICMP Port Unreachable Connect. This mode sends a short UDP packet to the target's UDP ports and looks for an ICMP Port Unreachable message in return. The absence of that message indicates either the port is used, or the target does not return the ICMP message which can lead to false positives. It can save any data or banners returned from the target. This mode is also easily recognized by IDS.
? TCP Full/UDP ICMP Combined. This mode combines the previous two modes into one operation.

? TCP SYN Half Open. (Windows XP/2000 only) This mode sends out a SYN packet to the target port and listens for the appropriate response. Open ports respond with a SYN|ACK and closed ports respond with ACK|RST or RST. This mode is less likely to be noted by IDS, but since the connection is never fully completed, it cannot gather data or banner information. However, the attacker has full control over TTL, Source Port, MTU, Sequence number, and Window parameters in the SYN packet.
? TCP Other. (Windows XP/2000 only) This mode sends out a TCP packet with any
combination of the SYN, FIN, ACK, RST, PSH, URG flags set to the target port and listens for the response. Again, the attacker can have full control over TTL, Source Port, MTU, Sequence number, and Window parameters in the custom TCP packet. The Analyze feature helps with analyzing the response based on the flag settings chosen. Each operating system responds differently to these special combinations. The tool includes presets for XMAS, NULL, FIN and ACK flag settings.

NEW QUESTION 56
- (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 59
- (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 62
- (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)
What are the four steps is used by nmap scanning?

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

Answer: ACDF

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

NEW QUESTION 69
- (Topic 3)
Which FTP transfer mode is required for FTP bounce attack?

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

Answer: B

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

NEW QUESTION 73
- (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.

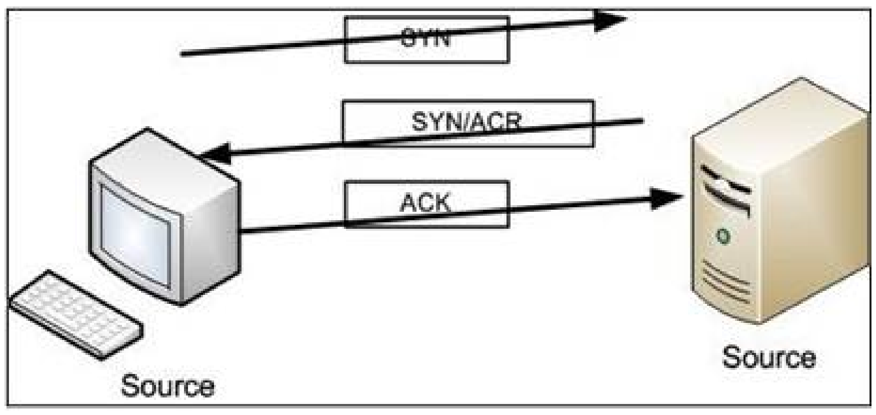
NEW QUESTION 74
- (Topic 3)
You are conducting a port scan on a subnet that has ICMP blocked. You have discovered 23 live systems and after scanning each of them you notice that they all show port 21 in closed state.
What should be the next logical step that should be performed?

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 77
- (Topic 3)
Exhibit:



Please study the exhibit carefully.
Which Protocol maintains the communication on that way?

A. UDP
B. IP
C. TCP
D. ARP
E. RARP

Answer: C

Explanation:
A TCP connection is always initiated with the 3-way handshake, which establishes and negotiates the actual connection over which data will be sent.

NEW QUESTION 78
- (Topic 3)
Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

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

Answer: ABCF

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

NEW QUESTION 79
- (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 84
- (Topic 3)
You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different protocols as possible.
Which kind of scan would you use to achieve this? (Choose the best answer)

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

Answer: D

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

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

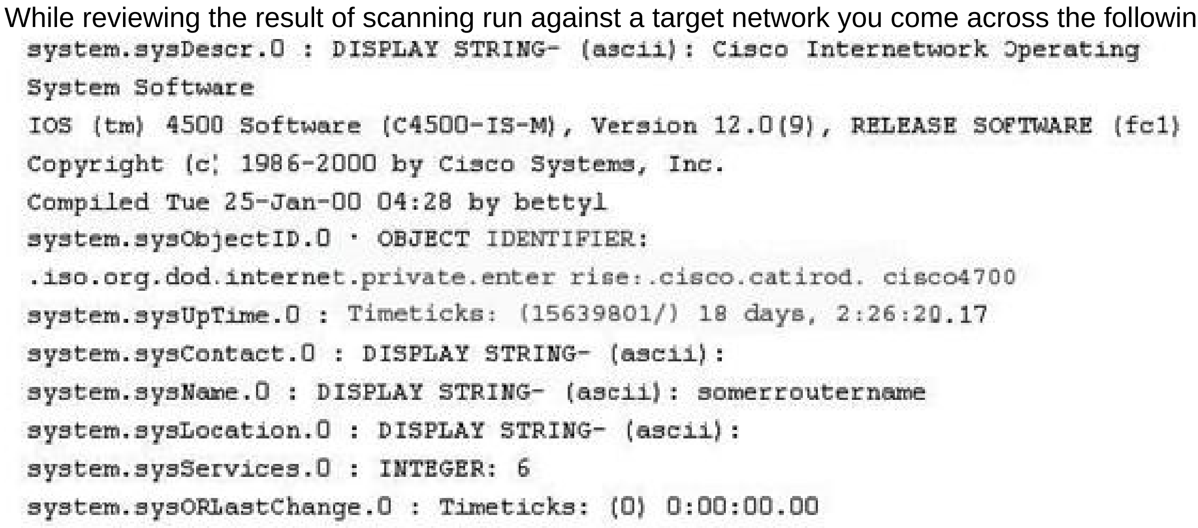
A. services
B. nmap-services
C. protocols
D. ports

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)
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 93
- (Topic 3)
While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

