**PRACTICAL: 6**

**AIM:**

A medium-sized enterprise is concerned about the security posture of its internal network after a recent breach. The IT security team uses OpenVAS to conduct a comprehensive vulnerability assessment of the network’s servers and devices to identify exploitable vulnerabilities. Perform a vulnerability scan on a network using OpenVAS and analyse the results to identify and mitigate potential security risks.

**THEORY:**

OpenVAS is an open-source vulnerability scanning and management tool that helps to identify security issues like misconfigurations, outdated software, and weak passwords that could be exploited by attackers. OpenVAS is widely used by security professionals to assess and improve the security posture of their networks and is known for its effectiveness and flexibility.

**Working of OpenVAS**

OpenVAS consists of a server and various client-side tools for scanning and reporting. It uses a regularly updated database of known vulnerabilities and checks systems against these to detect potential weaknesses. The tool performs a comprehensive scan of the specified targets, identifying potential vulnerabilities such as outdated software, misconfigurations, and weak passwords and generates comprehensive reports detailing the identified vulnerabilities and provide recommendations for remediation.

A vulnerability assessment tool works in the following way as follows.

1. Classifies the system resources.

2. Allocates the enumerable values to the classified resources.

3. Detects the possible threats (vulnerabilities) in each resource.

4. Eliminates the vulnerabilities on a priority basis.

**Components of OpenVAS architecture**

* **OpenVAS Scanner**:
* The primary engine that performs the actual scanning of target systems. It uses Network Vulnerability Tests (NVTs) to detect security vulnerabilities.
* **OpenVAS Manager**:
* Manages scan configurations, schedules, and stores scan results. It acts as an intermediary between the scanner and the user interfaces, handling scan requests and processing results.
* **Green bone Security Assistant (GSA)**:
* A web-based graphical user interface (GUI) that allows users to manage scans, configure settings, and view scan results. It provides an easy-to-use platform for interacting with OpenVAS.
* **OpenVAS CLI**:
* A command-line interface for users who prefer scripting and command-line operations. It enables management of scans, targets, and results through commands and scripts.
* **Green bone Security Feed (GSF)**:
* A continuously updated feed that provides the latest Network Vulnerability Tests (NVTs) and security information. It ensures OpenVAS can detect the most recent vulnerabilities.
* **OpenVAS Libraries**:
* These libraries provide essential functionalities required by the scanner and manager, such as network communication, data storage, and cryptographic operations.
* **Database**:
* The database stores scan results, configurations, and other essential data. It ensures data persistence and retrieval for analysis and reporting purposes.

**CODE:**

|  |
| --- |
| * sudo su * apt update && apt upgrade * apt-get update --fix-missing * apt install gvm |

