CHAPTER 6

1. SNMP stands for\_\_\_\_\_

A. Simple Network Messaging Protocol

B. Simple Network Mailing Protocol

C. Simple Network Management Protocol

D. Simple Network Master Protocol

Ans: C

2. Which of the following tool is used for Network Testing and port Scanning\_\_\_\_\_\_

A. NetCat

B. SuperScan

C. NetScan

D. All of above

Ans: D

3. Banner grabbing is used for A. White Hat Hacking

B. Black Hat Hacking

C. Grey Hat Hacking

D. Script Kiddies

Ans: A

4. An attacker can create an\_\_\_\_\_\_\_\_attack by sending hundreds or thousands of e-mails a with

very large attachments.

A. Connection Attack

B. Auto responder Attack

C. Attachment Overloading Attack

D. All the above

Ans: B

5. Which of the following tool is used for Windows for network queries from DNS lookups to

trace routes?

A. Sam Spade

B. SuperScan

C. NetScan

D. Netcat

Ans: A

6. Which tool is used for ping sweeps and port scanning?

A. Netcat

B. SamSpade

C. SuperScan

D. All the above

Ans: C

7. Which of the following tool is used for security checks as port scanning and firewall testing?

A. Netcat

B. Nmap

C. Data communication

D. Netscan

Ans: A

8. What is the most important activity in system cracking? A. Information gathering

B. Cracking password

C. Escalating privileges

D. Covering tracks

Ans: B

9. Which Nmap scan is does not completely open a TCP connection?

A. SYN stealth scan

B. TCP scan

C. XMAS tree scan

D. ACK scan

Ans: A

10.Key loggers are form of

A. Spyware

B. Shoulder surfing

C. Trojan

D. Social engineering

Ans: A

11. Nmap is abbreviated as Network Mapper.

A. True

B. False

Ans: A

12. \_\_\_\_\_\_\_\_\_is a popular tool used for discovering network as well as security auditing.

A. Ettercap

B. Metasploit

C. Nmap

D. Burp Suit

Ans: C

13. Which of this Nmap do not check?

A. Services different hosts are offering

B. On what OS they are running.

C. What kind of firewall in use?

D. What type of antivirus in use?

Ans: D

14. What is purpose of Denial of Service attacks?

A. Exploit weakness in TCP/IP attack.

B. Toexecute a trojan horse on a system.

C. To overload a system so it is no longer operational.

D. To shutdown services by turning them off.

Ans: C

15. What are the some of the most common vulnerabilities that exist in a network system?

A.Changing manufacturer, or recommended settings of newly installed application.

B. Additional unused feature on commercial software package.

C. Utilizing open source application code.

D. Balancing security and ease of use of system.

Ans: B

16. Which of the following is not a characteristic of ethical hacker? A. Excellent knowledge of

Windows.

B. Understands the process of exploiting network vulnerabilities.

C. Patience, persistence and perseverance.

D. Has the highest level of security for the organization.

Ans: D

17. Attempting to gain access to a network using an employee’s credentials is called the

\_\_\_\_\_\_\_\_\_\_\_\_\_ mode of ethical hacking.

A. Local networking

B. Social engineering

C. Physical entry

D. Remote networking

Ans: A

18. The first phase of hacking an IT system is compromise of which foundation of security?

A. Availability

B. Confidentiality

C. Integrity

D. Authentication

Ans: B

19. Why would a ping sweep be used?

A. To identify live systems

B. To locate live systems

C. To identify open ports

D. To locate firewalls

Ans: A

20. What are the port states determined by Nmap?

A. Active, inactive, standby

B. Open, half-open, closed

C. Open, filtered, unfiltered

D. Active, closed, unused

Ans: C

21. What port does Telnet use?

A. 22

B. 80

C. 20

D. 23

Ans: D

22. Which of the following will allow foot printing to be conducted without detection?

A. PingSweep

B. Traceroute

C. War Dialers

D. ARIN

Ans: D

23. Performing hacking activities with the intent on gaining visibility for an unfair situation is

called \_\_\_\_\_\_\_\_.

