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)
Which of the following best describes Vulnerability?

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

Answer: D

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

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

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

Answer: A

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

NEW QUESTION 4
- (Topic 1)
What does the term “Ethical Hacking” mean?

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

Answer: C

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

NEW QUESTION 5
- (Topic 1)
Who is an Ethical Hacker?

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

Answer: C

Explanation:
The Ethical hacker is a security professional who applies his hacking skills for defensive purposes.

NEW QUESTION 6
- (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 7
- (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 8
- (Topic 2)
You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com websire for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

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

Answer: B

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

NEW QUESTION 9
- (Topic 2)
How does Traceroute map the route that a packet travels from point A to point B?

A. It uses a TCP Timestamp packet that will elicit a time exceed in transit message.
B. It uses a protocol that will be rejected at the gateways on its way to its destination.
C. It manipulates the value of time to live (TTL) parameter packet to elicit a time exceeded in transit message.
D. It manipulated flags within packets to force gateways into generating error messages.

Answer: C

Explanation:
Traceroute works by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and

sends an ICMP time exceeded (type 11) packet to the sender. The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

NEW QUESTION 10
- (Topic 2)
According to the CEH methodology, what is the next step to be performed after footprinting?

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

Answer: B

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

NEW QUESTION 10
- (Topic 2)
The terrorist organizations are increasingly blocking all traffic from North America or from Internet Protocol addresses that point to users who rely on the English Language.
Hackers sometimes set a number of criteria for accessing their website. This information is shared among the co-hackers. For example if you are using a machine with the Linux Operating System and the Netscape browser then you will have access to their website in a convert way. When federal investigators using PCs running windows and using Internet Explorer visited the hacker's shared site, the hacker's system immediately mounted a distributed denial-of-service attack against the federal system.
Companies today are engaging in tracking competitor's through reverse IP address lookup sites like whois.com, which provide an IP address's domain. When the competitor visits the companies website they are directed to a products page without discount and prices are marked higher for their product. When normal users visit the website they are directed to a page with full-blown product details along with attractive discounts. This is based on IP-based blocking, where certain addresses are barred from accessing a site.
What is this masking technique called?

A. Website Cloaking
B. Website Filtering
C. IP Access Blockade
D. Mirrored WebSite

Answer: A

Explanation:
Website Cloaking travels under a variety of alias including Stealth, Stealth scripts, IP delivery, Food Script, and Phantom page technology. It's hot- due to its ability to manipulate those elusive top-ranking results from spider search engines.

NEW QUESTION 13
- (Topic 2)
Which of the following activities would not be considered passive footprinting?

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

Answer: C

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

NEW QUESTION 16
- (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 19
- (Topic 2)

User which Federal Statutes does FBI investigate for computer crimes involving e- mail scams and mail fraud?

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

Answer: B

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

NEW QUESTION 24
- (Topic 2)
Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing
B. Domain Name Server (DNS) poisoning
C. Reverse Address Resolution Protocol (ARP)
D. Port scanning

Answer: B

Explanation:
This reference is close to the one listed DNS poisoning is the correct answer.
This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert this data into the cache of there server instead of replacing the actual records, which is referred to as cache poisoning.

NEW QUESTION 29
- (Topic 2)
A very useful resource for passively gathering information about a target company is:

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

Answer: B

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

NEW QUESTION 33
- (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 38
- (Topic 2)
System Administrators sometimes post questions to newsgroups when they run into technical challenges. As an ethical hacker, you could use the information in newsgroup posting to glean insight into the makeup of a target network. How would you search for these posting using Google search?

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

Answer: B

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

NEW QUESTION 41
- (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 45
- (Topic 2)
Which of the following tools are used for footprinting?(Choose four.

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

Answer: ABCD

Explanation:
All of the tools listed are used for footprinting except Cheops.

NEW QUESTION 46
- (Topic 3)
You want to know whether a packet filter is in front of 192.168.1.10. Pings to 192.168.1.10 don't get answered. A basic nmap scan of 192.168.1.10 seems to hang without returning any information. What should you do next?

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

Answer: C

NEW QUESTION 48
- (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 52
- (Topic 3)
Which of the following ICMP message types are used for destinations unreachables?

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

Answer: B

Explanation:

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

NEW QUESTION 53
- (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 54
- (Topic 3)
Study the log below and identify the scan type.
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)
tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060) 4500
0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000

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

Answer: D

NEW QUESTION 57
- (Topic 3)
Destination unreachable administratively prohibited messages can inform the hacker to what?

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

Answer: D

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

NEW QUESTION 61
- (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 65
- (Topic 3)
The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence number of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. True
B. False

Answer: A

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

NEW QUESTION 67
- (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 70
- (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 74
- (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 75
- (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 80
- (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 85
- (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 90
- (Topic 3)
Which of the following would be the best reason for sending a single SMTP message to an address that does not exist within the target company?

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

Answer: C

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

NEW QUESTION 91
- (Topic 3)
Nathalie would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point. Which of the following type of scans would be the most accurate and reliable?

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

Answer: D

Explanation:
The connect() system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable. One strong advantage to this technique is that you don't need any special privileges. This is the fastest scanning method supported by nmap, and is available with the -t (TCP) option. The big downside is that this sort of scan is easily detectable and filterable.

NEW QUESTION 93
- (Topic 3)
What are the default passwords used by SNMP?(Choose two.)

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

Answer: CE

Explanation:
Besides the fact that it passes information in clear text, SNMP also uses well-known passwords. Public and private are the default passwords used by SNMP.

NEW QUESTION 97
- (Topic 3)
An attacker is attempting to telnet into a corporation’s system in the DMZ. The attacker doesn’t want to get caught and is spoofing his IP address. After numerous tries he remains unsuccessful in connecting to the system. The attacker rechecks that the target system is actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system.
What is the most probable reason?