**OUTPUT:**

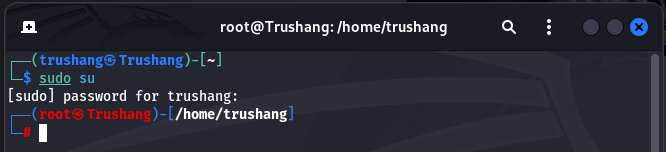


Figure 1: Gain root access

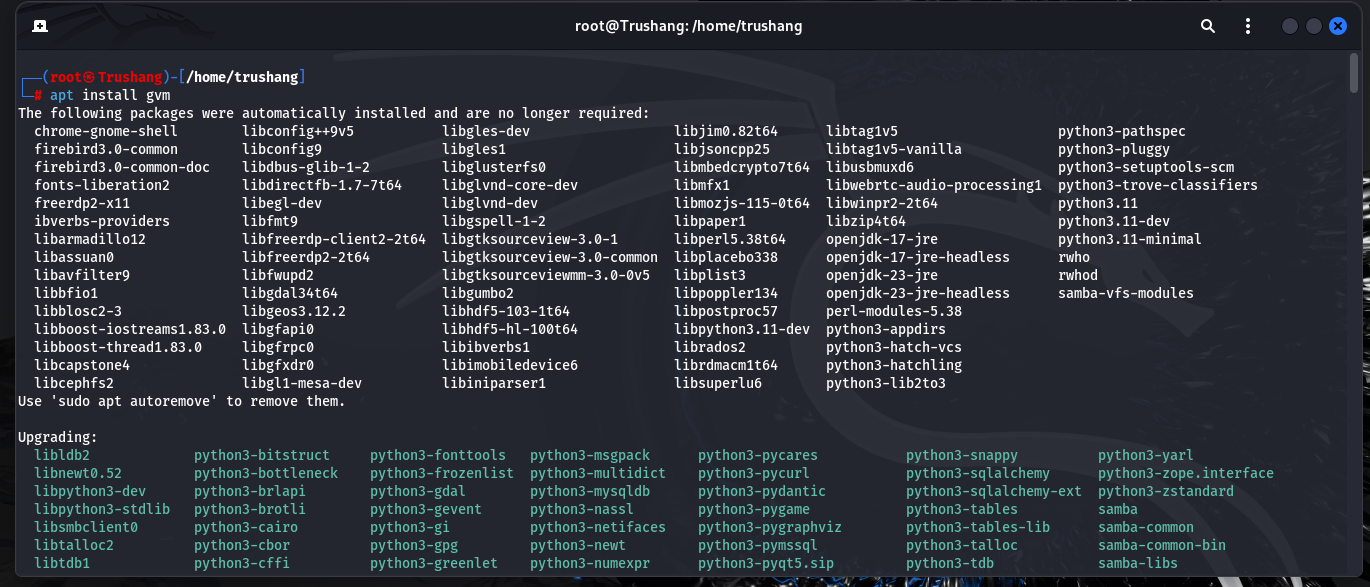


Figure 2: Install gvm in your system

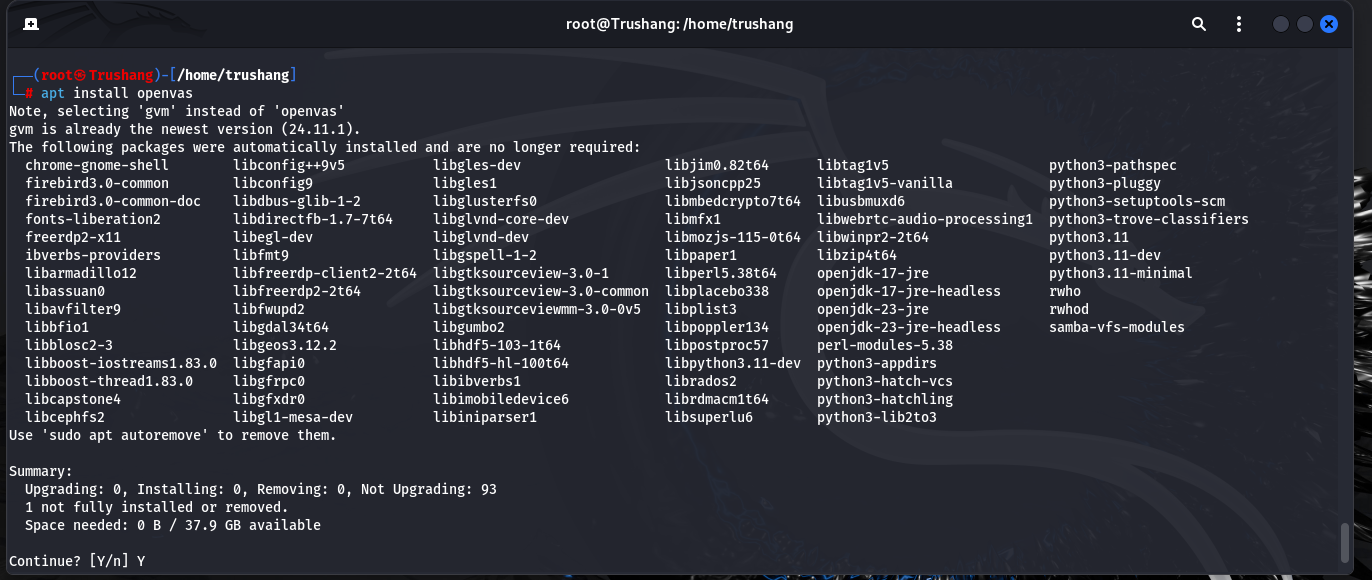


Figure 3: Install OpenVAS in your system

