Project Executable Files:

---

1. Web Application Testing Scripts

Purpose:

Automate **web security assessments** by scanning applications for vulnerabilities such as **SQL Injection (SQLi), Cross-Site Scripting (XSS), and security misconfigurations**.

Key Features:

✅ **Automated Security Scanning:** Uses tools like **Nessus, Burp Suite, and OWASP ZAP** to detect application vulnerabilities.
✅ **SQL Injection & XSS Detection:** Sends crafted requests to input fields and monitors for signs of exploitation.
✅ **Misconfiguration Analysis:** Identifies weak authentication, missing security headers, and improper server settings.

Use Case:

A security analyst can run the script before application deployment to detect vulnerabilities early, reducing the risk of exploitation.

---

2. Nessus Scan & Reporting

Purpose:

Automate **Nessus vulnerability scans** and generate structured reports in **CSV or PDF format** for further analysis.

Key Features:

✅ **Automated Nessus Scan Execution:** Remotely triggers Nessus scans via API.
✅ **Report Generation:** Extracts scan results and exports them for compliance documentation.
✅ **Risk Prioritization:** Highlights **Critical, High, Medium, and Low-risk vulnerabilities**.

Use Case:

A security team can schedule daily scans to detect **outdated software, misconfigurations, and network weaknesses** before attackers exploit them.

---

3. SOC & SIEM Automation

Purpose:

Enhance **Security Operations Center (SOC) efficiency** by automating log collection and **threat intelligence processing** for SIEM solutions like **Splunk and IBM QRadar**.

Key Features:

✅ **Log Collection Automation:** Gathers security logs from **firewalls, servers, and endpoints** and forwards them to the SIEM.
✅ **Threat Intelligence Integration:** Fetches **Indicators of Compromise (IoCs) from MISP** and integrates them into SIEM for proactive defense.
✅ **Real-time Event Correlation:** Automatically analyzes logs to detect suspicious behavior patterns.

Use Case:

A SIEM system automatically correlates **failed login attempts, unusual network traffic, and malware detections**, alerting the SOC for investigation.

---

4. Incident Response Automation

Purpose:

Detect security incidents, categorize them based on severity, and **trigger automated alerts** to security analysts.

Key Features:

✅ **Incident Detection & Categorization:** Assigns severity levels to threats (e.g., **Critical, High, Medium, Low**).
✅ **Automated Alerting System:** Sends **email or SMS notifications** when a security breach is detected.
✅ **Incident Response Workflow:** Helps SOC teams **contain, analyze, and mitigate** threats efficiently.

Use Case:

When unauthorized access to a critical system is detected, the system automatically alerts **SOC analysts** and initiates an **account lockout** to prevent further compromise.

Conclusion

These **automated cybersecurity scripts** improve efficiency, reduce manual effort, and **enhance real-time threat detection and response**. By integrating automation into security operations, organizations can **identify, analyze, and mitigate threats faster**, ensuring a more resilient cybersecurity posture.