Part 2 : Find vulnerabilities in openVas

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

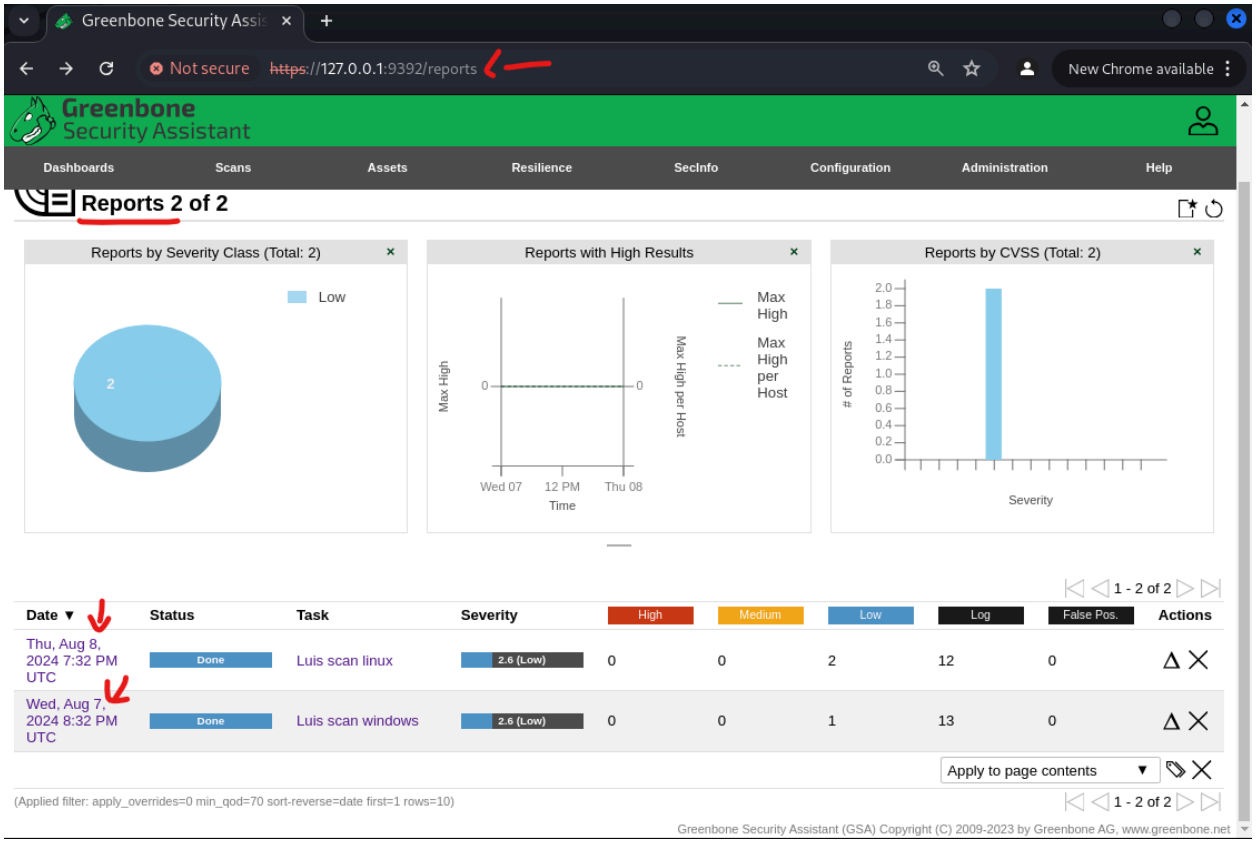
Repeat the same process for finding the windows vulnerabilities.