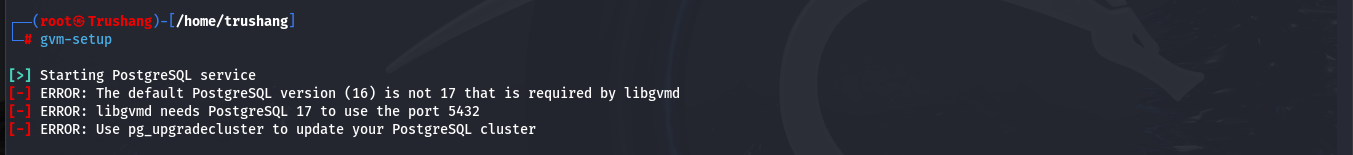


Figure 4: We have to change the port of PostgreSQL

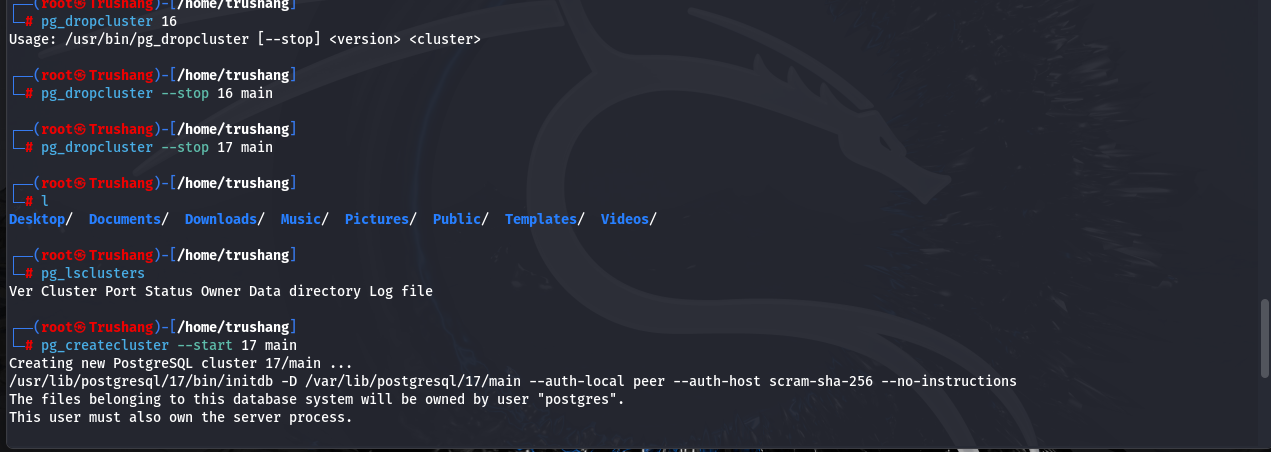


Figure 5: Delete PostgreSQL 16 and 17 and then create 17 main cluster

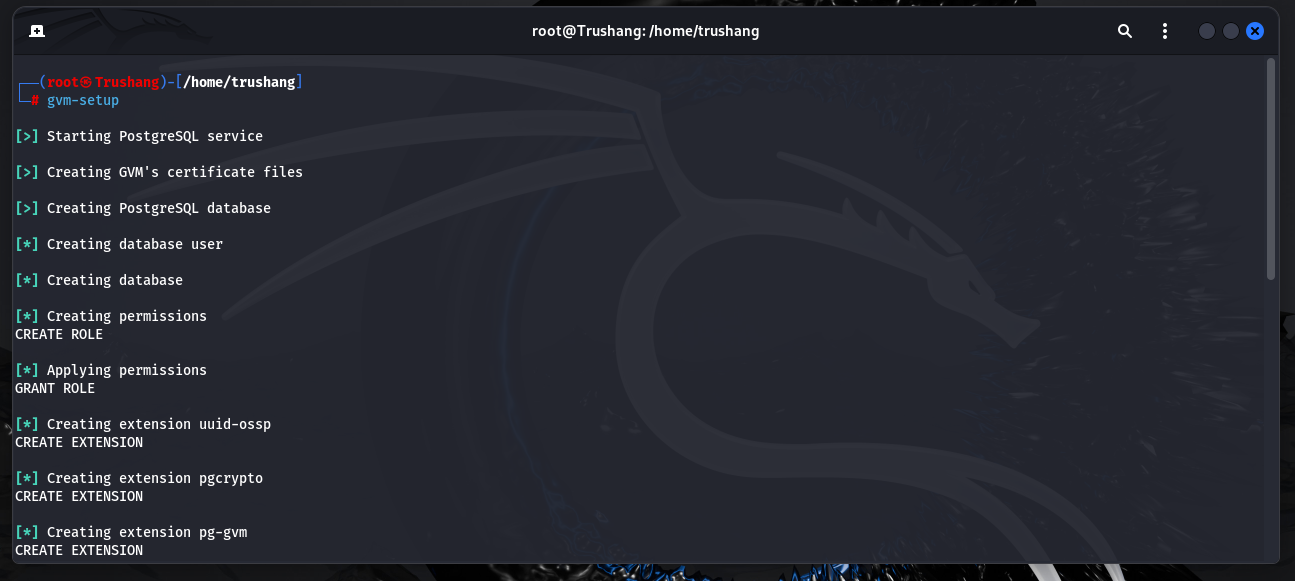


Figure 6: Start GVM setup

