Greenbone Security Manager (GSM) and Metasploitable

Overview

This project demonstrates practical experience in setting up and performing vulnerability assessments in a controlled lab environment. The lab focused on deploying **Greenbone Security Manager (GSM)**, configuring a virtualized network environment, and scanning a deliberately vulnerable machine (**Metasploitable**) to identify and analyze security weaknesses.

This exercise replicates real-world vulnerability management workflows commonly used in enterprise security operations.

Objectives

- Install and configure **Greenbone Security Manager Trial** on VirtualBox.
- Run and manage multiple virtual machines simultaneously within a secure, isolated network.
- Perform **Nmap** and **OpenVAS/GSM vulnerability scans** against the Metasploitable target.
- Analyze scan results and verify detected vulnerabilities.

Environment Setup

This lab required running the following virtual machines concurrently:

1. **Outside-Firewall** – Provided internet connectivity and DNS resolution.
2. **Client2-DMZ** – Used as a management workstation to initiate scans.
3. **Greenbone Security Manager (GSM)** – Hosted the OpenVAS vulnerability scanning engine.
4. **Metasploitable** – A vulnerable Linux system serving as the target host.

Configuration Steps

1. Import and Configure GSM Virtual Machine in VirtualBox

- Downloaded the **GSM Trial OVA** file from Greenbone's official site.
- Opened VirtualBox → **File** → **Import Appliance**, selected the .ova file (GSM-TRIAL-21.04.5-VirtualBox.ova) → Clicked **Import**.
- After import completed, updated GSM VM settings as follows:

- **Display → Graphics Controller:** VMSVGA
- **System → Processor:** Reduced to 1 CPU core
- **System → Motherboard:** Set Base Memory to 3072 MB
- **Network → Adapter 1:**
  - Enabled Adapter
  - Attached to: Internal Network
  - Name: DMZ

This configuration ensured that GSM operated within the same VLAN as other DMZ systems.

---

2. Start GSM and Configure Networking

- Powered on the GSM virtual machine while **Outside-Firewall** was active.
- Logged in using default credentials:
  - Username: admin
  - Password: admin

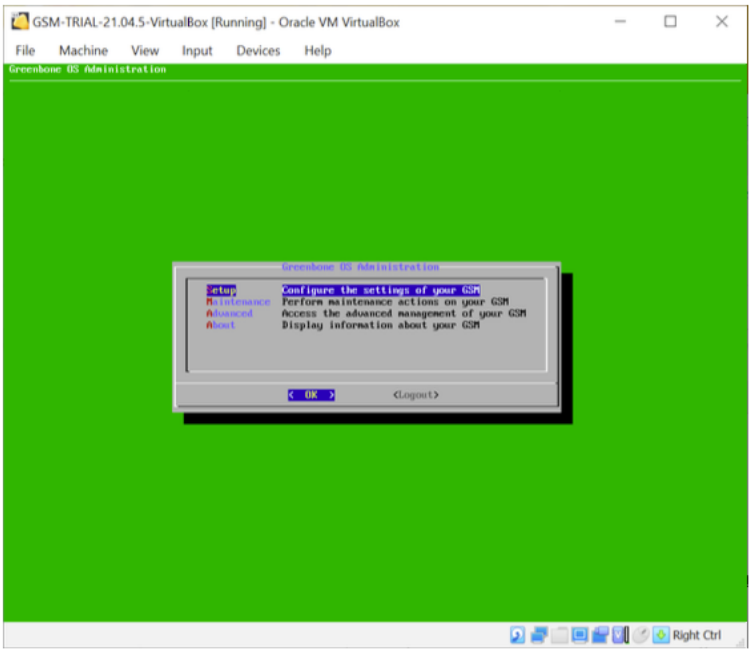

Figure 1/GSM

- In the GSM console, navigated to **Setup → Networking → Interfaces**.
- Enabled **IPv4** and **Static IP**, then entered:
  - IP Address: 192.168.4.80/24