1. Go to the reports page.

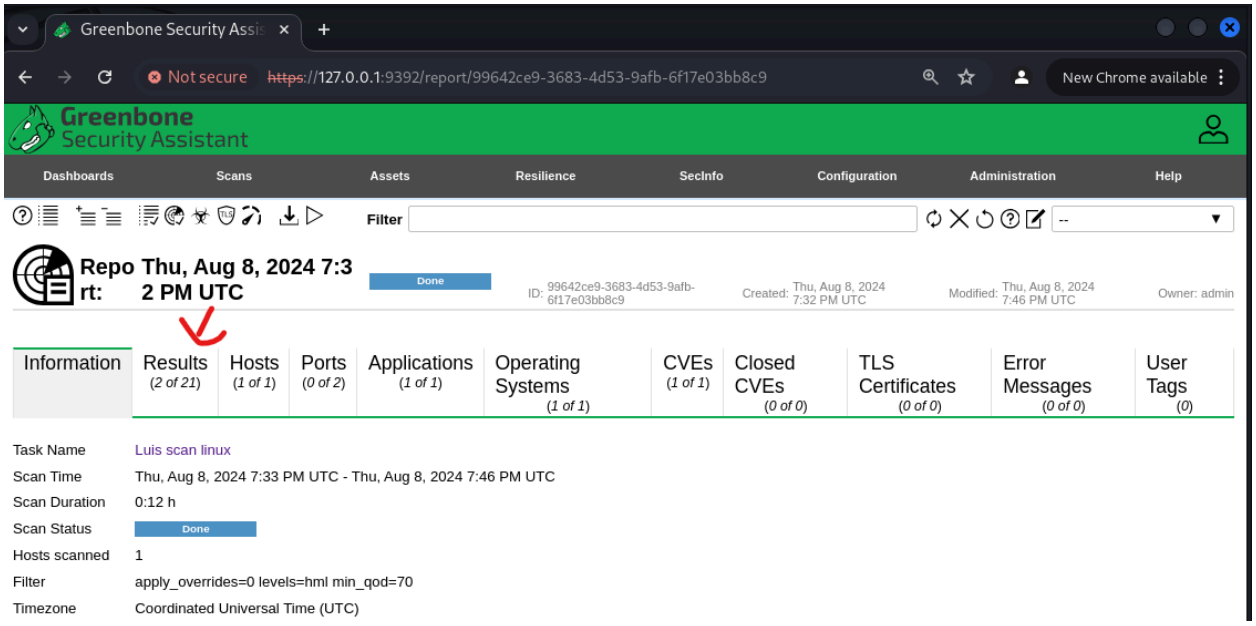
You will have two reports.

Each report contains information about one scan.

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

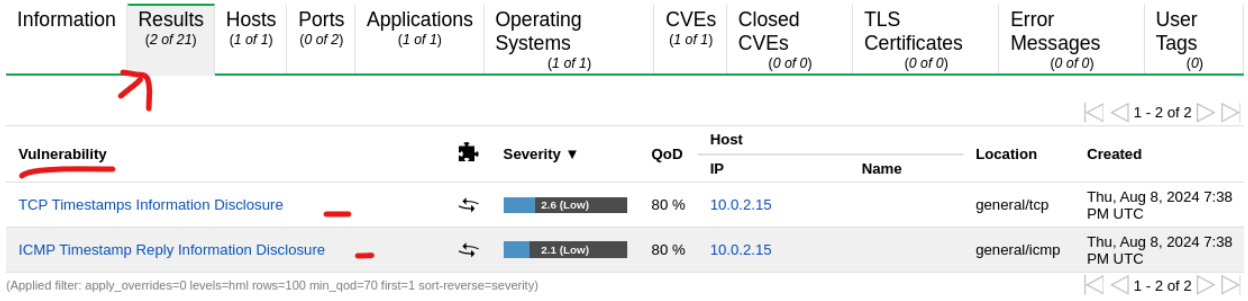


3. Click on the results tab next to information



4. View the list of vulnerabilities for linux host

For the linux scan, we have two vulnerabilities.



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		Location	Created
				IP	Name		
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.