NETWORK VULNERABILITY ASSESSMENT

EXTION INFOTECH PROJECT - I

BY

SELVA ARASU R

TABLE OF CONTENTS

Introduction

In very simple terms, vulnerability is nothing but a weakness in a system or a weakness in the safeguard/countermeasure. If a vulnerability is successfully exploited, it could result in loss or damage to the target asset. Some common examples of vulnerability are as follows:

- Weak password set on a system
- An unpatched application running on a system
- Lack of input validation causing XSS
- Lack of database validation causing SQL injection
- Antivirus signatures not updated

Vulnerabilities could exist at both the hardware and software level. A malware-infected BIOS is an example of hardware vulnerability while SQL injection is one of the most common software vulnerabilities.

Vulnerability Assessment VS. Pen Testing

Vulnerability assessment and penetration testing are quite often used interchangeably. However, both are different with respect to the purpose they serve. To understand the difference between the two terms, let's consider a real-world example. There is a bank that is located on the outskirts of a city and in quite a secluded area. There is a gang of robbers who intend to rob this bank. The robbers start planning on how they could execute their plan. Some of them visit the bank dressed as normal customers and note a few things:

- The bank has only one security guard who is unarmed
- The bank has two entrances and three exits
- There are no CCTV cameras installed
- The door to the locker compartment appears to be weak

With these findings, the robbers just did a vulnerability assessment. Now whether or not these vulnerabilities could be exploited in reality to succeed with the robbery plan would become evident only when they actually rob the bank. If they rob the bank and succeed in exploiting the vulnerabilities, they would have achieved penetration testing.

So, in a nutshell, checking whether a system is vulnerable is vulnerability assessment, whereas actually exploiting the vulnerable system is penetration testing. An organization may choose to do either or both as per their requirement. However, it's worth noting that a penetration test cannot be successful if a comprehensive vulnerability assessment hasn't been performed first.

Assessment Types

Based on the location the test is conducted from, the vulnerability assessment could be divided into two main types:

- External vulnerability assessment
- Internal vulnerability assessment

External vulnerability assessment

External vulnerability assessment is the best fit for assets exposed over public networks hosting public services. It is done from outside the target network and thus helps simulate

the actual scenario of a real attacker attacking the target. An external vulnerability assessment is mainly focused on the servers, infrastructure, and the underlying software components related to the target. This type of testing will involve in-depth analysis of publicly available information about the target, a network enumeration phase where all active target hosts are identified and analyzed, and the behavior of intermediate security screening devices such as firewalls. Vulnerabilities are then identified, verified, and the impact gets assessed. It is the most traditional approach to vulnerability assessment.

Internal vulnerability assessment

Internal vulnerability assessment is carried out on assets that are exposed to the private networks (internal to the company) hosting internal services. An internal vulnerability assessment is primarily conducted to ensure that the network insiders cannot gain unauthorized access to any of the systems by misusing their own privileges. The internal vulnerability assessment is used to identify weaknesses in a particular system inside the organization's network. When the vulnerability assessment team performs the tests from within the target network, all external gateways, filters, and firewalls get bypassed and the tests are targeted directly at the systems in scope. The internal vulnerability assessment may involve testing from various network segments to check virtual isolation.

Vulnerability Assessment using OpenVAS

Vulnerability Assessment includes probing each service for possible open vulnerabilities. There are many tools, both commercial as well as open source, available for performing vulnerability assessments. Some of the most popular tools are Nessus, Nexpose, and OpenVAS. OpenVAS is a framework consisting of several tools and services that provide an effective and powerful vulnerability management solution.

Scan Report

Summary

This document reports on the results of an security scan. The task was Immediate scan of IP 127.0.0.1. The report rst summarises the results found. Then, for each host, the report describes every issue found. We should consider the advice given in each description, in order to rectify the issue.

Result

1 Result Overview

Host	High	Medium	Low	Log	False Positive
127.0.0.1 localhost	0	2	0	0	0
Total: 1	0	2	0	0	0

Vendor security updates are not trusted.
Overrides are o. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report. Notes
are included in the report.
This report might not show details of all issues that were found. Issues
with the threat level Log are not shown.
Issues with the threat level Debug are not shown.
Issues with the threat level False Positive are not shown. Only
results with a minimum QoD of 70 are shown.

