Automated Report

Report Summary

Overall Risk Rating: **Critical**

The overall risk rating, derived from the Risk Rating Matrix, reflects the average risk levels of identified vulnerabilities. This rating incorporates a 25% bias towards critical-level vulnerabilities and a 10% bias towards high-level vulnerabilities, effectively emphasising the most significant risks. The ARW tool assesses overall risk exposure, considering the potential impact of malicious actors attempting to exploit these vulnerabilities to compromise or control resources within the information environment. As such, the overall risk rating of **Critical** serves as an indicator for prioritising security efforts and implementing necessary safeguards.

Average CVSS Score: **8.54**

The Average CVSS Score provides a quantitative measure of the severity of identified vulnerabilities, calculated using the Common Vulnerability Scoring System (CVSS). The ARW tool computes the average score based on the highest CVSS values of detected vulnerabilities. For penetration testing tools that do not generate CVSS scores of detected vulnerabilities, the ARW will estimate the CVSS based on the risk level of the vulnerability. An Average CVSS Score of **8.54** underscores the need for focused attention on vulnerabilities that pose the greatest risk to the system's security and integrity.

Recommendations

Based on the results achieved during the penetration tests, the automated report generator makes the following recommendations (presented in order of priority):

- Patch **Critical** vulnerabilities:
  - Shellshock
  - MS17-010
  - BlueKeep
  - EternalBlue
  - Unauthorized Access
  - Denial of Service
- Run automated penetration testing tool on a **weekly** basis depending on the overall risk rating.

Scope

The following penetration testing tools were detected and processed by the ARW tool. Their results were used by the ARW to generate, where needed, an approximate risk rating, CVSS score, and recommendations:

- Metasploit
- Nmap
- Smod1

Metasploit Vulnerability Report

Host: 192.168.1.50

Vulnerability Name: MS08-067
Risk Level: High
CVSS Score: 7.0 - 8.9 (estimated from risk level)
Vulnerability Details:

> • Description: Remote code execution in Microsoft Windows Server 2008.
> • Result: Exploit successful: Command shell opened.

Vulnerability Name: Shellshock
Risk Level: Critical
CVSS Score: 9.0 - 10.0 (estimated from risk level)
Vulnerability Details:
- Description: Remote code execution in Bash.
- Result: Exploit successful: Remote access obtained.

Vulnerability Name: MS17-010
Risk Level: Critical
CVSS Score: 9.0 - 10.0 (estimated from risk level)
Vulnerability Details:
- Description: Remote code execution vulnerability in Microsoft Windows SMBv1.
- Result: Exploit successful: Meterpreter session opened.

Vulnerability Name: Heartbleed
Risk Level: Medium
CVSS Score: 4.0 - 6.9 (estimated from risk level)
Vulnerability Details:
- Description: Information disclosure vulnerability in OpenSSL.
- Result: Exploit successful: Sensitive information leaked.

Vulnerability Name: Poodle
Risk Level: Low
CVSS Score: 0.1 - 3.9 (estimated from risk level)
Vulnerability Details:
- Description: Man-in-the-middle attack vulnerability in SSL 3.0.
- Result: Exploit failed: Target not vulnerable.

Host: 192.168.1.51

Vulnerability Name: Apache Struts 2 OGNL Injection
Risk Level: High
CVSS Score: 7.0 - 8.9 (estimated from risk level)
Vulnerability Details:
- Description: Remote code execution vulnerability in Apache Struts 2.
- Result: Exploit successful: Command shell opened.

Vulnerability Name: BlueKeep
Risk Level: Critical
CVSS Score: 9.0 - 10.0 (estimated from risk level)
Vulnerability Details:
- Description: Remote code execution vulnerability in Microsoft Windows RDP.
- Result: Exploit successful: Remote access obtained.

Vulnerability Name: Spectre
Risk Level: Medium
CVSS Score: 4.0 - 6.9 (estimated from risk level)
Vulnerability Details:
- Description: Information disclosure vulnerability in CPUs.
- Result: Exploit successful: Sensitive information leaked.