A. The firewall is blocking port 23 to that system.
B. He cannot spoof his IP and successfully use TCP.
C. He needs to use an automated tool to telnet in.
D. He is attacking an operating system that does not reply to telnet even when open.

Answer: B

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

NEW QUESTION 98
- (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 101
- (Topic 3)
Paula works as the primary help desk contact for her company. Paula has just received a call from a user reporting that his computer just displayed a Blue Screen of Death screen and he ca no longer work. Paula walks over to the user’s computer and sees the Blue Screen of Death screen. The user’s computer is running Windows XP, but the Blue screen looks like a familiar one that Paula had seen a Windows 2000 Computers periodically.
The user said he stepped away from his computer for only 15 minutes and when he got back, the Blue Screen was there. Paula also noticed that the hard drive activity light was flashing meaning that the computer was processing some thing. Paula knew this should not be the case since the computer should be completely frozen during a Blue screen. She checks the network IDS live log entries and notices numerous nmap scan alerts.
What is Paula seeing happen on this computer?

A. Paula’s Network was scanned using FloppyScan
B. Paula’s Netwrok was scanned using Dumpsec
C. There was IRQ conflict in Paula’s PC
D. Tool like Nessus will cause BSOD

Answer: A

Explanation:
Floppyscan is a dangerous hacking tool which can be used to portscan a system using a floppy disk Bootsup mini Linux Displays Blue screen of death screen Port scans the network using NMAP Send the results by e-mail to a remote server.

NEW QUESTION 104
- (Topic 3)
Name two software tools used for OS guessing.(Choose two.

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

Answer: AC

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

NEW QUESTION 108
- (Topic 3)
An nmap command that includes the host specification of 202.176.56-57.* will scan ____ number of hosts.

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

Answer: C

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

NEW QUESTION 110
- (Topic 3)
Your are trying the scan a machine located at ABC company’s LAN named mail.abc.com. Actually that machine located behind the firewall. Which port is used by nmap to send the TCP synchronize frame to on mail.abc.com?

A. 443
B. 80
C. 8080
D. 23

Answer: A

NEW QUESTION 112
- (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 113
- (Topic 3)
Bob has been hired to perform a penetration test on ABC.com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information of have any technical details online.
Within the context of penetration testing methodology, what phase is Bob involved with?

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

Answer: A

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

NEW QUESTION 115
- (Topic 3)
What are twp types of ICMP code used when using the ping command?

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

Answer: A

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

NEW QUESTION 120
- (Topic 3)
What is the proper response for a FIN scan if the port is open?

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

Answer: F

Explanation:
Open ports respond to a FIN scan by ignoring the packet in question.

NEW QUESTION 123
- (Topic 3)
Study the log below and identify the scan type. tcpdump –w host 192.168.1.10

```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)

tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060) 4500 0014 a44c 0000 3b82
57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

A. nmap R 192.168.1.10
B. nmap S 192.168.1.10
C. nmap V 192.168.1.10
D. nmap –sO –T 192.168.1.10

Answer: D

Explanation:
-sO: IP protocol scans: This method is used to determine which IP protocols are supported on a host. The technique is to send raw IP packets without any further protocol header to each specified protocol on the target machine.

NEW QUESTION 127
- (Topic 3)
You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

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

Answer: A

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

NEW QUESTION 129
- (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 130
- (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 134
- (Topic 3)
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

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

Answer: B

NEW QUESTION 139
- (Topic 3)
An Nmap scan shows the following open ports, and nmap also reports that the OS guessing results to match too many signatures hence it cannot reliably be identified:
21 ftp
23 telnet
80 http
443 https
What does this suggest ?

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

Answer:

D

Explanation:
If the answer was A nmap would guess it, it holds the MS
signature database, the host not being firewalled makes no difference. The host is not linux or solaris, well it very well could be. The host is not properly patched? That is the closest; nmaps OS detection architecture is based solely off the TCP ISN issued by the operating systems TCP/IP stack, if the stack is modified to show output from randomized ISN's or if your using a program to change the ISN then OS detection will fail. If the TCP/IP IP ID's are modified then os detection could also fail, because the machine would most likely come back as being down.

NEW QUESTION 140
- (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 143
- (Topic 3)
You want to scan the live machine on the LAN, what type of scan you should use?

A. Connect
B. SYN
C. TCP
D. UDP
E. PING

Answer: E

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

NEW QUESTION 146
- (Topic 3)
What does an ICMP (Code 13) message normally indicates?

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

Answer: C

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

NEW QUESTION 147
- (Topic 3)
____ is an automated vulnerability assessment tool.

A. Whack a Mole

B. Nmap
C. Nessus
D. Kismet
E. Jill32

Answer: C

Explanation:
Nessus is a vulnerability assessment tool.

NEW QUESTION 150
- (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 153
- (Topic 3)
home/root # traceroute www.targetcorp.com <http://www.targetcorp.com> traceroute to www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18), 64 hops may, 40 byte packets
1 router.anon.com (192.13.212.254) 1.373 ms 1.123 ms 1.280 ms
2 192.13.133.121 (192.13.133.121) 3.680 ms 3.506 ms 4.583 ms
3 firewall.anon.com (192.13.192.17) 127.189 ms 257.404 ms 208.484 ms
4 anon-gw.anon.com (192.93.144.89) 471.68 ms 376.875 ms 228.286 ms
5 fe5-0.lin.isp.com (192.162.231.225) 2.961 ms 3.852 ms 2.974 ms
6 fe0-0.lon0.isp.com (192.162.231.234) 3.979 ms 3.243 ms 4.370 ms
7 192.13.133.5 (192.13.133.5) 11.454 ms 4.221 ms 3.333 ms
6 * * *
7 * * *
8 www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18) 5.392
ms 3.348 ms 3.199 ms
Use the traceroute results shown above to answer the following question:
The perimeter security at targetcorp.com does not permit ICMP TTL-expired packets out.

A. True
B. False

Answer: A

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

NEW QUESTION 156
- (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 160
- (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 162
- (Topic 3)
Bob is a Junior Administrator at ABC.com is searching the port number of POP3 in a file. The partial output of the file is look like:

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

In which file he is searching?

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

Answer: A

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

NEW QUESTION 165
- (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 168
- (Topic 3)
You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?

