Exam Questions 312-50

Ethical Hacking and Countermeasures (CEHv6)

https://www.2passeasy.com/dumps/312-50/

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

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

Answer: A

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

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

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

Answer: C

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

NEW QUESTION 3
- (Topic 1)
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 4
- (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 5

- (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 6
- (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 7
- (Topic 2)
Which of the following activities would not be considered passive footprinting?

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

Answer: C

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

NEW QUESTION 8
- (Topic 2)
Bill has started to notice some slowness on his network when trying to update his company's website while trying to access the website from the Internet. Bill asks the help desk manager if he has received any calls about slowness from the end users, but the help desk manager says that he has not. Bill receives a number of calls from customers that can't access the company website and can't purchase anything online. Bill logs on to a couple of this routers and notices that the logs shows network traffic is at all time high. He also notices that almost all the traffic is originating from a specific address.
Bill decides to use Geotrace to find out where the suspect IP is originates from. The Geotrace utility runs a traceroute and finds that IP is coming from Panama. Bill knows that none of his customers are in Panama so he immediately thinks that his company is under a Denial of Service attack. Now Bill needs to find out more about the originating IP Address.
What Internet registry should Bill look in to find the IP Address?

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

Answer: A

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

NEW QUESTION 9
- (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 10
- (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 10
- (Topic 2)
NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?
nslookup
> server <ipaddress>
> set type =any
> ls -d <target.com>

A. Enables DNS spoofing
B. Loads bogus entries into the DNS table
C. Verifies zone security
D. Performs a zone transfer
E. Resets the DNS cache

Answer: D

Explanation:
If DNS has not been properly secured, the command sequence displayed above will perform a zone transfer.

NEW QUESTION 11
- (Topic 3)
John has scanned the web server with NMAP. However, he could not gather enough information to help him identify the operating system running on the remote host
accurately.
What would you suggest to John to help identify the OS that is being used on the remote web server?

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

Answer: D

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

NEW QUESTION 16
- (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 17
- (Topic 3)
What port scanning method involves sending spoofed packets to a target system and then looking for adjustments to the IPID on a zombie system?

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

Answer: B

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

NEW QUESTION 22
- (Topic 3)
Which of the following is a patch management utility that scans one or more computers on your network and alerts you if you important Microsoft Security patches are missing. It then provides links that enable those missing patches to be downloaded and installed.

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

Answer: A

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

NEW QUESTION 25
- (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 29
- (Topic 3)
War dialing is a very old attack and depicted in movies that were made years ago. Why would a modem security tester consider using such an old technique?

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

Answer: B

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

NEW QUESTION 32

- (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 34
- (Topic 3)
What is the disadvantage of an automated vulnerability assessment tool?

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

Answer: E

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

NEW QUESTION 38
- (Topic 3)
While reviewing the results of a scan run against a target network you come across the following:

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

What was used to obtain this output?

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

Answer: A

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

NEW QUESTION 41
- (Topic 3)

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

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

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

Answer: A

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

NEW QUESTION 43
- (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 47
- (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 50
- (Topic 3)
What port scanning method is the most reliable but also the most detectable?

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

Answer: B

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

NEW QUESTION 53
- (Topic 3)
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 55
- (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 58
- (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 62
- (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" as or as "loud" as necessary!

NEW QUESTION 67
- (Topic 3)
Which type of scan does not open a full TCP connection?

A. Stealth Scan
B. XMAS Scan
C. Null Scan
D. FIN Scan

Answer: A

Explanation:
Stealth Scan: Instead of completing the full TCP three-way-handshake a full connection is not made. A SYN packet is sent to the system and if a SYN/ACK packet is received it is assumed that the port on the system is active. In that case a RST/ACK will be sent which will determined the listening state the system is in. If a RST/ACK packet is received, it is assumed that the port on the system is not active.

NEW QUESTION 70
- (Topic 3)
Gerald, the systems administrator for Hyped Enterprise, has just discovered that his network has been breached by an outside attacker. After performing routine maintenance on his servers, his discovers numerous remote tools were installed that no one claims to have knowledge of in his department.
Gerald logs onto the management console for his IDS and discovers an unknown IP address that scanned his network constantly for a week and was able to access his network through a high-level port that was not closed. Gerald traces the IP address he found in the IDS log to proxy server in Brazil.
Gerald calls the company that owns the proxy server and after searching through their logs, they trace the source to another proxy server in Switzerland. Gerald calls the company in Switzerland that owns the proxy server and after scanning through the logs again, they trace the source back to a proxy server in China.
What tool Geralds's attacker used to cover their tracks?

