Week-4

Asad Muhammad Channar
DHC-56

Task-1:

Threat Mitigation Strategies:

Learn how to mitigate realworld threats, including patching vulnerabilities and implementing firewalls

Required:

- Identify the vulnerabilities exploited in Week 3 (using Metasploit, Nmap, or OWASP Juice Shop).
- Develop mitigation strategies such as patching, firewall rules, or network segmentation.
- Implement these strategies in a controlled environment.

Deliverables:

A comprehensive report outlining the mitigation steps for each vulnerability and their impact on security.

Threat Mitigation Strategy Development

Vulnerabilities Exploited

1. **Backdoor Vulnerability**
   - **Description:** This vulnerability allowed unauthorized access to the system through a backdoor.
   - **Tool Used:** Metasploit was utilized to exploit this vulnerability.
2. **SQL Injection Vulnerability**
   - **Description:** An SQL injection vulnerability was identified, allowing attackers to manipulate database queries, potentially leading to unauthorized data access or modification.
   - **Tool Used:** Metasploit and manual testing were used to exploit this vulnerability.
3. **Cross-Site Scripting (XSS) Vulnerability**
   - **Description:** An XSS vulnerability was found, enabling attackers to inject malicious scripts into web pages viewed by users, compromising user data and sessions.
   - **Tool Used:** OWASP Juice Shop was utilized to demonstrate this vulnerability.

2. Develop Mitigation Strategies

Mitigation Strategies

1. **Patching**
   - **Action:** Update all systems and applications to close the identified vulnerabilities.
   - **Implementation:** Regularly check for patches from vendors for all software used.
2. **Firewall Rules**
   - **Action:** Configure firewalls to block unauthorized access.
   - **Implementation:**
     - Block ports used by the backdoor.
     - Monitor and restrict access to web applications to trusted IP addresses.
3. **Network Segmentation**
   - **Action:** Segment the network to isolate vulnerable systems from sensitive data.
   - **Implementation:** Create separate VLANs to protect databases and web servers.
4. **Input Validation and Parameterized Queries (for SQL Injection)**
   - **Action:** Implement strong input validation and use parameterized queries to prevent SQL injection attacks.
   - **Implementation:** Review and refactor application code to ensure proper sanitization of user inputs.
5. **Content Security Policy (for XSS)**
   - **Action:** Implement a Content Security Policy to mitigate the risk of XSS attacks.
   - **Implementation:** Configure HTTP headers to restrict the sources of executable scripts.

6. **Intrusion Detection Systems (IDS)**
    - **Action:** Deploy IDS to detect and alert on suspicious activities related to all identified vulnerabilities.
    - **Implementation:** Select an IDS that can monitor web traffic and system logs.
7. **Access Controls**
    - **Action:** Strengthen authentication and authorization mechanisms.
    - **Implementation:**
        - Enforce strong password policies.
        - Implement MFA for accessing sensitive areas of applications.
8. **Regular Audits**
    - **Action:** Conduct periodic security assessments.
    - **Implementation:** Schedule vulnerability scans and penetration tests at regular intervals.

3. Implement Strategies in a Controlled Environment

Testing Environment

- **Setup:** Create a controlled environment (e.g., virtual machines) that mimics the production system.
- **Implementation:** Apply the developed mitigation strategies and test their effectiveness without impacting live systems.

Documentation

- **Records:** Maintain a detailed log of all strategies implemented, configurations, and any issues encountered during testing.

Review and Iterate

- **Monitoring:** Continuously monitor the systems for any signs of vulnerability exploitation.
- **Adjustments:** Refine the strategies based on findings and evolving threats.

Conclusion

By addressing the backdoor, SQL injection, and XSS vulnerabilities through these mitigation strategies, we enhance our overall security posture. Ongoing monitoring and adaptation are crucial to defend against emerging threats.