

Performing a Vulnerability Scan with Greenbone

By

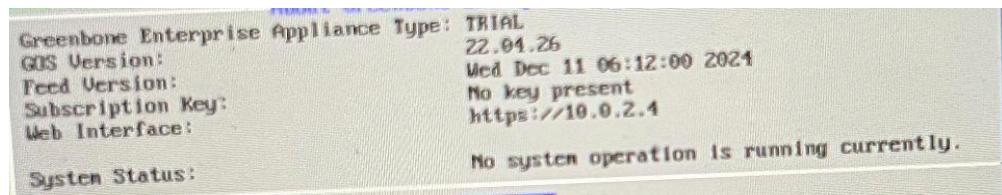
Russell Robinson

Vulnerability scanning is a critical step in identifying security weaknesses within a system or network. Using Greenbone Vulnerability Manager, you can efficiently detect, analyze, and address vulnerabilities in your target systems. This guide walks through the process of setting up and running a vulnerability scan, including configuring your Greenbone VM, connecting to your target machine, and interpreting the results.

1. Start Greenbone VM

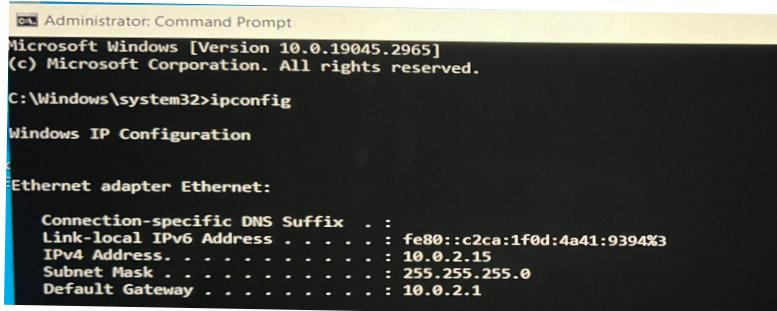
I started my Greenbone VM, logged in with my username and password, and located the IP address to access my Greenbone account for performing a vulnerability scan.

```
Welcome to Greenbone OS 22.04.26 (tty1)
The web interface is available at:
http://10.0.2.4
gsm login: _
```



2. Start Windows 10 Target Machine

I started my Windows 10 target machine, opened the terminal under administrator, and typed ipconfig at the prompt to retrieve the IP address. I saved this IP address in my notes.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

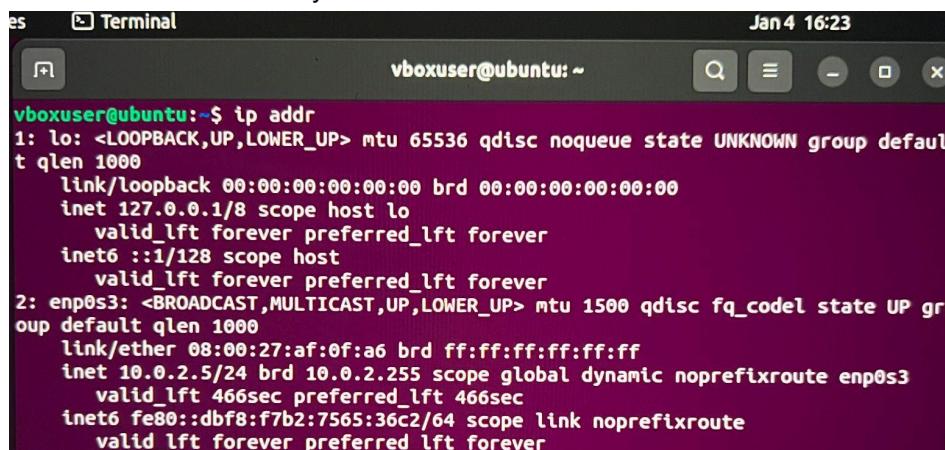
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c2ca:1f0d:4a41:9394%3
IPv4 Address . . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1
```

3. Start Ubuntu Machine

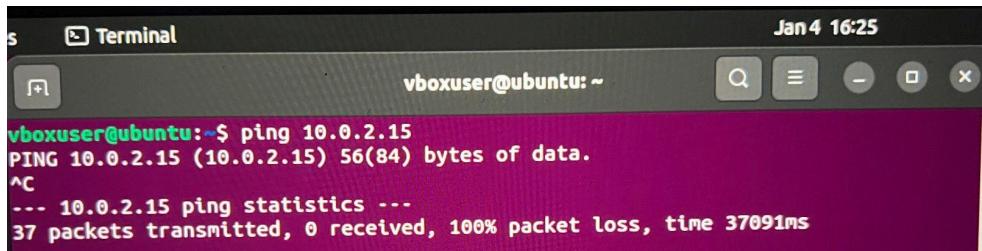
I started my Ubuntu machine, logged in, opened the terminal, and entered the command ip addr to get my IP address. I saved it in my notes and closed the terminal.



