模組三

1.

Your team is hired to test a business named Matt’s Bait ’n’ Tackle Shop (domain name mattsBTshop.com). A team member runs the following command:metagoofil -d mattsBTshop.com -t doc,docx -l 50 -n 20 -f results.html

Which of the following best describes what the team member is attempting to do?

C Extracting metadata info from Microsoft Word documents found in mattsBTshop.com, outputting results in an HTML file

2.

You have a zombie system ready and begin an IDLE scan. As the scan moves along,

you notice that fragment identification numbers gleaned from the zombie machine are incrementing randomly. What does this mean?

A Your IDLE scan results will not be useful to you.

3.

You want to perform a ping sweep of a subnet within your target organization. Which of the following nmap command lines is your best option?

C nmap -sP 192.168.1.0/24

4.

A pen tester is performing banner grabbing and executes the following command:

$ nmap -sV host.domain.com -p 80

He gets the following output:

Starting Nmap 6.47 ( http://nmap.org ) at 2022-07-08 19:10 EST

Nmap scan report for host.domain.com (108.61.158.211)

Host is up (0.032s latency).

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd

Service detection performed. Please report any incorrect results at

http://nmap.org/submit/.

VCEConvert.com

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

Which of the following is a true statement?

B The pen tester was successful in banner grabbing.

5.

A colleague enters the following command:

root@mybox: # hping3 -A 192.168.2.x -p 80

What is being attempted here?

B An ACK scan using hping3 on port 80 for a group of addresses

6.

. You are examining traffic between hosts and note the following exchange:

Source Prot Port Flag Destination

192.168.5.12 TCP 4082 FIN/URG/PSH 192.168.5.50

192.168.5.12 TCP 4083 FIN/URG/PSH 192.168.5.50

192.168.5.12 TCP 4084 FIN/URG/PSH 192.168.5.50

192.168.5.50 TCP 4083 RST/ACK 192.168.5.12

192.168.5.12 TCP 4085 FIN/URG/PSH 192.168.5.50

Which of the following statements are true regarding this traffic? (Choose all that apply.) (多選題兩個答案)

B B. It appears to be part of an XMAS scan.

D It appears port 4083 is closed.

7.

You are examining traffic and notice an ICMP Type 3, Code 13 response. What does this

normally indicate?

D A firewall is prohibiting connection.

8.

Which port-scanning method presents the most risk of discovery but provides the most

reliable results?

A Full-connect

9.

As a pen test on a major international business moves along, a colleague discovers an IIS

server and a mail exchange server on a DMZ subnet. You review a ping sweep accomplished

earlier in the day on that subnet and note neither machine responded to the ping. What

is the most likely reason for the lack of response?

B ICMP is being filtered.

10.

Which of the following commands is the best choice to use on a Linux machine when

attempting to list processes and the UIDs associated with them in a reliable manner?

D lsof

11.

An administrator enters the following command on a Linux system:

iptables -t nat -L

Which of the following best describes the intent of the command entered?

B The administrator is configuring IP masquerading.

12.

The following results are from an nmap scan:

Starting nmap V. 3.10A ( www.insecure.org/nmap/

<http://www.insecure.org/nmap/> )

Interesting ports on 192.168.15.12:

(The 1592 ports scanned but not shown below are in state: filtered)

Port State Service

21/tcp open ftp

25/tcp open smtp

53/tcp closed domain

80/tcp open http

443/tcp open https

Remote operating system guess: Too many signatures match to

reliably guess the OS.

Nmap run completed -- 1 IP address (1 host up) scanned in 263.47 seconds

Which of the following is the best option to assist in identifying the operating system?

D Attempt banner grabbing.

13.

You want to run a scan against a target network. You’re concerned about it being a reliable

scan, with legitimate results, but want to take steps to ensure it is as stealthy as possible.

Which scan type is best in this situation?

C nmap -sS targetIPaddress

14.

What is the second step in the TCP three-way handshake?

C SYN/ACK

15.

Nmap is a powerful scanning and enumeration tool. What does the following nmap

command attempt to accomplish?

nmap -sA -T4 192.168.15.0/24

D A parallel, fast ACK scan of a Class C subnet

16.

You are examining a packet capture of all traffic from a host on the subnet. The host sends a segment with the SYN flag set in order to set up a TCP communications channel. The destination port is 80, and the sequence number is set to 10. Which of the following statements are not true regarding this communications channel? (Choose all that apply.) (多選題兩個答案)

A The host will be attempting to retrieve an HTML file.

D The packet returned in answer to this SYN request will acknowledge the sequence number by returning 10.

17.

Which TCP flag instructs the recipient to ignore buffering constraints and immediately send all data?

B PSH

18.

You receive a RST-ACK from a port during a SYN scan. What is the state of the port?

B Closed

19.

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

invictus@victim\_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!

What seems to be wrong?

D OS Scan requires root privileges.

20.

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

TCP port 21 no response

TCP port 22 no response

TCP port 23 Time-to-live exceeded

C The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall

21.

An attacker scans a host with the below command. Which three flags are set? # nmap -sX host.domain.com

B This is Xmas scan. URG, PUSH and FIN are set.

22.

While scanning with Nmap, Patin found several hosts that have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p- -si kiosk.adobe.com www.riaa.com. kiosk.adobe.com is the host with an incremental IP ID sequence. What is the purpose of using "-si" with Nmap?

C Conduct IDLE scan

23.

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A Protocol analyzer

24.

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

A The switches will drop into hub mode if the ARP cache is successfully flooded.

25.

Which of the following provides a security professional with the most information about the system's security posture?

D Port scanning, banner grabbing service identification

26.

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lowercase letters, capital letters, numbers, and special characters. With your existing knowledge of users, likely user account names, and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password-cracking attack you can run against these hash values and still get results?

D Hybrid Attack

27.

2 Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user. What is the enumeration technique used by Henry on the organization?

B DNS cache snooping

28.

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

B The attacker makes a request to the DNS resolver.

29.

An attacker runs a netcat tool to transfer a secret file between two hosts. He is worried about information being sniffed on the network. How would the attacker use Netcat to encrypt the information before transmitting it onto the wire?

D Use cryptcat instead of netcat

30.

某管理員監控網路上的 IP 封包時，發現封包標頭包含了一個協定欄位 （Protocol Number），而此欄位的值為 1，請問此封包是屬於何種協定 的封包？

C ICMP

31.

有關位址解析協定（Address Resolution Protocol, ARP）功能之敘述，下列何者正確？ (A) (B) (C) (D)

A 以 IP 位址查詢其相對應之媒體存取控制（MAC）位址

32.

中間人攻擊 （ Man-in-the-Middle Attack ， 又稱為 MITM Attack）是一種用來竊聽、竄改流量的攻擊行為。以下列舉 了幾種用來防範中間人攻擊的防禦機制，請問哪一種防範機制已經被驗證有明顯的弱點並且已被建議棄用？

B 在 HTTPS 或 SMTPS 使用 SSLv2 協定來保護傳輸資 料，避免被看到明文內容

33.

關於電子郵件安全威脅的敘述，下列何者錯誤？

D 電子郵件的安全以詐騙為主，未曾發現針對技術性 弱點的攻擊