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

Answer: A

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

NEW QUESTION 75
- (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 76
- (Topic 3)
Exhibit

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

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

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

Answer: B

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

NEW QUESTION 81
- (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 85
- (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 90
- (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 94
- (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 97
- (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 102
- (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 107
- (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 108
- (Topic 3)
You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different protocols as possible.
Which kind of scan would you use to achieve this? (Choose the best answer)

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

Answer: D

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

NEW QUESTION 109
- (Topic 3)
What does a type 3 code 13 represent?(Choose two.

A. Echo request
B. Destination unreachable
C. Network unreachable
D. Administratively prohibited
E. Port unreachable
F. Time exceeded

Answer: BD

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

NEW QUESTION 110
- (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 112
- (Topic 3)
While reviewing the result of scanning run against a target network you come across the following:

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

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

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

Answer: D

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

NEW QUESTION 114
- (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 117
- (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 122
- (Topic 3)
What flags are set in a X-MAS scan?(Choose all that apply.

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

Answer: CDF

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

NEW QUESTION 124
- (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 129
- (Topic 3)
Because UDP is a connectionless protocol: (Select 2)

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

Answer: DE

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

NEW QUESTION 131
- (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 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 134
- (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 136
- (Topic 3)
You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don't want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

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

Answer: C

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

NEW QUESTION 140
- (Topic 3)
You are scanning the target network for the first time. You are able to detect few convention open ports. While attempting to perform conventional service identification by connecting to the open ports, the scan yields either bad or no result. As you are unsure of the protocols in use, you want to discover as many different protocols as possible. Which of the following scan options can help you achieve this?

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

Answer: D

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

protocol header to each specified protocol on the target machine. If we receive an ICMP protocol unreachable message, then the protocol is not in use. Otherwise we assume it is open. Note that some hosts (AIX, HP-UX, Digital UNIX) and firewalls may not send protocol unreachable messages.

NEW QUESTION 145
- (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 149
- (Topic 3)
What is the proper response for a X-MAS scan if the port is closed?

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

Answer: E

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

NEW QUESTION 150
- (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 153
- (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 155
- (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 157
- (Topic 3)
Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by and IDS?

A. SYN scan
B. ACK scan
C. RST scan
D. Connect scan
E. FIN scan

Answer: D

Explanation:
The TCP full connect (-sT) scan is the most reliable.

NEW QUESTION 159
- (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 161
- (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 162
- (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 167
- (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 170
- (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 172
- (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 177
- (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 182
- (Topic 4)
What did the following commands determine?
C : user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe Domain is EARTH

A. That the Joe account has a SID of 500
B. These commands demonstrate that the guest account has NOT been disabled
C. These commands demonstrate that the guest account has been disabled
D. That the true administrator is Joe
E. Issued alone, these commands prove nothing

Answer: D

Explanation:
One important goal of enumeration is to determine who the true administrator is. In the example above, the true administrator is Joe.

NEW QUESTION 183
- (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 186
- (Topic 4)
Exhibit:

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î>TOÐ.¯pxP.)
Application ~Calculat6e 25 2e 32 31 33 75 25 33 30 31 24 6e 1Ë.Ísize 0.75in 0.25in 0.50in 0.05inxvÝ..
42 42 20 f7 ff bf 21 32 24 6e 25 2e 31 39 32 75 25 33 30 33 .1Ë.y¿!÷y¿"÷y¿#÷y¿XX
58 58 58 58 58 58 58 90 90 90 90 90 90 90 90 90 90 90 90 90 XXXXXXXXXXXXXXXX¼.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u¼300$n¼.213u¼301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu¼302$n¼.192u¼303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.EC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ifÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.Eø.Eü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 43 cd 80 89 d0 43 43 cd 80 89 d0 43 cd 1Í.ÐCÍ..Å1É°?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 41 cd 80 eb 18 41 41 cd 80 eb 18 5e 89 .1É.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c f3 8d 4d 08 8d f3 f3 8d 4d 08 8d 55 0c .1É..U.Í.ëâyyy/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

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

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

Answer: D

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

NEW QUESTION 189
- (Topic 4)
You have the SOA presented below in your Zone. Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA,cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

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

Answer: C

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

NEW QUESTION 194
- (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 199
- (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 204
- (Topic 4)
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK
B. LOGIN, NICK
C. USER, PASS
D. LOGIN, USER

Answer: A

Explanation:
A "PASS" command is not required for either client or server connection to be registered, but it must precede the server message or the latter of the NICK/USER combination. (RFC 1459)

NEW QUESTION 205
- (Topic 4)
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!"
From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!
After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact.
How did the attacker accomplish this hack?