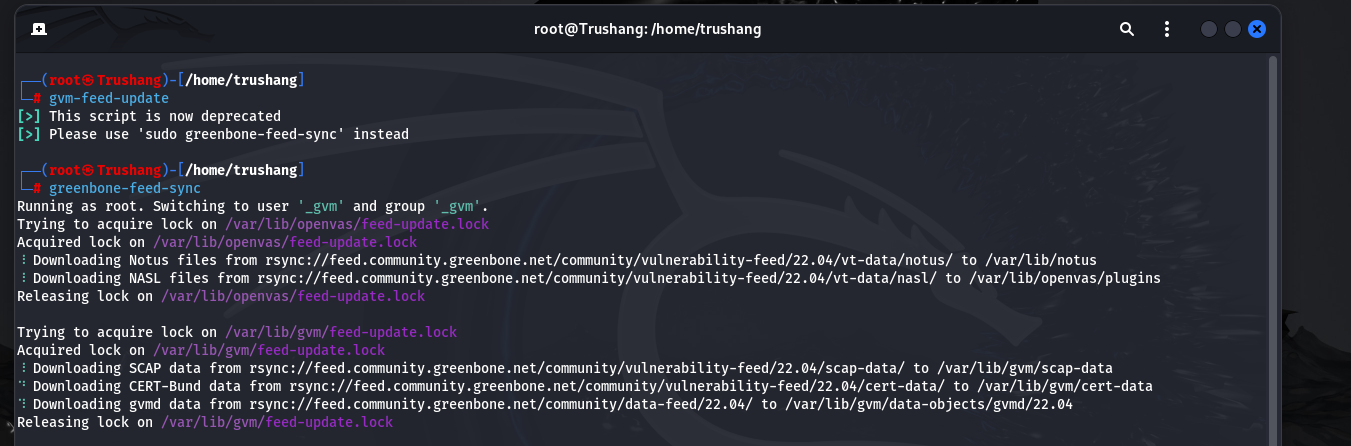


Figure 7: Sync NVT, SCAP, CERT, GVMD\_DATA



Figure 8: Start GVM

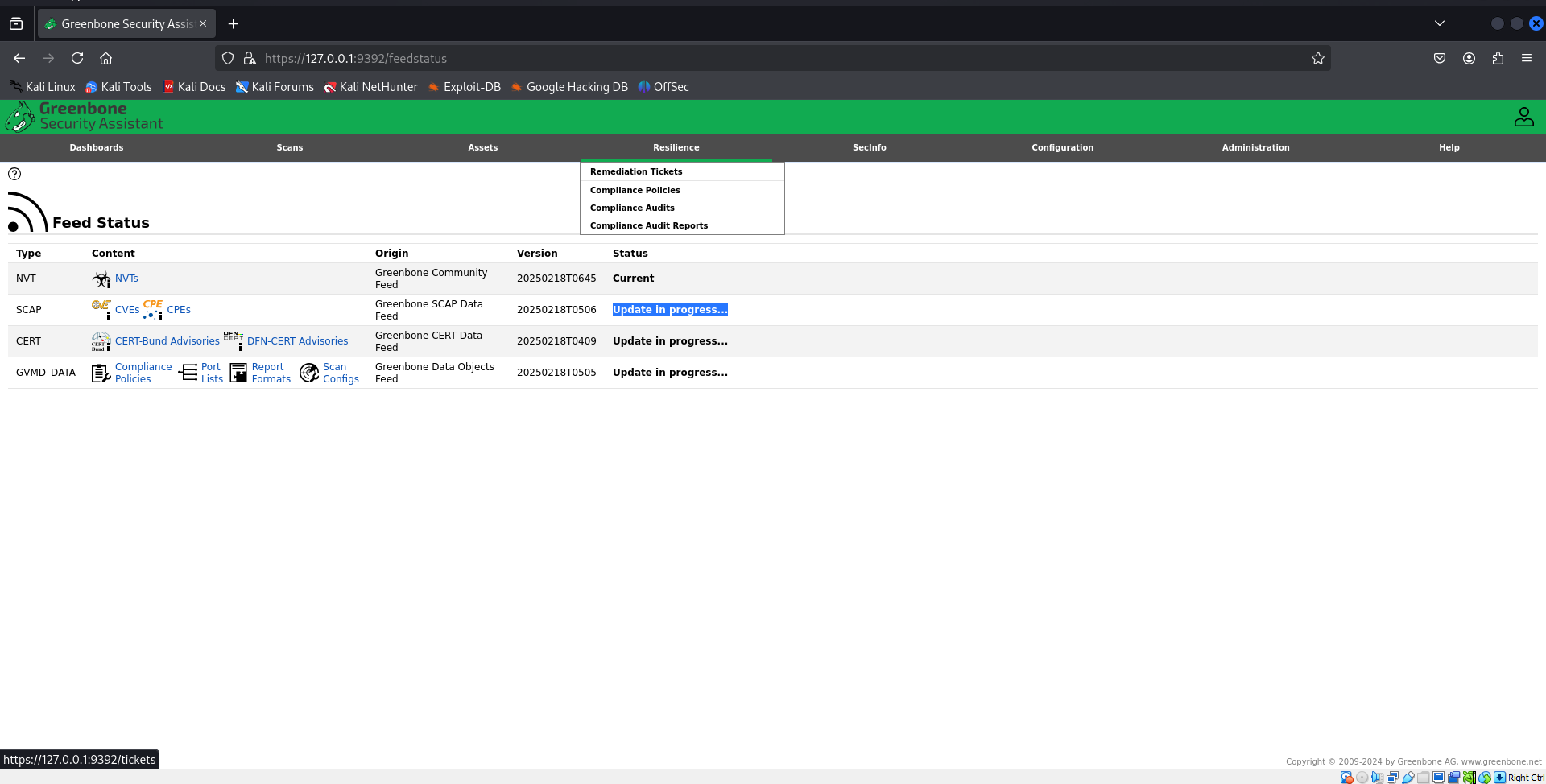


Figure 9: Check feed status

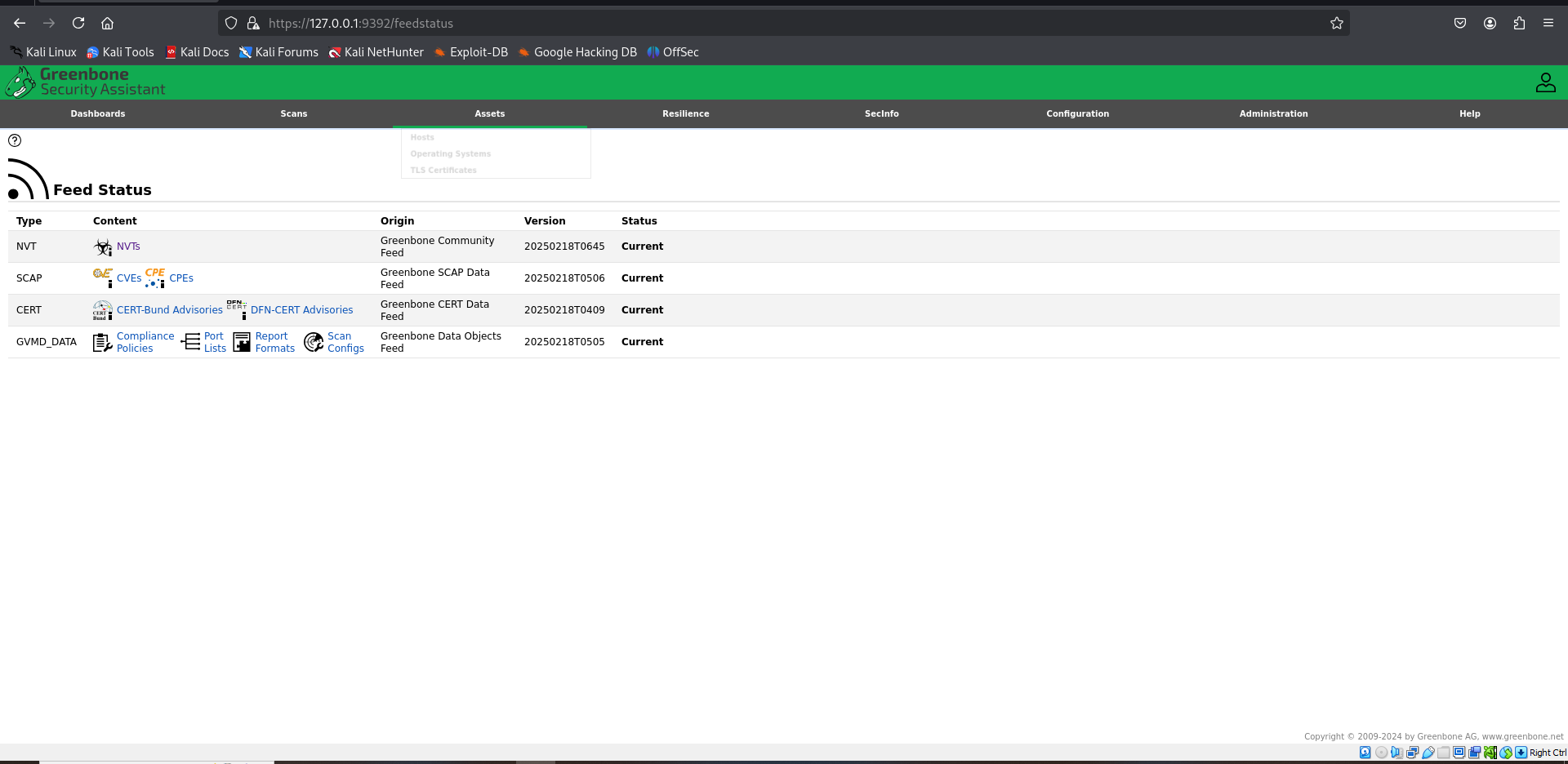


Figure 10: Feed status is now current