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

Answer: B

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

NEW QUESTION 95
- (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 97
- (Topic 3)
Because UDP is a connectionless protocol: (Select 2)

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

Answer: DE

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

NEW QUESTION 98
- (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 102
- (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

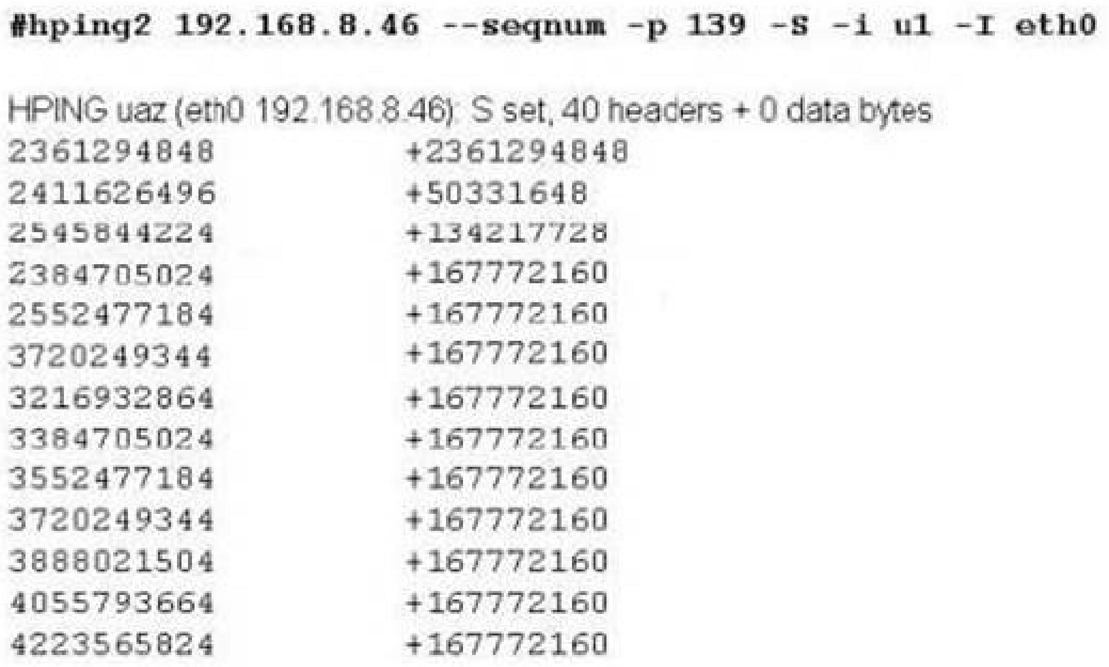
NEW QUESTION 107
- (Topic 3)
Which of the following is an automated vulnerability assessment tool.

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

Answer: C

Explanation:
Nessus is a vulnerability assessment tool.

NEW QUESTION 110
- (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 115
- (Topic 3)
A distributed port scan operates by:

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

Answer: D

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

NEW QUESTION 116
- (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 121
- (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 122
- (Topic 3)
Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

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

Answer: C

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

NEW QUESTION 123
- (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 127
- (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 132
- (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 136
- (Topic 3)
What does ICMP (type 11, code 0) denote?

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

Answer: B

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

NEW QUESTION 139
- (Topic 3)
Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop
B. It is a worm that is malfunctioning or hardcoded to scan on port 500
C. The attacker is trying to detect machines on the network which have SSL enabled
D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Answer: D

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

NEW QUESTION 144
- (Topic 3)
Why would an attacker want to perform a scan on port 137?

A. To discover proxy servers on a network
B. To disrupt the NetBIOS SMB service on the target host
C. To check for file and print sharing on Windows systems

D. To discover information about a target host using NBTSTAT

Answer: D

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

NEW QUESTION 149
- (Topic 3)
John is using a special tool on his Linux platform that has a signature database and is therefore able to detect hundred of vulnerabilities in UNIX, Windows, and commonly-used web CGI scripts. Additionally, the database detects DDoS zombies and Trojans. What would be the name of this multifunctional tool?

A. nmap
B. hping
C. nessus
D. make

Answer: C

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

NEW QUESTION 150
- (Topic 4)
SNMP is a connectionless protocol that uses UDP instead of TCP packets? (True or False)

A. True
B. False

Answer: A

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

NEW QUESTION 151
- (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 154
- (Topic 4)
What is a NULL scan?

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

Answer: A

Explanation:
A null scan has all flags turned off.

NEW QUESTION 155
- (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 157
- (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 160
- (Topic 4)
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e- mails from company B. How do you prevent DNS spoofing? (Select the Best Answer.)

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

Answer: C

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

NEW QUESTION 161
- (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 166
- (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 168
- (Topic 4)
MX record priority increases as the number increases.(True/False.

A. True
B. False

Answer: B

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

NEW QUESTION 172
- (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 177
- (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 182
- (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 185
- (Topic 5)

_____ is the process of converting something from one representation to the simplest form. It deals with the way in which systems convert data from one form to another.

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

Answer: A

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

NEW QUESTION 188
- (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 190
- (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.

