IT-Pruefungen.de

Hochwertige Qualität, neueste Prüfungsunterlagen

Exam : 312-50

Title ： Ethical Hacker Certified

Version : Demo

1. 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 How would it be possible for you to retrieve information from the website that is outdated?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

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

A. 18 U.S.C 1029 Possession of Access Devices

B. 18 U.S.C 1030 Fraud and related activity in connection with computers

C. 18 U.S.C 1343 Fraud by wire, radio or television

D. 18 U.S.C 1361 Injury to Government Property

E. 18 U.S.C 1362 Government communication systems

F. 18 U.S.C 1831 Economic Espionage Act

G. 18 U.S.C 1832 Trade Secrets Act

Answer: B

3. You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but not it is not there.

How would it be possible for you to retrieve information from the website that is outdated?
A. Visit google's search engine and view the cached copy.
B. Visit Archive.org web site to retrieve the Internet archive of the company's website.
C. Crawl the entire website and store them into your computer.
D. Visit the company's partners and customers website for this information.
Answer: B

4. You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but not it is not there. How would it be possible for you to retrieve information from the website that is outdated?
A. Visit google's search engine and view the cached copy.
B. Visit Archive.org web site to retrieve the Internet archive of the company's website.
C. Crawl the entire website and store them into your computer.
D. Visit the company's partners and customers website for this information.
Answer: B

5. 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?
(Note: The student is being tested on concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read

packet signatures from a sniff dumo.)

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

What is odd about this attack? (Choose the most appropriate statement)

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 from port 31337.

C. The attacker wants to avoid creating a sub-carrier connection that is not normally

valid.

D. There packets were created by a tool; they were not created by a standard IP stack.

Answer: B

6. You receive an email with the following message:

Hello Steve,

We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com

and change your password.

http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.ht

m

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

Sincerely,

Technical Support

SuperEmailServices

From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers.

You immediately enter the following at Windows 2000 command prompt:

Ping0xde.0xad.0xbe.0xef

You get a response with a valid IP address.

What is the obstructed IP address in the e-mail URL?

A. 222.173.190.239

B. 233.34.45.64

C. 54.23.56.55

D. 199.223.23.45

Answer: A

7. According to the CEH methodology, what is the next step to be performed after footprinting?

A. Enumeration

B. Scanning

C. System Hacking

D. Social Engineering

E. Expanding Influence

Answer: B

8. 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

9. 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 domains. Both are AD integrated.

B. All external DNS is done by an ISP.

C. Internal AD Integrated DNS servers are using private DNS names that are

A. unregistered.

D. Private IP addresses are used on the internal network and are registered with the

internal AD integrated DNS server.
Answer: A

10. 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: A, B, C, F

11. While performing a ping sweep of a subnet you receive an ICMP reply of Code 3/Type 13 for all the pings sent out.
What is the most likely cause behind this response?
A. The firewall is dropping the packets.
B. An in-line IDS is dropping the packets.
C. A router is blocking ICMP.
D. The host does not respond to ICMP packets.
Answer: C

12. 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

13. 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

14. 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

15. 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

16. 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 beidentified:
21 ftp
23 telnet
80 http
443https

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. Thehost is not properly patched

Answer: D

17. What does an ICMP (Code 13) message normally indicates?

A. It indicates that the destination host is unreachable

B. It indicates to the host that the datagram which triggered the source quench message

will need to be re-sent

C. It indicates that the packet has been administratively dropped in transit

D. It is a request to the host to cut back the rate at which it is sending traffic to the

Internet destination

Answer: C

18. 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: D, E

19. 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

20. Richard is a network Administrator working at a student loan company in lowa.

This company processes over 20,000 students loan a year from colleges all over the state. Most communication between the company, schools and lenders is carried out through email. Because of privacy laws that are in the process of being implemented, Richard wants to get ahead of the game and become compliant before any sort of auditing occurs. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, Richard wants to utilize email encryption agency-wide. The only problem for Richard is that his department only has couple of servers and they are utilized to their full capacity. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt email.

What should Richard use?

A. PGP

B. RSA

C. 3DES

D. OTP

Answer: A