Practice Final Exam

📄 SECTION 1: QUESTIONS ONLY

Part 1: Multiple Choice Questions

1. Which of the following is NOT a characteristic of a strong password?
A) At least 8 characters long
B) Includes uppercase, lowercase, numbers, and symbols
C) Is reused across multiple websites
D) Is difficult to guess

2. What is the function of an Intrusion Prevention System (IPS)?
A) Logs suspicious activity
B) Encrypts VPN traffic
C) Blocks detected threats in real time
D) Protects wireless access points

3. What cyberattack does this input represent: admin' OR '1'='1?
A) Command Injection
B) XSS
C) SQL Injection
D) Privilege Escalation

4. What type of hacker is authorized to legally test systems for vulnerabilities?
A) Black Hat
B) Grey Hat
C) White Hat
D) Red Hat

5. Which OWASP threat relates to poor encryption practices?
A) Insecure Deserialization
B) Cryptographic Failures
C) Broken Authentication
D) Security Misconfiguration

6. Which of the following are valid incident response phases? (Select all that apply)
☐ Preparation
☐ Containment
☐ Code Injection
☐ Recovery

7. True or False: A VPN hides your IP address and encrypts your internet traffic.
☐ True
☐ False

8. True or False: Reconnaissance is performed after exploitation in a hacking sequence.
☐ True
☐ False

Part 1 (Continued): Definitions

1. **Define “Firewall.”**

2. **Define “Incident Response Plan.”**

3. **Define “Cross-Site Scripting (XSS).”**

4. **Define “Penetration Testing.”**

Part 2: Scenario-Based Case

📌 **Scenario:**
You're a cybersecurity analyst for a small healthcare company. A data breach occurred when an employee accessed internal systems from public Wi-Fi at a coffee shop. Investigation shows no VPN was used, and personal health records may have been intercepted by a third party.

Short Answer 1
What critical security mistake did the employee make, and how could it have been avoided?

Short Answer 2
What policy or technical control could the organization implement to reduce the risk of this happening again?

Long Answer

Describe the steps the company should take as part of an effective incident response to this breach. Include at least 3 phases.

📝 SECTION 2: ANSWER KEY

Part 1: Multiple Choice Answers

1. C
2. C
3. C
4. C
5. B
6. Preparation, Containment, Recovery
7. True
8. False

Part 1 (Continued): Definitions

1. **Firewall:** A firewall is a security device or software that monitors and filters incoming and outgoing network traffic based on security rules.
2. **Incident Response Plan:** A formal process outlining how an organization detects, responds to, and recovers from cybersecurity incidents.
3. **Cross-Site Scripting (XSS):** A vulnerability where attackers inject malicious scripts into trusted websites, affecting users who visit the page.
4. **Penetration Testing:** A simulated cyberattack performed by ethical hackers to identify and exploit vulnerabilities in a system before real attackers can.

Part 2: Scenario-Based Answers

Short Answer 1:

The critical mistake was accessing sensitive internal systems over an unsecured public Wi-Fi connection without using a VPN. Public networks are highly vulnerable to man-in-the-middle (MITM) attacks, where malicious actors can intercept unencrypted data, including login credentials and patient records. This situation could have been avoided by enforcing a security policy that mandates the use of a corporate VPN for all remote connections. Additionally, employee training on secure work practices would have helped prevent the user from making this risky decision.

Short Answer 2:
The organization should implement a Remote Access Policy requiring VPN usage for all off-site connections to internal systems. This policy should be enforced technically by configuring systems to deny access from unknown IPs or non-VPN traffic, using endpoint detection and response (EDR) tools. Moreover, the company should deploy network access control (NAC) to ensure devices meet security standards before connecting.
Regular cybersecurity awareness training should be conducted to reinforce safe remote work behavior.

Long Answer:

The company should follow a structured incident response process to contain, investigate, and recover from the breach:

1. **Detection & Analysis:**
    - Begin by reviewing firewall and VPN logs to determine the time, scope, and nature of the unauthorized access.
    - Check for indicators of compromise (IoCs) and monitor for suspicious activity in affected systems.
2. **Containment & Eradication:**
    - Immediately disable the affected employee's account to prevent further access.
    - Block access from unrecognized IP addresses or devices that connected during the breach window.
    - Enforce stricter access controls and update VPN enforcement policies across endpoints.
3. **Recovery:**
    - Restore affected services and systems from clean backups if necessary.
    - Reset user credentials, especially for accounts that were used without protection.
    - Reconfigure access policies to allow only encrypted remote connections and enable full disk encryption on mobile devices.
    - Monitor systems for signs of reinfection or continued unauthorized access.
4. **Post-Incident Review:**
    - Conduct a debriefing with IT and security teams to analyze what went wrong.
    - Update incident response procedures and employee training materials.
    - Ensure the remote access policy is communicated clearly to all staff.

By executing these steps, the company can contain the current threat, reinforce its security posture, and reduce the likelihood of future breaches.