Vendor:EC-COUNCIL

Exam Code:312-50

Exam Name: Ethical Hacker Certified

Version: Demo

QUESTION 1

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

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites

B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system

C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number

D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Correct Answer: B

QUESTION 2

Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service

B. It creates a buffer overflow

C. It replaces legitimate programs

D. It provides an undocumented opening in a program

Correct Answer: C

Actually the objective of the rootkit is more to hide the fact that a system has been compromised and the normal way to do this is by exchanging, for example, ls to a version that doesn\\'t show the files and process implanted by the attacker.

QUESTION 3

Ethereal works best on _____.

A. Switched networks

B. Linux platforms

C. Networks using hubs

D. Windows platforms

E. LAN\\'s

Correct Answer: C

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

QUESTION 4

You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discover the internal structure of publicly accessible areas of the network. How can you achieve this?

A. Block ICMP at the firewall.

B. Block UDP at the firewall.

C. Both A and B.

D. There is no way to completely block doing a trace route into this area.

Correct Answer: D

When you run a traceroute to a target network address, you send a UDP packet with one time to live (TTL) to the target address. The first router this packet hits decreases the TTL to 0 and rejects the packet. Now the TTL for the packet is expired. The router sends back an ICMP message type 11 (Exceeded) code 0 (TTL-- Exceeded) packet to your system with a source address. Your system displays the round-trip time for that first hop and sends out the next UDP packet with a TTL of 2.This process continues until you receive an ICMP message type 3 (Unreachable) code 3 (Port--Unreachable) from the destination system. Traceroute is completed when your machine receives a Port-Unreachable message.If you receive a message with three asterisks [* * *] during the traceroute, a router in the path doesn\\'t return ICMP messages. Traceroute will continue to send UDP packets until the destination is reached or the maximum number of hops is exceeded.

QUESTION 5

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.

Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers.

A. Hardware, Software, and Sniffing.

B. Hardware and Software Keyloggers.

C. Passwords are always best obtained using Hardware key loggers.

D. Software only, they are the most effective.

Correct Answer: A

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

QUESTION 6

The following excerpt is taken from a honeyput log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful. Study the log given below and answer the following question:

(Note: The objective of this questions is to test whether the student has learnt about passive OS fingerprinting (which should tell them the OS from log captures):

can they tell a SQL injection attack signature; can they infer if a user ID has been created by an attacker and whether they can read plain source destination entries from log entries.)

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 ->
172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 63.226.81.13:1351 -> 172.16.1.107:11
Apr 25 10:17:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 ->
172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM pwdb[12509]: (login) session opened for user simple by
(uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by
simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->
213.28.22.189:4558
```

What can you infer from the above log?

A. The system is a windows system which is being scanned unsuccessfully.

B. The system is a web application server compromised through SQL injection.

C. The system has been compromised and backdoored by the attacker.

D. The actual IP of the successful attacker is 24.9.255.53.

Correct Answer: A

QUESTION 7

802.11b is considered a _____ protocol.

A. Connectionless

B. Secure

C. Unsecure

D. Token ring based

E. Unreliable

Correct Answer: C

802.11b is an insecure protocol. It has many weaknesses that can be used by a hacker.

QUESTION 8

Theresa is an IT security analyst working for the United Kingdom Internet Crimes Bureau in London. Theresa has been assigned to the software piracy division which focuses on taking down individual and organized groups that distribute copyrighted software illegally. Theresa and her division have been responsible for taking down over 2,000 FTP sites hosting copyrighted software. Theresa\\'s supervisor now wants her to focus on finding and taking down websites that host illegal pirated software. What are these sights called that Theresa has been tasked with taking down?

A. These sites that host illegal copyrighted software are called Warez sites

B. These sites that Theresa has been tasked to take down are called uTorrent sites

C. These websites are referred to as Dark Web sites

D. Websites that host illegal pirated versions of software are called Back Door sites

Correct Answer: A

The Warez scene, often referred to as The Scene (often capitalized) is a term of self-reference used by a community that specializes in the underground distribution of pirated content, typically software but increasingly including movies and music.

QUESTION 9

Which Steganography technique uses Whitespace to hide secret messages?

A. snow

B. beetle

C. magnet

D. cat

Correct Answer: A

QUESTION 10

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

Correct Answer: A

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.

QUESTION 11

Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

A. Configure Port Security on the switch

B. Configure Port Recon on the switch

C. Configure Switch Mapping

D. Configure Multiple Recognition on the switch

Correct Answer: A

QUESTION 12

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

Correct Answer: A

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.