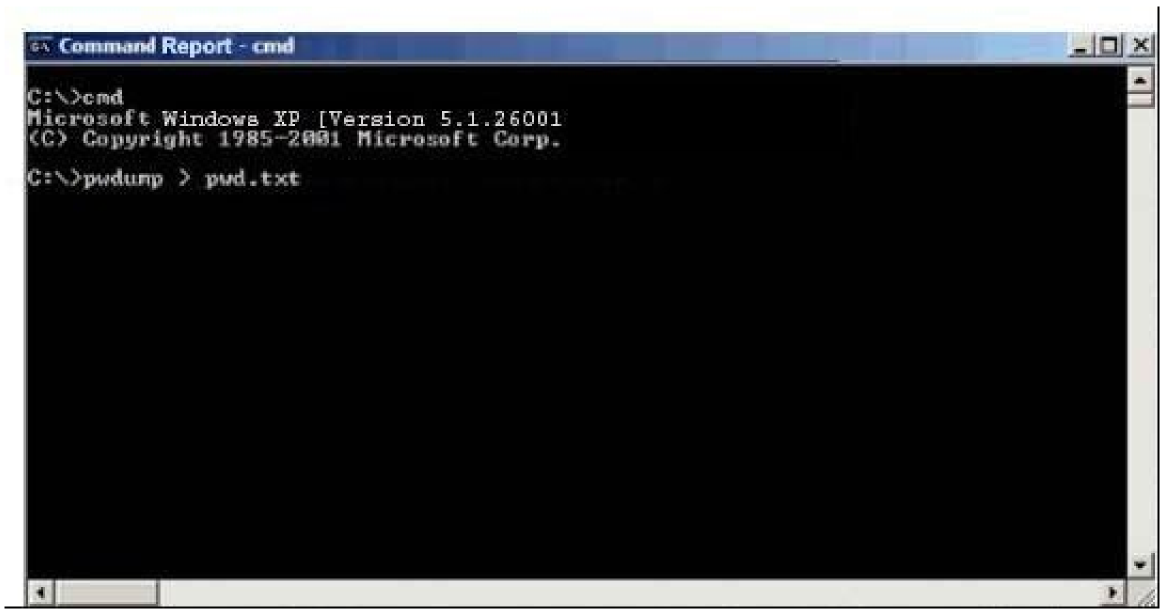
NEW QUESTION 195
- (Topic 5)
Which of the following is the primary objective of a rootkit?

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 198
- (Topic 5)
Michael is the security administrator for the for ABC company. Michael has been charged with strengthening the company’s security policies, including its password policies. Due to certain legacy applications. Michael was only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He has informed the company’s employes, however that the new password policy requires that everyone must have complex passwords with at least 14 characters. Michael wants to ensure that everyone is using complex passwords that meet the new security policy requirements. Michael has just logged on to one of the network’s domain controllers and is about to run the following command:
What will this command accomplish?



```
C:\>cmd
Microsoft Windows XP [Version 5.1.26001
(C) Copyright 1985-2001 Microsoft Corp.

C:\>pwdump > pwd.txt
```

A. Dumps SAM password hashes to pwd.txt
B. Password history file is piped to pwd.txt
C. Dumps Active Directory password hashes to pwd.txt
D. Internet cache file is piped to pwd.txt

Answer: A

Explanation:
Pwdump is a hack tool that is used to grab Windows password hashes from a remote Windows computer. Pwdump > pwd.txt will redirect the output from pwdump to a text file named pwd.txt

NEW QUESTION 199
- (Topic 5)
You are the IT Manager of a large legal firm in California. Your firm represents many important clients whose names always must remain anonymous to the public. Your boss, Mr. Smith is always concerned about client information being leaked or revealed to the pres or public. You have just finished a complete security overhaul of your information system including an updated IPS, new firewall, email encryption and employee security awareness training. Unfortunately, many of your firm's clients do not trust technology to completely secure their information, so couriers routinely have to travel back and forth to and from the office with sensitive information.
Your boss has charged you with figuring out how to secure the information the couriers must transport. You propose that the data be transferred using burned CD's or USB flash drives. You initially think of encrypting the files, but decide against that method for fear the encryption keys could eventually be broken.
What software application could you use to hide the data on the CD's and USB flash drives?

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

Answer: A

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

NEW QUESTION 200
- (Topic 5)
Samuel is the network administrator of DataX communications Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours time after more than three unsuccessful attempts. He is confident that this rule will secure his network hackers on the Internet.
But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall use.
Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts.
Samuel wants to completely block hackers brute force attempts on his network.
What are the alternatives to defending against possible brute-force password attacks on his site?

A. Enforce a password policy and use account lockouts after three wrong logon attempts even through this might lock out legit users
B. Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the intruder so that you can block them at the firewall manually
C. Enforce complex password policy on your network so that passwords are more difficult to brute force
D. You can't completely block the intruders attempt if they constantly switch proxies

Answer: D

Explanation:
Without knowing from where the next attack will come there is no way of proactively block the attack. This is becoming a increasing problem with the growth of large bot nets using ordinary workstations and home computers in large numbers.

NEW QUESTION 201
- (Topic 5)

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

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

Answer: B

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

NEW QUESTION 204
- (Topic 5)
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

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

Answer: E

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

NEW QUESTION 209
- (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 214
- (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 218
- (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 220
- (Topic 5)
You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption.
What encryption algorithm will you be decrypting?

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

Answer: B

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

NEW QUESTION 224
- (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)