This report contains all 2 results selected by the Itering described above. Before Itering there were 27 results.

2 Results per Host

2.1 127.0.0.1

Host scan start Sat Aug 10 10:49:21 2024 UTC
Host scan end Sat Aug 10 10:56:25 2024 UTC

Service (Port)	Threat Level
1883/tcp	Medium
5432/tcp	Medium

2.1.1 Medium 1883/tcp

Medium (CVSS: 6.4) NVT: MQTT Broker Does Not Require Authentication
Summary The remote MQTT broker does not require authentication.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: Mitigation Enable authentication.
Vulnerability Detection Method Checks if authentication is required for the remote MQTT broker. Details: MQTT Broker Does Not Require Authentication OID:1.3.6.1.4.1.25623.1.0.140167 Version used: 2022-07-11T10:16:03Z
References url: https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-vo ⟷n-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html

2.1.2 Medium 5432/tcp

Medium (CVSS: 5.9) NVT: SSL/TLS: Report Weak Cipher Suites
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0. ⟷802067)
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are con gured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA

Solution:
Solution type: Mitigation
The con guration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

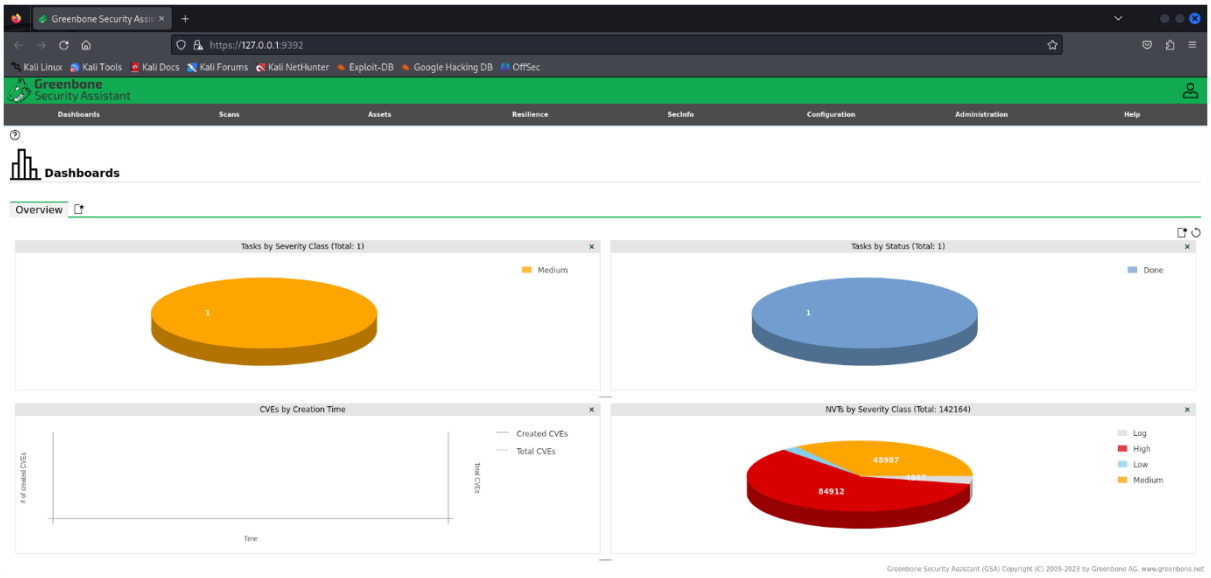
Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
Any other cipher is considered as strong