```
vboxuser@ubuntu:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:af:0f:a6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 466sec preferred_lft 466sec
    inet6 fe80::dbf8:f7b2:7565:36c2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

4. Ping the Target Machine

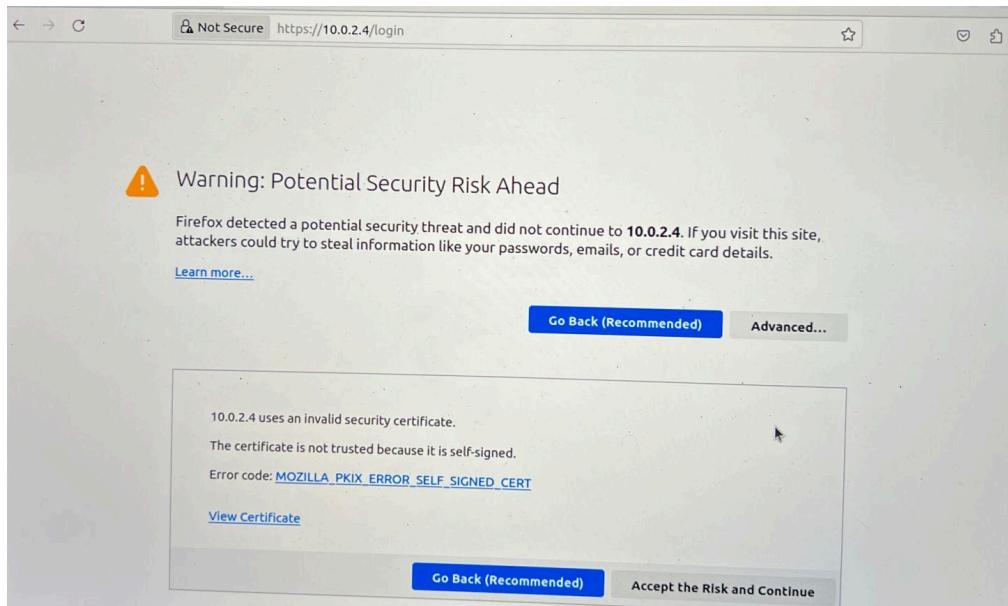
I opened a new terminal and entered the command ping <IP address> (using the IP address of the target machine) to establish a connection. Once the connection was established, I pressed Ctrl + C to stop the ping.

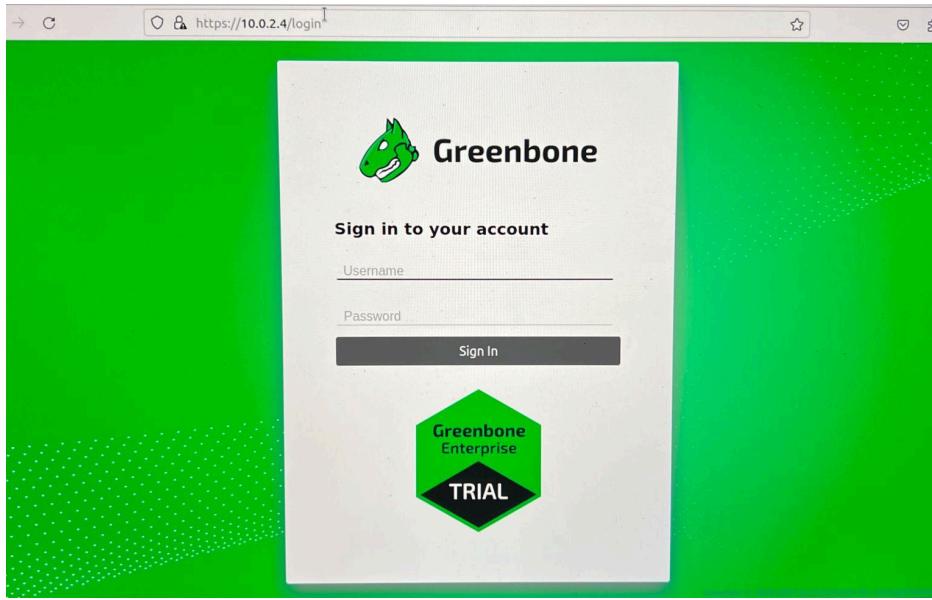


```
vboxuser@ubuntu:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
^C
--- 10.0.2.15 ping statistics ---
37 packets transmitted, 0 received, 100% packet loss, time 37091ms
```