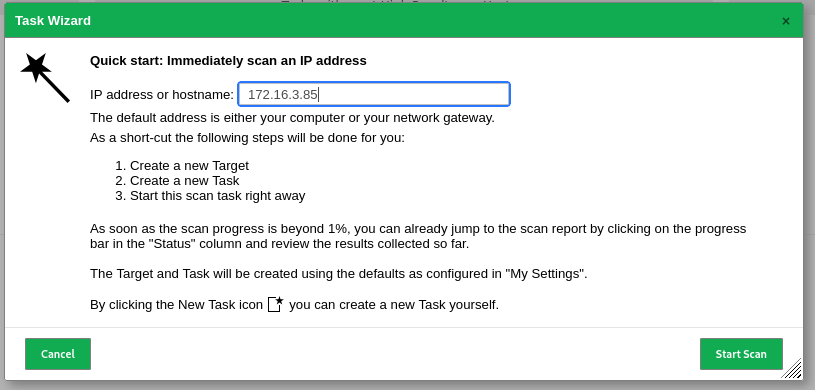


Figure 11: Write IP address for scan

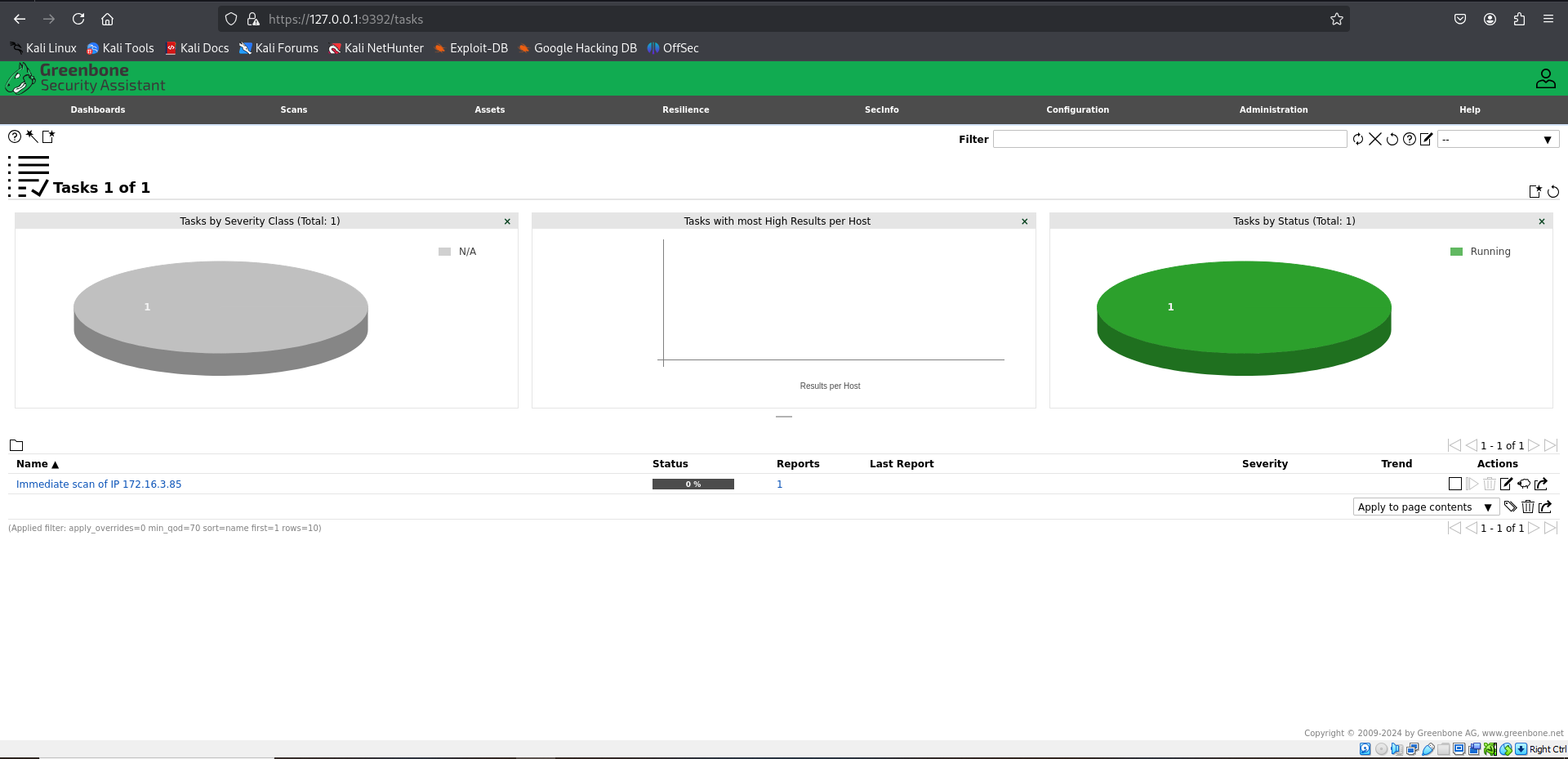
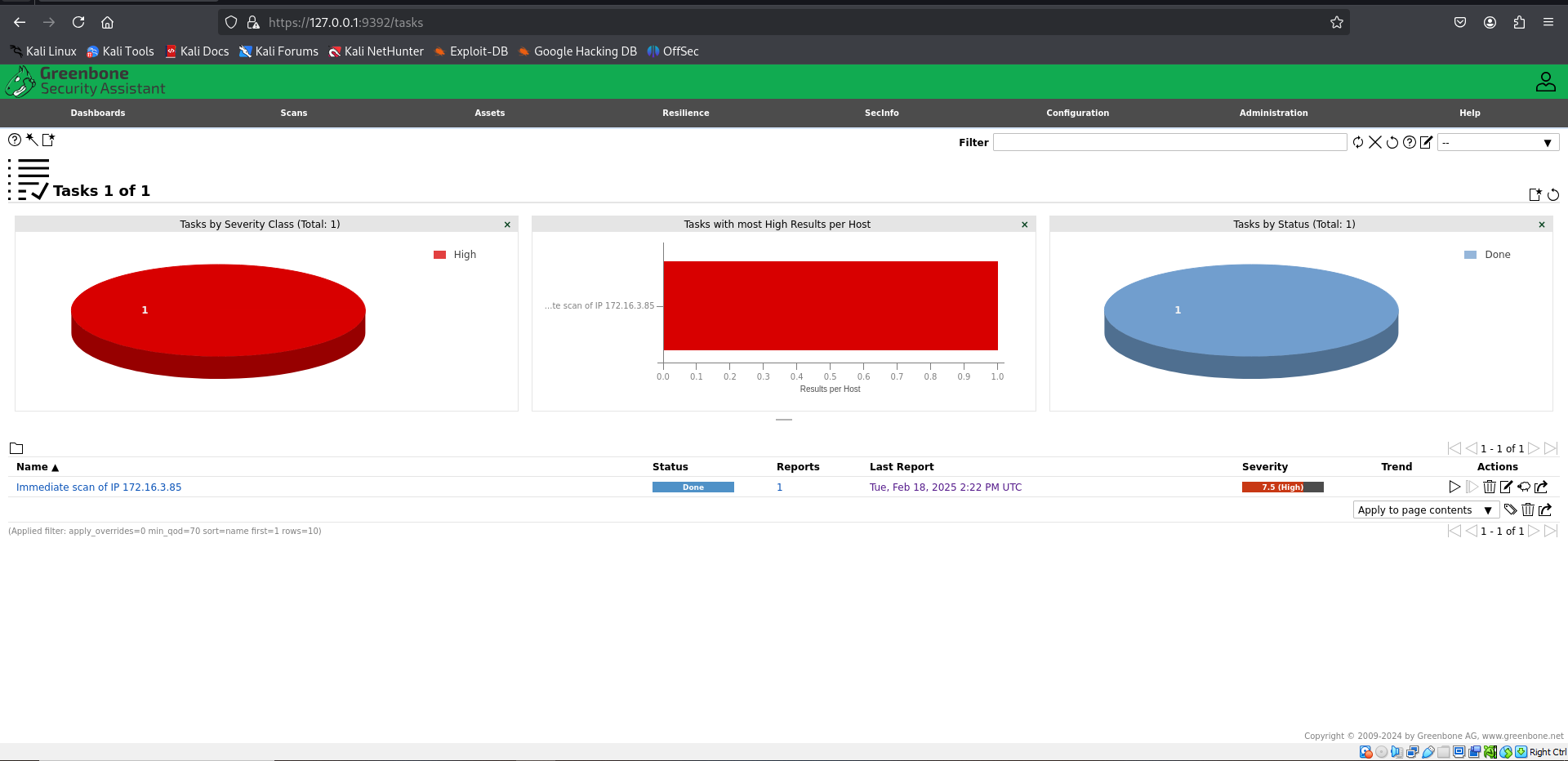
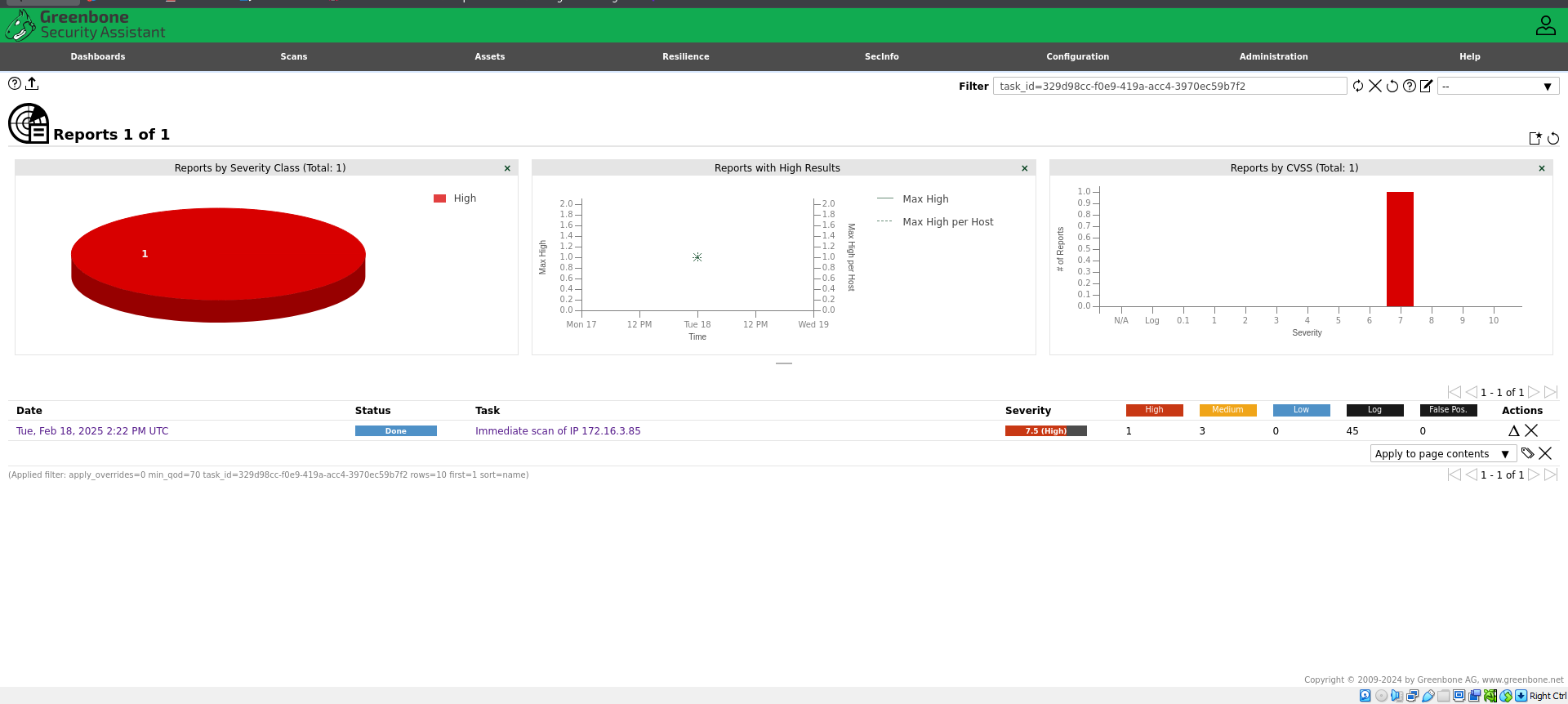
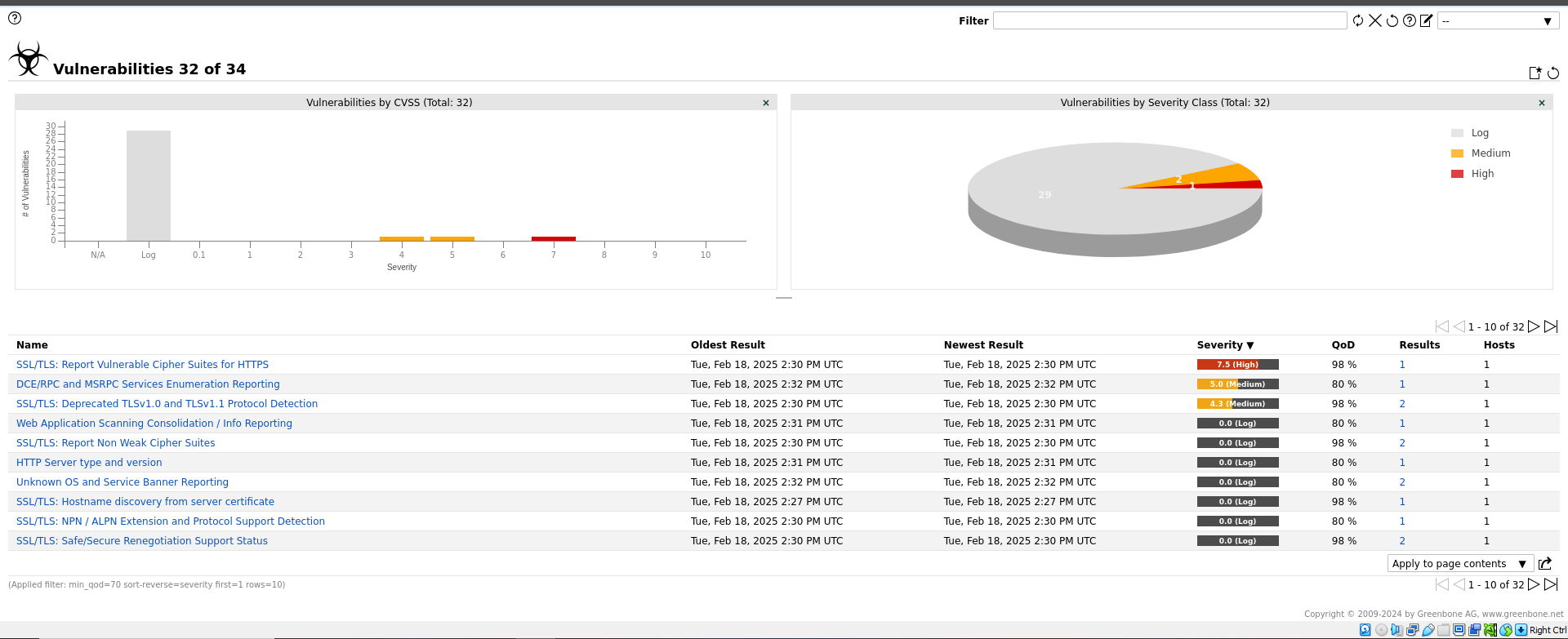
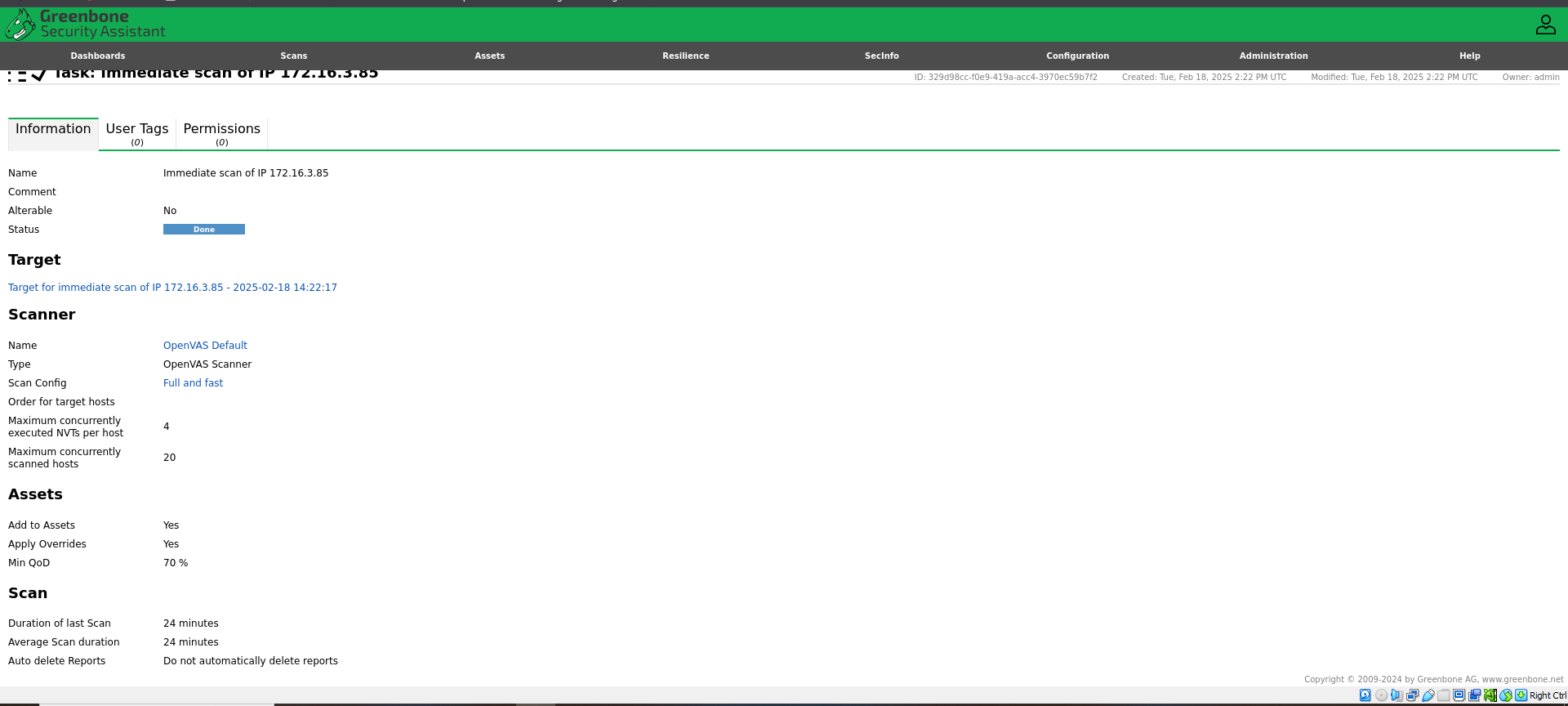