```
[ceh]# ping 10.2.3.4
PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms len=46 ip=10.2.3.4
flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms
--- 10.2.3.4 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.7/0.8/0.8 ms
```

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

Answer: C

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

NEW QUESTION 171
- (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 173
- (Topic 3)
John has performed a scan of the web server with NMAP but did not gather enough information to accurately identify which operating system is running on the remote host. How could you use a web server to help in identifying the OS that is being used?

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

Answer: A

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

NEW QUESTION 178
- (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 182
- (Topic 3)
Which of the following ICMP message types are used for destinations unreachables?

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

Answer: B

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

NEW QUESTION 186
- (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 188
- (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 191
- (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 192
- (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 196
- (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 198
- (Topic 4)
SNMP is a protocol used to query hosts, servers and devices about performance or health status data. Hackers have used this protocol for a long time to gather great amount of information about remote hosts. Which of the following features makes this possible?

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

Answer: AD

Explanation:

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

NEW QUESTION 203
- (Topic 4)
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and
XP?(Choose all that apply.

A. 110
B. 135
C. 139
D. 161
E. 445
F. 1024

Answer: BCE

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

NEW QUESTION 205
- (Topic 4)
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

A. 137 and 139
B. 137 and 443
C. 139 and 443
D. 139 and 445

Answer: D

Explanation:
NULL sessions take advantage of “features” in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Primarily the following ports are vulnerable if they are accessible:
139
TCP
NETBIOS Session Service 139
UDP
NETBIOS Session Service
445
TCP SMB/CIFS

NEW QUESTION 209
- (Topic 4)
Susan has attached to her company’s network. She has managed to synchronize her boss’s sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory. What kind of attack is Susan carrying on?

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

Answer: C

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

NEW QUESTION 210
- (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 212
- (Topic 4)
SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts.
Which of the following features makes this possible? (Choose two)

A. It used TCP as the underlying protocol.
B. It uses community string that is transmitted in clear text.
C. It is susceptible to sniffing.
D. It is used by all network devices on the market.

Answer: BC

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

NEW QUESTION 214
- (Topic 4)
One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800

Answer: A

Explanation:
The SOA starts with the format of YYYYMMDDVV where VV is the version.

NEW QUESTION 219
- (Topic 4)
Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for?
Select the best answers.

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

Answer: ABD

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

NEW QUESTION 224
- (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 225
- (Topic 4)
John is a keen administrator, and has followed all of the best practices as he could
find on securing his Windows Server. He has renamed the Administrator account to a new name that he is sure cannot be easily guessed. However, there are people who already attempt to compromise his newly renamed administrator account.
How is it possible for a remote attacker to decipher the name of the administrator account if it has been renamed?

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

Answer: B

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

NEW QUESTION 227
- (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 231
- (Topic 4)
Which of the following tools can be used to perform a zone transfer?

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

Answer: ACDE

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

NEW QUESTION 236
- (Topic 4)
Exhibit:

```
c:\> cmd /c type c:\winnt\repair\sam > c:\har.txt
Volume in drive C has no label.
Volume Serial Number is 8403-6A0E
Director facs\
11/26/00 12:34p 0 AUFCEXEC.BAT
11/26/00 06:57p 322 boot.ini
11/26/00 12:34p CONFIG.SYS
12/26/00 07:36p < DIR > exploits
02/04/01 07:07a 5,327 har.txt
12/07/00 03:30p < DIR > InetPub
12/07/00 03:12p < DIR > Multimedia Files
12/26/00 07:10p < DIR > New Folder
01/26/01 02:10p 78,643,200 pagefile.sys
12/21/00 08:59p < DIR > Program Files
02/04/01 06:49a 69 README.NOW.HaxOr
12/21/00 08:59p < DIR > TEMP
02/04/01 07:05a < DIR > WINNT
12/26/00 07:09p < DIR > wiretrip
02/04/01 06:43a 0 mine.txt
15 File(s) 78,648,918 bytes
1,689,455,616 bytes free