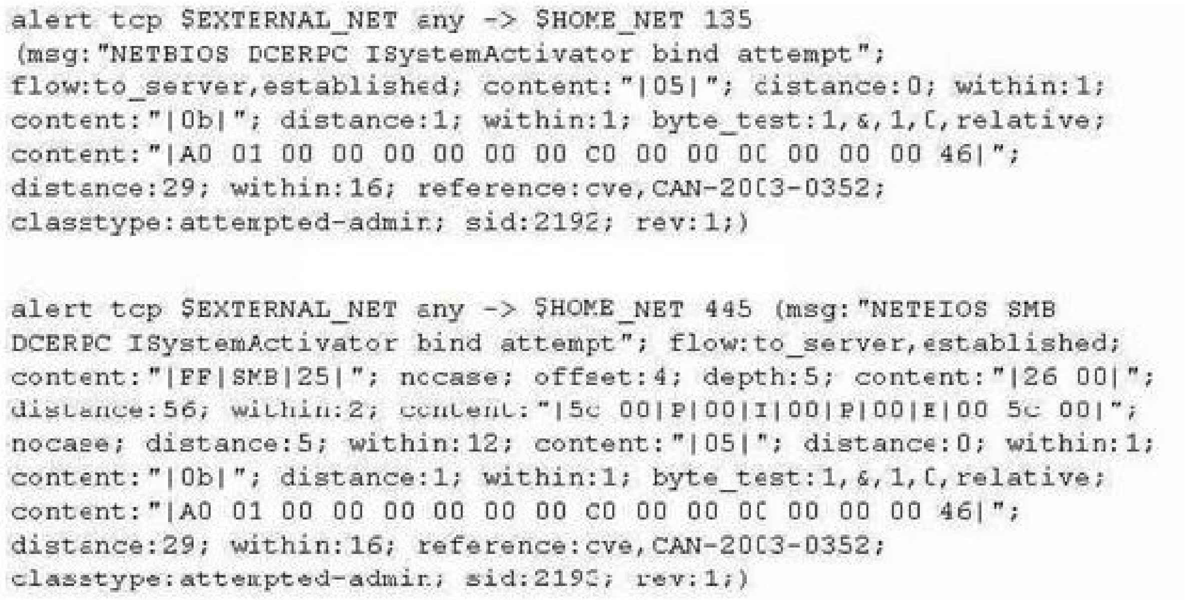
NEW QUESTION 229
- (Topic 5)
LM authentication is not as strong as Windows NT authentication so you may want to disable its use, because an attacker eavesdropping on network traffic will attack the weaker protocol. A successful attack can compromise the user's password. How do you disable LM authentication 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 233
- (Topic 5)
Study the snort rule given below:



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


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

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

A. WebDav
B. SQL Slammer

C. MS Blaster
D. MyDoom

Answer: C

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

NEW QUESTION 238
- (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 240
- (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 242
- (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?

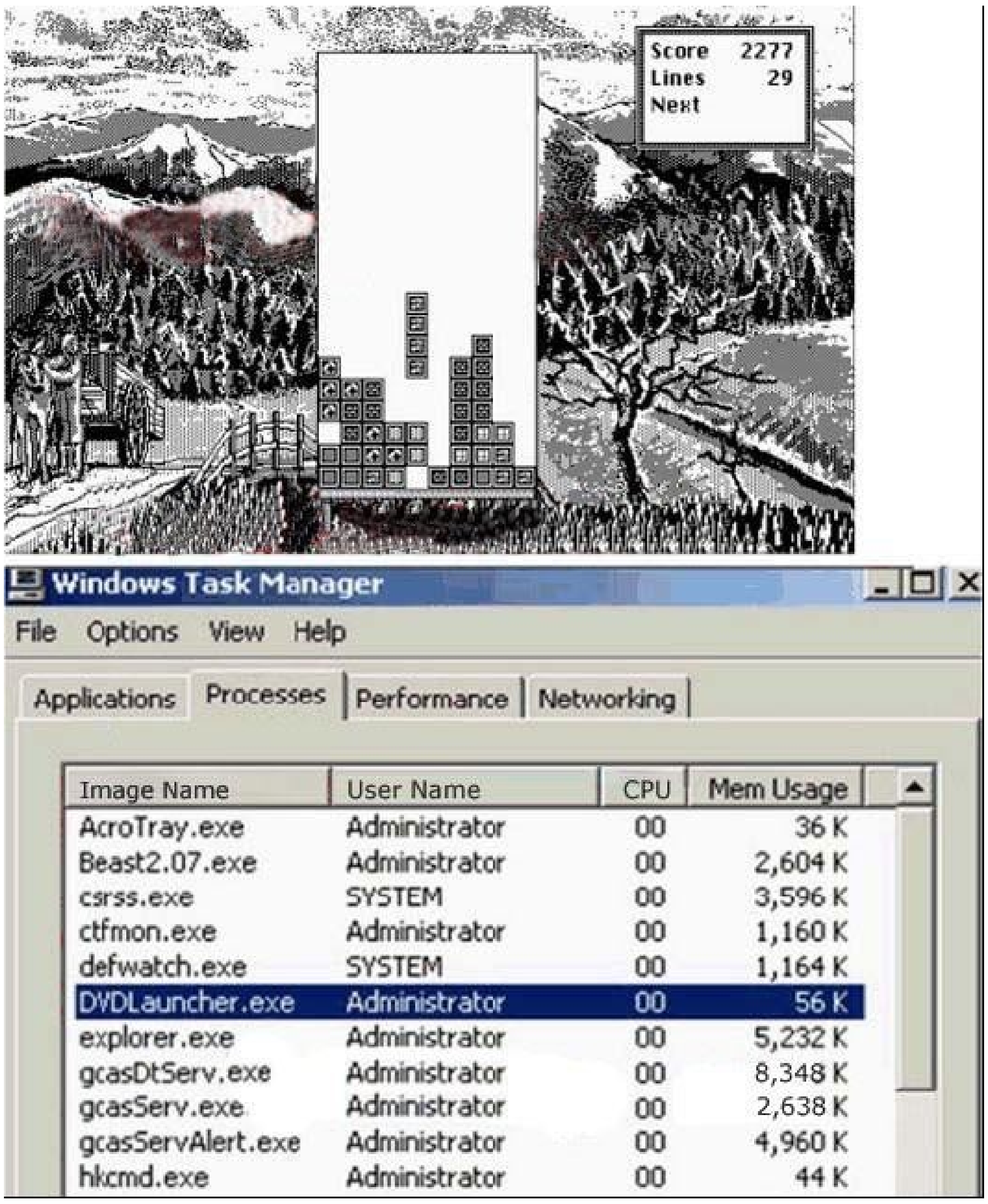


Image Name	User Name	CPU	Mem Usage
AcroTray.exe	Administrator	00	36 K
Beast2.07.exe	Administrator	00	2,604 K
csrss.exe	SYSTEM	00	3,596 K
ctfmon.exe	Administrator	00	1,160 K
defwatch.exe	SYSTEM	00	1,164 K
DVDLauncher.exe	Administrator	00	56 K
explorer.exe	Administrator	00	5,232 K
gcasDtServ.exe	Administrator	00	8,348 K
gcasServ.exe	Administrator	00	2,638 K
gcasServAlert.exe	Administrator	00	4,960 K
hkcmd.exe	Administrator	00	44 K

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 245
- (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 AAAAAAAAAAAAAAAAAAAAAA | nc –v –v –l –p 2222 > /dev/null Machine B#yes BBBBBBBBBBBBBBBBBBBBBB | 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 246
- (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 247
- (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 251
- (Topic 6)
Sniffing is considered an active attack.

