Cybersecurity Test

Part 1: Introduction to Security

Asma Khoudour

April 5, 2025

Instructions

- Time allowed: 90 minutes
- Total points: 150
- Answer all questions in the spaces provided

1 Multiple Choice (2 points each, 40 total)

1. What is the primary purpose of a sniffer?
   a) Encrypting network traffic
   b) Capturing and analyzing network packets
   c) Blocking unauthorized access
   d) Scanning for viruses
2. Which type of hacker is authorized to test system vulnerabilities?
   a) Black hat
   b) Gray hat
   c) White hat
   d) Script kiddie

3. What does a vulnerability scanner do?

    a) Encrypts sensitive data
    b) Identifies weaknesses in a system
    c) Blocks all incoming traffic
    d) Creates backups

4. Which mechanism ensures data integrity?

    a) Firewall
    b) Hashing
    c) Proxy
    d) VPN

5. What is the main difference between a virus and a worm?

    a) Viruses require user interaction; worms self-propagate
    b) Worms only infect files; viruses infect networks
    c) Viruses are harmless; worms are always malicious
    d) Worms encrypt data; viruses delete files

6. What does a DMZ (Demilitarized Zone) protect?

    a) Internal networks from external attacks
    b) Only email servers
    c) User passwords
    d) VPN connections

7. Which attack involves encrypting data and demanding ransom?

    a) Phishing
    b) Ransomware
    c) Spyware
    d) Trojan

8. What is the role of a firewall?

a) To store backups

b) To filter network traffic based on rules

c) To encrypt all outgoing emails

d) To detect malware signatures

9. Which authentication method uses biometrics?

a) Password

b) Smart card

c) Fingerprint scan

d) CAPTCHA

10. What does IDS stand for?

a) Intrusion Detection System

b) Internet Data Service

c) Internal Defense System

d) Integrated Data Security

11. What is the primary function of a VPN?

a) Block malware

b) Create encrypted tunnels for secure communication

c) Scan for vulnerabilities

d) Monitor CPU usage

12. Which tool would a hacker use to intercept unencrypted web traffic?

a) Antivirus

b) Wireshark

c) Firewall

d) Checksum calculator

13. What makes a zero-day exploit dangerous?

a) It targets multiple systems simultaneously

b) There are no existing patches for it

c) It only works on Windows systems

d) It requires physical access

14. In the CIA triad, "Availability" refers to:

a) Data encryption

b) Ensuring authorized access when needed

c) Preventing data modification

d) User authentication

15. Which attack intercepts communication between two parties?

a) Phishing

b) MITM (Man-in-the-Middle)

c) DDoS

d) SQL injection

16. What is the main purpose of salting in password security?

a) To make passwords shorter

b) To add random data before hashing

c) To encrypt password databases

d) To bypass authentication

17. Which protocol provides secure web browsing?

a) HTTP

b) FTP

c) HTTPS

d) SMTP

18. What does a honeypot primarily do?

a) Stores backup data

b) Attracts and monitors attackers

c) Encrypts network traffic

d) Scans for viruses

19. Which of these is NOT a biometric authentication method?

    a) Fingerprint scan

    b) Retina scan

    c) Password

    d) Voice recognition

20. What is the main risk of public Wi-Fi networks?

    a) Slow speeds

    b) Data interception

    c) Hardware failure

    d) Software incompatibility

2 True/False (2 points each, 30 total)

Mark each statement as True (T) or False (F):

21. ___ A gray hat hacker acts without malicious intent but without authorization.

22. ___ Hashing ensures data confidentiality.

23. ___ A proxy server encrypts all traffic like a VPN.

24. ___ Script kiddies are highly skilled hackers.

25. ___ Non-repudiation prevents senders from denying their actions.

26. ___ Wireshark is an example of a sniffer.

27. ___ A Trojan horse appears legitimate but contains malicious code.