c:\> type har.txt

c:\> hapr har.txt c:\inetpub\www out
c:\> GET har.txt HTTP/1.1
Server: Microsoft-IIS/4.0
Date: Sun, 04 Feb 2001 13:11:28 GMT
Content-Type: text/plain
Accept-Ranges: bytes
Last-Modified: Sun, 04 Feb 2001 13:07:33 GMT
ETag: "5063fd6fab8ec01:b85"
Content-Length: 5327
```

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt
B. SAM file
C. wwwroot
D. Repair file

Answer: B

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

NEW QUESTION 238
- (Topic 4)
What sequence of packets is sent during the initial TCP three-way handshake?

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

Answer: D

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

NEW QUESTION 241
- (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 242
- (Topic 4)
What tool can crack Windows SMB passwords simply by listening to network traffic? Select the best answer.

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

Answer: D

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

NEW QUESTION 247
- (Topic 4)
Which of the following tools are used for enumeration? (Choose three.)

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

Answer: BDE

Explanation:
USER2SID, SID2USER, and DumpSec are three of the tools used for system enumeration. Others are tools such as NAT and Enum. Knowing which tools are used in each step of the hacking methodology is an important goal of the CEH exam. You should spend a portion of your time preparing for the test practicing with the tools and learning to understand their output.

NEW QUESTION 248
- (Topic 4)
What does FIN in TCP flag define?

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

Answer: A

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

NEW QUESTION 252
- (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 253
- (Topic 4)
What is the proper response for a NULL scan if the port is open?

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

F. No response

Answer: F

Explanation:
A NULL scan will have no response if the port is open.

NEW QUESTION 256
- (Topic 4)
Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two.
What would you call this attack?

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

Answer: B

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

NEW QUESTION 258
- (Topic 4)
Which DNS resource record can indicate how long any "DNS poisoning" could last?

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

Answer: B

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

NEW QUESTION 263
- (Topic 4)
Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

A. Overloading Port Address Translation
B. Dynamic Port Address Translation
C. Dynamic Network Address Translation
D. Static Network Address Translation

Answer: D

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

NEW QUESTION 266
- (Topic 4)
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?
Select the best answers.

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

Answer: BCDE

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

NEW QUESTION 271
- (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 274
- (Topic 4)
Exhibit:

What type of attack is shown in the above diagram?

A. SSL Spoofing Attack
B. Identity Stealing Attack
C. Session Hijacking Attack
D. Man-in-the-Middle (MiTM) Attack

Answer: D

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

NEW QUESTION 275
- (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 280
- (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.