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

Answer: C

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

NEW QUESTION 206
- (Topic 4)
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e- mails from company B. How do you prevent DNS spoofing? (Select the Best Answer.)

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

Answer: C

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

NEW QUESTION 209
- (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 211
- (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 213
- (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 215
- (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 220
- (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 222
- (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 225
- (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 228
- (Topic 4)
What port number is used by LDAP protocol?

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

Answer: B

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

NEW QUESTION 230
- (Topic 4)
Jonathan being a keen administrator has followed all of the best practices he could find on securing his Windows Server. He renamed the Administrator account to a new name that can't be easily guessed but there remain people who attempt to
compromise his newly renamed administrator account. How can a remote attacker decipher the name of the administrator account if it has been renamed?

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

Answer: C

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

NEW QUESTION 235
- (Topic 4)
Which of the following statements about a zone transfer correct?(Choose three.

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

Answer: ACE

Explanation:
Securing DNS servers should be a priority of the organization. Hackers obtaining DNS information can discover a wealth of information about an organization. This information can be used to further exploit the network.

NEW QUESTION 238
- (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 241
- (Topic 5)
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

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

Answer: B

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

NEW QUESTION 242
- (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 247
- (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 251
- (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 254
- (Topic 5)
An attacker runs netcat tool to transfer a secret file between two hosts.
Machine A: netcat -l -p 1234 < secretfile Machine B: netcat 192.168.3.4 > 1234
He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt the information before transmitting onto the wire?

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

Answer: D

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

NEW QUESTION 259
- (Topic 5)
Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

Explanation:
When a cracker knows what OS and Services you use he also knows which exploits might work on your system. If he would have to try all possible exploits for all possible Operating Systems and Services it would take too long time and the possibility of being detected increases.

NEW QUESTION 263
- (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 266
- (Topic 5)
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

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

Answer: B

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

NEW QUESTION 269
- (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 273
- (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 275
- (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 280
- (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 285
- (Topic 5)
LAN Manager passwords are concatenated to 14 bytes and split in half. The two halves are hashed individually. If the password is 7 characters or less, than the second half of the hash is always:

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

Answer: A

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

NEW QUESTION 290
- (Topic 5)
Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

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

Answer: A

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

NEW QUESTION 293
- (Topic 5)
You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption.
What encryption algorithm will you be decrypting?

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

Answer: B

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

NEW QUESTION 296
- (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 297
- (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 301
- (Topic 5)
What is GINA?

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

Answer: D

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

NEW QUESTION 305
- (Topic 5)
____ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

A. Steganography
B. Merge Streams
C. NetBIOS vulnerability
D. Alternate Data Streams

Answer: D

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 306
- (Topic 5)
This kind of password cracking method uses word lists in combination with numbers and special characters:

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

Answer: A

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

NEW QUESTION 309
- (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 310
- (Topic 5)
Study the snort rule given below:

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

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

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

A. WebDav
B. SQL Slammer
C. MS Blaster
D. MyDoom

Answer: C

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

NEW QUESTION 312
- (Topic 5)
You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assesments to protect the company's network. During one of your periodic checks to see how well policy is being observed by the employees, you discover an employee has attached a modem to his telephone line and workstation. He has used this modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

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

Answer: D

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

NEW QUESTION 314
- (Topic 5)
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

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

Answer: D

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

NEW QUESTION 315
- (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 317
- (Topic 5)
What is the algorithm used by LM for Windows2000 SAM ?

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

Answer: B

Explanation:
Okay, this is a tricky question. We say B, DES, but it could be A “MD4” depending on what their asking - Windows 2000/XP keeps users passwords not "apparently", but as hashes, i.e. actually as "check sum" of the passwords. Let's go into the passwords keeping at large. The most interesting structure of the complex SAM-file building is so called V-block. It's size is 32 bytes and it includes hashes of the password for the local entering: NT Hash of 16-byte length, and hash used during the authentication of access to the common resources of other computers LanMan Hash, or simply LM Hash, of the same 16-byte length.
Algorithms of the formation of these hashes are following:
NT Hash formation:
? User password is being generated to the Unicode-line.
? Hash is being generated based on this line using MD4 algorithm.
? Gained hash in being encoded by the DES algorithm, RID (i.e. user identifier) had been used as a key. It was necessary for gaining variant hashes for users who have equal passwords. You remember that all users have different RIDs (RID of the Administrator's built in account is 500, RID of the Guest's built in account is 501, all other users get RIDs equal 1000, 1001,1002, etc.).
LM Hash formation:
? User password is being shifted to capitals and added by nulls up to 14-byte length.
? Gained line is divided on halves 7 bytes each, and each of them is being encoded separately using DES, output is 8-byte hash and total 16-byte hash.
? Then LM Hash is being additionally encoded the same way as it had been done in the NT Hash formation algorithm step 3.

