Practical Cybersecurity Lecture #4 Quiz

Full Name:

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

You can use the space provided below the long-answer question to write your responses.

Use a pen or a dark pencil.

Each MCQ/True-False question is worth 0.25 points. Long answer is worth 0.75 points.

1. What is the first phase in the ethical hacking process?
A) Exploitation
B) Scanning
C) Reconnaissance
D) Covering Tracks

2. Which of the following is a valid example of passive reconnaissance?
A) Port scanning
B) Using Shodan to find exposed systems
C) SQL Injection
D) Password cracking

3. What tool is commonly used for port scanning?
A) Burp Suite
B) Mimikatz
C) Nmap
D) Wireshark

4. What is the primary goal of privilege escalation?
A) To hide the attacker's presence
B) To bypass firewall protections
C) To gain higher system access
D) To perform phishing attacks

5. Which law applies to unauthorized access of computer systems in Canada?
A) CFAA
B) GDPR
C) PIPEDA
D) HIPAA

6. Ethical hackers must always get permission before performing security tests.
A) True
B) False

7. HackThis.io requires a verified account and software download to participate.
A) True
B) False

8. Describe a real-world case of a web-based cyberattack (e.g., Capital One, British Airways, Colonial Pipeline).

Please explain how the breach occurred, what was targeted, and what security controls could have prevented it.

End of Quiz