Module 1 – Final Quiz: Introduction to Cybersecurity

1 - Which of the following best defines cybersecurity?

A) The protection of physical assets from theft
B) The process of securing digital systems, networks, and data from unauthorized access or attacks
C) Installing antivirus software on a personal computer
D) Only protecting personal data on social media

2 - Who needs cybersecurity?

A) Only governments and large corporations
B) Only banks and financial institutions
C) Everyone, from individuals to global organizations
D) Only IT professionals

3 - Which of the following is a common example of a cyberattack?

A) Formatting a hard drive
B) Installing software updates
C) Phishing emails asking for login credentials
D) Deleting temporary files

4 - What is ransomware?

A) Software that scans for malware on your system
B) Malware that locks files and demands payment to restore access
C) A phishing attack through email
D) A brute-force attack against a password

5 - Which of the following attacks targets the human layer of security?

A) Denial-of-Service
B) Brute-Force Attack
C) Phishing and Social Engineering
D) Zero-Day Exploit

6 - What does the “C” in the CIA Triad stand for?

A) Control
B) Cryptography
C) Confidentiality
D) Communication

7 - Which principle ensures users get only the access they strictly need?

A) Defense in Depth
B) Least Privilege
C) Zero Trust
D) Security by Design

8 - A firewall primarily protects a system by:

A) Encrypting all files on the computer
B) Filtering incoming and outgoing network traffic based on rules
C) Detecting and removing viruses
D) Blocking access to social media websites

9 - Which of these tasks is performed by antivirus software?

A) Encrypting internet traffic
B) Detecting and quarantining malicious files
C) Blocking suspicious IP addresses
D) Monitoring firewall rules

10 - Why is it often recommended to use both a firewall and antivirus software?

A) They do the exact same thing, so redundancy is good
B) Firewalls stop intrusions, antivirus removes infections
C) Antivirus software makes firewalls obsolete
D) Firewalls only work on Linux, antivirus only on Windows

11 - Which Linux command enables the firewall using UFW?

A) sudo firewall on
B) ufw allow all
C) sudo ufw enable
D) enable ufw firewall

12 - In antivirus tools, quarantining a file means:

A) Automatically deleting it permanently
B) Encrypting it with a strong password
C) Isolating it so it cannot harm the system
D) Sending it to a backup server

13 - You receive an email from your “bank” asking you to confirm your password by clicking a link. Which concept helps you identify this as phishing?

A) Confidentiality
B) Defense in Depth
C) Social Engineering Awareness
D) Zero Trust

14 - Which of the following best illustrates Zero Trust Architecture?

A) Employees have unlimited access once inside the network
B) Devices and users must be continuously verified before accessing resources
C) The company only uses one strong firewall
D) All security relies on antivirus scans alone

15 - Your firewall logs show repeated attempts from an unknown IP on port 22 (SSH). What is the best immediate action?

A) Ignore it since it's just noise
B) Block the IP and review SSH firewall rules
C) Uninstall the firewall and reinstall antivirus
D) Allow the connection to see what happens

Lab 1.1 – Firewall Questions

16 - Which of the following best describes a firewall?

A) A tool for encrypting files
B) A barrier that filters network traffic based on rules
C) A scanner that detects viruses
D) A program that monitors CPU usage

17 - Which Windows tool is used to configure advanced firewall rules?

A) Task Manager
B) Command Prompt
C) Windows Defender Firewall with Advanced Security
D) Device Manager

18 - What is the purpose of blocking port 22 (SSH) in a firewall configuration?

A) To prevent email spam
B) To stop unauthorized remote logins
C) To disable web browsing
D) To improve system performance

19 - Which command lists active firewall rules in Linux UFW?

A) ufw rules list
B) sudo ufw status
C) firewall list
D) netstat --ufw

20 - In the lab challenge (allow HTTP, block everything else), which port must remain open?

A) 22
B) 25
C) 80
D) 443

Lab 1.2 – Antivirus Questions

21 - What is the first step before running an antivirus scan?

A) Disable your firewall
B) Update virus definitions
C) Reinstall the antivirus tool
D) Run a system restore

22 - In Microsoft Defender, which option performs the most thorough check?

A) Quick Scan
B) Custom Scan
C) Full Scan
D) History Scan

23 - Which Linux command updates the ClamAV virus database?

A) sudo freshclam
B) sudo update-av
C) clamav --update
D) av-refresh

24 - If a suspicious file is detected by antivirus, what is the safest first action?

A) Delete it immediately without review
B) Quarantine it to prevent execution
C) Ignore the warning if the file seems harmless
D) Send it to all coworkers for inspection

25 - Which best practice should be followed after reviewing antivirus scan results?

A) Disable the antivirus to save CPU power
B) Review logs and confirm false positives before taking action
C) Run only one scan per year
D) Assume no further action is needed

Answer Key

1. **B** – Cybersecurity = securing digital systems and data.
2. **C** – Everyone needs cybersecurity.
3. **C** – Phishing emails are classic cyberattacks.
4. **B** – Ransomware locks files, demands ransom.
5. **C** – Social engineering targets humans, not machines.
6. **C** – "C" = Confidentiality.
7. **B** – Least Privilege = minimum necessary access.
8. **B** – Firewalls filter traffic, not files.
9. **B** – Antivirus detects/quarantines malicious files.
10. **B** – They complement each other: intrusion vs infection.
11. **C** – Correct command: sudo ufw enable.
12. **C** – Quarantine = isolate suspicious files.
13. **C** – Awareness of social engineering prevents phishing.
14. **B** – Zero Trust = continuous verification.
15. **B** – Best action: block IP, check firewall rules.
16. **B** – Firewall = traffic filter.
17. **C** – Windows tool: Defender Firewall with Advanced Security.
18. **B** – Blocking SSH prevents remote logins.
19. **B** – sudo ufw status shows active rules.
20. **C** – HTTP uses port 80.
21. **B** – Always update virus definitions first.
22. **C** – Full Scan is most thorough.
23. **A** – sudo freshclam updates ClamAV database.
24. **B** – Quarantine first, then review.
25. **B** – Always check logs, confirm before deleting.