Task 3: Vulnerability Assessment Report

This report details the findings of a vulnerability assessment conducted on a local network host as per the requirements of the internship task. The primary objective was to use a free, open-source tool to identify common vulnerabilities on the local machine. The OpenVAS scanner within the Greenbone Vulnerability Manager (GVM) framework was used for this assessment. The scan targeted the local IP address

`192.168.1.20`.

The scan completed successfully and found **zero vulnerabilities** of High, Medium, or Low severity. All findings were informational logs with a severity rating of 0.0.

2. Scan Configuration & Process

- **Scanner Used**: OpenVAS (GVM)
- **Scan Target**: `192.168.1.20`
- **Scan Type**: Uncredentialed Full Scan
- **Scan Date**: Sun, Aug 10, 2025

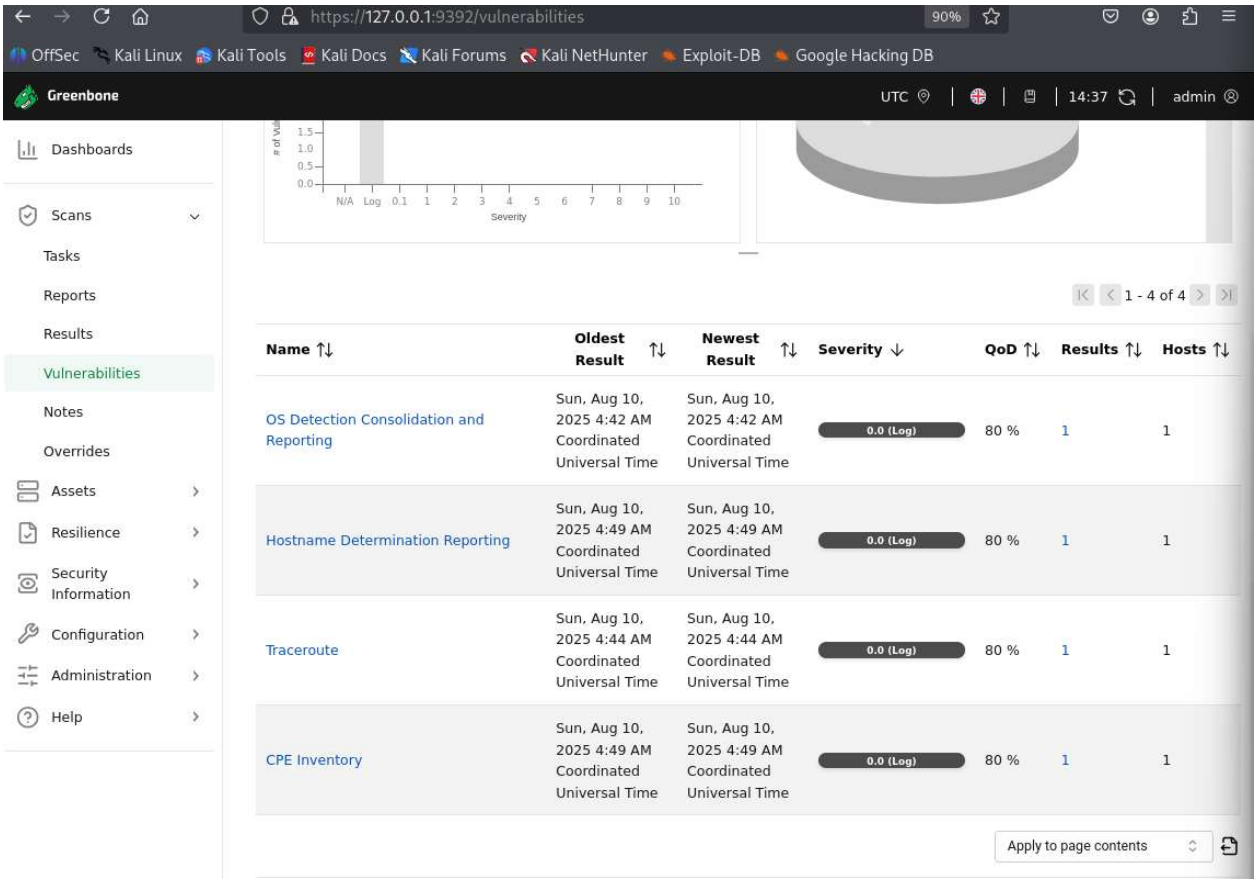
The process involved installing and configuring the GVM framework, defining the local host as a target, and launching a comprehensive network scan.