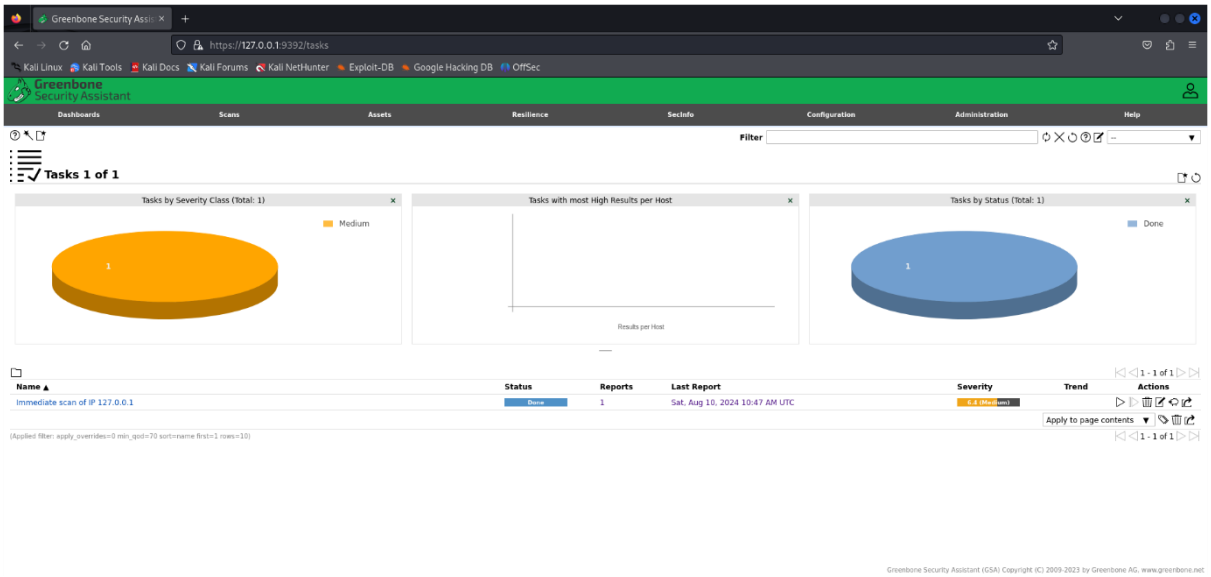
Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-06-14T05:05:48Z

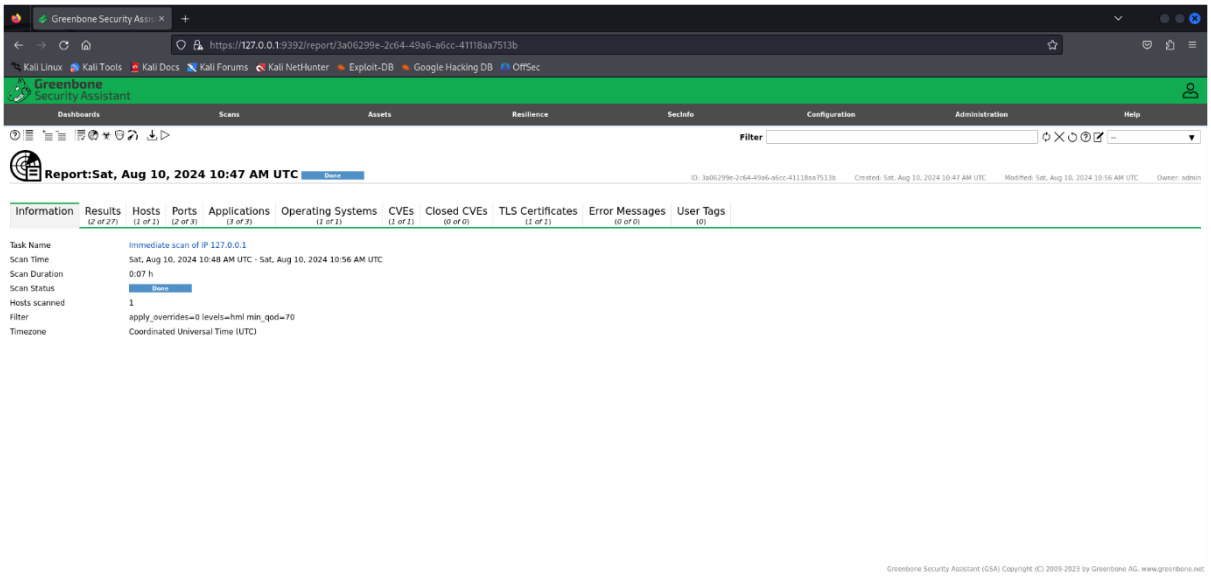
Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)