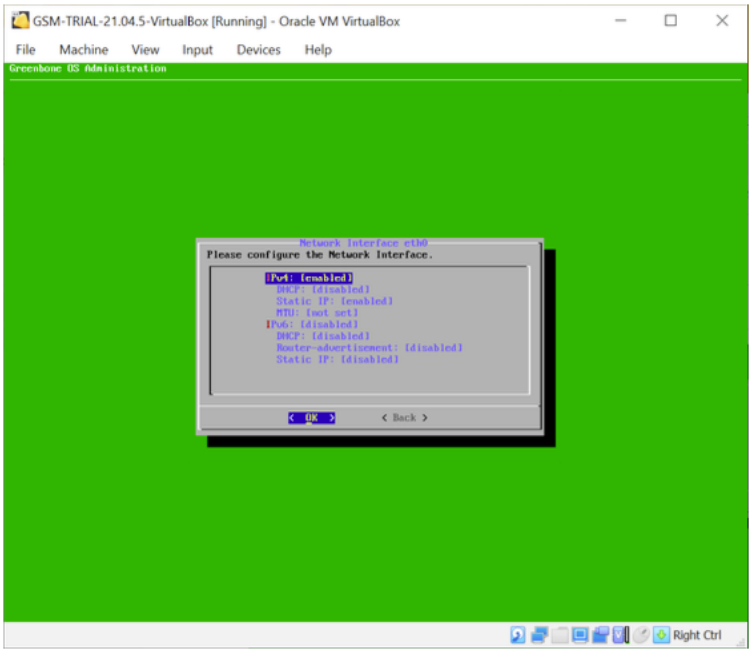

Figure 2/Networking

- Configured **DNS** under **Networking → DNS**:
  - DNS Servers: 8.8.8.8, 1.1.1.1, 192.168.4.1

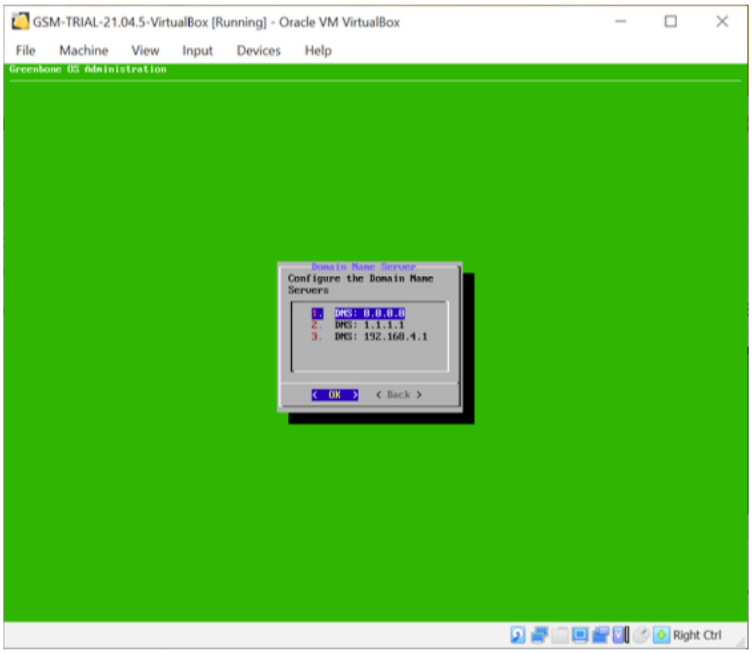

Figure 3/Dns

- Set the **Global Gateway** to:
  - 192.168.4.1 (Outside-Firewall)

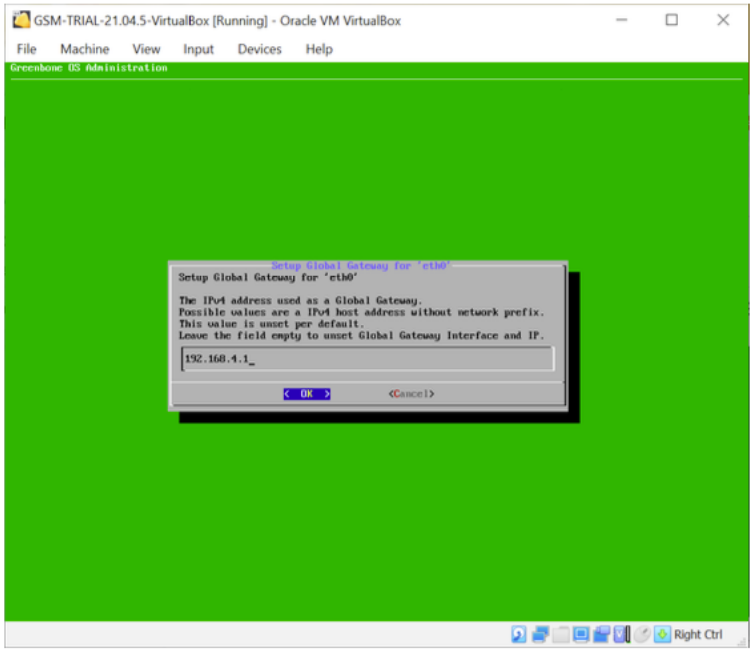

Figure 4/Gateway

- Navigated to **User and Password Management → Manage Web Users**, created a new global admin account for GSM web access.
- Noted the web interface URL:
  - https://192.168.4.80