5. Access Greenbone VM

In my Firefox browser, I used the IP address of my Greenbone VM: [https://<IP address>](https://10.0.2.4). A warning screen appeared; I scrolled down and clicked "Accept Risk" to access the Greenbone login page.





6. Configure Greenbone Targets

I navigated to the **Configuration** section and selected **Targets**. I clicked **Create New Target** and gave the target a name (*Windows 10*). In the **Host** section, I entered the IP address of the target machine and clicked **Save**.

A screenshot of a Firefox browser window showing the Greenbone Enterprise Appliance configuration interface. The URL is https://10.0.2.4/targets. The page has a green header with the Greenbone logo and navigation links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The Configuration menu is open, and the Targets option is selected. The main content area shows a summary: "Targets 0 of 0" and "No targets available". A note at the bottom says "(Applied filter: sort=name first=1 rows=10)". On the right side, there is a sidebar with a "Targets" section containing links: Port Lists, Credentials, Scan Configs, Report Formats, Scanners, Filters, and Tags. A cursor is hovering over the "Targets" link.

The screenshot shows two overlapping windows from the Greenbone Enterprise Appliance web interface.

The top window is the main 'Targets' page. It has a green header bar with the 'Greenbone Enterprise Appliance' logo. Below the header are navigation tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. A search bar labeled 'Filter' is at the top right. The main content area shows a button labeled 'New Target' and a message 'Targets 0 of 0'. Below this, it says 'No targets available'.

The bottom window is a modal dialog titled 'New Target'. It contains fields for 'Name' (set to 'windows 10'), 'Comment' (empty), and 'Hosts' (set to 'Manual' with IP '10.0.2.15'). There are also sections for 'Exclude Hosts', 'Allow simultaneous scanning via multiple IPs' (set to 'Yes'), 'Port List' (set to 'All IANA assigned TCP'), and 'Alive Test' (set to 'Scan Config Default'). Under 'Credentials for authenticated checks', there are fields for 'SSH' (port 22) and 'SMB'. At the bottom of the dialog are 'Cancel' and 'Save' buttons, with 'Save' being highlighted.

7. Create a Scan Task

I selected the **Scans** section, then chose **Tasks** and clicked **Create New Task**. named the task (*Scan Windows 10*) and selected the target I created (*Windows 10*) from the **Scan Targets** dropdown. Finally, I saved the task.

Firefox Web Browser Jan 4 16:51

Greenbone Enterprise Appliance https://10.0.2.4/tasks

Dashboard Scans Assets Resilience SecInfo Configuration Administration Help

Tasks 0 ✓ Tasks by Results per Host Tasks with most High Results per Host Tasks by Status (Total: 0)

No Tasks available
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

This screenshot shows the Greenbone Enterprise Appliance dashboard for the URL https://10.0.2.4/tasks. The top navigation bar includes links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The main menu on the left has 'Tasks' selected, with sub-options for Reports, Results, Vulnerabilities, Notes, and Overrides. The central area displays three cards: 'Tasks with most High Results per Host' (empty), 'Tasks by Status (Total: 0)' (empty), and 'Results per Host' (empty). A message at the bottom states 'No Tasks available' and provides a note about the applied filter: '(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)'.