28. ___ Availability ensures only authorized users access data.

29. ___ A DMZ is placed behind the internal firewall only.

30. ___ Phishing attacks always involve malware.

31. ___ A checksum verifies data integrity but not authenticity.

32. ___ All hackers operate with malicious intent.

33. ___ SSL and TLS are identical protocols.

34. ___ Biometric authentication is considered part of "something you know" factor.

35. ___ A honeypot is designed to attract attackers for monitoring.

3 Short Answer (4 points each, 40 total)

36. Define "vulnerability" and give one example.

37. What are the three main goals of cybersecurity (CIA triad)?

38. How does a digital signature work?

39. Name two differences between HTTP and HTTPS.

40. What is the purpose of a rootkit?

41. Explain the difference between active and passive attacks with examples.

42. What are two limitations of antivirus software?

43. Describe how a DDoS attack works.

44. Why is social engineering effective despite technical security measures?

45. Define "salting" in password security context.

4 Essay Questions (10 points each, 40 total)

46. Compare symmetric and asymmetric encryption with examples.

47. Explain the steps of a typical cyberattack (from reconnaissance to covering tracks).

48. Describe how a firewall and IDS work together to secure a network.

49. Discuss the ethical implications of gray hat hacking.

5 Scenario-Based Questions (10 points each, 20 total)

50. A company's web server was compromised via SQL injection. What mitigation steps would you recommend?

51. An employee received an email requesting password verification from "IT Support". Identify the attack type and response protocol.

Answer Key

Multiple Choice

1. b (Capturing and analyzing network packets)
2. c (White hat)
3. b (Identifies weaknesses in a system)
4. b (Hashing)
5. a (Viruses require user interaction; worms self-propagate)
6. a (Internal networks from external attacks)
7. b (Ransomware)
8. b (To filter network traffic based on rules)
9. c (Fingerprint scan)
10. a (Intrusion Detection System)
11. b (Create encrypted tunnels)
12. b (Wireshark)
13. b (No existing patches)
14. b (Ensuring authorized access)
15. b (MITM)
16. b (Add random data before hashing)
17. c (HTTPS)
18. b (Attracts and monitors attackers)
19. c (Password)
20. b (Data interception)

True/False

21. T
22. F (Hashing ensures integrity)
23. F (Proxies don't encrypt like VPNs)
24. F (Script kiddies lack advanced skills)
25. T
26. T
27. T
28. F (Confidentiality restricts access)
29. F (DMZ is between firewalls)
30. F (Phishing uses deception)
31. T
32. F
33. F
34. F (It's "something you are")
35. T

Short Answer

36. **Vulnerability**: A weakness in a system that can be exploited. *Example*: Unpatched software flaw (e.g., Heartbleed bug).

37. **CIA Triad**: Confidentiality, Integrity, Availability.

38. **Digital Signature**: Sender encrypts message hash with private key; receiver verifies with sender's public key.

39. **HTTP vs HTTPS**:

    - HTTPS encrypts data (SSL/TLS); HTTP sends plaintext
    - HTTPS requires certificates; HTTP does not

40. **Rootkit Purpose**: To hide malicious activity by gaining privileged access.

41. **Active vs Passive**:

    - Active: Alters system (e.g., DDoS)
    - Passive: Eavesdrops (e.g., sniffing)

42. **Antivirus Limitations**:
    - Cannot detect zero-day exploits
    - May slow system performance
43. **DDoS**: Overwhelms target with traffic from multiple sources.
44. **Social Engineering**: Exploits human psychology rather than technical flaws.
45. **Salting**: Adding random data to passwords before hashing.

Scenario Answers

50. **SQL Injection Mitigation**:
    - Input validation/sanitization
    - Prepared statements
    - Web Application Firewall
    - Least privilege database access
51. **Phishing Response**:
    - Do not click links/attachments
    - Report to IT security
    - Verify sender through official channels
    - Security awareness training