A. True
B. False

Answer: B

Explanation:
Sniffing is considered a passive attack.

NEW QUESTION 253
- (Topic 6)
Spears Technology, Inc is a software development company located in Los Angeles, California. They reported a breach in security, stating that its “security defenses has
been breached and exploited for 2 weeks by hackers. “The hackers had accessed and downloaded 90,000 address containing customer credit cards and password. Spears Technology found this attack to be so to law enforcement officials to protect their intellectual property.
How did this attack occur? The intruder entered through an employees home machine, which was connected to Spears Technology, Inc’s corporate VPN network. The application called BEAST Trojan was used in the attack to open a “Back Door” allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge.
The hackers were traced back to Beijing China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Spears Technology’s network from a remote location, posing as employees. The intent of the attacker was to steal the source code for their VOIP system and “hold it hostage” from Spears Technology, Inc exchange for ransom.
The hackers had intended on selling the stolen VOIP software source code to competitors.
How would you prevent such attacks from occurring in the future at Spears Technology?

A. Disable VPN access to all your employees from home machines
B. Allow VPN access but replace the standard authentication with biometric authentication
C. Replace the VPN access with dial-up modem access to the company’s network
D. Enable 25 character complex password policy for employees to access the VPN network.

Answer: A

Explanation:
As long as there is a way in for employees through all security measures you can’t be secure because you never know what computer the employees use to access recourses at their workplace.

NEW QUESTION 254
- (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 259
- (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 263
- (Topic 7)
John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MiTM attack. What is the destination MAC address of a broadcast frame?

A. 0xFFFFFFFFFFFF
B. 0xAAAAAAAAAAAA
C. 0xBBBBBBBBBBBB
D. 0xDDDDDDDDDDDD

Answer: A

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

NEW QUESTION 268
- (Topic 7)
Daryl is a network administrator working for Dayton Technologies. Since Daryl's background is in web application development, many of the programs and applications his company uses are web-based. Daryl sets up a simple forms-based logon screen for all the applications he creates so they are secure.
The problem Daryl is having is that his users are forgetting their passwords quite often and sometimes he does not have the time to get into his applications and change the passwords for them. Daryl wants a tool or program that can monitor
web-based passwords and notify him when a password has been changed so he can use that tool whenever a user calls him and he can give them their password right then.
What tool would work best for Daryl's needs?

A. Password sniffer
B. L0phtcrack
C. John the Ripper
D. WinHttrack

Answer: A

Explanation:
L0phtCrack is a password auditing and recovery application (now called LC5), originally produced by Mudge from L0pht Heavy Industries. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords.
John the Ripper is one of the most popular password testing/breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customisable cracker. It can be run against various encrypted password formats including several crypt password hash types
WinHttrack is a offline browser.
A password sniffer would give Daryl the passwords when they are changed as it is a web based authentication over a simple form but still it would be more correct to give the users new passwords instead of keeping a copy of the passwords in clear text.

NEW QUESTION 272
- (Topic 7)
A remote user tries to login to a secure network using Telnet, but accidently types in an invalid user name or password. Which responses would NOT be preferred by an experienced Security Manager? (multiple answer)

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

Answer: AB

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

NEW QUESTION 274
- (Topic 7)
The follows is an email header. What address is that of the true originator of the message?
Return-Path: <bgates@microsoft.com>

Received: from smtp.com (fw.emumail.com [215.52.220.122].
by raq-221-181.ev1.net (8.10.2/8.10.2. with ESMTP id h78NIn404807 for <mikeg@thesolutionfirm.com>; Sat, 9 Aug 2003 18:18:50 -0500
Received: (qmail 12685 invoked from network.; 8 Aug 2003 23:25:25 -0000
Received: from ([19.25.19.10]. by smtp.com with SMTP
Received: from unknown (HELO CHRISLAPTOP. (168.150.84.123. by localhost with SMTP; 8 Aug 2003 23:25:01 -0000
From: "Bill Gates" <bgates@microsoft.com> To: "mikeg" <mikeg@thesolutionfirm.com> Subject: We need your help!
Date: Fri, 8 Aug 2003 19:12:28 -0400
Message-ID: <51.32.123.21@CHRISLAPTOP>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0052_01C35DE1.03202950" X-Priority: 3 (Normal.
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.2627
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165 Importance: Normal