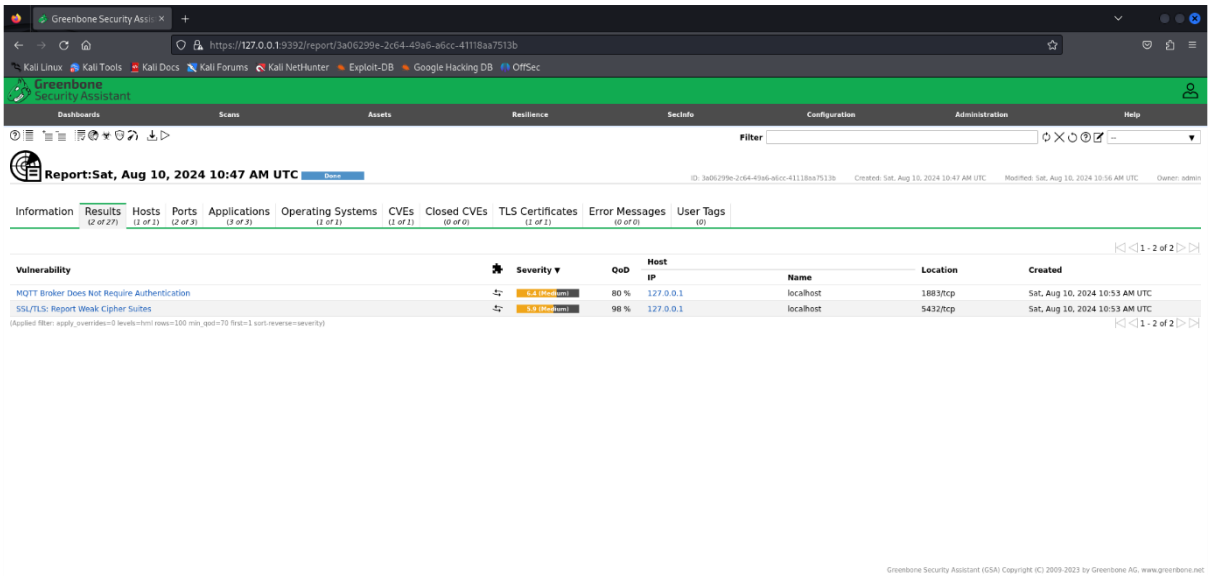
References
cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
⟷465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/