A. Cracking

B. Analysis

C. Hacktivism

D. Exploitation

Ans: C

24. Why would a hacker use a proxy server?

A. To create a stronger connection with the target.

B. To create a ghost server on the network.

C. To obtain a remote access connection

D. To hide malicious activity on the network

Ans: A

25. Which phase of hacking performs actual attack on a network or system?

A. Reconnaissance

B. Maintaining Access

C. Scanning

D. Gaining Access

Ans: D

26. Sniffing is used to perform \_\_\_\_\_\_\_\_\_\_\_\_\_\_ fingerprinting.

A. Passive stack

B. Active stack

C. Passive banner grabbing

D. Scanned

Ans: A

27. Services running on a system are determined by \_\_\_\_\_\_\_\_\_\_\_\_\_.

A. The system’s IP address

B. The Active Directory

C. The system’s network name

D. The port assigned

Ans: D

28. What are the types of scanning?

A. Port, network, and services

B. Network, vulnerability, and port

C. Passive, active, and interactive

D. Server, client, and network

Ans: B

29. Enumeration is part of what phase of ethical hacking?

A. Reconnaissance

B. Maintaining Access

C. Gaining Access

D. Scanning

Ans: C

30. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ framework made cracking of vulnerabilities easy like point and click.

A. Net

B. Metasploit

C. Zeus

D. Ettercap

Ans: B

31.\_\_\_\_\_\_\_\_\_\_ is a popular IP address and port scanner.

A. Cain and Abel

B. Snort

C. Angry IP Scanner

D. Ettercap

Ans: C

32.\_\_\_\_\_\_\_\_ is a popular tool used for network analysis in multiprotocol diverse network

A. Snort

B. SuperScan

C. Burp Suit

D. EtterPeak

Ans: D

33\_\_\_\_\_\_\_\_\_\_\_ scans TCP ports and resolves different hostnames.

A. SuperScan

B. Snort

C. Ettercap

D. QualysGuard .

Ans: A

34. What tool can be used to perform SNMP enumeration?

A. DNSlookup

B. Whois

C. Nslookup

D. IP Network Browser

Ans: D

35. Wireshark is a \_\_\_\_\_\_\_\_\_\_\_\_ tool.

A. network protocol analysis

B. network connection security

C. connection analysis

D. defending malicious packet-filtering

Ans: A

36. Aircrack-ng is used for \_\_\_\_\_\_\_\_\_\_\_\_

A. Firewall bypassing

B. Wi-Fi attacks

C. Packet filtering

D. System password cracking

Ans: B

37. Phishing is a form of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

A. Spamming

B. Identify Theft

C. Impersonation

D. Scanning

Ans: C

38. What are the types of scanning?

A. Port, network, and services

B. Network, vulnerability, and port

C. Passive, active, and interactive

D. Server, client, and network

Ans: B

39 \_\_\_\_\_ is used for searching of multiple hosts in order to target just one specific open port.

A. Ping Sweep

B. Port scan

C. Ipconfig

D. Spamming

Ans: A

40. ARP spoofing is often referred to as\_\_\_\_\_

A. Man-in-the-Middle attack

B. Denial-of-Service attack

C. Sniffing

D. Spoofing

Ans: A

41. \_\_\_\_\_\_is a tool that allows you to look into network and analyze data going across the wire

for network optimization, security and troubleshooting purposes.

A. Network analyzer

B. Crypt tool

C. John-the -Ripper

D. Back track

Ans: A

42. \_\_\_\_\_\_\_\_\_ is not a function of network analyzer tool.

A. Captures all network traffic

B. Interprets or decodes what is found into a human-readable format.

C. Displays it all in chronological order.

D. Banner grabbing

Ans: D

44. What is the attack called “evil twin”?

A. rouge access point

B. ARP poisoning

C. session hijacking

D. MAC spoofing

Ans: A

45.What is the primary goal of an ethical hacker?

A. avoiding detection

B. testing security controls

C. resolving security vulnerabilities

D. determining return on investment for security measures

Ans: C

46. What are the forms of password cracking technique?

A. Attack syllable

B. Attack brute forcing

C. Attacks hybrid

D. All the above

Ans: D

45.Which type of hacker represents the highest risk to your network?

A. black-hat hackers

B. grey-hat hackers

C. script kiddies

D. disgruntled employees

Ans: D

46. Hacking for a cause is called\_\_\_\_\_\_

A. hacktivism

B. black-hat hacking

C. active hacking

D. activism

Ans: A

47. When a hacker attempts to attack a host via the internet it is known as what type of attack?

A.local access

B. remote attack

C. internal attack

D. physical access

Ans: B

49. A type of attack that overloads the resources of a single system to cause it to crash or hang.

A. Resource Starvation

B. Active Sniffing

C. Passive Sniffing

D. Session Hijacking

Ans. C

50.In computer networking, \_\_\_\_ is any technical effort to manipulate the normal behavior of

network connections and connected systems.

A. Hacking

B. Evidence

C. Tracing

D. None of above

Ans:-A