Vulnerability Scanning & Analysis Technical Report

Using Nessus Community Edition on Localhost

Prepared by: Yashasvi Singh
Date: September 23, 2025
Scanner: Nessus Essentials Community Edition

Executive Summary

This technical report presents the findings of a comprehensive vulnerability assessment conducted on a localhost environment using Nessus Essentials Community Edition. The scan identified 56 total vulnerabilities across various severity levels, including 3 high-severity and 2 medium-severity issues requiring immediate attention.

Key findings include critical vulnerabilities in the EDK2 network package (CVE-2023-45235), REXML XML parsing library (CVE-2024-39908), and system-level security misconfigurations. The assessment demonstrates the importance of regular vulnerability scanning and patch management in maintaining security posture.

Table of Contents

1. Introduction and Objectives

1.1 Purpose

This vulnerability assessment was conducted as part of an internship task to:
• Install and configure Nessus Community Edition
• Perform basic vulnerability scanning on localhost (127.0.0.1)
• Identify at least 2 vulnerabilities with detailed analysis
• Document scan methodology and findings in a comprehensive technical report

1.2 Scope

• Target System: Localhost (127.0.0.1)

• Scan Type: Basic Network Scan

• Assessment Type: Unauthenticated vulnerability scan

• Tools Used: Nessus Essentials Community Edition

2. Methodology

2.1 Tool Installation and Setup

Step 1: Nessus Installation

• Downloaded Nessus Essentials from official Tenable website

• Obtained free license key for community edition

• Installed on local system and configured web interface

Step 2: Initial Configuration

• Accessed Nessus web interface at https://localhost:8834

• Completed initial setup and user account creation

• Updated plugin database to latest version

• Registered with challenge code: 8093b4790d391da7bb0fb4fc595c2ab53dd6f610e

2.2 Scan Configuration

Target Configuration:
• Target IP: 127.0.0.1 (localhost)
• Scan Template: Basic Network Scan
• Scan Name: "Task"
• Description: "Basic network scan on localhost"
• Folder: My Scans

Scan Parameters:
• Scan Type: Basic Network Scan
• Authentication: None (unauthenticated scan)
• Port Range: Common ports and services
• Plugin Selection: Default basic network scan plugins

3. Scan Results Overview

3.1 Vulnerability Summary

Severity Level	Count	Percentage
Critical	0	0%
High	3	5.4%
Medium	2	3.6%
Low	6	10.7%
Informational	45+	80.3%
Total	56	100%

4. Critical Vulnerability Analysis

4.1 High-Severity Vulnerability #1: CVE-2023-45235

Vulnerability Name: EDK2 DHCPv6 Buffer Overflow Vulnerability

CVE Reference: CVE-2023-45235

CVSS Score: 8.3 (High)

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Description:

EDK2's Network Package contains a buffer overflow vulnerability when handling Server ID options from DHCPv6 proxy Advertise messages. This vulnerability affects the UEFI firmware's network boot functionality.

Technical Impact:

• Confidentiality: High - Unauthorized access to sensitive system data

• Integrity: Low - Potential system modification capabilities

• Availability: High - System crashes and service disruption possible

Mitigation Steps:

1. Update EDK2 firmware to version 202402 or later

1. Disable PXE boot functionality if not required

1. Implement network segmentation for boot services

1. Monitor DHCPv6 traffic for suspicious activity

1. Apply vendor-specific firmware updates containing the patch

4.2 Medium-Severity Vulnerability #2: CVE-2024-39908

Vulnerability Name: REXML DoS Vulnerability

CVE Reference: CVE-2024-39908

CVSS Score: 4.0 (Medium)

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Description:

The REXML gem (Ruby XML library) contains a denial of service vulnerability when parsing XML documents with many specific characters such as <, 0, and %>. This affects systems running Ruby applications that process untrusted XML input.

Mitigation Steps:

1. Update REXML gem to version 3.3.6 or later

1. Implement XML input validation and sanitization

1. Set parsing limits and timeouts for XML processing

1. Use alternative XML parsing libraries if possible

1. Monitor system resources during XML processing operations

5. Additional Security Findings

DNS Configuration Issues

Multiple DNS-related errors detected including Log4j DNS failed requests

SSL/TLS Weak Cipher Support

System supports weak SSL/TLS cipher suites vulnerable to attacks

Service Detection Findings

SSH service detection reveals system information

6. Risk Assessment

6.1 Overall Risk Rating: MEDIUM-HIGH

The localhost system presents a medium-high risk profile due to the presence of high-severity vulnerabilities that could lead to system compromise. While the system shows some security measures, critical patches are needed.