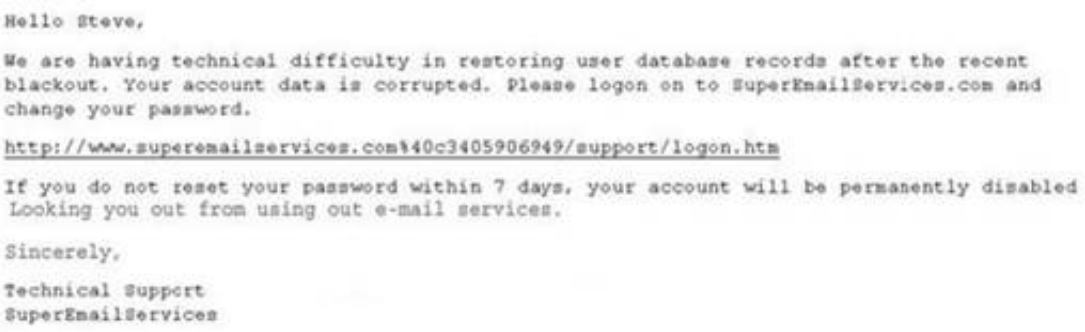
NEW QUESTION 282
- (Topic 5)
Travis works primarily from home as a medical transcriptions.
He just bought a brand new Dual Core Pentium Computer with over 3 GB of RAM. He uses voice recognition software is processor intensive, which is why he bought the new computer. Travis frequently has to get on the Internet to do research on what he is working on. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to.
Travis uses antivirus software, anti-spyware software and always keeps the computer up-to-date with Microsoft patches.
After another month of working on the computer, Travis computer is even more noticeable slow. Every once in awhile, Travis also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Travis is really worried about his computer because he spent a lot of money on it and he depends on it to work. Travis scans his through Windows Explorer and check out the file system, folder by folder to see if there is anything he can find. He spends over four hours pouring over the files and folders and can't find anything but before he gives up, he notices that his computer only has about 10 GB of free space available. Since has drive is a 200 GB hard drive, Travis thinks this is very odd.
Travis downloads Space Monger and adds up the sizes for all the folders and files on his computer. According to his calculations, he should have around 150 GB of free space. What is mostly likely the cause of Travi's problems?

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

Answer: A

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

NEW QUESTION 283
- (Topic 5)
Exhibit


Hello Steve,

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

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

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

Sincerely,

Technical Support
SuperEmailServices

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

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

Answer: C

Explanation:
Convert the number in binary, then start from last 8 bits and convert them to decimal to get the last octet (in this case .5)

NEW QUESTION 287
- (Topic 5)
Which of the following is an attack in which a secret value like a hash is captured and then reused at a later time to gain access to a system without ever decrypting or decoding the hash.

A. Replay Attacks
B. Brute Force Attacks
C. Cryptography Attacks

D. John the Ripper Attacks

Answer: A

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

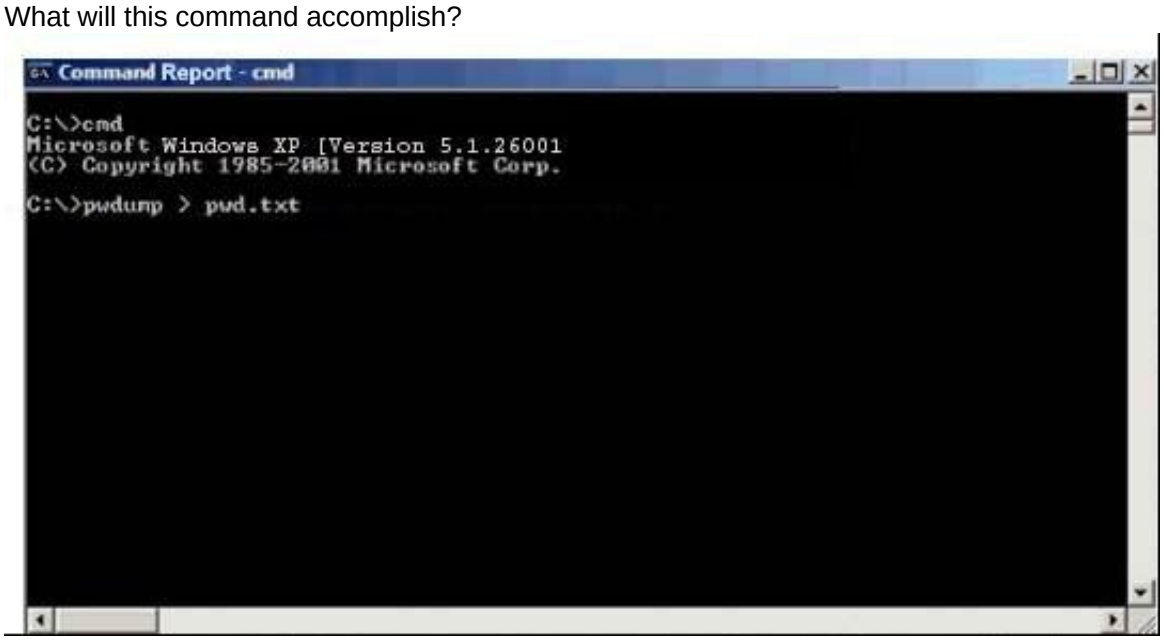
NEW QUESTION 290
- (Topic 5)
Which of the following is the primary objective of a rootkit?

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 292
- (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?



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 293
- (Topic 5)
Password cracking programs reverse the hashing process to recover passwords.(True/False.

A. True
B. False

Answer: B

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

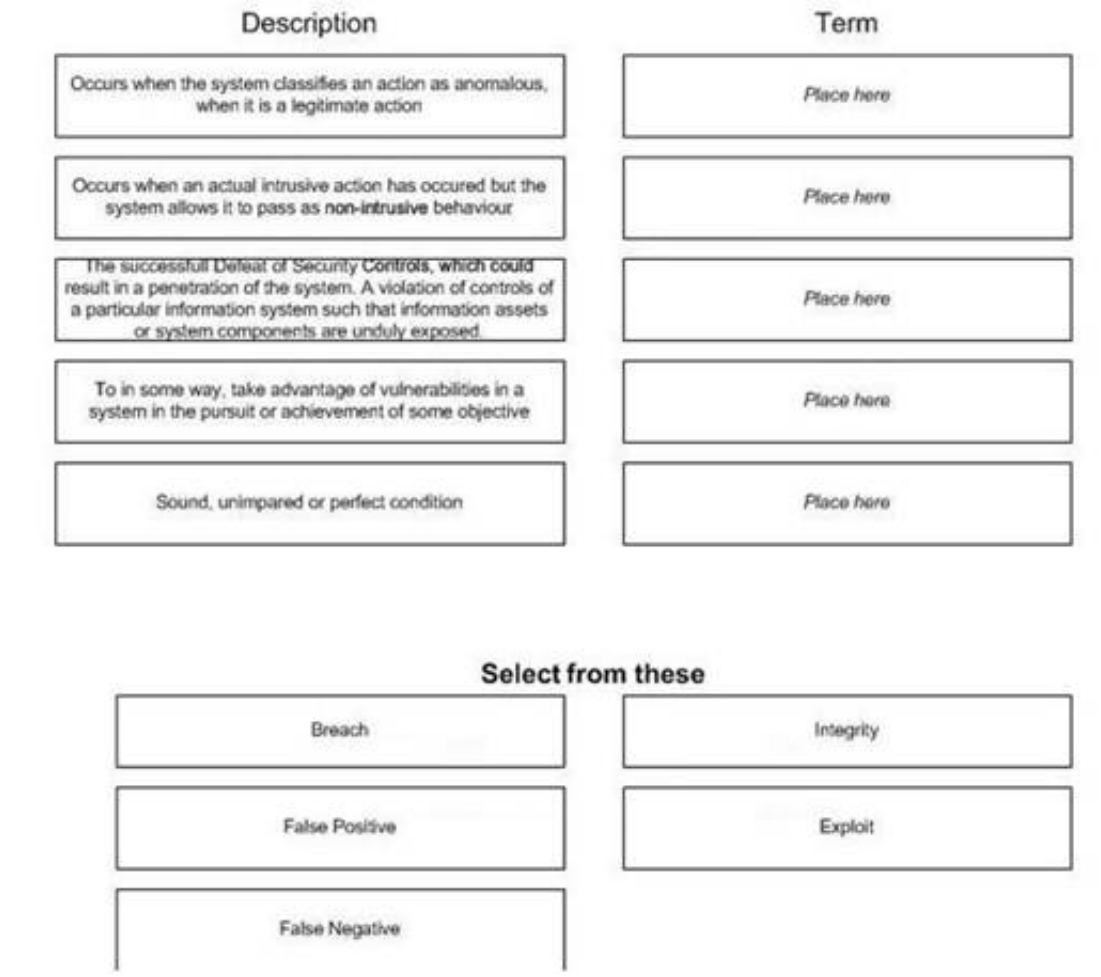
NEW QUESTION 294
- (Topic 5)
When discussing passwords, what is considered a brute force attack?

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

Answer: A

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

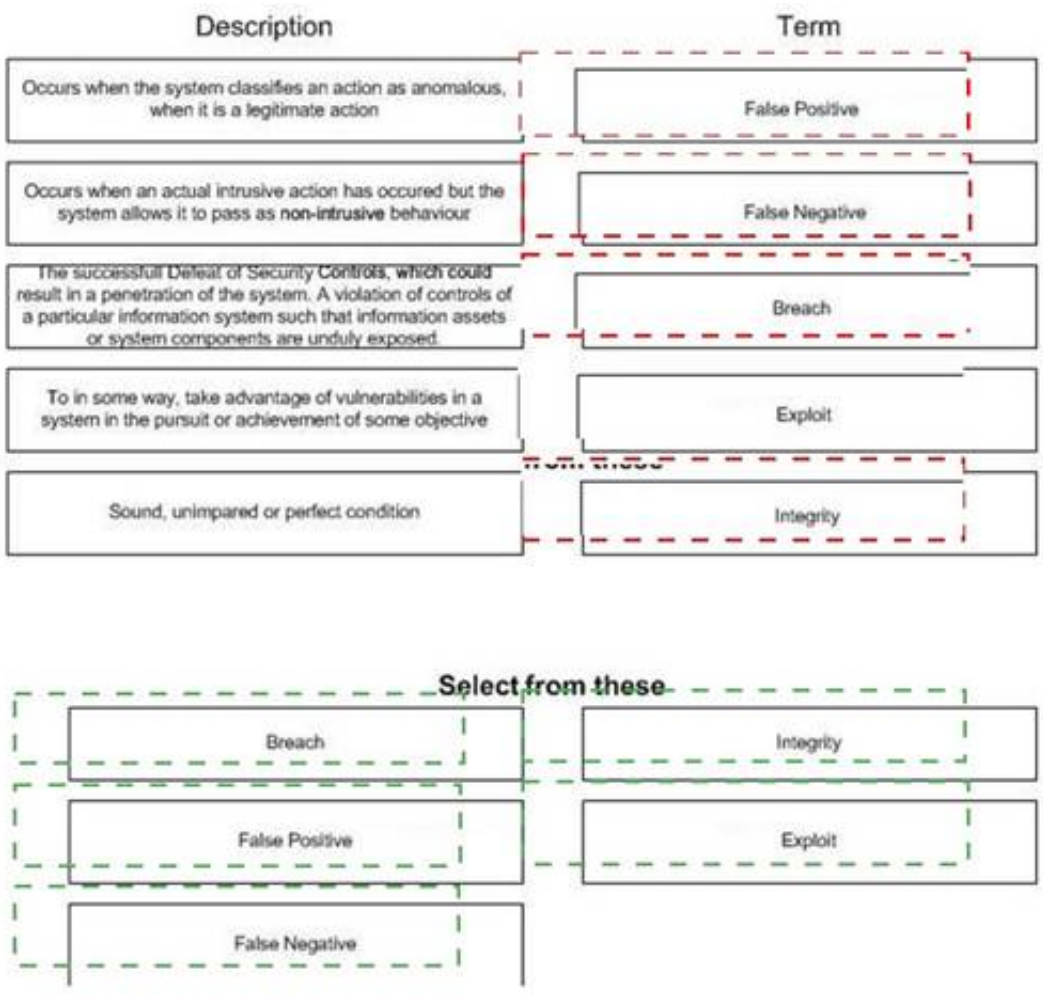
NEW QUESTION 296
DRAG DROP - (Topic 5)
Drag the term to match with it's description
Exhibit:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 298