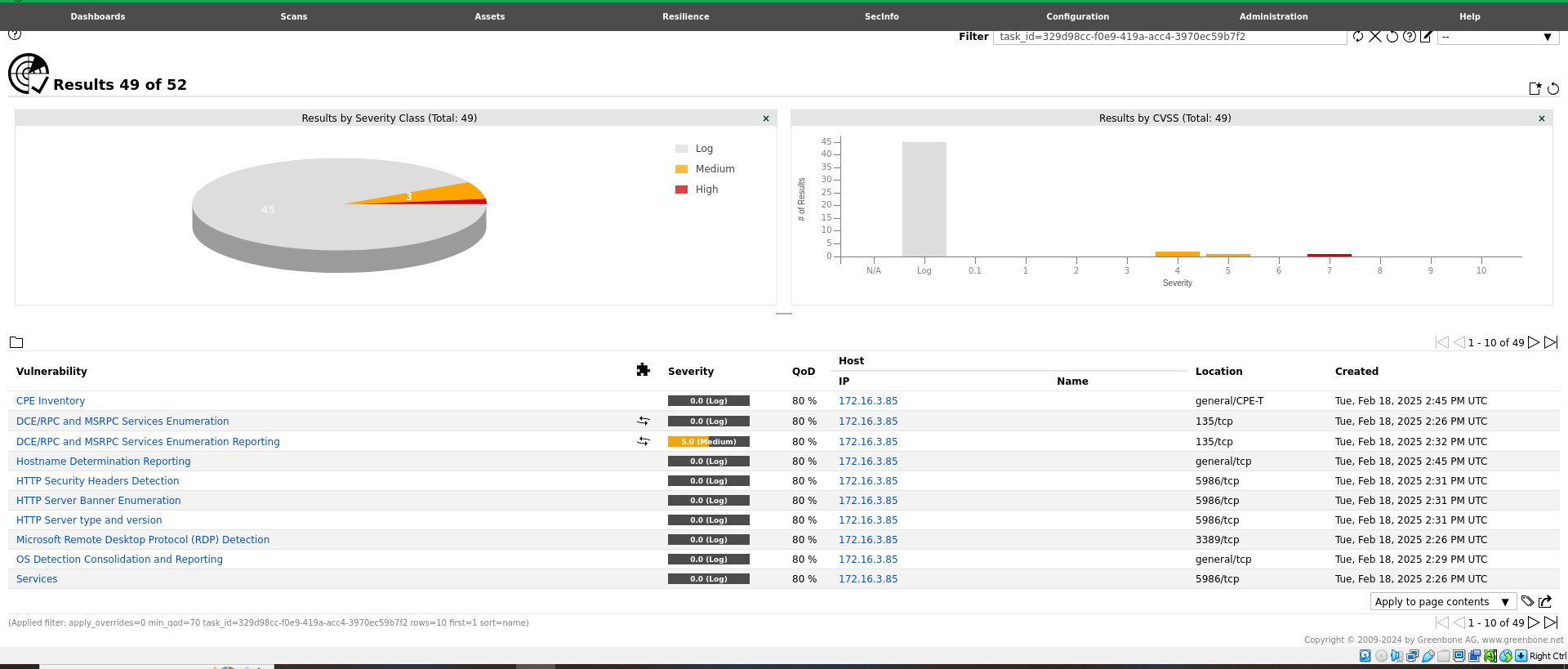
Figure 12: Scanning IP address

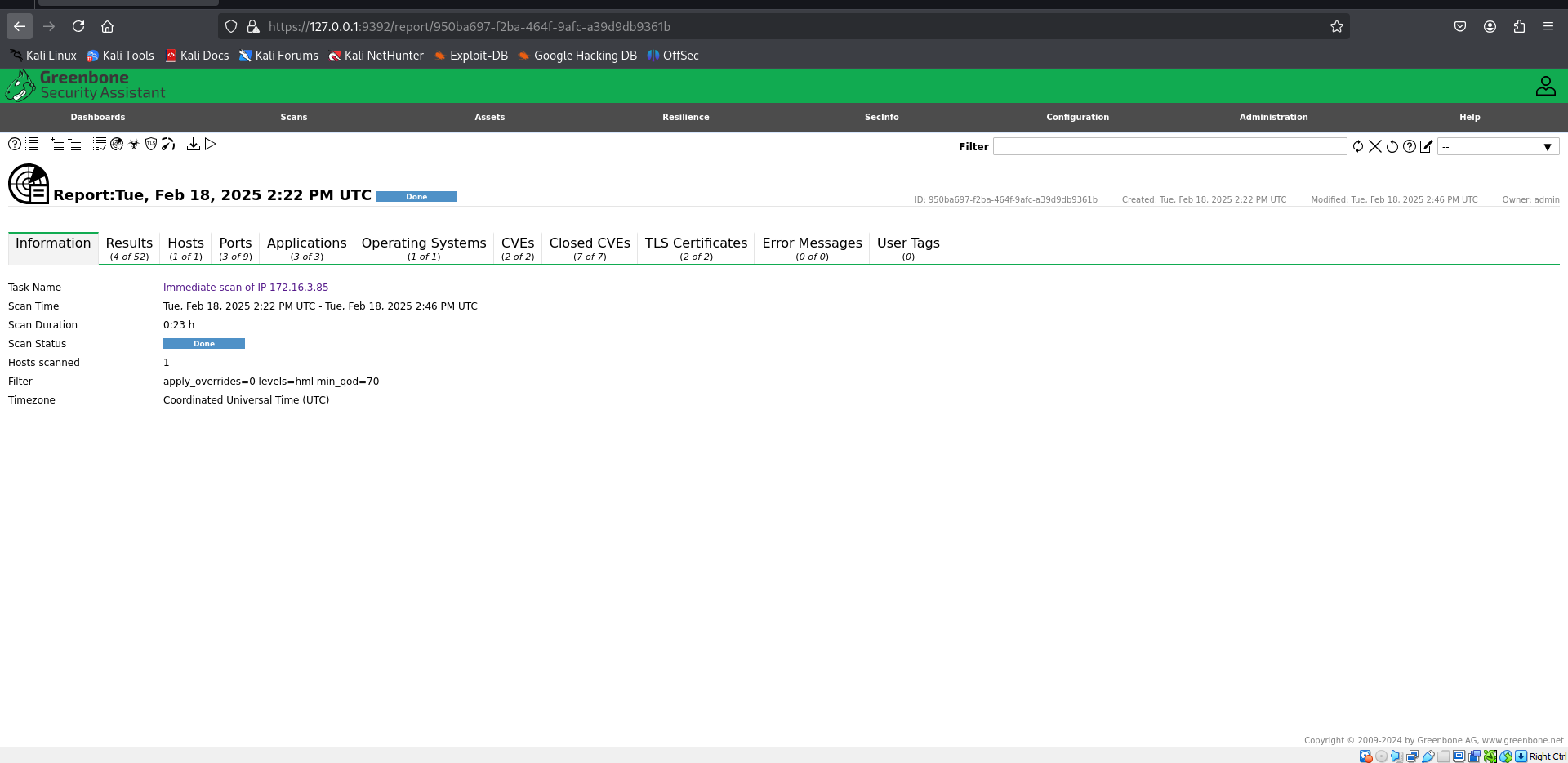


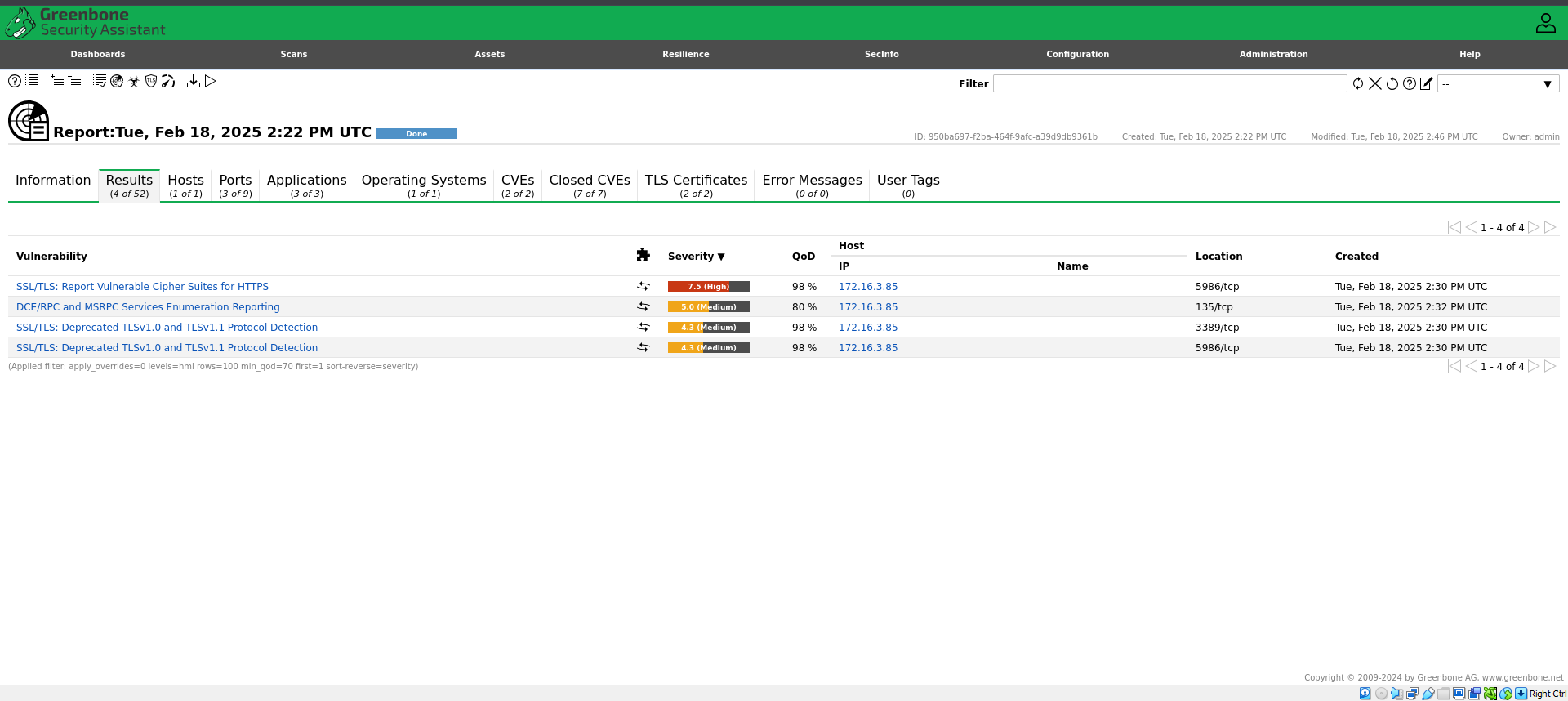


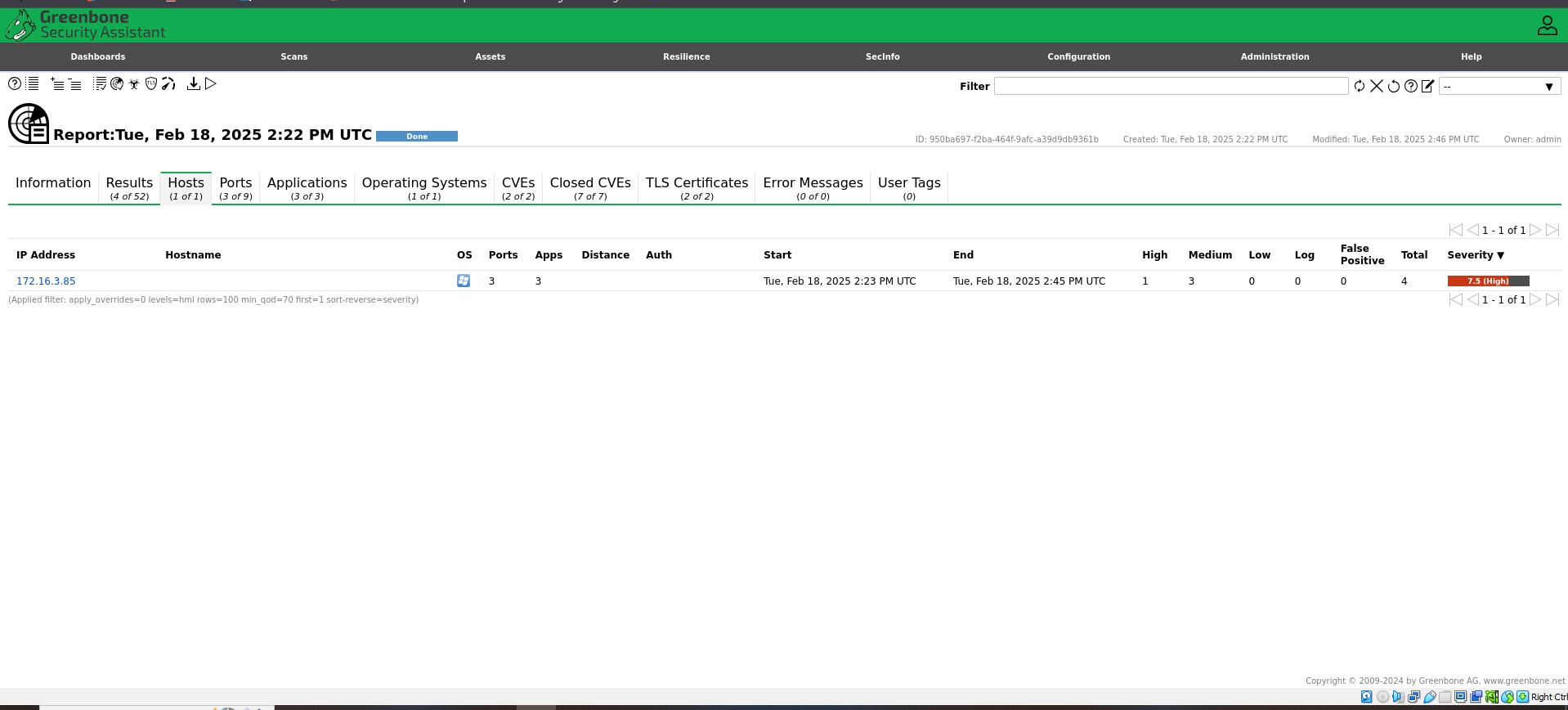


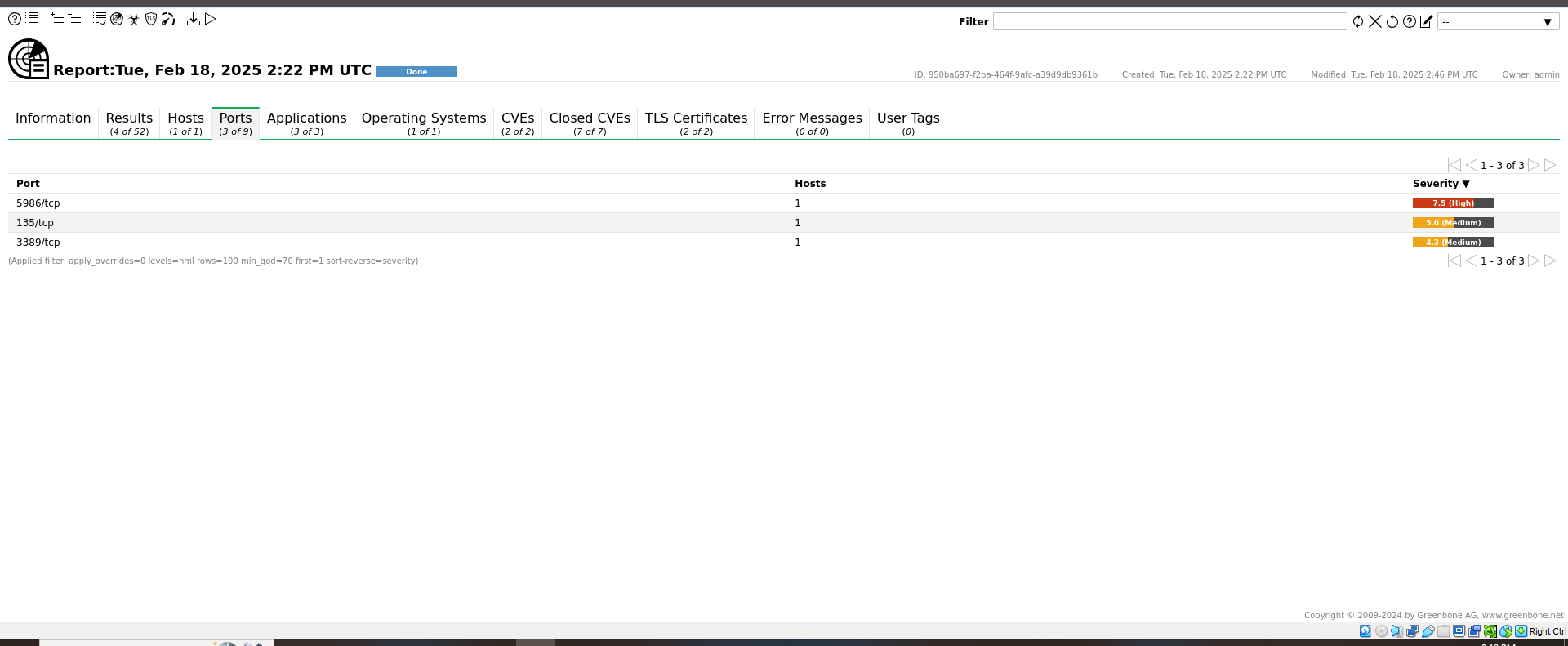


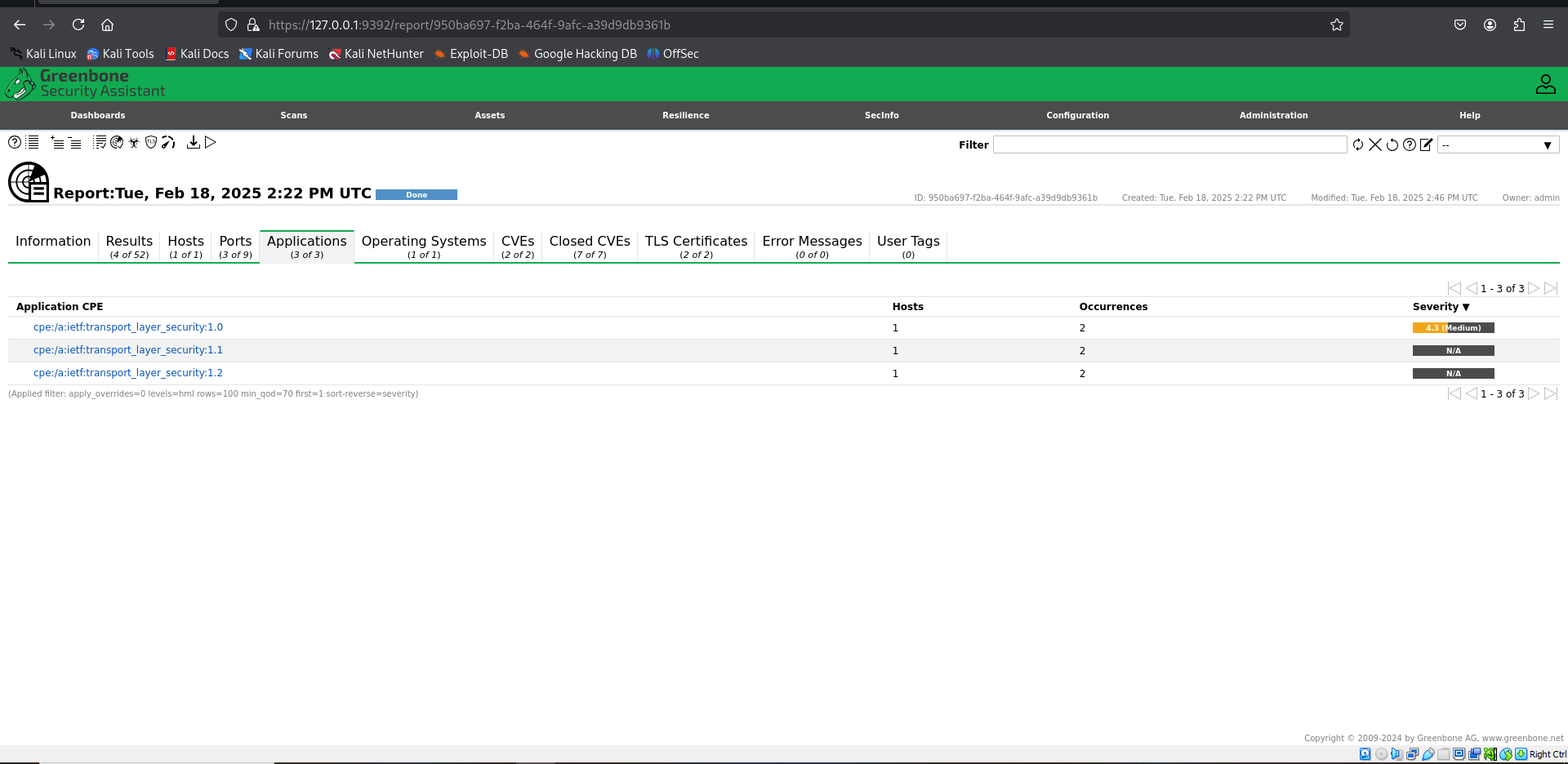


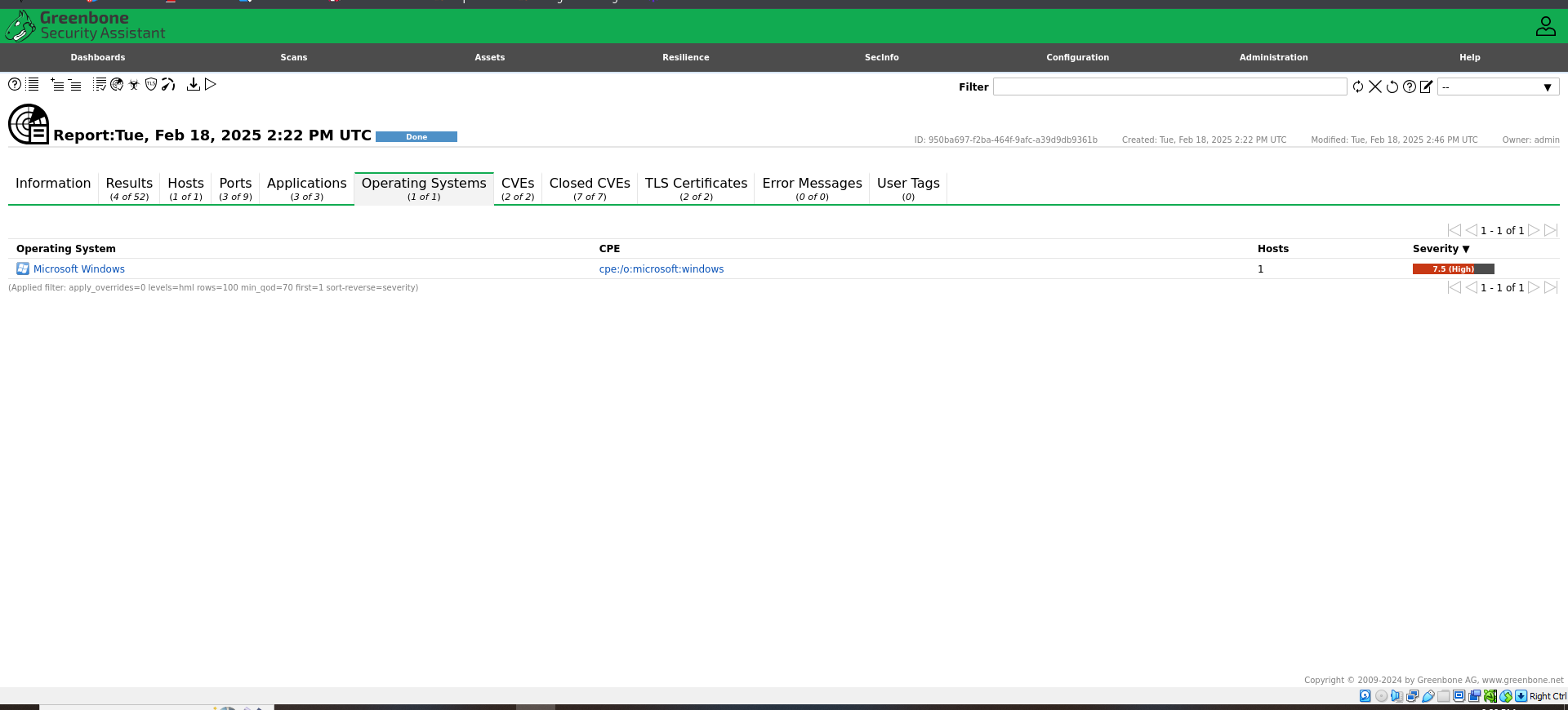


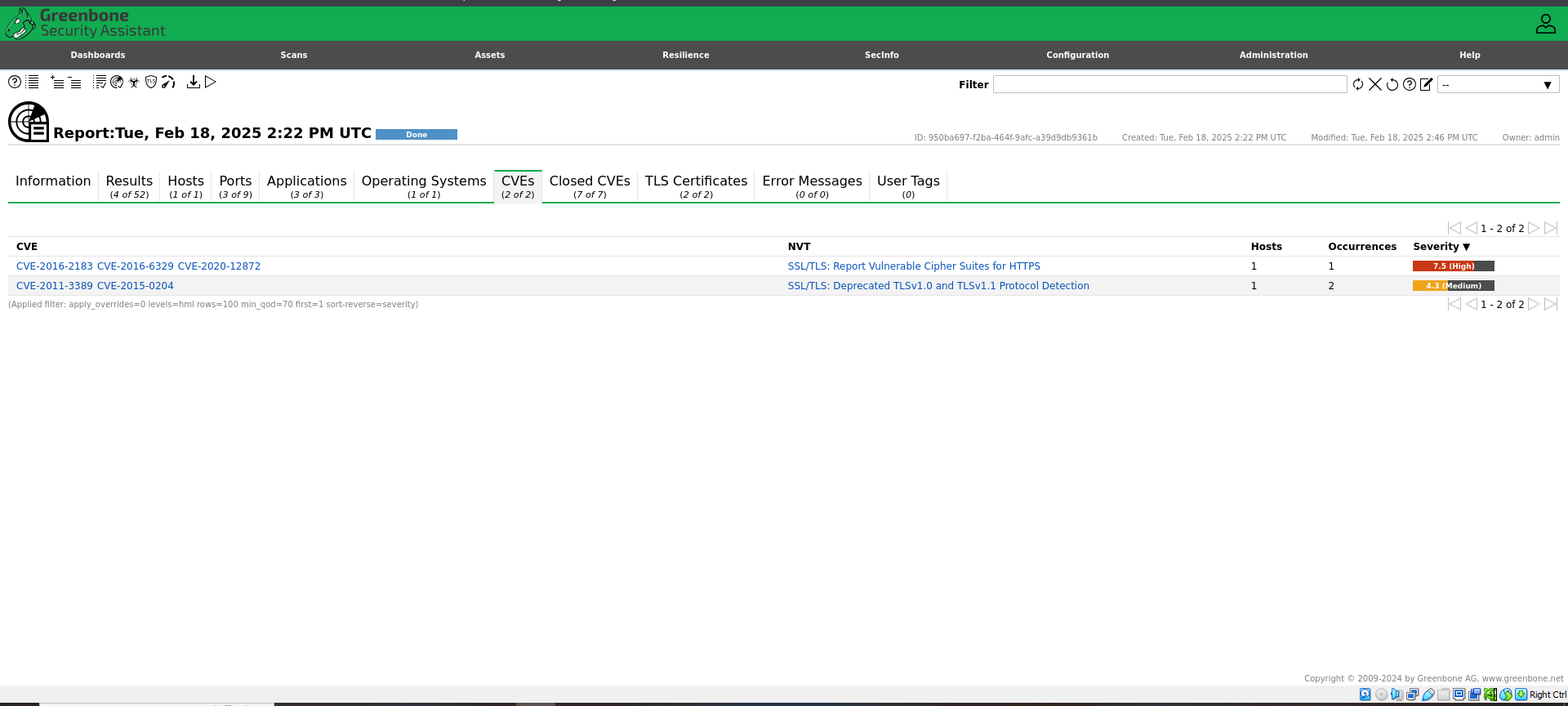


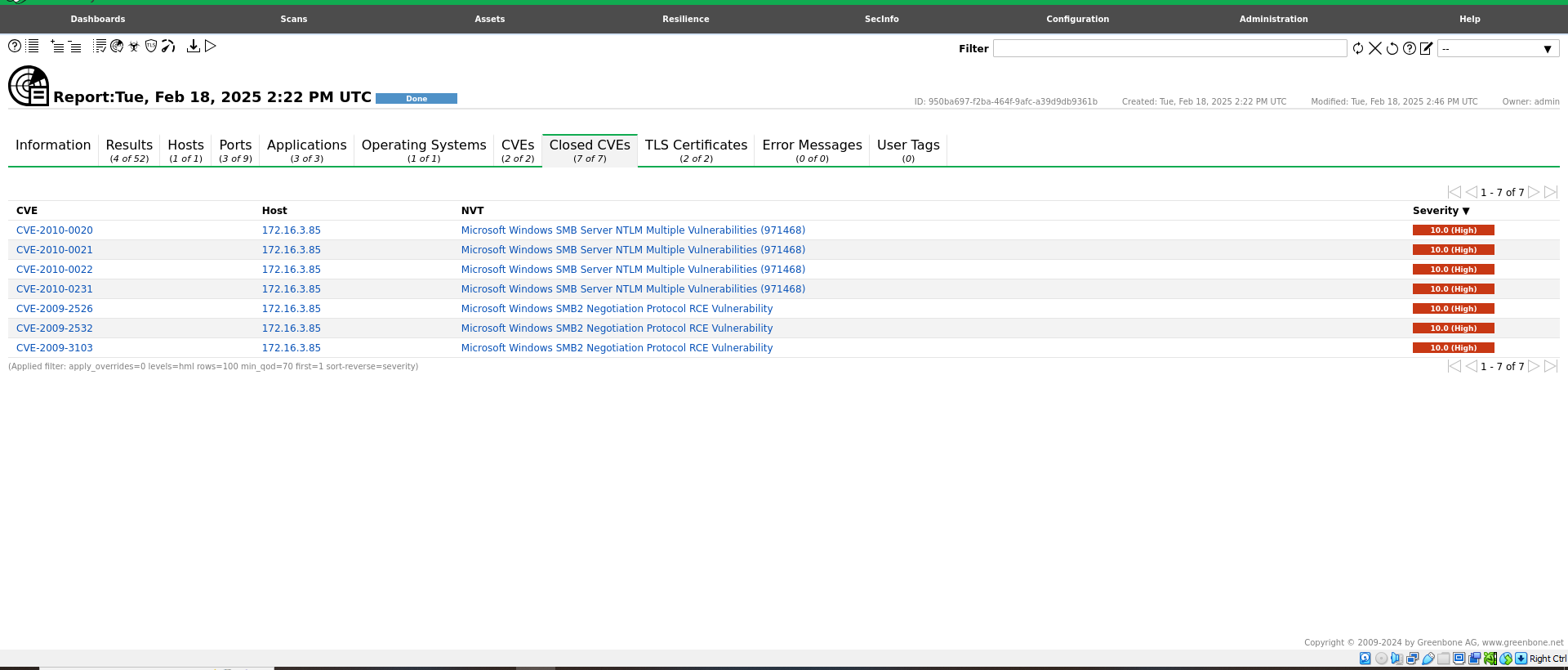


