Free Questions for CPEH-001 by go4braindumps

Shared by West on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How many bits encryption does SHA-1 use?

Options:

A- 64 bits

B- 128 bits

C- 160 bits

D- 256 bits

Answer:

C

Explanation:

SHA-1 (as well as SHA-0) produces a 160-bit digest from a message with a maximum length of 264 - 1 bits, and is based on principles similar to those used by Professor Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms.

Question 2

Question Type: **MultipleChoice**

A program that defends against a port scanner will attempt to:

Options:

A- Sends back bogus data to the port scanner

B- Log a violation and recommend use of security-auditing tools

C- Limit access by the scanning system to publicly available ports only

D- Update a firewall rule in real time to prevent the port scan from being completed

Answer:

D

Question 3

Question Type: **MultipleChoice**

John has a proxy server on his network which caches and filters web access. He shuts down all unnecessary ports and services. Additionally, he has installed a firewall (Cisco PIX) that will not allow users to connect to any outbound ports. Jack, a network user has successfully connected to a remote server on port 80 using netcat. He could in turn drop a shell from the remote machine. Assuming an attacker wants to penetrate John's network, which of the following options is he likely to choose?

Options:

A- Use ClosedVPN

B- Use Monkey shell

C- Use reverse shell using FTP protocol

D- Use HTTPTunnel or Stunnel on port 80 and 443

Answer:

D

Explanation:

As long as you allow http or https traffic attacks can be tunneled over those protocols with Stunnel or HTTPTunnel.

Question 4

Question Type: **MultipleChoice**

Basically, there are two approaches to network intrusion detection: signature detection, and anomaly detection. The signature detection approach utilizes well-known signatures for network traffic to identify potentially malicious traffic. The anomaly detection approach utilizes a previous history of network traffic to search for patterns that are abnormal, which would indicate an intrusion. How can an attacker disguise his buffer overflow attack signature such that there is a greater probability of his attack going undetected by the IDS?

Options:

A- He can use a shellcode that will perform a reverse telnet back to his machine

B- He can use a dynamic return address to overwrite the correct value in the target machine computer memory

C- He can chain NOOP instructions into a NOOP 'sled' that advances the processor's instruction pointer to a random place of choice

D- He can use polymorphic shell code-with a tool such as ADMmutate - to change the signature of his exploit as seen by a network IDS

Answer:

D

Explanation:

ADMmutate is using a polymorphic technique designed to circumvent certain forms of signature based intrusion detection. All network based remote buffer overflow exploits have similarities in how they function. ADMmutate has the ability to emulate the protocol of the service the attacker is attempting to exploit. The data payload (sometimes referred to as an egg) contains the instructions the attacker wants to execute on the target machine. These eggs are generally interchangeable and can be utilized in many different buffer overflow exploits. ADMmutate uses several techniques to randomize the contents of the egg in any given buffer overflow exploit. This randomization effectively changes the content or 'signature' of the exploit without changing the functionality of the exploit.

Question 5

Question Type: MultipleChoice

Eric notices repeated probes to port 1080. He learns that the protocol being used is designed to allow a host outside of a firewall to connect transparently and securely through the firewall. He wonders if his firewall has been breached. What would be your inference?

Options:

A- Eric network has been penetrated by a firewall breach

B- The attacker is using the ICMP protocol to have a covert channel

C- Eric has a Wingate package providing FTP redirection on his network

D- Somebody is using SOCKS on the network to communicate through the firewall

Answer:

D

Explanation:

Port Description:

SOCKS. SOCKS port, used to support outbound tcp services (FTP, HTTP, etc). Vulnerable similar to FTP Bounce, in that attacker can connect to this port and \bounce\ out to another internal host. Done to either reach a protected internal host or mask true source of attack. Listen for connection attempts to this port -- good sign of port scans, SOCKS-probes, or bounce attacks. Also a means to access restricted resources. Example: Bouncing off a MILNET gateway SOCKS port allows attacker to access web sites, etc. that were restricted only to.mil domain hosts.

Question 6

Question Type: MultipleChoice

Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-todate content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

Options:

A- They are using UDP that is always authorized at the firewall

B- They are using an older version of Internet Explorer that allow them to bypass the proxy server

C- They have been able to compromise the firewall, modify the rules, and give themselves proper access

D- They are using tunneling software that allows them to communicate with protocols in a way it was not intended

Answer:

D

Explanation:

This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

Question 7

Question Type: MultipleChoice

Most NIDS systems operate in layer 2 of the OSI model. These systems feed raw traffic into a detection engine and rely on the pattern matching and/or statistical analysis to determine what is malicious. Packets are not processed by the host's TCP/IP stack allowing the NIDS to analyze traffic the host would otherwise discard. Which of the following tools allows an attacker to intentionally craft packets to confuse pattern-matching NIDS systems, while still being correctly assembled by the host TCP/IP stack to render the attack payload?