- (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 301
- (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 304
- (Topic 5)
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

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

Answer: E

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

NEW QUESTION 309
- (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 313
- (Topic 5)
____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

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

Answer: B

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

NEW QUESTION 316
- (Topic 5)
You have successfully brute forced basic authentication configured on a Web Server using Brutus hacking tool. The username/password is “Admin” and “Bettlemani@”. You logon to the system using the brute forced password and plant backdoors and rootkits.
After downloading various sensitive documents from the compromised machine, you proceed to clear the log files to hide your trace..
Which event log located at C:\Windows\system32\config contains the trace of your brute force attempts?

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

Answer: B

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

NEW QUESTION 318
- (Topic 5)
What file system vulnerability does the following command take advantage of? type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

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

Answer: B

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

NEW QUESTION 323
- (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 327
- (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 329
- (Topic 5)
Which of the following are well know password-cracking programs?(Choose all that apply.

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

Answer: AE

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

NEW QUESTION 330
- (Topic 5)
How would you describe an attack where an attacker attempts to deliver the payload over multiple packets over long periods of time with the purpose of defeating simple pattern matching in IDS systems without session reconstruction? A characteristic of this attack would be a continuous stream of small packets.

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

Answer: A

NEW QUESTION 331
- (Topic 5)
Which of the following LM hashes represent a password of less than 8 characters? (Select 2)

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

Answer: BE

Explanation:
Notice the last 8 characters are the same

NEW QUESTION 333
- (Topic 5)
E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.
B. pa
C. 1030 Fraud and Related activity in connection with Computers
D. 18 U.S.
E. pa
F. 1029 Fraud and Related activity in connection with Access Devices
G. 18 U.S.
H. pa
I. 1362 Communication Lines, Stations, or Systems
J. 18 U.S.
K. pa
L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

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

NEW QUESTION 335
- (Topic 5)

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

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

Answer: ACE

Explanation:
Explanations:
