Simeon Hawkins
Phase 4: Threat Assessment

Scenario 1: Unpatched RDP is exposed to the internet

Description of Vulnerability:

- Unpatched Remote Desktop Protocol (RDP) servers are exposed to the internet, allowing attackers to connect remotely and potentially exploit known vulnerabilities to gain unauthorized access.

CVSS Score: 9.8 (Critical)

Operating Systems/versions affected:

- Windows Server 2012, 2016, 2019.

Risks of Attempting to Exploit:

- May cause system instability or crash the host.
- Could lead to account lockout if brute force attempts are detected.

Risk:

- **Attack Vectors:**
    - Direct remote access leading to lateral movement within the network.
- **Blocking Mechanisms:**
    - Use of AV software and IDS/IPS to detect and block unauthorized access attempts.
- **Password Cracking:**
    - Use tools like Hydra or John the Ripper to perform brute force attacks on RDP passwords.

Remediation action:

- Apply the latest security patches to RDP servers.
- Use strong, unique passwords for RDP access.
- Implement multi-factor authentication (MFA).
- Restrict RDP access to specific IP addresses.

Scenario 2: Web application is vulnerable to SQL injection

Description of the Vulnerability:

- The web application does not properly sanitize user inputs, allowing attackers to execute arbitrary SQL commands on the database.

CVSS Score: 9.0 (Critical)

Operating Systems/Versions Affected:

- Web applications using vulnerable database systems.

Risks of Attempting to Exploit:

- Could corrupt the database.
- Might disrupt normal operations

Risk:

- **Attack Vectors:**
  - Injection of malicious SQL code to extract or alter database contents.
- **Blocking Mechanism:**
  - Use of web application firewalls (WAF) to detect and block SQL injection attempts.
- **SQL Injection Tools:**
  - Use tools like SQLmap to automate SQL injection attacks.

Remediation Action:

- Implement input validation and parameterized queries.
- Use ORM frameworks to prevent direct SQL execution.
- Regularly update and patch the web application.

Scenario 3: Default password on Cisco admin portal

Description of the Vulnerability:

- The Cisco admin portal is using default credentials, making it vulnerable to unauthorized access.

CVSS Score: 8.8 (High)

Operating Systems/Versions Affected:

Risk of Attempting to Exploit:

- Unauthorized access to the admin portal.

- Potential misconfiguration leading to network disruption.

Risk:

- **Attack Vectors:**
    - Gain administrative access to the network device.
    - Modify device configurations.
    - Disable security features.
- **Blocking Mechanisms:**
    - Use of access control lists (ACLs) to restrict access.
- **Password Cracking:**
    - Use tools like Hydra to perform dictionary attacks on the admin portal.

Remediation Action:

- Change default credentials to strong, unique passwords.
- Implement access controls to restrict admin portal access.
- Regularly review and update device configurations.

Scenario 4: Apache web server vulnerable to CVE-2019-0211

Description of the Vulnerability:

- A privilege escalation vulnerability in Apache HTTP Server that allows local users to gain root privileges.

CVSS Score: 7.2 (High)

Operating Systems/Versions Affected:

- Apache HTTP Server 2.4.17 to 2.4.38 on various OS.

Risks of Attempting to Exploit:

- May crash the server.
- Could lead to complete system compromise.

Risk:

- **Attack Vectors:**
    - Local exploitation leading to server compromise
- **Blocking Mechanisms:**

    - Use of intrusion detection/prevention systems (IDS/IPS).
- **Exploit Tools:**
    - Use proof-of-concept exploits available in security repositories.the web

Remediation Action

- Update Apache HTTP Server to the latest version.
- Restrict local access to the server.
- Monitor server logs for suspicious activity.

Scenario 5: Web server is exposing sensitive data

Description of the Vulnerability:

- The web server is configured to expose sensitive data such as configuration files, backup files, and logs.

CVSS Score: 7.5 (High)

Operating Systems/Versions Affected:

- All systems running the vulnerable web server.

Risks of Attempting to Exploit:

- Disclosure of sensitive information.
- Potential misuse of exposed data.