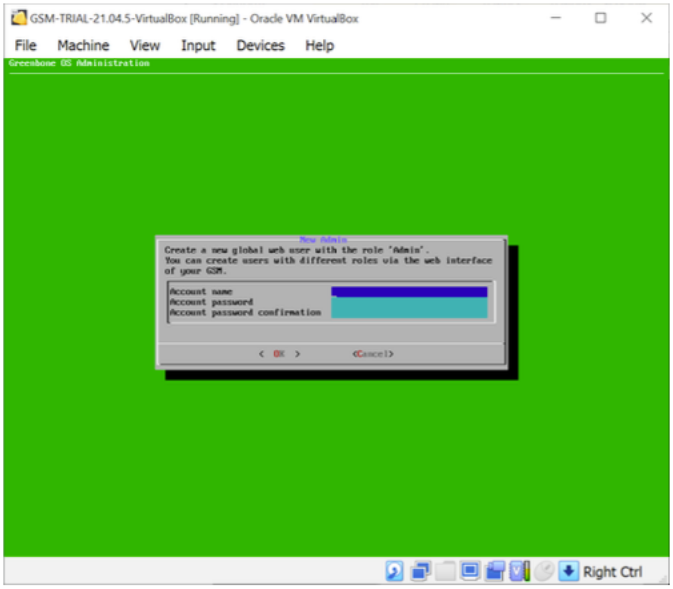

Figure 5/Users

3. Import and Configure Metasploitable Virtual Machine

- Downloaded **Metasploitable 2** from SourceForge (https://sourceforge.net/projects/metasploitable/).
- Extracted the ZIP file to reveal Metasploitable.vmdk.
- In VirtualBox, created a new VM named "Metasploitable":
  - Type: Linux
  - Version: Ubuntu (32-bit)
  - Selected **Use an existing virtual hard disk file** → Browsed to Metasploitable.vmdk.
- Configured the network:
  - **Adapter 1 → Attached to:** Internal Network
  - **Name:** DMZ

---

4. Configure Static IP on Metasploitable

- Started the Metasploitable VM.
- Logged in with:
  - Username: msfadmin
  - Password: msfadmin
- Assigned a static IP:
- sudo ifconfig eth0 192.168.4.85 netmask 255.255.255.0 up
- sudo route add default gw 192.168.4.1
- Verified connectivity:
- ping -c 4 192.168.4.1

  Successful replies confirmed connection to the Outside-Firewall.

---

5. Verify Connectivity Between Client2-DMZ, GSM, and Metasploitable

- Started **Client2-DMZ** virtual machine.
- Verified connectivity to all systems in the DMZ VLAN:
- ping -c 4 192.168.4.85 # Metasploitable
- ping -c 4 192.168.4.80 # GSM
- ping -c 4 192.168.4.1 # Firewall Gateway
- All responses were successful, confirming proper DMZ network configuration.

---

6. Conduct Nmap Reconnaissance Scan

- Opened Terminal on **Client2-DMZ** and executed:
- nmap -sS -sV -A -T4 192.168.4.85 -oN ~/nmap-metasploitable.txt
  - -sS: Stealth SYN scan

    - -sV: Service version detection
    - -A: OS and service script detection
    - -T4: Aggressive timing for faster results
- Saved the results as nmap-metasploitable.txt.
- The output revealed multiple open services such as:
    - FTP (21/tcp)
    - SSH (22/tcp)
    - Telnet (23/tcp)
    - HTTP (80/tcp)
    - MySQL (3306/tcp)
    - SMB (445/tcp)

