

Course Code: CS627 Cyber Security
Final term File # 1 (Week No. 7-15)
Prepared by DL

1. **What is Nmap primarily used for?**
 - A) Web development
 - B) Network discovery and security auditing**
 - C) Data analysis
 - D) File management

2. **Which of the following is a feature of Nikto?**
 - A) Scans for outdated versions of servers**
 - B) Provides a graphical user interface
 - C) Only scans for open ports
 - D) Is a paid tool

3. **What does the -sV flag in Nmap do?**
 - A) Scans all ports
 - B) Detects the version of services running**
 - C) Performs a fast port scan
 - D) Disables DNS resolution

4. **Which tool is known for its graphical user interface as frontend for Nmap?**
 - A) Zenmap**
 - B) Nessus
 - C) Qualys
 - D) Nikto

5. **What is the primary purpose of Nessus?**
 - A) Network mapping
 - B) Vulnerability scanning**
 - C) Web application testing
 - D) Data encryption

6. **What does CIS stand for?**
 - A) Center for Internet Security**
 - B) Cyber Information Security
 - C) Computer Information Systems
 - D) Centralized Internet Security

7. **How many total CIS benchmarks are there?**
 - A) 50
 - B) 107**
 - C) 75
 - D) 200

8. Which of the following is NOT a category of CIS benchmarks?
- A) Operating Systems
 - B) Server Software
 - C) Mobile Applications**
 - D) Network Devices
9. What is the purpose of CIS benchmarks?
- A) To provide financial guidelines
 - B) To offer configuration recommendations for security**
 - C) To develop software applications
 - D) To manage network traffic
10. What is the primary focus of Level 1 CIS benchmarks?
- A) Advanced security configurations
 - B) Basic configurations to lower attack surface**
 - C) Compliance with legal standards
 - D) Performance optimization
11. What does the term "malware" refer to?
- A) Software designed for data analysis
 - B) Malicious software intended to disrupt or damage systems**
 - C) Software for managing databases
 - D) Operating system software
12. Which of the following is NOT a type of malware?
- A) Virus
 - B) Worm
 - C) Firewall**
 - D) Trojan horse
13. What is ransomware primarily designed to do?
- A) Encrypt files and demand payment for decryption**
 - B) Steal personal information
 - C) Monitor user activity
 - D) Spread to other systems without detection
14. Which of the following describes a computer worm?
- A) Requires a host program to replicate
 - B) Self-replicates and spreads independently**
 - C) Only affects mobile devices
 - D) Is a type of antivirus software
15. What is a common method used by malware to evade detection?
- A) Using strong passwords
 - B) Regular software updates
 - C) Modifying its code to avoid signature detection**
 - D) Encrypting data

16. What is a key factor that increases the security risk of wireless networks?
- A) Channel
 - B) Mobility
 - C) Limited resources
 - D) All of the above**
17. Which standard is used for port-based network access control in wireless networks?
- A) IEEE 802.3
 - B) IEEE 802.11
 - C) IEEE 802.1X**
 - D) IEEE 802.15
18. What does WEP stand for in wireless security?
- A) Wired Equivalent Privacy**
 - B) Wireless Encryption Protocol
 - C) Wireless Equivalent Privacy
 - D) Wired Encryption Protocol
19. Which of the following is a major weakness of WEP?
- A) Strong encryption
 - B) Easily cracked keys**
 - C) High performance
 - D) Compatibility with all devices
20. What is the main purpose of WPA2?
- A) To provide basic network access
 - B) To enhance security over WEP**
 - C) To manage network traffic
 - D) To monitor user activity
21. What was the primary purpose of the Morris worm?
- A) To steal data
 - B) To gauge the size of ARPANET**
 - C) To create a backdoor
 - D) To spread malware
22. Which of the following worms exploited buffer overflow vulnerability in Microsoft SQL Server 2000?
- A) Morris Worm
 - B) Code Red
 - C) SQL Slammer**
 - D) WannaCry
23. What is a buffer overflow?
- A) A type of denial-of-service attack
 - B) A condition where more input is placed into a buffer than its capacity**