John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case. John the Ripper is a very effective password cracker. It can crack passwords for many different types of operating systems. However, one limitation is that the output doesn't show if the password is upper or lower case. BY using NTLMV1, you have implemented an effective countermeasure to password cracking. NTLM Version 2 (NTLMV2) is a good countermeasure to LM password cracking (and therefore a correct answer). To do this, set Windows 9x and NT systems to "send NTLMv2 responses only". SYSKEY is an effective countermeasure. It uses 128 bit encryption on the local copy of the Windows SAM. If a Windows LM password is 7 characters or less, the has will be passed with the following characters: 0xAAD3B435B51404EE
Enforcing Windows complex passwords is an effective countermeasure to password cracking. Complex passwords are- greater than 6 characters and have any 3 of the following 4 items: upper case, lower case, special characters, and numbers.

NEW QUESTION 337
- (Topic 5)
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers.

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

Answer: A

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

NEW QUESTION 341
- (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 344
- (Topic 5)
In the context of Windows Security, what is a 'null' user?

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

Answer: C

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

NEW QUESTION 349
- (Topic 6)

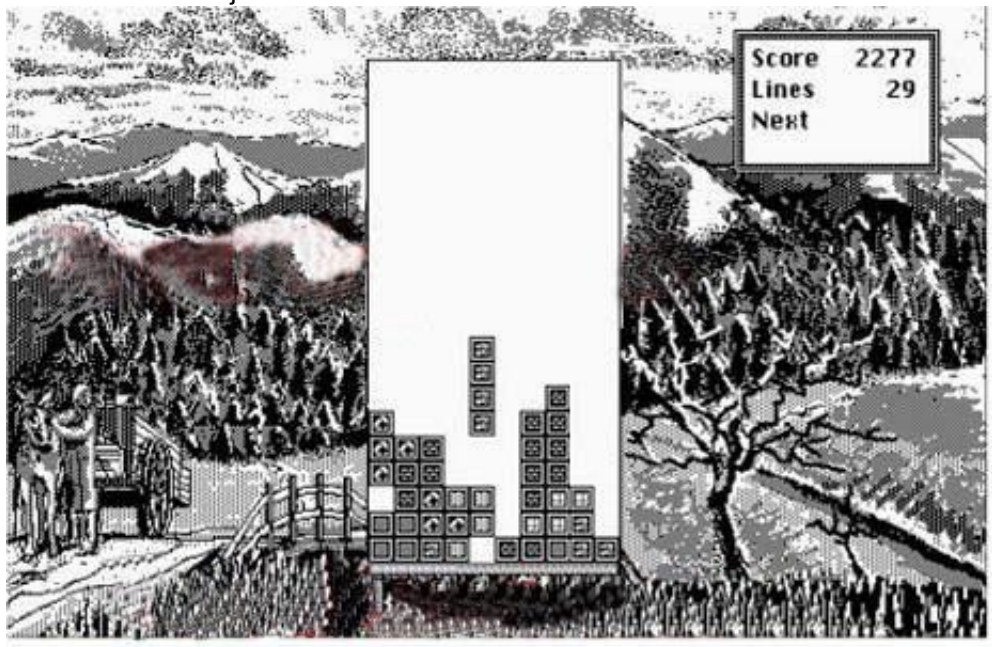
Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?

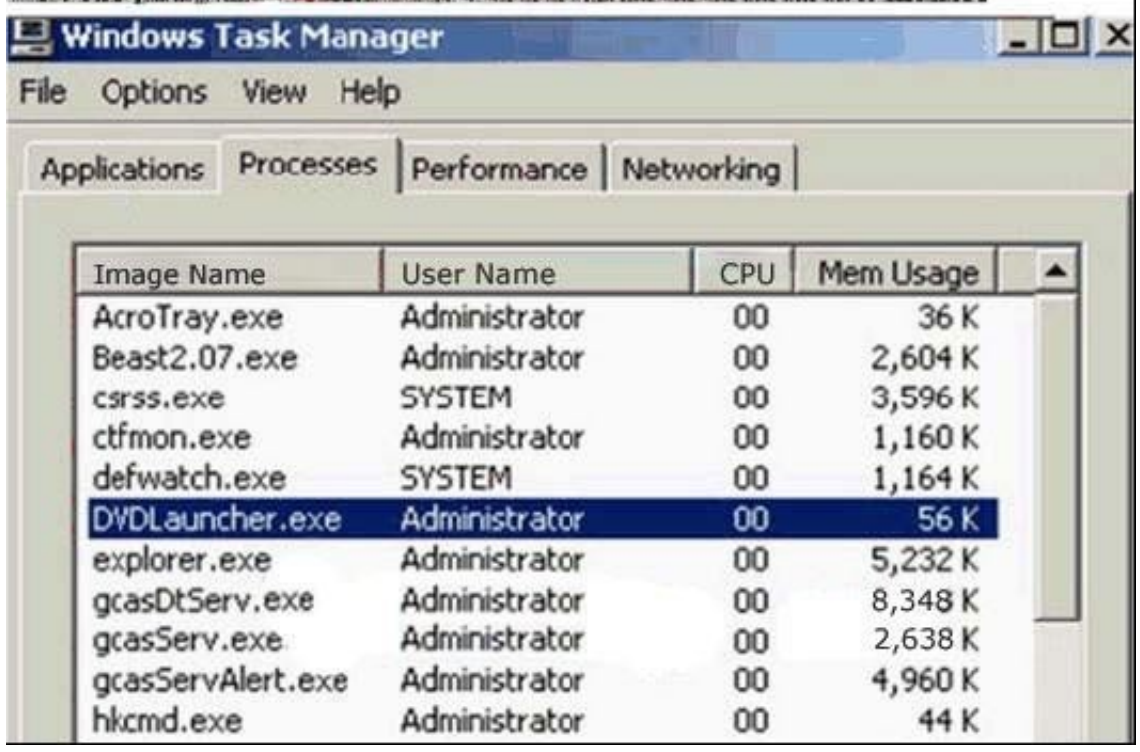
A. Spoof Attack
B. Smurf Attack
C. Man in the Middle Attack
D. Trojan Horse Attack
E. Back Orifice Attack

Answer: DE

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

NEW QUESTION 352
- (Topic 6)
William has received a Tetris game from someone in his computer programming class through email. William does not really know the person who sent the game very well, but decides to install the game anyway because he really likes Tetris.
After William installs the game, he plays it for a couple of hours. The next day, William plays the Tetris game again and notices that his machines have begun to slow down. He brings up his Task Manager and sees the following programs running (see Screenshot):
What has William just installed?





A. Remote Access Trojan (RAT)
B. Zombie Zapper (ZoZ)
C. Bot IRC Tunnel (BIT)
D. Root Digger (RD)

Answer: A

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

NEW QUESTION 355
- (Topic 6)
You want to use netcat to generate huge amount of useless network data continuously for various performance testing between 2 hosts.
Which of the following commands accomplish this?

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

Answer: A

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

NEW QUESTION 356
- (Topic 6)
In the context of Trojans, what is the definition of a Wrapper?

A. An encryption tool to protect the Trojan.
B. A tool used to bind the Trojan with legitimate file.
C. A tool used to encapsulated packets within a new header and footer.
D. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan.

Answer: B

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

NEW QUESTION 357
- (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 361
- (Topic 6)
You have hidden a Trojan file virus.exe inside another file readme.txt using NTFS streaming.
Which command would you execute to extract the Trojan to a standalone file?

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

Answer: C

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

NEW QUESTION 365
- (Topic 6)
A file integrity program such as Tripwire protects against Trojan horse attacks by:

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

Answer: D