A. 19.25.19.10
B. 51.32.123.21
C. 168.150.84.123
D. 215.52.220.122
E. 8.10.2/8.10.2

Answer: C

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

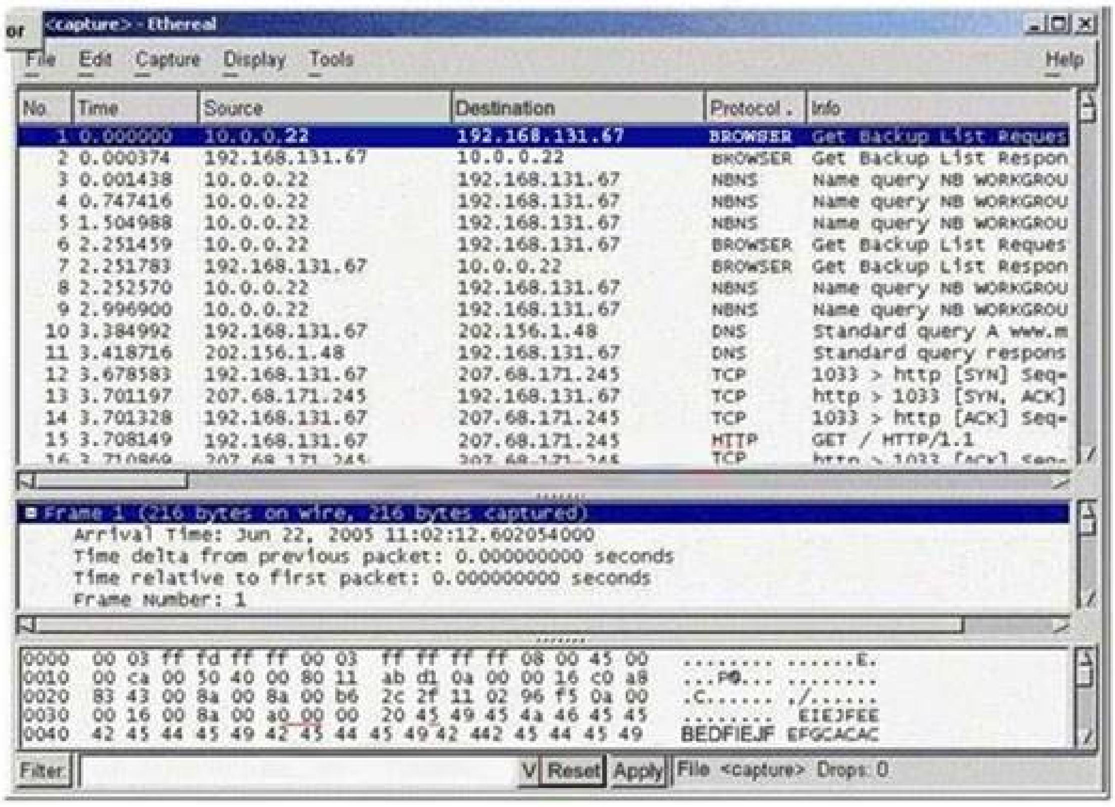
NEW QUESTION 279
- (Topic 7)
What is the command used to create a binary log file using tcpdump?

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 283
- (Topic 7)
Exhibit:



No.	Time	Source	Destination	Protocol .	Info
1	0.000000	10.0.0.22	192.168.131.67	BROWSER	Get Backup List Reques
2	0.000374	192.168.131.67	10.0.0.22	BROWSER	Get Backup List Respon
3	0.001438	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
4	0.747416	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
5	1.504988	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
6	2.251459	10.0.0.22	192.168.131.67	BROWSER	Get Backup List Reques
7	2.251783	192.168.131.67	10.0.0.22	BROWSER	Get Backup List Respon
8	2.252570	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
9	2.996900	10.0.0.22	192.168.131.67	NBNS	Name query NB WORKGROU
10	3.384992	192.168.131.67	202.156.1.48	DNS	Standard query A www.m
11	3.418716	202.156.1.48	192.168.131.67	DNS	Standard query respons
12	3.678583	192.168.131.67	207.68.171.245	TCP	1033 > http [SYN] Seq=
13	3.701197	207.68.171.245	192.168.131.67	TCP	http > 1033 [SYN, ACK]
14	3.701328	192.168.131.67	207.68.171.245	TCP	1033 > http [ACK] Seq=
15	3.708149	192.168.131.67	207.68.171.245	HTTP	GET / HTTP/1.1
16	3.710869	207.68.171.245	207.68.171.245	TCP	http > 1033 [ACK] Seq=

```
⊟ Frame 1 (216 bytes on wire, 216 bytes captured)
    Arrival Time: Jun 22, 2005 11:02:12.602054000
    Time delta from previous packet: 0.000000000 seconds
    Time relative to first packet: 0.000000000 seconds
    Frame Number: 1
```

```
0000  00 03 ff fd ff ff 00 03  ff ff ff ff 08 00 45 00   ........ ......E.
0010  00 ca 00 50 40 00 80 11  ab d1 0a 00 00 16 c0 a8   ...P@... ........
0020  83 43 00 8a 00 8a 00 b6  2c 2f 11 02 96 f5 0a 00   .C...... ,/......
0030  00 16 00 8a 00 a0 00 00  20 45 49 45 4a 46 45 45   ........  EIEJFEE
0040  42 45 44 45 49 42 45 44  45 49 42 442 45 44 45 49  BEDFIEJF EFGCACAC
```

You have captured some packets in Ethereal. You want to view only packets sent from 10.0.0.22. What filter will you apply?

A. ip = 10.0.0.22
B. ip.src == 10.0.0.22
C. ip.equals 10.0.0.22
D. ip.address = 10.0.0.22

Answer: B

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

NEW QUESTION 285
- (Topic 7)
Ethernet switches can be adversely affected by rapidly bombarding them with spoofed ARP responses. He port to MAC Address table (CAM Table) overflows on the switch and rather than failing completely, moves into broadcast mode, then the hacker can sniff all of the packets on the network.
Which of the following tool achieves this?

A. ./macof
B. ./sniffof
C. ./dnsiff
D. ./switchsnarf

Answer: A

Explanation:
macof floods the local network with random MAC addresses (causing some switches to fail open in repeating mode, facilitating sniffing).

NEW QUESTION 288
- (Topic 7)
You are sniffing as unprotected WiFi network located in a JonDonalds Cybercafe with Ethereal to capture hotmail e-mail traffic. You see lots of people using their laptops browsing the web while snipping brewed coffee from JonDonalds. You want to sniff their email message traversing the unprotected WiFi network.
Which of the following ethereal filters will you configure to display only the packets with the hotmail messages?