Firefox Web Browser

Greenbone Enterprise Appliance https://10.0.2.4/tasks

Dashboard Scans Assets Resilience SecInfo Configuration Administration Help

New Task New Container Task Tasks 0 of 0

Tasks by Severity Class (Total: 0) Tasks with most High Results per Host Tasks by Status (Total: 0)

No Tasks available

This screenshot shows the same Greenbone Enterprise Appliance dashboard as the previous one, but with a new task listed in the main menu under 'Tasks'. The 'New Task' option is highlighted. The central area shows the same three empty cards as the first screenshot. A message at the bottom states 'No Tasks available'.

Tasks 0 of 0

Tasks by Severity

No Tasks available

(Applied filter: apply_overrides=0 min)

New Task

Name: scan windows 10

Comment:

Scan Targets: windows 10

Add results to Assets: Yes No

Apply Overrides: Yes No

Min QoD: 70

Alterable Task: Yes No

Auto Delete Reports: Do not automatically delete reports Automatically delete oldest reports but always keep newest reports

Scanner: OpenVAS Default

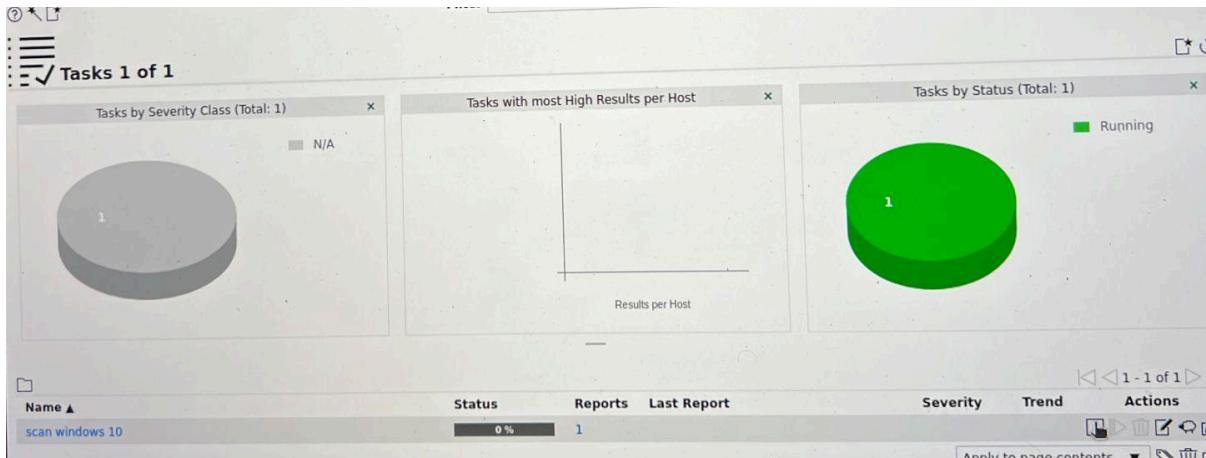
Scan Config: Full and fast

Order for target hosts: Sequential

Maximum concurrently executed NVTs per host: 4

Cancel **Save**

8. **Run the Scan** From the dashboard, I started the scan I had created. I monitored the progress, and once the status reached **100%**, the scan was complete.



The screenshot shows the Greenbone Enterprise Appliance dashboard under the 'Tasks' section. It displays three main cards:

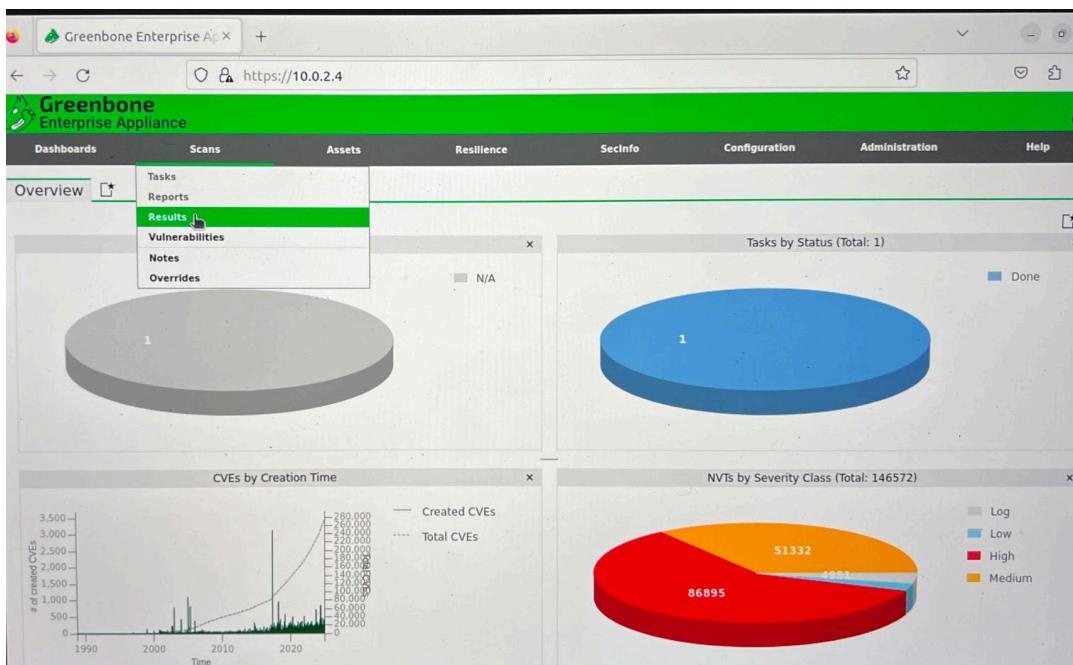
- Tasks by Severity Class (Total: 1)**: A pie chart showing 1 task in the 'Log' category.
- Tasks with most High Results per Host**: A card showing 'Results per Host' with no data displayed.
- Tasks by Status (Total: 1)**: A pie chart showing 1 task in the 'Done' category.

Below the cards, there is a detailed view of a single task:

- Status**: Done
- Reports**: 1
- Last Report**: Sun, Jan 5, 2025 12:55 AM UTC
- Severity**: 0.0 (Log)
- Trend**: 1 - 1
- Activity**: 0

At the bottom, there is a filter bar: `filter: apply_overrides=0 min_qod=70 sort=name first=10 rows=10`.

9. Review Results Under the **Scans** section, I selected **Results** to view any vulnerabilities discovered during the scan. Vulnerabilities were listed by their severity. By double-clicking on a vulnerability, I accessed a summary with references such as CVE, CERT, and other resources providing instructions on how to address the issue.



The screenshot shows the Greenbone Enterprise Appliance web interface. At the top, there's a navigation bar with links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the navigation bar, there's a table with two rows of data. The first row is for 'OS Detection Consolidation and Reporting' and the second for 'Traceroute'. Both rows show a status of '0.0 (Log)', 80% completion, and an IP address of 10.0.2.15. To the right of the table, there are two timestamped entries: 'Sun, Jan 5, 2025 1:15 AM UTC' and 'Sun, Jan 5, 2025 1:15 AM UTC'. On the left side of the main content area, there's a sidebar with a search icon and a 'Summary' section. The 'Summary' section contains a brief description of what tracerouting does. Below it is a 'Detection Result' section which lists the network route from the scanner to the target. It shows the scanner's IP (10.0.2.4) and the target's IP (10.0.2.15). It also states that the network distance between them is 2. There's also an 'Insight' section with a note about network distances, a 'Detection Method' section with details about the protocol used, and a 'Details' section with the OID and version information.

Greenbone Enterprise Appliance

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

	IP	Name	
OS Detection Consolidation and Reporting	0.0 (Log)	80 % 10.0.2.15	general/tcp Sun, Jan 5, 2025 1:15 AM UTC
Traceroute	0.0 (Log)	80 % 10.0.2.15	general/tcp Sun, Jan 5, 2025 1:15 AM UTC

Summary

Collect information about the network route and network distance between the scanner host and the target host.

Detection Result

Network route from scanner (10.0.2.4) to target (10.0.2.15):

10.0.2.4
10.0.2.15

Network distance between scanner and target: 2

Insight

For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Detection Method

A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.

Details: Traceroute OID: 1.3.6.1.4.1.25623.1.0.51662

Version used: 2022-10-17T11:13:19Z

Copyright © 2009-2024 by Greenbone Networks. 2025-11-17

Conclusion

This project demonstrated a full vulnerability scanning workflow using Greenbone. Key skills included configuring virtual environments, performing network tests, and analyzing scan results. With zero severity findings, the project emphasized the importance of regular vulnerability assessments and proactive security measures.