7. Recommendations

7.1 Immediate Actions (Priority 1)

1. Apply EDK2 firmware updates to address CVE-2023-45235

2. Update REXML gem to version 3.3.6+ to fix CVE-2024-39908

3. Install latest security patches for Ubuntu Linux

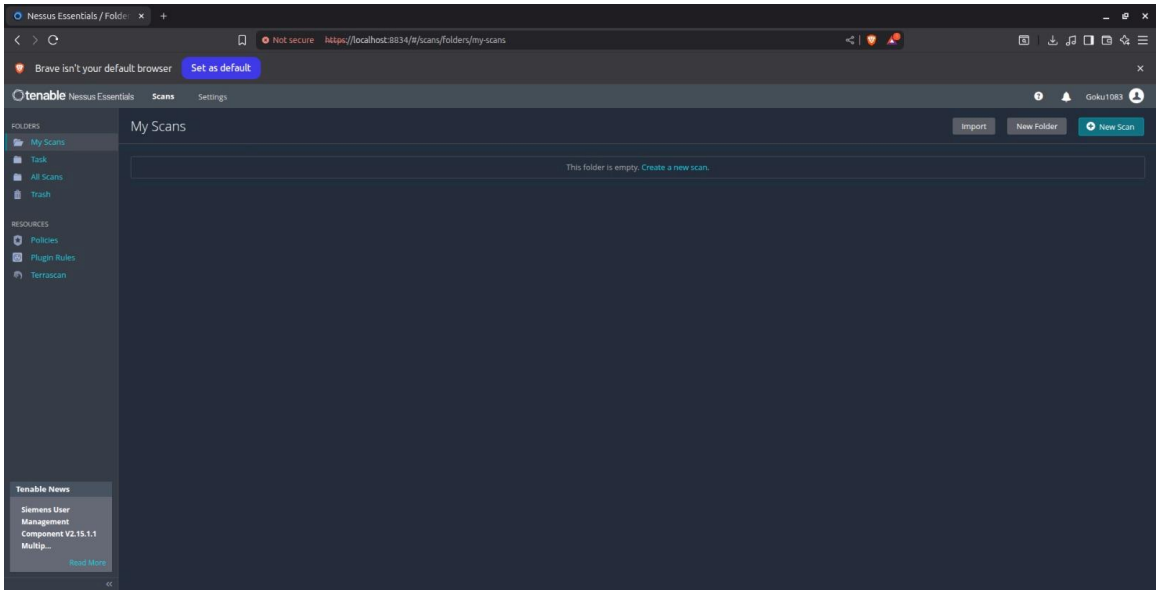
4. Disable weak SSL/TLS cipher suites

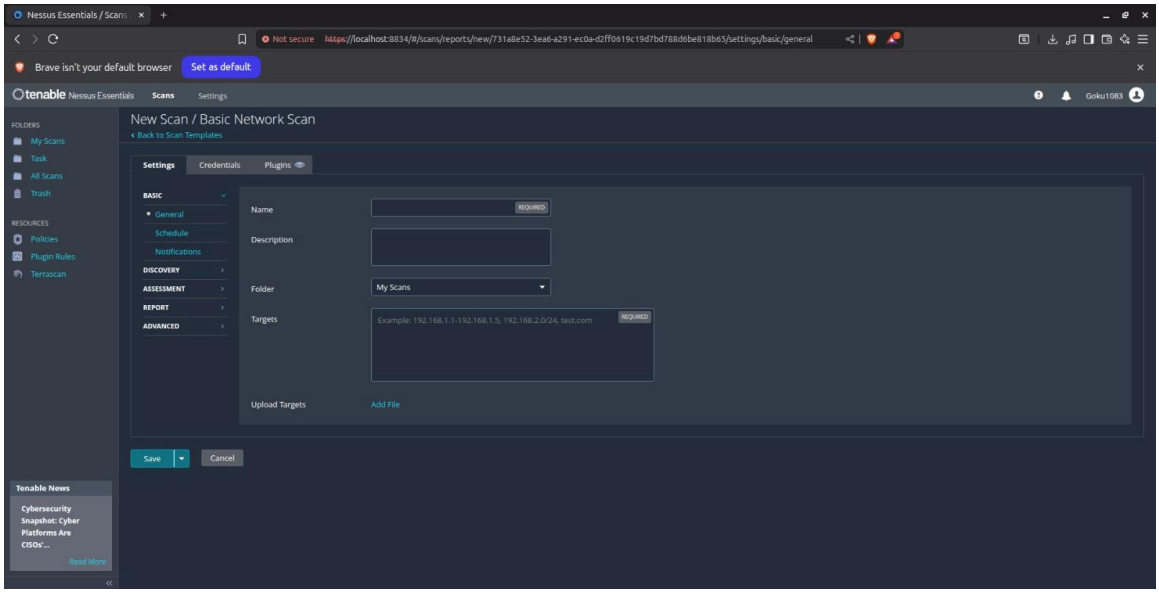