Host: 192.168.1.52

Vulnerability Name: Meltdown
Risk Level: Medium
CVSS Score: 4.0 - 6.9 (estimated from risk level)
Vulnerability Details:
- Description: Information disclosure vulnerability in CPUs.
- Result: Exploit successful: Sensitive information leaked.

Vulnerability Name: EternalBlue
Risk Level: Critical
CVSS Score: 9.0 - 10.0 (estimated from risk level)
Vulnerability Details:

- Description: Remote code execution vulnerability in Microsoft Windows SMBv1.
- Result: Exploit successful: Remote access obtained.

Nmap Vulnerability Report

Host: 192.168.1.10

Service: Port 80 (TCP)
State: Open
Product: Apache httpd 2.4.38
Service Name: HTTP

Vulnerability Name: Clickjacking
Risk Level: Medium (estimated from name)
CVSS Score: 4.0 - 6.9 (estimated from risk level)
Vulnerability Details:

> Possible SQL injection vulnerability detected: URI: /index.php?id=1' Payload: id=1' OR '1'='1 Output: SQL error detected

Service: Port 3306 (TCP)
State: Open
Product: MySQL 5.7.23
Service Name: MYSQL

Vulnerability Name: Sql-injection
Risk Level: High (estimated from name)
CVSS Score: 7.0 - 8.9 (estimated from risk level)
Vulnerability Details:

> Possible SQL injection vulnerability detected: URI: /login.php Payload: username=admin' OR '1'='1 -- Output: Login successful

Host: 192.168.1.20

Service: Port 80 (TCP)
State: Open
Product: Apache httpd 2.4.38
Service Name: HTTP

Vulnerability Name: Sql-injection
Risk Level: High (estimated from name)
CVSS Score: 7.0 - 8.9 (estimated from risk level)
Vulnerability Details:

> Possible SQL injection vulnerability detected: URI: /view_data.php?record=5 Payload: record=5' AND 1=1 -- Output: SQL error detected

Service: Port 3306 (TCP)
State: Open
Product: MySQL 5.7.23
Service Name: MYSQL

Vulnerability Name: Sql-injection
Risk Level: High (estimated from name)
CVSS Score: 7.0 - 8.9 (estimated from risk level)

Vulnerability Details:

> Possible SQL injection vulnerability detected: URI: /data.php?id=3 Payload: id=3' UNION SELECT NULL, NULL, NULL -- Output: SQL error detected

Host: 192.168.1.30

Service: Port 80 (TCP)
State: Open
Product: Apache httpd 2.4.38
Service Name: HTTP

Vulnerability Name: Sql-injection
Risk Level: High (estimated from name)
CVSS Score: 7.0 - 8.9 (estimated from risk level)
Vulnerability Details:

> Possible SQL injection vulnerability detected: URI: /submit.php Payload: data=xyz' OR '1'='1 Output: SQL error detected

Service: Port 3306 (TCP)
State: Open
Product: MySQL 5.7.23
Service Name: MYSQL

Vulnerability Name: Sql-injection
Risk Level: High (estimated from name)
CVSS Score: 7.0 - 8.9 (estimated from risk level)
Vulnerability Details:

> Possible SQL injection vulnerability detected: URI: /info.php?item=7 Payload: item=7' AND 1=2 -- Output: SQL error detected

Smod-1 Report

Host: 192.168.1.80

Vulnerability Name: Unauthorized Access
Risk Level: Critical (estimated from name)
CVSS Score: 9.0 - 10.0 (estimated from risk level)
Vulnerability Details:

- Successfully gained access to the PLC and modified configuration settings.
- Timestamp: 2024-07-15T13:00:00

Host: 192.168.1.100

Vulnerability Name: Denial of Service
Risk Level: Critical (estimated from name)
CVSS Score: 9.0 - 10.0 (estimated from risk level)
Vulnerability Details:

- Successfully launched DoS attack causing PLC to crash.
- Timestamp: 2024-07-15T14:00:00