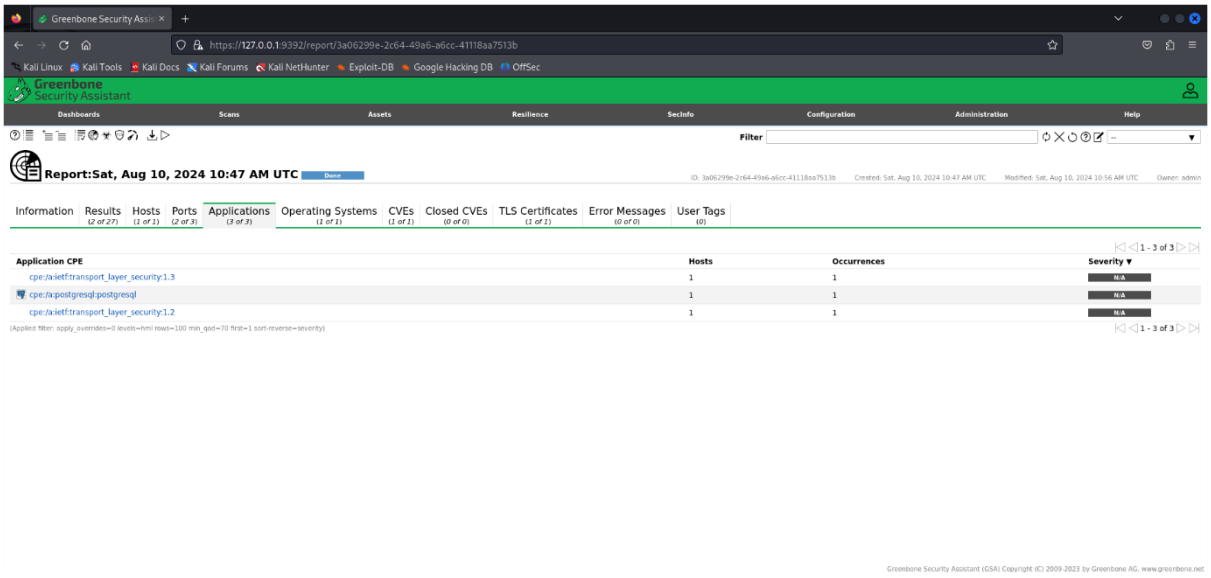
VISUAL DOCUMENTATION






Greenbone Security Assistant
https://127.0.0.1:9392/report/3a06299e-2c64-49a6-a6cc-41118aa7513b
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Sat, Aug 10, 2024 10:47 AM UTC Done
ID: 3a06299e-2c64-49a6-a6cc-41118aa7513b Created: Sat, Aug 10, 2024 10:47 AM UTC Modified: Sat, Aug 10, 2024 10:56 AM UTC Owner: admin
Information Results (2 of 27) Hosts (1 of 1) Ports (2 of 3) Applications (3 of 3) Operating Systems (1 of 1) CVEs (1 of 1) Closed CVEs (0 of 0) TLS Certificates (1 of 1) Error Messages (0 of 0) User Tags (0)
Task Name Immediate scan of IP 127.0.0.1
Scan Time Sat, Aug 10, 2024 10:48 AM UTC - Sat, Aug 10, 2024 10:56 AM UTC
Scan Duration 0:07 h
Scan Status Done
Hosts scanned 1
Filter apply_overrides=0 levels=hml min_qod=70
Timezone Coordinated Universal Time (UTC)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net


Greenbone Security Assistant
https://127.0.0.1:9392/report/3a06299e-2c64-49a6-a6cc-41118aa7513b
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Sat, Aug 10, 2024 10:47 AM UTC Done
ID: 3a06299e-2c64-49a6-a6cc-41118aa7513b Created: Sat, Aug 10, 2024 10:47 AM UTC Modified: Sat, Aug 10, 2024 10:56 AM UTC Owner: admin
Information Results (2 of 27) Hosts (1 of 1) Ports (2 of 3) Applications (3 of 3) Operating Systems (1 of 1) CVEs (1 of 1) Closed CVEs (0 of 0) TLS Certificates (1 of 1) Error Messages (0 of 0) User Tags (0)
1 - 2 of 2
Vulnerability Severity QoD Host IP Name Location Created
MQTT Broker Does Not Require Authentication 6.4 (Medium) 80 % 127.0.0.1 localhost 1883/tcp Sat, Aug 10, 2024 10:53 AM UTC
SSL/TLS: Report Weak Cipher Suites 5.9 (Medium) 98 % 127.0.0.1 localhost 5432/tcp Sat, Aug 10, 2024 10:53 AM UTC
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 2 of 2
Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net


Greenbone Security Assistant
https://127.0.0.1:9392/report/3a06299e-2c64-49a6-a6cc-41118aa7513b
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Sat, Aug 10, 2024 10:47 AM UTC Done
ID: 3a06299e-2c64-49a6-a6cc-41118aa7513b Created: Sat, Aug 10, 2024 10:47 AM UTC Modified: Sat, Aug 10, 2024 10:56 AM UTC Owner: admin
Information Results (2 of 27) Hosts (1 of 1) Ports (2 of 3) Applications (3 of 3) Operating Systems (1 of 1) CVEs (1 of 1) Closed CVEs (0 of 0) TLS Certificates (1 of 1) Error Messages (0 of 0) User Tags (0)
1 - 3 of 3
Application CPE Hosts Occurrences Severity
cpe:/a:ietf:transport_layer_security:1.3 1 1 N/A
cpe:/a:postgresql:postgresql 1 1 N/A
cpe:/a:ietf:transport_layer_security:1.2 1 1 N/A
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 3 of 3
Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net