A. (http contains “hotmail”) && (http contains “Reply-To”)
B. (http contains “e-mail”) && (http contains “hotmail”)
C. (http = “login.passport.com”) && (http contains “SMTP”)
D. (http = “login.passport.com”) && (http contains “POP3”)

Answer: A

Explanation:
Each Hotmail message contains the tag Reply-To:<sender address> and “xxxx-xxx-xxx.xxxx.hotmail.com” in the received tag.

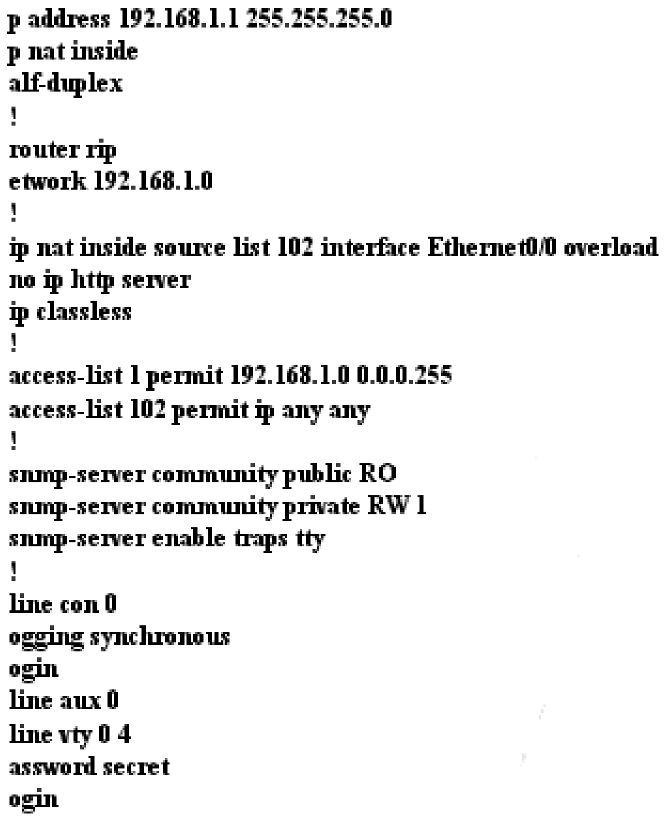
NEW QUESTION 292
- (Topic 7)
Samantha was hired to perform an internal security test of company. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing.
Which of the following techniques 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 297
- (Topic 7)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco Router’s access-list as below:



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

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

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

Answer: AB

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

NEW QUESTION 301
- (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 304
- (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 308
- (Topic 8)
What happens during a SYN flood attack?

A. TCP connection requests floods a target machine is flooded with randomized source address & ports for the TCP ports.
B. A TCP SYN packet, which is a connection initiation, is sent to a target machine, giving the target host's address as both source and destination, and is using the same port on the target host as both source and destination.

C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

Answer: A

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

NEW QUESTION 309
- (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 314
- (Topic 8)
When working with Windows systems, what is the RID of the true administrator account?

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

Answer: A

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

NEW QUESTION 319
- (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 324
- (Topic 8)
When working with Windows systems, what is the RID of the true administrator account?

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

Answer: A

Explanation:

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

NEW QUESTION 327
- (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 331
- (Topic 8)
If you send a SYN to an open port, what is the correct response?(Choose all correct answers.

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

Answer: AB

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

NEW QUESTION 334
- (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 337
- (Topic 8)
A Buffer Overflow attack involves:

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

Answer: D

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

NEW QUESTION 339
- (Topic 8)
You have been called to investigate a sudden increase in network traffic at company. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do you think was the most likely cause behind this sudden increase in traffic?

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

Answer: A

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

NEW QUESTION 343
- (Topic 8)
How does a denial-of-service attack work?

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

Answer: C

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

NEW QUESTION 346
- (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 347
- (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 348
- (Topic 9)
Sabotage, Advertising and Covering are the three stages of

A. Social engineering
B. Reverse Social Engineering
C. Reverse Software Engineering
D. Rapid Development Engineering

Answer: B

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

NEW QUESTION 349
- (Topic 9)
Within the context of Computer Security, which of the following statements best

describe Social Engineering?

A. Social Engineering is the act of publicly disclosing information.
B. Social Engineering is the act of getting needed information from a person rather than breaking into a system.
C. Social Engineering is the means put in place by human resource to perform time accounting.
D. Social Engineering is a training program within sociology studies.

Answer: B

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

NEW QUESTION 353
- (Topic 9)
Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to tell him her password 'just to double check our records'. Jane believes that Jack is really an administrator, and tells him her password. Jack now has a user name and password, and can access Brown Co.'s computers, to find the cookie recipe. This is an example of what kind of attack?

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

Answer: B

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

NEW QUESTION 357
- (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 359
- (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 361
- (Topic 9)
Jake works as a system administrator at Acme Corp. Jason, an accountant of the firm befriends him at the canteen and tags along with him on the pretext of appraising him about potential tax benefits. Jason waits for Jake to swipe his access card and follows him through the open door into the secure systems area.
How
would you describe Jason's behavior within a security context?

A. Trailing
B. Tailgating
C. Swipe Gating
D. Smooth Talking

Answer: B

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

NEW QUESTION 366
- (Topic 9)
Why is Social Engineering considered attractive by hackers and also adopted by experts in the field?

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

Answer: C

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

NEW QUESTION 368
- (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 371
- (Topic 10)
What is Hunt used for?

A. Hunt is used to footprint networks
B. Hunt is used to sniff traffic
C. Hunt is used to hack web servers
D. Hunt is used to intercept traffic i.
E. man-in-the-middle traffic
F. Hunt is used for password cracking

Answer: D

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

NEW QUESTION 372
- (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 374
- (Topic 10)
Which is the right sequence of packets sent during the initial TCP three way handshake?

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

Answer: D

Explanation:

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

NEW QUESTION 377
- (Topic 10)
Bob is going to perform an active session hijack against company. He has acquired the target that allows session oriented connections (Telnet) and performs sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network.
So, what is Bob most likely to do next?

