Final Exam Version 2 Answer Key

Part 1:

| Question # | Correct Answer | Option |
| --- | --- | --- |
| 1 | Added security even if a password is compromised | C |
| 2 | Scanning | C |
| 3 | Outdated or unpatched components | C |
| 4 | SQL Injection | B |
| 5 | Improve future defenses and IR plans | B |
| 6 | Exploitation | C |
| 7 | HTTPS | True |
| 8 | Nmap | C |
| 9 | Cross-Site Scripting (XSS) | C |
| 10 | Security Misconfiguration | D |
| 11 | Identify and report vulnerabilities ethically | C |
| 12 | MITRE ATT&CK | D |
| 13 | Encrypts network traffic and hides IP | A |
| 14 | Brute-force attacks | B |
| 15 | Hashed Password Decryption | False |

Definitions (1 mark each)

16. **Incident Containment** – The process of isolating affected systems and stopping the attacker from causing more damage.

17. **Cross-Site Scripting (XSS)** – A web vulnerability where malicious scripts are injected into trusted websites to hijack user sessions or steal data.

18. **Threat Intelligence** – Data and insights about current or emerging cyber threats used to inform defensive strategies.

19. **Social Engineering** – Manipulating individuals into revealing confidential information or performing actions that compromise security.

20. **Principle of Least Privilege** – Ensuring users and systems only have access to the data and functions necessary for their role.

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Retail store using outdated CMS was breached via script injection.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 1

**Poor Security Practices**:

• Weak/default passwords

• No account lockout policy after failed login attempts

Short Answer 2

Authentication Controls:

• Implement MFA (1 mark)

• Account lockout or rate limiting after multiple failed attempts (1 mark)

• Enforce password complexity

• Use CAPTCHA or login throttling

• Monitor login attempts using logs/SIEM

Long Answers

Authentication Hardening Plan (3 Points)

• **Strong Password Policy:**

Minimum length, complexity, no reuse

• **Multi-Factor Authentication (MFA):**

Required for all admin and high-privilege accounts

• **Account Lockout/Rate Limiting:**

Lockout after 3–5 failed attempts or implement login throttling

• **(Optional Add-On):** CAPTCHA, IP filtering, security awareness for staff

Incident Response Plan (4 Points)

1. **Detection & Analysis:**

Review login activity, identify attack vector, confirm data leak

2. **Containment:**

Disable affected accounts, restrict access to admin portal

3. **Eradication & Recovery:**

Remove malicious access, reset passwords, update systems

4. **Post-Incident Review:**

Review weaknesses, update policies, improve awareness