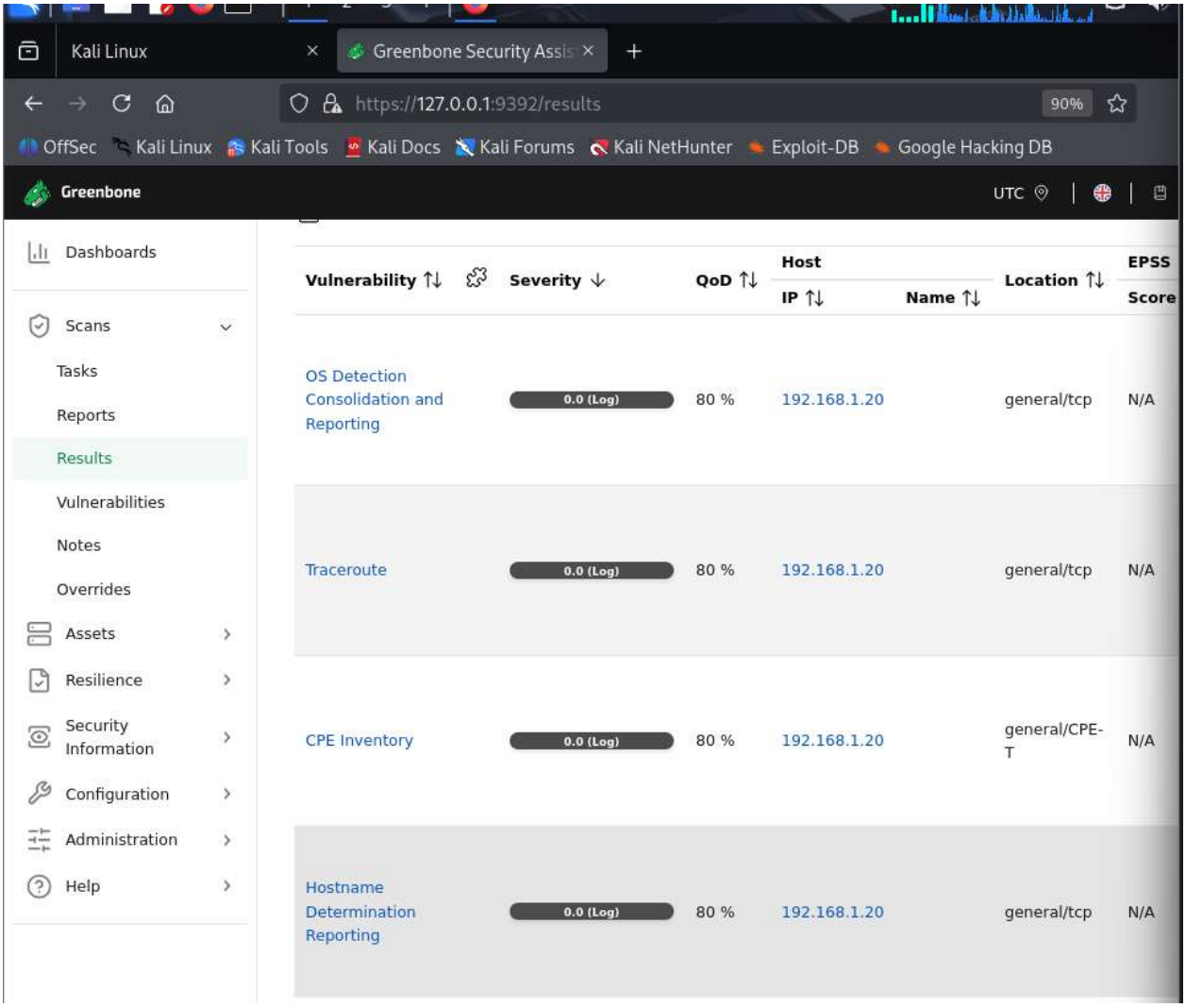
3. Findings and Observations

The scan did not identify any exploitable vulnerabilities. The results consist entirely of informational logs that are used to build a profile of the target machine.

The absence of detected vulnerabilities is a positive result from a network security perspective. However, it is crucial to understand the limitations of the scan that was

performed.


https://127.0.0.1:9392/vulnerabilities
90%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Greenbone
UTC
14:37
admin
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Severity
1 - 4 of 4
Name
Oldest Result
Newest Result
Severity
QoD
Results
Hosts
OS Detection Consolidation and Reporting
Sun, Aug 10, 2025 4:42 AM Coordinated Universal Time
Sun, Aug 10, 2025 4:42 AM Coordinated Universal Time
0.0 (Log)
80 %
1
1
Hostname Determination Reporting
Sun, Aug 10, 2025 4:49 AM Coordinated Universal Time
Sun, Aug 10, 2025 4:49 AM Coordinated Universal Time
0.0 (Log)
80 %
1
1
Traceroute
Sun, Aug 10, 2025 4:44 AM Coordinated Universal Time
Sun, Aug 10, 2025 4:44 AM Coordinated Universal Time
0.0 (Log)
80 %
1
1
CPE Inventory
Sun, Aug 10, 2025 4:49 AM Coordinated Universal Time
Sun, Aug 10, 2025 4:49 AM Coordinated Universal Time
0.0 (Log)
80 %
1
1
Apply to page contents



4. Analysis and Recommendations

- **Analysis**: This was an **uncredentialed scan**, meaning the scanner acted as an outsider without login credentials. This type of scan cannot see local system details like installed software versions, missing security patches, or weak user account policies. The "clean" result indicates a reasonably secure network perimeter but does not guarantee the absence of internal vulnerabilities.
- **Recommendations**: For a more comprehensive assessment in the future, it is highly recommended to perform an **authenticated (or credentialed) scan**. This involves providing the scanner with secure login credentials, allowing it to inspect the system from the inside and provide a much more detailed and accurate report on software-based vulnerabilities.

5. Conclusion

The vulnerability scan of host `192.168.1.20` was completed successfully. While no immediate threats were identified from an uncredentialed network perspective, the primary value of this exercise was in learning the end-to-end process of a professional vulnerability assessment using OpenVAS.