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

Answer: C

NEW QUESTION 378
- (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 380
- (Topic 10)
You want to carry out session hijacking on a remote server. The server and the client are communicating via TCP after a successful TCP three way handshake. The server has just received packet #120 from the client. The client has a receive window of 200 and the server has a receive window of 250.
Within what range of sequence numbers should a packet, sent by the client fall in order to be accepted by the server?

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

Answer: B

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

NEW QUESTION 385
- (Topic 11)
Dan is conducting a penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network
B. The server will send replies back to the spoofed IP address
C. Dan can establish an interactive session only if he uses a NAT
D. The scenario is incorrect as Dan can spoof his IP and get responses

Answer: B

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

NEW QUESTION 389
- (Topic 11)
You wish to determine the operating system and type of web server being used. At the same time you wish to arouse no suspicion within the target organization.
While some of the methods listed below work, which holds the least risk of detection?

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

Answer: D

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

NEW QUESTION 392
- (Topic 11)
Sara is making use of Digest Authentication for her Web site. Why is this considered to be more secure than Basic authentication?

A. Basic authentication is broken
B. The password is never sent in clear text over the network
C. The password sent in clear text over the network is never reused.
D. It is based on Kerberos authentication protocol

Answer: B

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

NEW QUESTION 395
- (Topic 11)
What is Form Scalpel used for?

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

Answer: A

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

NEW QUESTION 398
- (Topic 11)
What are the differences between SSL and S-HTTP?

A. SSL operates at the network layer and S-HTTP operates at the application layer
B. SSL operates at the application layer and S-HTTP operates at the network layer
C. SSL operates at the transport layer and S-HTTP operates at the application layer
D. SSL operates at the application layer and S-HTTP operates at the transport layer

Answer: C

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

NEW QUESTION 401
- (Topic 11)
You have successfully run a buffer overflow attack against a default IIS installation running on a Windows 2000 Server. The server allows you to spawn a shell. In order to perform the actions you intend to do, you need elevated permission. You need to know what your current privileges are within the shell. Which of the following options would be your current privileges?

A. Administrator
B. IUSR_COMPUTERNAME
C. LOCAL_SYSTEM
D. Whatever account IIS was installed with

Answer: C

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

NEW QUESTION 402
- (Topic 11)
You are gathering competitive intelligence on ABC.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two job postings for network and system administrators. How can this help you in footprint the organization?

A. The IP range used by the target network

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

Answer: D

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

NEW QUESTION 406
- (Topic 11)
Take a look at the following attack on a Web Server using obstructed URL:
http://www.example.com/script.ext?template%2e%2e%2e%2e%2e%2f%2e%2f%65%74% 63%2f%70%61%73%73%77%64
The request is made up of:
? %2e%2e%2f%2e%2e%2f%2e%2f% = ../../../
? %65%74%63 = etc
? %2f = /
? %70%61%73%73%77%64 = passwd
How would you protect information systems from these attacks?

A. Configure Web Server to deny requests involving Unicode characters.
B. Create rules in IDS to alert on strange Unicode requests.
C. Use SSL authentication on Web Servers.
D. Enable Active Scripts Detection at the firewall and routers.

Answer: B

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

NEW QUESTION 409
- (Topic 11)
Bubba has just accessed he preferred ecommerce web site and has spotted an item that he would like to buy. Bubba considers the price a bit too steep. He looks at the source code of the webpage and decides to save the page locally, so that he can modify the page variables. In the context of web application security, what do you think Bubba has changes?

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

Answer: A

NEW QUESTION 412
- (Topic 11)
An attacker has been successfully modifying the purchase price of items purchased at a web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the IDS logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the price?

A. By using SQL injection
B. By using cross site scripting
C. By changing hidden form values in a local copy of the web page
D. There is no way the attacker could do this without directly compromising either the web server or the database

Answer: C

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

NEW QUESTION 414
- (Topic 12)
Ivan is auditing a corporate website. Using Winhex, he alters a cookie as shown below.
Before Alteration: Cookie: lang=en-us; ADMIN=no; y=1 ; time=10:30GMT ; After Alteration: Cookie: lang=en-us; ADMIN=yes; y=1 ; time=12:30GMT ; What attack is being depicted here?

A. Cookie Stealing
B. Session Hijacking
C. Cross Site Scripting
D. Parameter Manipulation

Answer: D

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

NEW QUESTION 415
- (Topic 12)
Kevin has been asked to write a short program to gather user input for a web application. He likes to keep his code neat and simple. He chooses to use printf(str) where he should have ideally used printf(?s? str). What attack will his program expose the web application to?

A. Cross Site Scripting
B. SQL injection Attack
C. Format String Attack
D. Unicode Traversal Attack

Answer: C

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

NEW QUESTION 416
- (Topic 12)
While testing web applications, you attempt to insert the following test script into the search area on the company's web site:
<script>alert('Testing Testing Testing')</script>
Afterwards, when you press the search button, a pop up box appears on your screen with the text "Testing Testing Testing". What vulnerability is detected in the web application here?

A. A hybrid attack
B. A buffer overflow
C. Password attacks
D. Cross Site Scripting

Answer: D

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

NEW QUESTION 417
- (Topic 12)
Jane has just accessed her preferred e-commerce web site and she has seen an item she would like to buy. Jane considers the price a bit too steep; she looks at the page source code and decides to save the page locally to modify some of the page variables. In the context of web application security, what do you think Jane has changed?

A. An integer variable
B. A 'hidden' price value
C. A 'hidden' form field value
D. A page cannot be changed locally; it can only be served by a web server

Answer: C

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

NEW QUESTION 419
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

312-50 Practice Exam Features:

* 312-50 Questions and Answers Updated Frequently

* 312-50 Practice Questions Verified by Expert Senior Certified Staff

* 312-50 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-50 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 312-50 Practice Test Here