Options:

A- Defrag

B- Tcpfrag

C- Tcpdump

D- Fragroute

Answer:

D

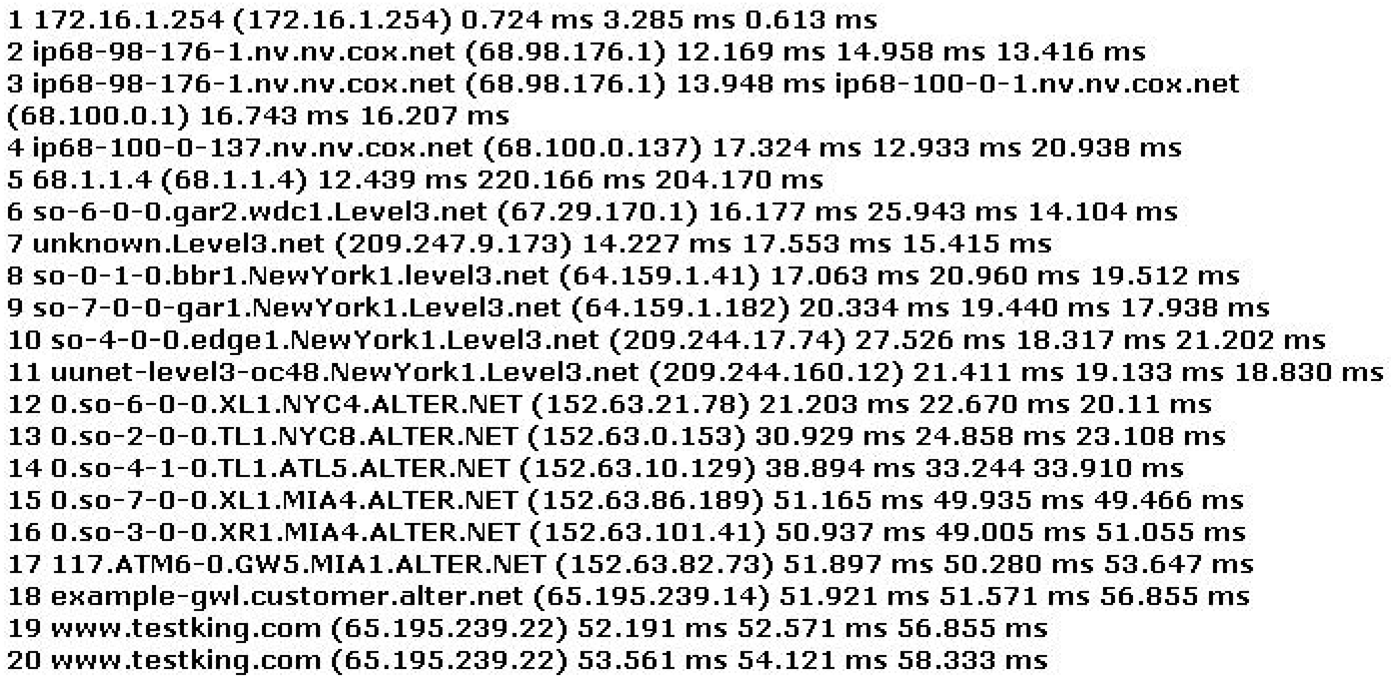
Explanation:

fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks 'Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection' paper of January 1998. It features a simple ruleset language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behaviour. This tool was written in good faith to aid in the testing of network intrusion detection systems, firewalls, and basic TCP/IP stack behaviour.

Question 8

Question Type: MultipleChoice

You have performed the traceroute below and notice that hops 19 and 20 both show the same IP address. What can be inferred from this output?



```
1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms
2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms 13.416 ms
3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv.cox.net
(68.100.0.1) 16.743 ms 16.207 ms
4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 12.933 ms 20.938 ms
5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms
7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms
8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms
9 so-7-0-0-gar1.NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms
10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms
11 uunet-level3-oc48.NewYork1.Level3.net (209.244.160.12) 21.411 ms 19.133 ms 18.830 ms
12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78) 21.203 ms 22.670 ms 20.11 ms
13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms 23.108 ms
14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 38.894 ms 33.244 33.910 ms
15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms 49.466 ms
16 0.so-3-0-0.XR1.MIA4.ALTER.NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms
17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms
18 example-gwl.customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms
19 www.testking.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms
20 www.testking.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms
```

Options:

A- An application proxy firewall

B- A stateful inspection firewall

C- A host based IDS

D- A Honeypot

Answer:

B

Question 9

Question Type: **MultipleChoice**

What is the tool Firewalk used for?

Options:

A- To test the IDS for proper operation

B- To test a firewall for proper operation

C- To determine what rules are in place for a firewall

D- To test the webserver configuration

E- Firewalk is a firewall auto configuration tool

Answer:

C

Explanation:

Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device 'firewall' will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets and no response will be returned.