

Part 2 : Find vulnerabilities in openVas

In this write-up you will find the process for finding the linux scan vulnerabilities.

Repeat the same process for finding the windows vulnerabilities.

1. Go to the reports page.

You will have two reports.

Each report contains information about one scan.

2. Click on the report date of the linux scan [Thu, Aug 8, 2024, 7:32pm].

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

3. Click on the results tab next to information

The screenshot displays the Greenbone Security Assistant (GSA) web interface in a Chrome browser. The address bar shows the URL `https://127.0.0.1:9392/report/99642ce9-3683-4d53-9afb-6f17e03bb8c9`. The interface has a green header with the GSA logo and navigation tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the header is a toolbar with various icons and a filter input field. The main content area shows a scan report for a target named 'Repo', dated 'Thu, Aug 8, 2024 7:32 PM UTC'. A red arrow points to the 'Results' tab in the report's navigation bar. The 'Results' tab is active, showing a table with columns: Information, Results (2 of 21), Hosts (1 of 1), Ports (0 of 2), Applications (1 of 1), Operating Systems (1 of 1), CVEs (1 of 1), Closed CVEs (0 of 0), TLS Certificates (0 of 0), Error Messages (0 of 0), and User Tags (0). The 'Information' section is expanded, showing details about the scan task 'Luis scan linux', including the scan time, duration, status (Done), and filter.

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Repo Thu, Aug 8, 2024 7:32 PM UTC

Done

ID: 99642ce9-3683-4d53-9afb-6f17e03bb8c9 Created: Thu, Aug 8, 2024 7:32 PM UTC Modified: Thu, Aug 8, 2024 7:46 PM UTC Owner: admin

Information Results (2 of 21) Hosts (1 of 1) Ports (0 of 2) Applications (1 of 1) Operating Systems (1 of 1) CVEs (1 of 1) Closed CVEs (0 of 0) TLS Certificates (0 of 0) Error Messages (0 of 0) User Tags (0)

Task Name Luis scan linux

Scan Time Thu, Aug 8, 2024 7:33 PM UTC - Thu, Aug 8, 2024 7:46 PM UTC

Scan Duration 0:12 h

Scan Status Done

Hosts scanned 1

Filter apply_overrides=0 levels=hml min_qod=70

Timezone Coordinated Universal Time (UTC)

4. View the list of vulnerabilities for linux host

For the linux scan, we have two vulnerabilities.

Information	Results (2 of 21)	Hosts (1 of 1)	Ports (0 of 2)	Applications (1 of 1)	Operating Systems (1 of 1)	CVEs (1 of 1)	Closed CVEs (0 of 0)	TLS Certificates (0 of 0)	Error Messages (0 of 0)	User Tags (0)	
<div>⏪ ⏩ 1 - 2 of 2 ⏪ ⏩</div>											
Vulnerability						Severity ▼	QoD	Host IP	Name	Location	Created
TCP Timestamps Information Disclosure						<div><div></div>2.6 (Low)</div>	80 %	10.0.2.15		general/tcp	Thu, Aug 8, 2024 7:38 PM UTC
ICMP Timestamp Reply Information Disclosure						<div><div></div>2.1 (Low)</div>	80 %	10.0.2.15		general/icmp	Thu, Aug 8, 2024 7:38 PM UTC
<div>(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)</div>											
<div>⏪ ⏩ 1 - 2 of 2 ⏪ ⏩</div>											

5. View the details of a specific vulnerability

If you click on the first vulnerability [TCP timestamps information disclosure], you will see the summary, detection results, etc.

Vulnerability

Severity ▼

QoD

Host
IP

Name

Location

Created

TCP Timestamps Information Disclosure

2.6 (Low)

80 %

10.0.2.15

general/tcp

Thu, Aug 8, 2024
7:38 PM UTC

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Detection Result

It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 432635952
Packet 2: 432637030

Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.