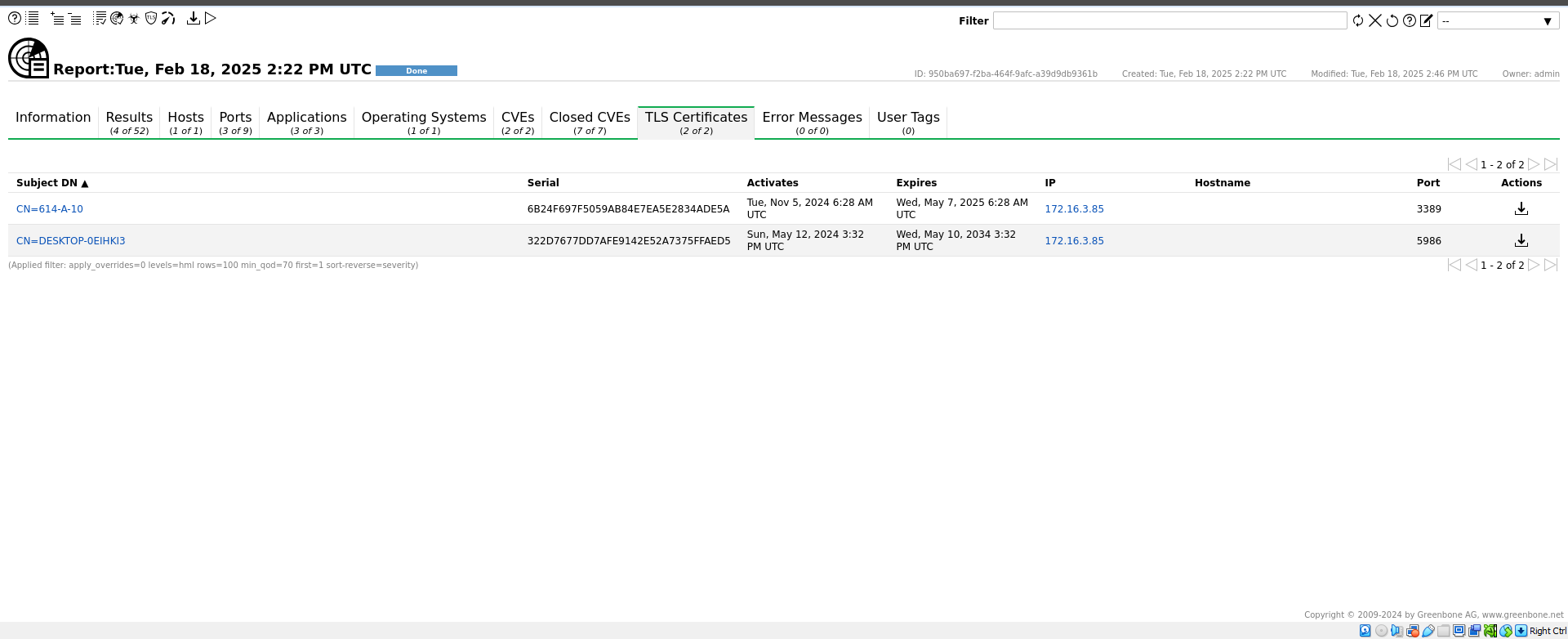












**LATEST APPLICATIONS:**

* + Enterprise IT Security
  + Cloud Security
  + IoT (Internet of Things) Security
  + Compliance Auditing
  + Penetration Testing and Ethical Hacking
  + Managed Security Service Providers (MSSPs)
  + Incident Response and Forensics
  + Security Automation Platforms
  + Educational Institutions and Training
  + Government and Defense Organizations

**LEARNING OUTCOME:**

In this practical, we use OpenVAS to perform vulnerability scans, analyze results, and apply security measures to protect systems from threats.

**REFERENCES:**

1. Open VAS: https://www.openvas.org/
2. GFG: <https://www.geeksforgeeks.org/security-assessment-openvas/>
3. Green bone: <https://greenbone.github.io/docs/latest/22.4/kali/index.html>