Final Exam Version 1 Answer Key

Part 1:

Multiple Choice Questions (1 mark each)

1. A) Firewall

2. C) Identification and Authentication Failures

3. B) Gathering information to plan an attack

4. B) Exploitation

5. D) Users get only the permissions necessary for their role

6. D) SFTP

7. C) Nmap

8. B) Personal data protection in Canada

9. C) Mapping attacker behaviors and tactics

10. A) XSS (Cross-Site Scripting)

11. D) Backdoor installation

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

13. C) Isolating affected systems to prevent further spread

14. C) Default credentials were unchanged

15. B) Multi-Factor Authentication (MFA)

Definitions (1 mark each)

1. Security Misconfiguration – A vulnerability resulting from default settings, unpatched systems, or unnecessary services being enabled.

2. Reconnaissance – The phase where attackers gather information about a target using public or passive techniques to plan an attack.

3. Privilege Escalation – When an attacker gains higher-level permissions or access than intended, often moving from user to admin rights.

4.. Bug Bounty Program – A system where organizations pay ethical hackers for responsibly reporting discovered vulnerabilities.

5. Zero-Day Exploit – A vulnerability that is unknown to the software vendor and has no official patch available when exploited.

Part 2:

Scenario Recap:

Retail store using outdated CMS was breached via script injection. No alerts triggered. Company lacked regular patching and traffic monitoring.

Short Answer

21. Key Failures:

• Failure to regularly patch the CMS or apply updates

• Lack of real-time monitoring or alerting system (e.g., IDS, log monitoring)

22. OWASP Vulnerability:

• This scenario matches Security Misconfiguration and/or Cross-Site Scripting (XSS) depending on how the script was injected

• Acceptable answers: Security Misconfiguration, XSS

Long Answers

23. Monitoring and Logging Prevention

• Company could use SIEM tools (e.g., Splunk, Wazuh) to monitor logs in real time.

• Web Application Firewalls (WAFs) could detect and block malicious script activity.

• Alert thresholds could notify IT when anomalies are detected (e.g., traffic spikes, modified JS).

• Logs from CMS and firewalls should be centrally analyzed.

24. Incident Response Plan

• Detection & Analysis: Review logs, identify breach source, assess scope of impact

• Containment: Block attacker access, isolate vulnerable system

• Eradication & Recovery: Patch CMS, remove malicious scripts, restore clean backups

• Post-Incident Review: Document findings, update security controls, conduct staff training