Final Exam Version 1

Full Name:

Please use the bubble sheet to answer the multiple choice and the True/False questions.

You can use the space provided below the short-answer and long-answer questions to write your responses.

The total weightage for the test is 30 points, Part 1 which includes MCQ and Definition Questions is weighted at 20 points while Part 2 which is a scenario-based question is weighted at 10 points.

Use a pen or a dark pencil.

No electronic aids allowed.

Part 1: Multiple Choice Questions. (1 Point per question)

1. Which security tool is responsible for preventing unauthorized inbound or outbound traffic?

A) Firewall

B) VPN

C) IDS

D) Proxy

2. Which OWASP category involves poor session management or broken login processes?

A) Cryptographic Failures

B) Injection

C) Identification and Authentication Failures

D) Security Misconfiguration

3. What is the key purpose of the reconnaissance phase in ethical hacking?

A) Exploiting known vulnerabilities

B) Gathering information to plan an attack

C) Installing malware

D) Encrypting stolen files

4. In penetration testing, which of the following comes after the vulnerability scan?

A) Planning

B) Exploitation

C) Scoping

D) Reporting

5. The term “least privilege” ensures that:

A) Only guests are restricted

B) Users can access everything by default

C) Developers have full administrative access Users

D) Users get only the permissions necessary for their role

6. Which protocol is typically used for secure file transfer?

A) FTP

B) SMTP

C) Telnet

D) SFTP

7. Which of the following tools is commonly used during reconnaissance or scanning in ethical hacking?

A) WireShark

B) Metasploit

C) Nmap

D) NetCat

8. PIPEDA governs which of the following?

A) Intellectual property laws

B) Personal data protection in Canada

C) Network encryption algorithms

D) Firewall implementation

9. What is the MITRE ATT&CK framework used for?

A) Logging network performance

B) Performing brute-force attacks

C) Mapping attacker behaviors and tactics

D) Encrypting endpoints

10. Which type of attack injects malicious JavaScript into user-facing pages?

A) XSS (Cross-Site Scripting)

B) Command Injection

C) SQL Injection

D) Cross-Site Request Forgery

11. What tactic allows attackers to retain access to a compromised system?

A) Credential stuffing

B) Port forwarding

C) Passive scanning

D) Backdoor installation

12. Why are passwords stored using hashing instead of plain encryption?

A) Hashing allows for recovery

B) Hashes are one-way and can’t be decrypted

C) It reduces file size

D) Encrypted passwords can’t be used in login systems

13. What is the goal of the “Containment” step in incident response?

A) Deploying MFA

B) Rebuilding the infrastructure

C) Isolating affected systems to prevent further spread

D) Notifying third parties

14. A successful brute-force attack usually implies:

A) Strong password policies were enforced

B) MFA was active

C) Default credentials were unchanged

D) The attacker used encryption

15. What is a secure way to verify a user’s identity during login?

A) CAPTCHA

B) Multi-Factor Authentication (MFA)

C) IP address matching

D) Username only

Part 1 (Continued): Definitions. (1 Point per question)

1. **Define "Security Misconfigurations."**

2. **Define "Reconnaissance** in the context of cybersecurity."

3. **Define "Privilege Escalation."**

4. **Define "Bug Bounty Program."**

5. Define "**Zero Day Exploit.**"

Part 2: Scenario-Based Case (10 Points)

Scenario:
A retail company uses outdated CMS software for its online store. A hacker finds a vulnerability and uses it to inject a malicious script that captures customer payment details. The logs show no alerts were triggered. The company does not regularly patch its systems or monitor traffic. This issue remained undetected for several days.

Short Answer 1 (2 Points)
What two key security practices did the company fail to follow that enabled this breach?

Short Answer 2 (1 Points)
What specific OWASP vulnerability does this attack most likely fall under?

Long Answer 1 (3 Points)
Outline how a proper **security monitoring and logging system** could have prevented or detected this breach. Include two tools or technologies.

Long Answer 2 (4 Points)
Provide a 4-step **incident response plan** the company should follow discovering this breach. Include the purpose of each step.