Course Code: CS627 Cyber Security
Finalterm File # 2 (Week No. 7-15)
Prepared by DL

1. Which command would you use to perform a basic Nmap scan against a host?
A) nmap -sV
B) nmap scanme.com
C) nmap -Pn 192.168.1.1
D) nmap -sn 192.168.1.1

2. What does the -A flag in Nmap do?
A) Performs a stealth scan
B) Activates several popular options
C) Scans for open ports only
D) Disables DNS resolution

3. Which of the following is NOT a benefit of using Nmap?
A) Open source
B) Paid software
C) Available on multiple platforms
D) Large community support

4. What type of scan does the -sn flag perform in Nmap?
A) Port scan
B) only Host discovery
C) OS detection
D) Service version detection

5. Which of the following tools is used for comparing results of two Nmap scans?
A) Ncat
B) Ndiff
C) Zenmap
D) Nessus

6. Which organization provides the DISA STIGs?
A) National Institute of Standards and Technology
B) Defense Information Systems Agency
C) Center for Internet Security
D) Federal Trade Commission

7. What is the main goal of implementing CIS benchmarks?
A) To increase software performance
B) To limit configuration-based security vulnerabilities
C) To enhance user experience
D) To reduce operational costs

8. Which of the following is a characteristic of CAT 1 controls in DISA STIGs?
A) Low risk vulnerabilities
B) Mandatory for compliance
C) Optional recommendations
D) Non-critical vulnerabilities

9. What does the acronym STIG stand for?
A) Security Technical Implementation Guide
B) Security Technology Integration Guide
C) System Technical Implementation Guide
D) Security Tool Integration Guide

10. Which of the following is a benefit of using CIS-CAT Pro Assessor?
A) Manual configuration checks
B) Automated evaluation against CIS benchmarks
C) Only available for Windows systems
D) Requires extensive programming knowledge

11. Which of the following is a characteristic of a Trojan horse?
A) It self-replicates
B) It disguises itself as legitimate software
C) It only affects mobile devices
D) It is a type of antivirus

12. What is the primary function of spyware?
A) To encrypt files
B) To monitor user activity and collect information
C) To spread to other computers
D) To manage network traffic

13. Which malware type is known for displaying fake security alerts?
A) Ransomware
B) Adware
C) Scareware
D) Spyware

14. How does a biological virus compare to a computer virus?
A) Both inject genetic material into a living cell
B) **Both replicate themselves once inside the host**
C) Both rely on human interaction to spread
D) Both are harmless and do not perform any tasks

15. What is the primary purpose of a backdoor in malware?
A) To encrypt files
B) To provide unauthorized access to a system

C) To monitor user activity
D) To manage network traffic

16. Which of the following is a feature of WPA3?
A) Uses TKIP for encryption
B) Requires specialized hardware
C) Provides improved security for open networks
D) Is not backward compatible

17. What is the role of the Wi-Fi Alliance?
A) To develop new wireless standards
B) To certify products for Wi-Fi interoperability
C) To manage network traffic
D) To provide technical support

18. What does the term "SSID" stand for?
A) Secure Service Identifier
B) Service Set Identifier
C) Standard Service Identifier
D) Secure Set Identifier

19. Which of the following is a recommended practice for securing wireless networks?
A) Disable SSID broadcast
B) Use default passwords
C) Place access points near windows
D) Allow all MAC addresses

20. What is the primary function of the 802.11i standard?
A) To define physical layer specifications
B) To enhance wireless security mechanisms
C) To manage network traffic
D) To provide basic network access

21. What is one of the primary defenses against buffer overflow attacks?
A) Using older programming languages
B) Implementing executable address space protection
C) Ignoring input validation
D) Using unencrypted data

22. What does SQL Slammer primarily cause?
A) Data theft
B) Denial of service
C) Data encryption
D) Data corruption

23. What is the main consequence of a buffer overflow attack?
A) Increased system performance
B) Corruption of program data

C) Enhanced security
D) Improved user experience

24. What is the purpose of fuzzing in identifying vulnerabilities?
A) To encrypt data
B) To automatically identify potentially vulnerable programs
C) To create backups
D) To improve user interfaces

25. What is the role of programming languages in handling buffer overflow attacks?
A) All programming languages are equally secure
B) High-level languages are not vulnerable to buffer overflows
C) Low-level languages are more secure
D) Programming languages have no impact on security

26. What is the purpose of a write blocker in digital forensics?
A) To enhance data recovery speed
B) To prevent modification of original data
C) To encrypt data during transfer
D) To compress data for storage

27. Which of the following is NOT a type of digital forensic category?
A) Computer forensics
B) Mobile device forensics
C) Network forensics
D) Environmental forensics

28. What is the role of digital evidence in legal cases?
A) To confuse the jury
B) To support or refute a hypothesis
C) To delay the trial process
D) To provide entertainment

29. What is a common tool used in digital forensics?
A) Microsoft Word
B) EnCase
C) Adobe Photoshop
D) Google Chrome

30. What is the significance of maintaining a chain of custody in digital forensics?
A) To ensure data is lost
B) To track the handling of evidence
C) To speed up the investigation
D) To confuse the defense

31. What is a key feature of SSH?
A) It is used for web browsing

B) It provides secure remote access
C) It is a type of malware
D) It is used for email communication

32. What is the main purpose of IPsec?
A) To secure email communications
B) To secure network communications at the IP layer
C) To enhance web page loading speed
D) To manage user accounts

33. What does FTPS stand for?
A) File Transfer Protocol Secure
B) Fast Transfer Protocol Secure
C) File Transmission Protocol Secure
D) File Transfer Process Secure

34. What is a key feature of SHTTPS?
A) It is a faster version of HTTPS
B) It includes additional security measures
C) It is only used for mobile devices
D) It is a deprecated protocol

35. What is the main benefit of using TLS over SSL?
A) TLS is older and more established
B) TLS offers enhanced security features
C) TLS is easier to implement
D) TLS is free to use

36. What is a critical control for maintaining system integrity?
A) Regularly updating software
B) Increasing the number of applications
C) Reducing user access
D) Ignoring system logs

37. What is the role of patch management in operating system security?
A) To install new applications
B) To keep security patches up to date
C) To enhance user interface
D) To increase system speed

38. What is the significance of resource controls in OS security?
A) To allow all users unrestricted access
B) To set appropriate permissions on data and resources
C) To enhance the graphical interface
D) To simplify software installation

39. What is the purpose of security testing in OS hardening?
A) To ensure the system is user-friendly
B) To identify vulnerabilities and ensure security measures are effective
C) To increase the number of applications
D) To improve system performance

40. What is a common method for securing Windows systems?
A) Using outdated software
B) Implementing mandatory integrity controls (MIC)
C) Allowing all users administrative access
D) Ignoring security updates

41. What is the main goal of ransomware?
A) To steal data
B) To encrypt files and demand payment for decryption
C) To destroy data
D) To monitor user activity

42. Which of the following is a characteristic of cyberbullying?
A) It is always anonymous
B) It only occurs in schools
C) It involves physical threats
D) It can occur through various online platforms

43. What is the purpose of the Prevention of Electronic Crimes Act (PECA) in Pakistan?
A) To promote internet usage
B) To regulate online businesses
C) To prevent and combat cybercrime
D) To enhance social media engagement

44. What is a common consequence of identity theft?
A) Increased credit score
B) Financial loss and damage to credit history
C) Legal immunity
D) Enhanced online privacy

45. What is the primary focus of cybercrime legislation?
A) To promote online shopping
B) To protect individuals and organizations from cyber threats
C) To enhance social media platforms
D) To regulate internet service providers

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