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

NEW QUESTION 370
- (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 373
- (Topic 6)
After an attacker has successfully compromised a remote computer, what would be one of the last steps that would be taken to ensure that the compromise is not traced back to the source of the problem?

A. Install pactehs
B. Setup a backdoor
C. Cover your tracks
D. Install a zombie for DDOS

Answer: C

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

NEW QUESTION 378
- (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 382
- (Topic 7)
Ethereal works best on .

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

Answer: C

Explanation:

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

NEW QUESTION 383
- (Topic 7)
ARP poisoning is achieved in steps

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

Answer: B

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

NEW QUESTION 385
- (Topic 7)
What port number is used by Kerberos protocol?

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

Answer: B

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

NEW QUESTION 388
- (Topic 7)
Bob is conducting a password assessment for one of his clients. Bob suspects that password policies are not in place and weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weakness and key loggers. What are the means that Bob can use to get password from his client hosts and servers?

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

Answer: A

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

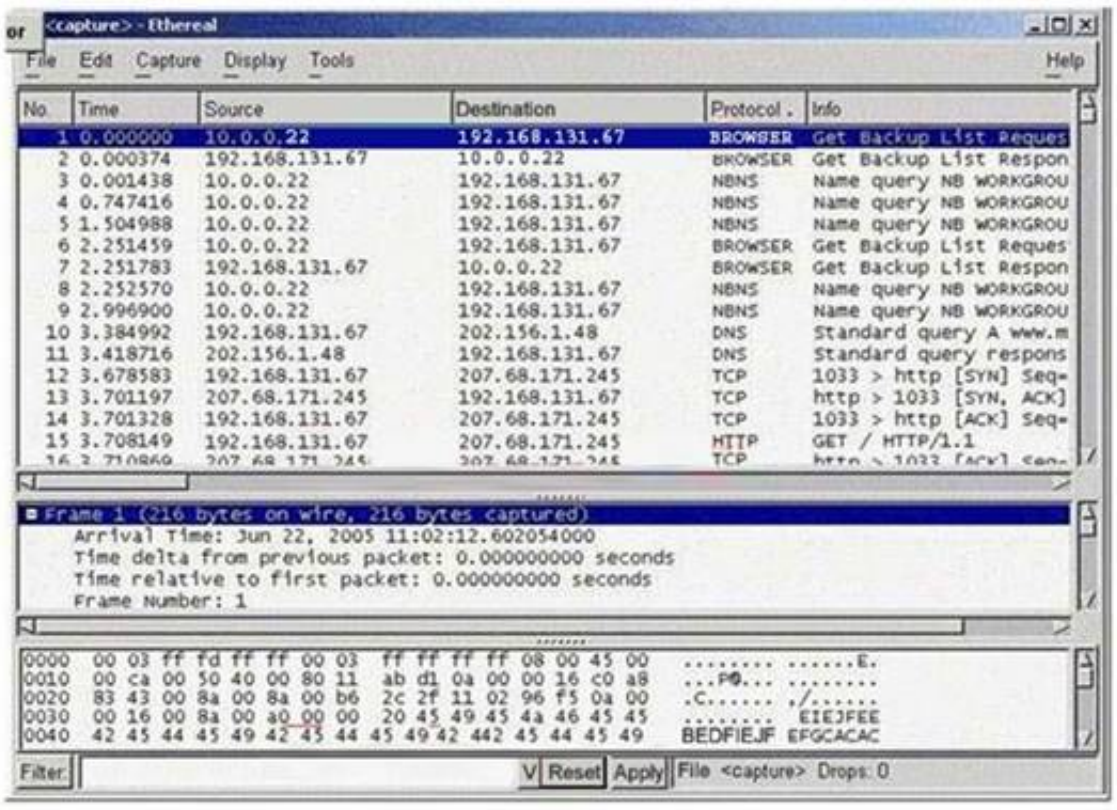
NEW QUESTION 391
- (Topic 7)
What is the command used to create a binary log file using tcpdump?

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 396
- (Topic 7)
Exhibit:



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

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

Answer: B

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

NEW QUESTION 398
- (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 403
- (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 406
- (Topic 7)
What does the following command in "Ettercap" do? ettercap –NCLzs –quiet

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

Answer: C

Explanation:

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

NEW QUESTION 410
- (Topic 7)
How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS's on a network?

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

Answer: A

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

NEW QUESTION 414
- (Topic 7)
Bob wants to prevent attackers from sniffing his passwords on the wired network. Which of the following lists the best options?

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

Answer: D

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

NEW QUESTION 417
- (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 420
- (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 425
- (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 426
- (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 428
- (Topic 8)
What is the goal of a Denial of Service Attack?

A. Capture files from a remote computer.
B. Render a network or computer incapable of providing normal service.
C. Exploit a weakness in the TCP stack.
D. Execute service at PS 1009.

Answer: B

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

NEW QUESTION 431
.....

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