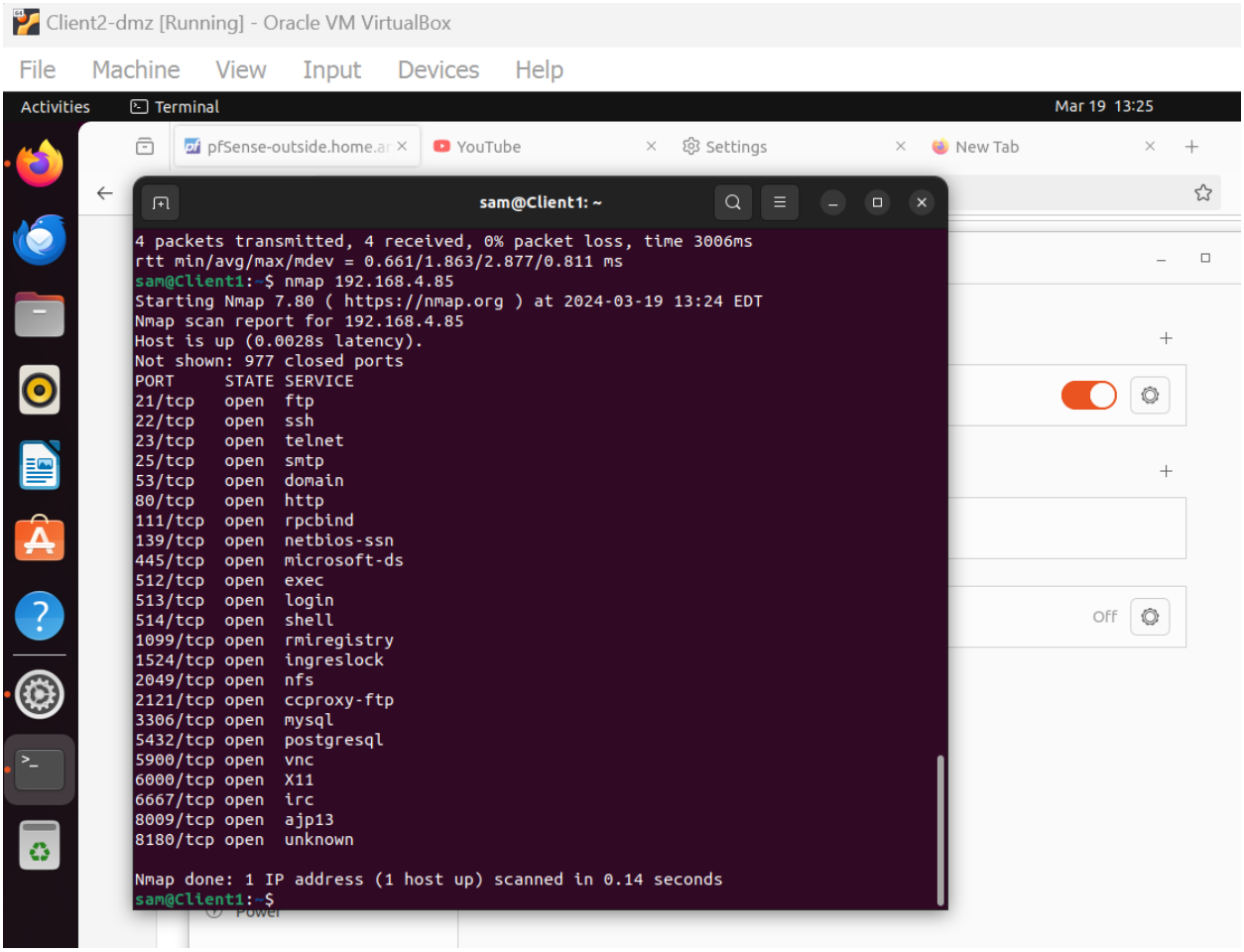

Figure 6/Nmap

---

7. Perform GSM Vulnerability Scan Against Metasploitable

- Opened Firefox on **Client2-DMZ** → navigated to https://192.168.4.80.
- Accepted the browser's SSL certificate warning (self-signed certificate).

- Logged into GSM web interface using the admin credentials.
- Navigated to **Scans → Tasks → Task Wizard**.