Risk:

- **Attack Vectors:**
    - Access to exposed files via web requests.
- **Blocking Mechanisms:**
    - Use of WAF to detect and block unauthorized access attempts.
- **Data Discovery Tools:**
    - Use tools like DirBuster to discover exposed files and directories.

Remediation Action:

- Configure the web server to restrict access to sensitive files.

- Use directory indexing controls to prevent exposure.
- Regularly audit web server configurations for security issues.

Scenario 6: Web application has broken access control

Description of the Vulnerability:

- The web application allows users to access resources and perform actions outside their intended permissions.

Operating Systems/Versions Affected:

- All systems running the vulnerable web application.

Risk:

- **Attack Vectors:**
  - Manipulation of access control mechanisms.
- **Blocking Mechanisms:**
  - Use of WAF to enforce access control policies.
- **Access Control Testing Tools:**
  - Use tools like Burp Suite to test for broken access control vulnerabilities.

Remediation Action:

- Implement robust access control mechanisms.
- Regularly review and update access control policies
- Conduct security testing to identify and fix access control issues.

Scenario 7: Oracle WebLogic Server vulnerable to CVE-2020-14882

Description of the Vulnerability:

- A remote code execution vulnerability in Oracle WebLogic Server allowing attackers to execute arbitrary code.

CVSS Score: 9.8 (Critical)

Operating Systems/Versions Affected:

- Oracle WebLogic Server versions 10.3.6.0, 12.1.3.0, 12.2.1.3, 12.2.1.4, 14.1.1.0.

Risks of Attempting to Exploit:

- May disrupt normal server operations.
- Could lead to full system compromise.

Risk:

- **Attack Vectors:**
  - Remote exploitation to execute arbitrary code
- **Blocking Mechanisms:**
  - Use of IDS/IPS to detect and block exploitation attempts.
- **Exploit Tools:**
  - Use available proof-of-concept exploits.

Remediation Action:

- Apply the latest security patches provided by Oracle.
- Restrict access to WebLogic management interfaces.
- Monitor server logs for signs of exploitation.

Scenario 8: Misconfigured Cloud Storage

Description of the Vulnerability:

- Cloud storage is misconfigured, leading to the exposure of sensitive data due to improper security group settings and lack of access restrictions.

CVSS Score: 7.4 (High)

Operating Systems/Versions Affected:

- Any system utilizing AWS cloud storage services with misconfigured security groups.

Risks of Attempting to Exploit:

- Unauthorized access to sensitive data.
- Potential data theft or leakage.

Risk:

- **Attack Vectors:**
    - Exploiting misconfigured security policies to access cloud data.
- **Blocking Mechanisms:**
    - Use of cloud security tools to detect and block unauthorized access attempts.
    - Implementing strict access control policies and monitoring access logs.
- **Data Extraction Tools:**
    - Use tools like AWS CLI to list and download files from exposed cloud storage.

Remediation Actions:

- Review and configure cloud storage security groups to ensure proper access restrictions.
- Implement encryption for data at rest and in transit.
- Regularly audit cloud storage settings and access logs for security compliance.

Scenario 9: Microsoft Exchange Server vulnerable to CVE-2021-26855

Description of the Vulnerability:

- Microsoft Exchange Server has a remote code execution vulnerability (CVE-2021-26855) that allows attackers to send specially crafted requests to the server, resulting in arbitrary code execution.

CVSS Score: 9.1 (Critical)

Operating Systems/Versions Affected:

- Microsoft Exchange Server versions 2013, 2016, and 2019.

Risks of Attempting to Exploit:

- Exploiting this vulnerability could crash the server or disrupt email services.
- Successful exploitation could lead to unauthorized access and data breaches.

Risk:

- **Attack Vectors:**
    - Remote exploitation leading to arbitrary code execution.
- **Blocking Mechanisms:**
    - Use of IDS/IPS to detect and block malicious requests.
    - Implementing proper firewall rules to restrict access to the Exchange Server.
- **Exploitation Tools:**

    - Utilize tools like Metasploit or custom scripts to exploit the vulnerability.

Remediation Action:

- Apply the latest security patches from Microsoft to address the vulnerability.
- Monitor network traffic and server logs for signs of attempted exploitation.
- Implement multi-factor authentication (MFA) for accessing the Exchange Server.