NEW QUESTION 319
- (Topic 6)
What is a Trojan Horse?

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

Answer: B

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

NEW QUESTION 324
- (Topic 6)
Which of the following Netcat commands would be used to perform a UDP scan of the lower 1024 ports?

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

Answer: D

Explanation:
The proper syntax for a UDP scan using Netcat is "Netcat -u -v -w2 <host> 1-1024". Netcat is considered the Swiss-army knife of hacking tools because it is so versatile.

NEW QUESTION 325
- (Topic 6)
Which definition below best describes a covert channel?

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

Answer: A

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

NEW QUESTION 330
- (Topic 6)
In Linux, the three most common commands that hackers usually attempt to Trojan are:

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

Answer: B

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

NEW QUESTION 335
- (Topic 6)
Sniffing is considered an active attack.

A. True
B. False

Answer: B

Explanation:
Sniffing is considered a passive attack.

NEW QUESTION 339
- (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 341
- (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 346
- (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 348
- (Topic 6)
John wants to try a new hacking tool on his Linux System. As the application comes from a site in his untrusted zone, John wants to ensure that the downloaded tool has not been Trojaned. Which of the following options would indicate the best course of action for John?

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

Answer: C

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

NEW QUESTION 349
- (Topic 6)
Exhibit: * Missing*
Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

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

Answer: D

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

NEW QUESTION 350
- (Topic 7)
John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MiTM attack. What is the destination MAC address of a broadcast frame?

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

Answer: A

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

NEW QUESTION 354
- (Topic 7)
Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library. What is the name of this library?

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

Answer: D

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

NEW QUESTION 357
- (Topic 7)
Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security- related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.
Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network

administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.
What technique could Harold use to sniff agency's switched network?

A. ARP spoof the default gateway
B. Conduct MiTM against the switch
C. Launch smurf attack against the switch
D. Flood switch with ICMP packets

Answer: A

Explanation:
ARP spoofing, also known as ARP poisoning, is a technique used to attack an Ethernet network which may allow an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether (known as a denial of service attack). The principle of ARP spoofing is to send fake, or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices, such as network switches. As a result frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or an unreachable host (a denial of service attack).

NEW QUESTION 360
- (Topic 7)
Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data. The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.
Why did capturing of traffic take much less time on the wireless network?

A. Because wireless access points act like hubs on a network
B. Because all traffic is clear text, even when encrypted
C. Because wireless traffic uses only UDP which is easier to sniff
D. Because wireless networks can't enable encryption

Answer: A

Explanation:
You can not have directed radio transfers over a WLAN. Every packet will be broadcasted as far as possible with no concerns about who might hear it.

NEW QUESTION 362
- (Topic 7)
Which of the following is not considered to be a part of active sniffing?

A. MAC Flooding
B. ARP Spoofing
C. SMAC Fueling
D. MAC Duplicating

Answer: C

NEW QUESTION 364
- (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 367
- (Topic 7)
A remote user tries to login to a secure network using Telnet, but accidently types in an invalid user name or password. Which responses would NOT be preferred by an experienced Security Manager? (multiple answer)

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

Answer: AB

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

NEW QUESTION 368
- (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 373
- (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 378
- (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 380
- (Topic 7)
How do you defend against ARP spoofing?

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

Answer: ABC

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

NEW QUESTION 383
- (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 386
- (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 387
- (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 388
- (Topic 7)
Exhibit:
ettercap –NCLzs --quiet
What does the command in the exhibit do in “Ettercap”?

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 from console and log all the collected passwords from the network to a file.
D. This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

Answer: C

Explanation:
-N = NON interactive mode (without ncurses)
-C = collect all users and passwords
-L = if used with -C (collector) it creates a file with all the password sniffed in the session in the form "YYYYMMDD-collected-pass.log"
-z = start in silent mode (no arp storm on start up)
-s = IP BASED sniffing
--quiet = "demonize" ettercap. Useful if you want to log all data in background.