- C) A method of data encryption
 - D) A programming language error
24. Which programming language is particularly vulnerable to buffer overflow attacks?
- A) Python
 - B) Java
 - C) C**
 - D) Ruby
25. What is shellcode?
- A) Code that is used to create a buffer overflow
 - B) Code supplied by an attacker to gain control of a system**
 - C) Code that protects against attacks
 - D) Code that is used for data encryption
26. What is the primary focus of digital forensics?
- A) Data encryption
 - B) Recovery and analysis of digital evidence**
 - C) Network security
 - D) Software development
27. What does Locard's Exchange Principle state?
- A) Every contact leaves a trace**
 - B) All evidence is unreliable
 - C) Digital evidence is always encrypted
 - D) Forensic evidence is not admissible in court
28. Which of the following is a type of digital forensic analysis?
- A) Network forensics**
 - B) Physical forensics
 - C) Chemical forensics
 - D) Biological forensics
29. What is the first step in a digital forensic investigation?
- A) Analysis
 - B) Reporting
 - C) Acquisition**
 - D) Testing
30. What is a common challenge in digital forensics?
- A) Lack of evidence
 - B) Encryption of data
 - C) Overabundance of data
 - D) Both B and C**
31. What does HTTPS stand for?
- A) Hypertext Transfer Protocol Secure**

- B) Hypertext Transfer Protocol Standard
- C) Hypertext Transfer Protocol Service
- D) Hypertext Transfer Protocol Security

32. What is the primary purpose of SSL/TLS?

- A) To speed up internet connections
- B) To secure data transmission over the internet**
- C) To create web pages
- D) To manage databases

33. Which of the following is a benefit of using HTTPS?

- A) Increased loading speed
- B) Data communication and confidentiality**
- C) Reduced server costs
- D) Easier website design

34. What is the first step in establishing an HTTPS connection?

- A) Server response
- B) Client request**
- C) Certificate verification
- D) Data exchange

35. What does SSH stand for?

- A) Secure Socket Host
- B) Secure Shell**
- C) Secure Hypertext
- D) Secure Hardware

36. What is the primary goal of operating system security?

- A) To enhance user experience
- B) To ensure secure operation in a networked environment**
- C) To increase system performance
- D) To simplify software installation

37. What is OS hardening?

- A) Making the operating system more user-friendly
- B) Minimizing exposure to threats by configuring the OS securely**
- C) Increasing the number of applications on the system
- D) Enhancing the graphical interface of the OS

38. Which of the following is a security mechanism in operating systems?

- A) User interface design
- B) Access control**
- C) Software installation
- D) Hardware upgrades

39. What should be done to user accounts during OS hardening?
- A) Grant all users administrative privileges
 - B) Remove unnecessary accounts and secure default accounts**
 - C) Allow all users to access all data
 - D) Disable all user accounts
40. What is the purpose of logging in operating system security?
- A) To improve system performance
 - B) To inform about past incidents and breaches**
 - C) To enhance user experience
 - D) To simplify software updates
41. What is cybercrime?
- A) A crime involving physical violence
 - B) A crime involving a computer or computer network**
 - C) A crime related to financial transactions
 - D) A crime that occurs only offline
42. Which of the following is a form of cybercrime?
- A) Identity theft**
 - B) Bank robbery
 - C) Vandalism
 - D) Shoplifting
43. What is the estimated annual damage caused by cybercrime according to a 2014 report?
- A) \$100 billion
 - B) \$445 billion**
 - C) \$1 trillion
 - D) \$50 billion
44. What is the primary concern of cyberterrorism?
- A) Theft of physical goods
 - B) Disruption of computer networks**
 - C) Vandalism of public property
 - D) Fraudulent financial transactions
45. What is a common method used in phishing attacks?
- A) Direct phone calls
 - B) Sending fake emails that appear to be from trusted sources**
 - C) Physical mail
 - D) In-person solicitation

Prepared by DL...

May You All Stay Success in your Whole Life, Ameen! Summ Ameen...
Just Remember us in your Deep Prayers. JazakAllah...