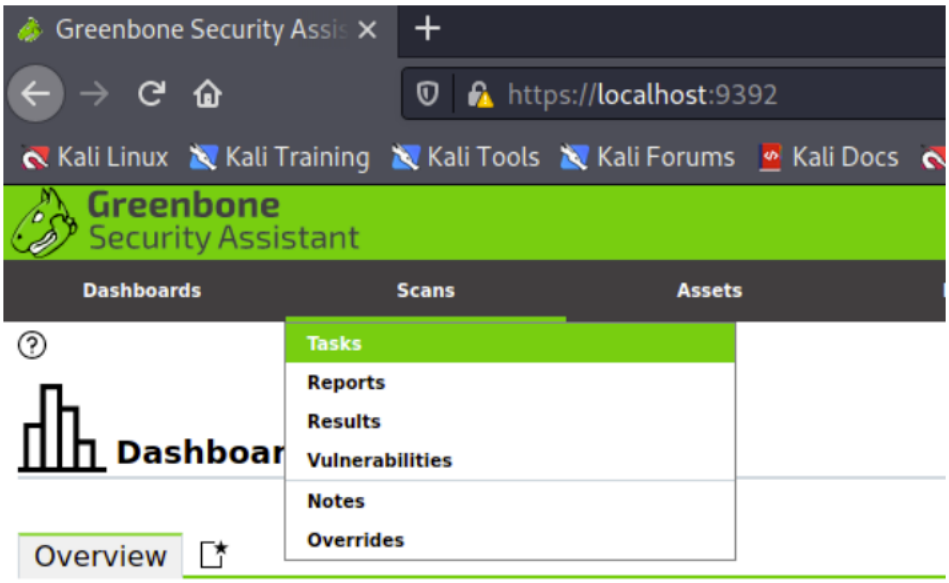

Figure 7/Tasks

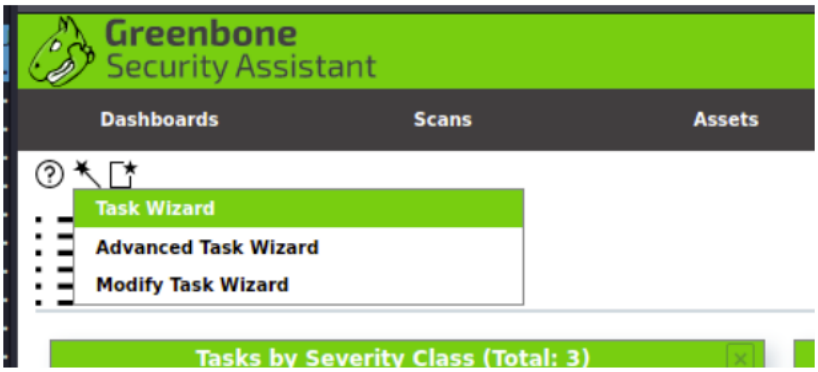

Figure 8/Task Wizard

- Entered the target IP: 192.168.4.85 and selected **Full and Fast** scan configuration.

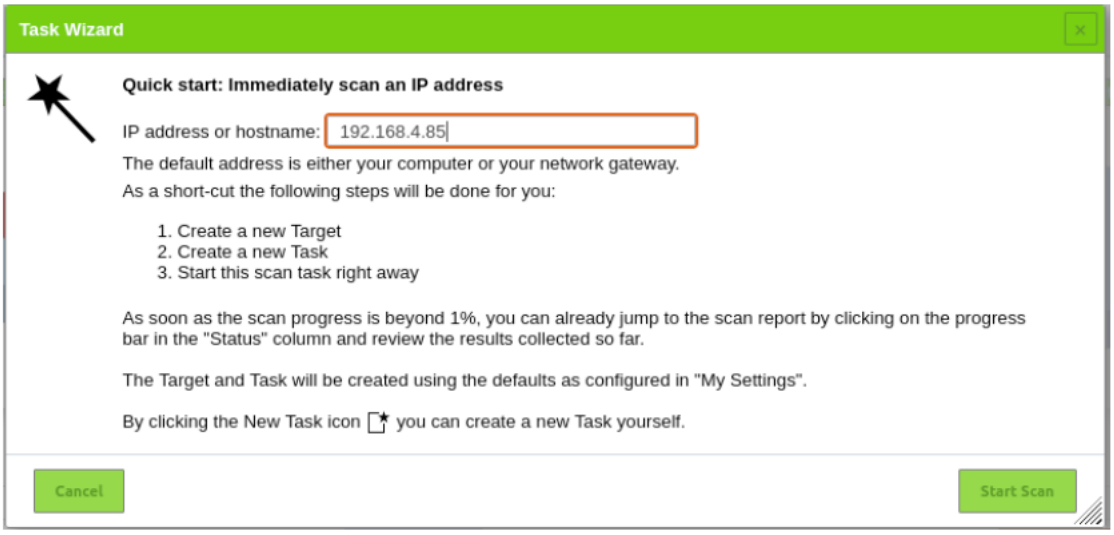

Figure 9/Scan

- Clicked **Start Scan** to begin the vulnerability assessment.