NEW QUESTION 389
- (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 391
- (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 393
- (Topic 8)
Bryce the bad boy is purposely sending fragmented ICMP packets to a remote target. The tool size of this ICMP packet once reconstructed is over 65,536 bytes. From the information given, what type of attack is Bryce attempting to perform?

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

Answer: D

Explanation:
A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65,536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.

NEW QUESTION 395
- (Topic 8)
When working with Windows systems, what is the RID of the true administrator account?

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

Answer: A

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

NEW QUESTION 400
- (Topic 8)
Global deployment of RFC 2827 would help mitigate what classification of attack?

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

Answer: C

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

NEW QUESTION 404
- (Topic 8)
Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. Smurf
C. Ping of Death

D. SYN flood
E. SNMP Attack

Answer: A

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

NEW QUESTION 408
- (Topic 8)
Steven, a security analyst for XYZ associates, is analyzing packets captured by Ethereal on a Linux Server inside his network when the server starts to slow down tremendously. Steven examines the following Ethereal captures:

File Edit Capture Display Tools

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

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

Answer: A

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

NEW QUESTION 411
- (Topic 8)
A denial of Service (DoS) attack works on the following principle:

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

Answer: D

Explanation:
Denial-of-service (often abbreviated as DoS) is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an Internet service, such as a web site. This can be done by exercising a software bug that causes the software running the service to fail (such as the “Ping of Death” attack against Windows NT systems), sending enough data to consume all available network bandwidth (as in the May, 2001 attacks against Gibson Research), or sending data in such a way as to consume a particular resource needed by the service.

NEW QUESTION 416
- (Topic 8)
A Buffer Overflow attack involves:

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

Answer: D

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

insert your own code.

NEW QUESTION 417
- (Topic 8)
You have been called to investigate a sudden increase in network traffic at company. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do you think was the most likely cause behind this sudden increase in traffic?

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

Answer: A

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

NEW QUESTION 418
- (Topic 8)
Smurf is a simple attack based on IP spoofing and broadcasts. A single packet (such as an ICMP Echo Request) is sent as a directed broadcast to a subnet on the Internet. All the machines on that subnet respond to this broadcast. By spoofing the source IP Address of the packet, all the responses will get sent to the spoofed IP Address. Thus, a hacker can often flood a victim with hundreds of responses for every request the hacker sends out.
Who are the primary victims of these attacks on the Internet today?

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

Answer: A

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

NEW QUESTION 422
- (Topic 8)
SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections.
The signature for SYN Flood attack is:

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

Answer: C

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

NEW QUESTION 427
- (Topic 8)
How does a denial-of-service attack work?

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

Answer: C

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

NEW QUESTION 432
- (Topic 8)
What do you call a system where users need to remember only one username and password, and be authenticated for multiple services?

A. Simple Sign-on

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

Answer: C

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

NEW QUESTION 435
- (Topic 9)
What does the following command achieve?
Telnet <IP Address> <Port 80> HEAD /HTTP/1.0
<Return>
<Return>

A. This command returns the home page for the IP address specified
B. This command opens a backdoor Telnet session to the IP address specified
C. This command returns the banner of the website specified by IP address
D. This command allows a hacker to determine the sites security
E. This command is bogus and will accomplish nothing

Answer: C

Explanation:
This command is used for banner grabbing. Banner grabbing helps identify the service and version of web server running.

NEW QUESTION 438
- (Topic 9)
Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. issue special cards to access secured doors at the company and provide a one-time only brief description of use of the special card
B. to post a sign that states “no tailgating” next to the special card reader adjacent to the secured door
C. setup a mock video camera next to the special card reader adjacent to the secured door
D. to educate all of the employees of the company on best security practices on a recurring basis

Answer: D

Explanation:
Tailgating will not work in small company’s where everyone knows everyone, and neither will it work in very large companies where everyone is required to swipe a card to pass, but it’s a very simple and effective social engineering attack against mid-sized companies where it’s common for one employee not to know everyone. There is two ways of stop this attack either by buying expensive perimeter defense in form of gates that only let on employee pass at every swipe of a card or by educating every employee on a recurring basis.

NEW QUESTION 441
- (Topic 9)
Which of these are phases of a reverse social engineering attack? Select the best answers.

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

Answer: ABD

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

NEW QUESTION 443
- (Topic 9)
Usernames, passwords, e-mail addresses, and the location of CGI scripts may be obtained from which of the following information sources?

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

Answer: A

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

Internet if you have the time needed.

NEW QUESTION 445

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-50 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-50 Product From:

https://www.2passeasy.com/dumps/312-50/

Money Back Guarantee

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