Final Exam Version 2

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. What is the primary benefit of using multi-factor authentication (MFA)?

A) It avoids the need for passwords

B) It provides faster network access

C) It provides added security even if a password is compromised

D) It prevents firewall misconfiguration

2. Which phase of ethical hacking focuses on identifying open ports and services?

A) Enumeration

B) Gaining Access

C) Scanning

D) Covering Tracks

3. What is a common cause of data leaks in web applications?

A) Use of VPNs

B) Regular updates

C) Outdated or unpatched components

D) Strong password policies

4. What type of vulnerability allows attackers to manipulate a query to the database?

A) CSRF

B) SQL Injection

C) SSRF

D) XSS

5. The post-incident review phase in incident response aims to:

A) Reboot the system

B) Improve future defenses and IR plans

C) Wipe all data

D) Create audit logs

6. Which of the following would not be a proper component of an incident response plan?

A) Recovery

B) Containment

C) Exploitation

D) Eradication

7. HTTPS ensures encryption of both HTTP headers and data in transit.

A) True

B) False

8. Which tool is commonly used for scanning open ports and detecting services on a target network?

A) NetCat

B) Nessus

C) Nmap

D) Hashcat

9. A script that captures user input from a form and sends it to an attacker likely indicates:

A) Brute-force attack

B) SQL Injection

C) Cross-Site Scripting (XSS)

D) Port Scanning

10. The use of default admin credentials in a system is an example of which OWASP threat?

A) Broken Access Control

B) Insecure Design

C) Injection

D) Security Misconfiguration

11. A bug bounty program helps organizations:

A) Avoid hiring internal security staff

B) Hide vulnerabilities from the public

C) Identify and report vulnerabilities ethically

D) Monitor physical access

12. What cybersecurity framework organizes known attack tactics and techniques?

A) OWASP

B) PIPEDA

C) ISO 27001

D) MITRE ATT&CK

13. What is the role of a VPN in securing network traffic?

A) Encrypts all network communication and hides IP

B) Provides virus protection

C) Allows access to open ports

D) Logs login attempts

14. Which of the following would most likely be found in the gaining access phase?

A) Phishing awareness training

B) Brute-force attacks

C) Log management

D) User onboarding

15. A hashed password can be reversed with the correct key.

A) True

B) False

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

1. **Define "Incident Containment."**

2. **Define "Cross-Site Scripting (XSS)**."

3. **Define "Threat Intelligence."**

4. **Define "Social Engineering."**

5. Define "**Principle of Least Privellege.**"

Part 2: Scenario-Based Case (10 Points)

Scenario:
A university's student portal was compromised after an attacker performed a brute-force login attack on administrative accounts. The attacker gained access due to weak passwords and no account lockout policy present. As a result, student grades and records were leaked online. The university lacked MFA and had no centralized logging in place.

Short Answer 1 (2 Points)
Identify two poor security practices that made the attack successful.

Short Answer 2 (1 Points)
What authentication controls could the university implement to stop brute-force attempts in the future?

Long Answer 1 (3 Points)
Describe a basic **authentication hardening plan** for the university's portal. Include at least 3 controls.

Long Answer 2 (4 Points)
Outline a 4-phase **incident response strategy** the university should adopt after discovering this breach.