The scan transitioned through stages:

- *Requested → Queued → Running → Done*
  and took approximately 30 minutes to complete.

---

8. Analyze GSM Scan Results

- After completion, clicked **Done → Report → Results**.
- The scan identified several high-severity vulnerabilities, including:
  - Outdated services (e.g., Apache, Samba, MySQL).
  - Known CVEs associated with remote code execution and privilege escalation.
  - Weak SSH and Telnet configurations.
- Exported the results as an HTML report and saved screenshots of:
  - The completed scan summary.
  - The high-severity findings list.

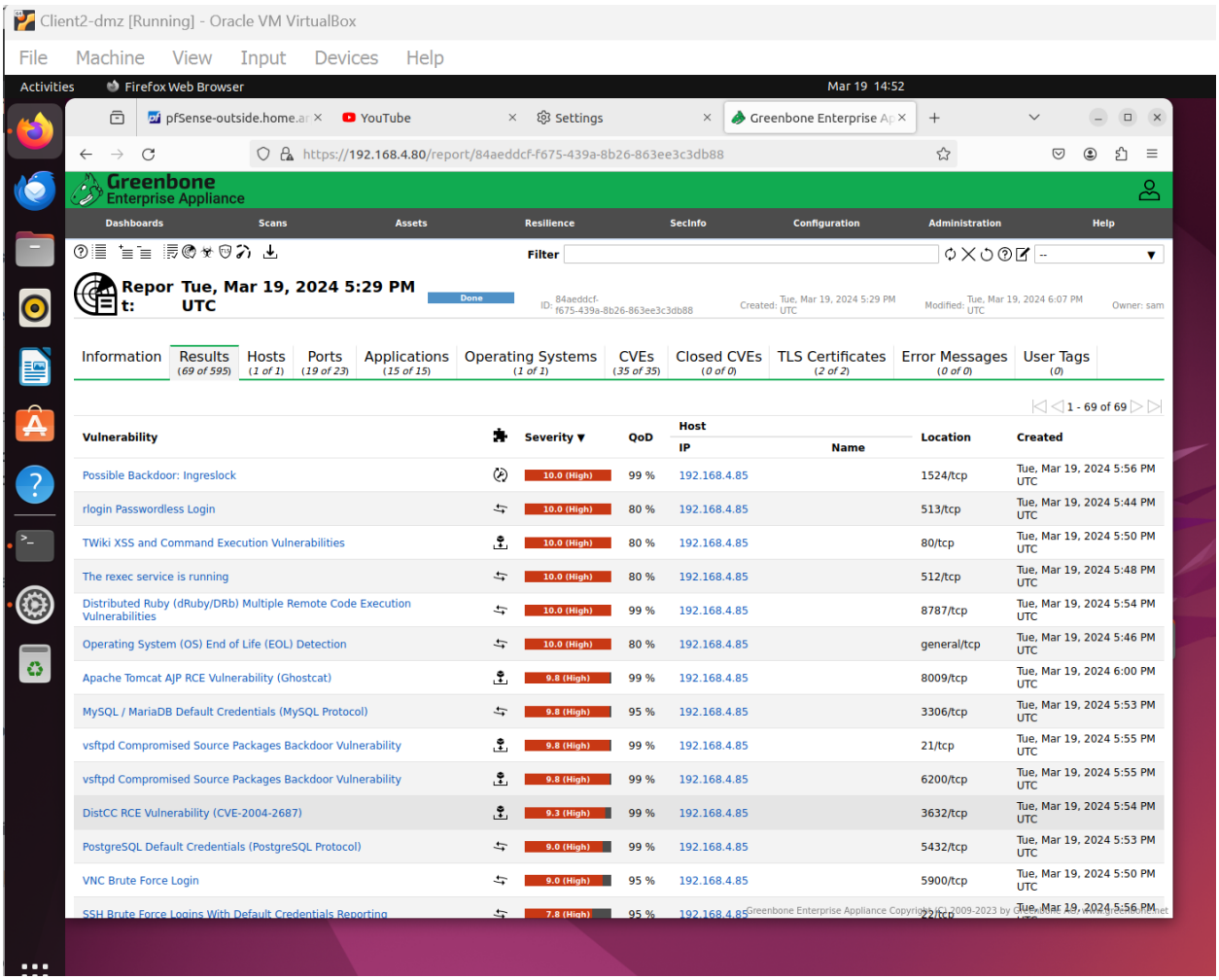

Figure 10/Results