Module 2 – Final Quiz: Operating System & Network Security

1 - What is the main goal of operating system security?

A) To improve the speed of the operating system
B) To protect the OS against unauthorized access and vulnerabilities
C) To allow unlimited administrative access
D) To ensure the OS looks visually appealing

2 - Which of the following is an example of a common OS security threat?

A) Outdated patches and missing updates
B) Using a dark mode theme
C) File compression
D) Installing fonts

3 - Why are software patches and updates critical to OS security?

A) They make the OS look more modern
B) They add new hardware drivers
C) They fix security vulnerabilities before attackers exploit them
D) They are optional and not security related

4 - Which method is commonly used to manage who can log into a system?

A) Access Control
B) File Compression
C) Network Caching
D) Data Backup

5 - Which technique improves security by disabling unnecessary services?

A) Application Whitelisting
B) OS Hardening
C) Encryption
D) Antivirus

6 - Why should default accounts be removed or restricted?

A) They are often insecure and exploited by attackers
B) They slow down system performance
C) They are not compatible with modern software
D) They consume too much disk space

7 - What is application whitelisting?

A) Allowing only approved applications to run
B) Blocking all applications by default
C) Encrypting applications during runtime
D) Uninstalling unused applications

8 - Which of the following helps detect unusual or malicious OS activity?

A) Defragmentation
B) Logging and Monitoring
C) Disk Cleanup
D) Virtualization

9 - What is memory corruption?

A) A problem with slow RAM
B) When attackers exploit flaws in how memory is handled
C) A storage error on the hard disk
D) A misconfigured operating system update

10 - What does Data Execution Prevention (DEP) do?

A) Prevents memory from being used to run malicious code
B) Encrypts all system files
C) Deletes corrupted memory
D) Creates new memory partitions

11 - What is the purpose of Address Space Layout Randomization (ASLR)?

A) To hide user accounts from attackers
B) To randomly arrange memory locations, making exploits harder
C) To encrypt network traffic
D) To block unknown IP addresses

12 - Which of these is NOT a common network security threat?

A) Man-in-the-Middle attacks
B) Packet sniffing
C) SQL injection
D) Defragmenting hard drives

13 - What is the purpose of using a VPN?

A) To block ads on websites
B) To create an encrypted tunnel for secure data transfer
C) To reduce internet speed
D) To scan for viruses

14 - Which wireless security standard is currently considered the strongest?

A) WEP
B) WPA
C) WPA2
D) WPA3

15 - Why is public Wi-Fi considered dangerous?

A) It consumes more battery power
B) It often has weak or no encryption, exposing user data
C) It is slower than private Wi-Fi
D) It doesn't allow large downloads

Lab 2.1 – Configuring Security Policies on a Virtual Machine

16 - Why are virtual machines useful for practicing security labs?

A) They are faster than physical machines
B) They isolate environments, reducing risks to the host system
C) They automatically fix vulnerabilities
D) They don't require hardware resources

17 - Which Windows tool enforces password policies?

A) Group Policy Editor
B) Task Manager
C) Device Manager
D) File Explorer

18 - In Linux, which file helps define password policies?

A) /etc/login.defs
B) /etc/services
C) /etc/networks
D) /etc/hosts

19 - What is the purpose of limiting administrative privileges?

A) To prevent unnecessary software updates
B) To reduce the chance of misuse or privilege escalation attacks

C) To improve the speed of logins
D) To allow users full system control

20 - Which of the following is used for system monitoring in Linux?

A) Event Viewer
B) Syslog
C) Disk Manager
D) Registry Editor

Lab 2.2 – Packet Analysis with Wireshark

21 - What is the main purpose of packet analysis?

A) To defragment hard drives
B) To examine and understand network traffic
C) To uninstall unused applications
D) To speed up system performance

22 - When starting Wireshark, what must you select first?

A) Browser type
B) Network interface to capture traffic
C) Antivirus tool
D) File explorer path

23 - Which Wireshark filter would you use to display only HTTP traffic?

A) dns
B) http
C) icmp
D) tcp.port == 22

24 - Why is spotting unencrypted traffic important?

A) It reveals system update history
B) It helps identify sensitive data exposed to attackers
C) It improves internet speed
D) It blocks spam emails

25 - In the lab challenge, what type of queries are students asked to capture and analyze?

A) FTP queries
B) DNS queries
C) SQL queries
D) VPN logs

Lab 2.3 – Setting Up and Testing a VPN

26 - What does a VPN primarily hide from third parties?

A) Browser history
B) IP address and network traffic contents
C) Installed applications
D) Hardware specifications

27 - Which test confirms your VPN is protecting your DNS traffic?

A) Speed test
B) DNS leak test
C) Antivirus scan
D) File integrity check

28 - What does a VPN “kill switch” do?

A) Shuts down the VPN after 1 hour
B) Prevents internet access if the VPN disconnects
C) Deletes browsing history after use
D) Increases VPN speed

29 - Why is it recommended to compare network captures with and without VPN?

A) To see if the VPN slows down browsing
B) To confirm encryption is being applied to the traffic
C) To test Wi-Fi performance
D) To reduce memory usage

30 - Which of the following is a common optional setting in VPN clients?

A) Auto-connect at startup
B) File compression
C) Power saving mode
D) Background theme color

Answer Key

1. **B** – OS security = protecting from unauthorized access/vulnerabilities.
2. **A** – Outdated patches are a big risk.
3. **C** – Updates patch vulnerabilities before attackers exploit them.
4. **A** – Access control manages logins/permissions.
5. **B** – Hardening disables unnecessary features/services.
6. **A** – Default accounts are exploitable if not restricted.
7. **A** – Whitelisting = only approved apps run.
8. **B** – Logs detect abnormal activity.
9. **B** – Memory corruption = flaw in handling memory.
10. **A** – DEP blocks execution from unsafe memory.
11. **B** – ASLR randomizes memory layout.
12. **D** – Defragging isn't a network threat.
13. **B** – VPNs secure traffic with encryption.
14. **D** – WPA3 is the strongest Wi-Fi standard.
15. **B** – Public Wi-Fi often lacks encryption.
16. **B** – VMs isolate labs, protect the host system.
17. **A** – Password policies: Group Policy Editor.
18. **A** – /etc/login.defs manages password settings.
19. **B** – Least privilege reduces abuse risk.
20. **B** – Syslog and auth.log are Linux monitoring tools.
21. **B** – Packet analysis = studying network traffic.
22. **B** – Must choose a network interface.
23. **B** – Filter "http" shows HTTP packets.
24. **B** – Unencrypted traffic exposes sensitive data.
25. **B** – Challenge = analyze DNS queries.
26. **B** – VPN hides IP + encrypts traffic.
27. **B** – DNS leak tests confirm privacy.
28. **B** – Kill switch blocks traffic if VPN drops.
29. **B** – Comparison shows encryption effect.
30. **A** – Auto-connect is a common VPN setting.