Cyber Security Assignment-7 Questions

P LOHENDRA

2406CYS124

1. Case Study Question:

Case Study: XYZ Corporation, a leading financial institution, recently experienced a security breach where sensitive customer data was compromised.

As part of the incident response team (IRT), outline the steps you would take to address this incident effectively. Consider incident categorization, detection,communication plan, documentation, and legal/regulatory considerations in your response.

Evaluate the importance of incident response planning in mitigating such incidents and maintaining trust with stakeholders.

2. Investigate the exploitation of vulnerabilities such as SQL injection and cross-site scripting (XSS) in ethical hacking scenarios.

3. Discuss privilege escalation as a hacking technique, its implications, and preventive measures.

4. Explain the process of password cracking and discuss its ethical implications.

Answer:-

1. **Incident Response at XYZ Corporation:**
   - **Incident Categorization**: For instance, if customer credit card information is leaked, it's a Category 1 (Critical) incident.

     ```
     if data_type == 'credit_card':
       incident_category = 'Category 1 (Critical)'
     ```

   - **Detection**: Implementing a SIEM system might involve setting up rules to detect anomalies.

     ```
     if login_attempts > threshold:
       alert_security_team()
     ```

   - **Communication Plan**: Drafting templates for breach notifications can expedite the communication process.

     Security Breach Notification
     Dear [Customer Name],
     We regret to inform you that your data may have been compromised...

   - **Documentation**: Documenting an incident could be as simple as updating an incident log.

     ```
     incident_log.append({
       'date': current_date,
       'incident_type': detected_incident,
       'response': action_taken
     })
     ```

   - **Legal/Regulatory Considerations**: Compliance checks might involve code that ensures data handling meets legal standards.

     ```
     if data_handling_compliance(data):
       proceed_with_data_processing()
     else:
     ```

```
   report_compliance_violation()
```

2. **Investigating Vulnerabilities:**
   - **SQL Injection**: Testing for SQL injection might involve input validation functions.

     ```
     def is_safe_query(query):
        # Check if the query is safe from SQL injection
        return 'DROP TABLE' not in query
     ```

   - **Cross-Site Scripting (XSS)**: Preventing XSS could involve sanitizing user input.

     ```
     function sanitizeInput(input) {
        return input.replace(/<script.*?>.*?<\/script>/gi, '');
     }
     ```

3. **Privilege Escalation:**

   Technique: An example is when a user exploits a vulnerability to gain root access.

   ```
   # Exploiting a vulnerable application
   vulnerable_app --execute "echo 'new_root ALL=(ALL) NOPASSWD:ALL' >> /etc/sudoers"
   ```

   - **Preventive Measures**: Regular system updates can prevent known privilege escalation exploits.

     ```
     sudo apt-get update && sudo apt-get upgrade
     ```

4. **Password Cracking:**
   - **Process**: A brute force attack script might look like this:

     ```
     for password in password_list:
        if try_login(username, password):
     print('Password found:', password)
     break
     ```

   Ethical Implications: Ethical considerations must be taken into account, ensuring that such tools are used responsibly and legally.