5. Configure secure DNS settings

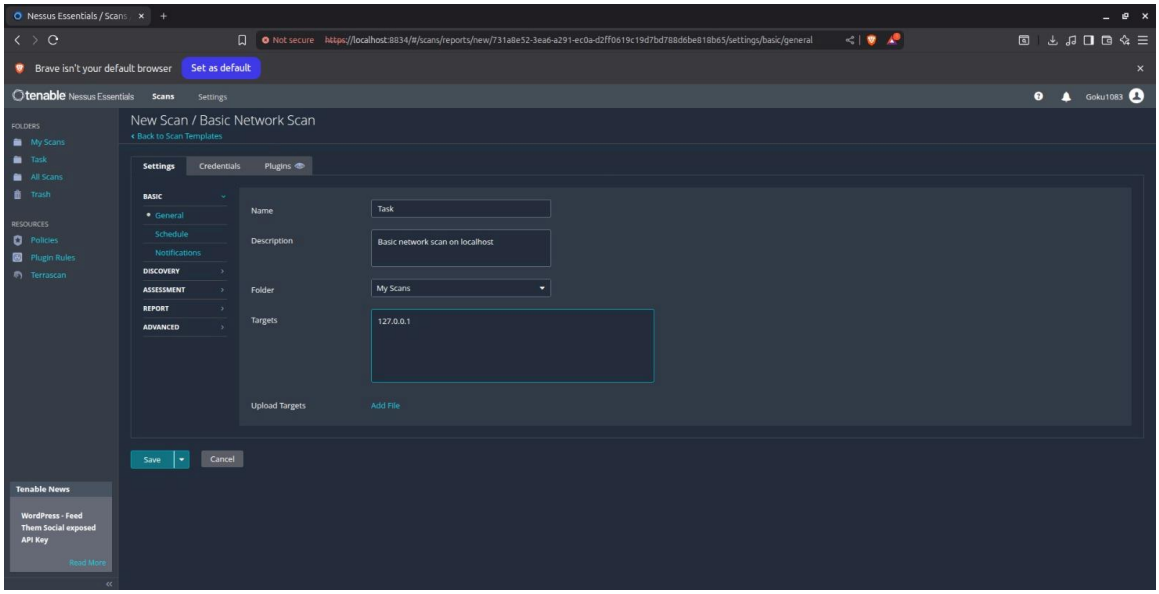
8. Conclusion

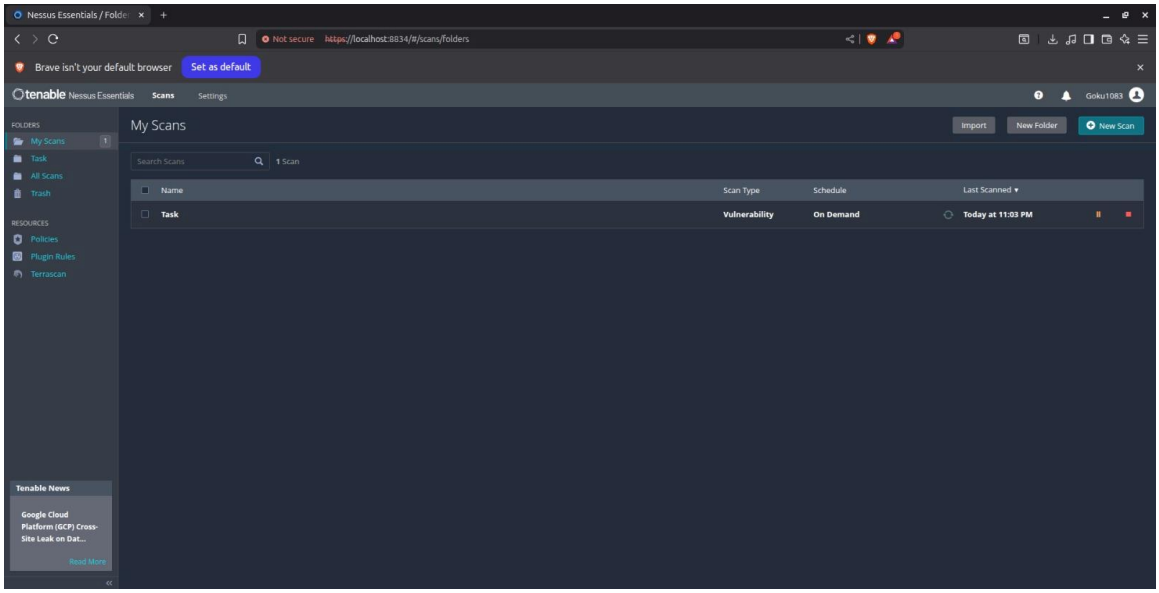
The vulnerability assessment of the localhost environment using Nessus Essentials revealed significant security concerns requiring immediate attention. The identification of high-severity vulnerabilities, particularly the EDK2 buffer overflow (CVE-2023-45235) and REXML DoS vulnerability (CVE-2024-39908), demonstrates the critical importance of maintaining current security patches and configurations.

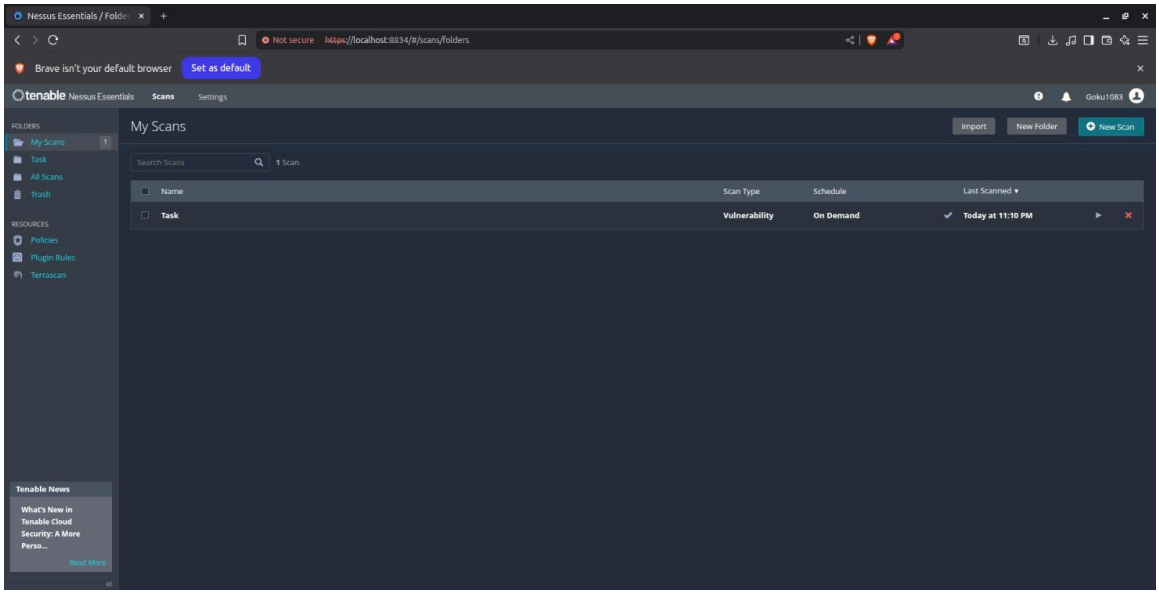
This assessment provides a solid foundation for improving the security posture of the scanned system and serves as a baseline for future security evaluations.

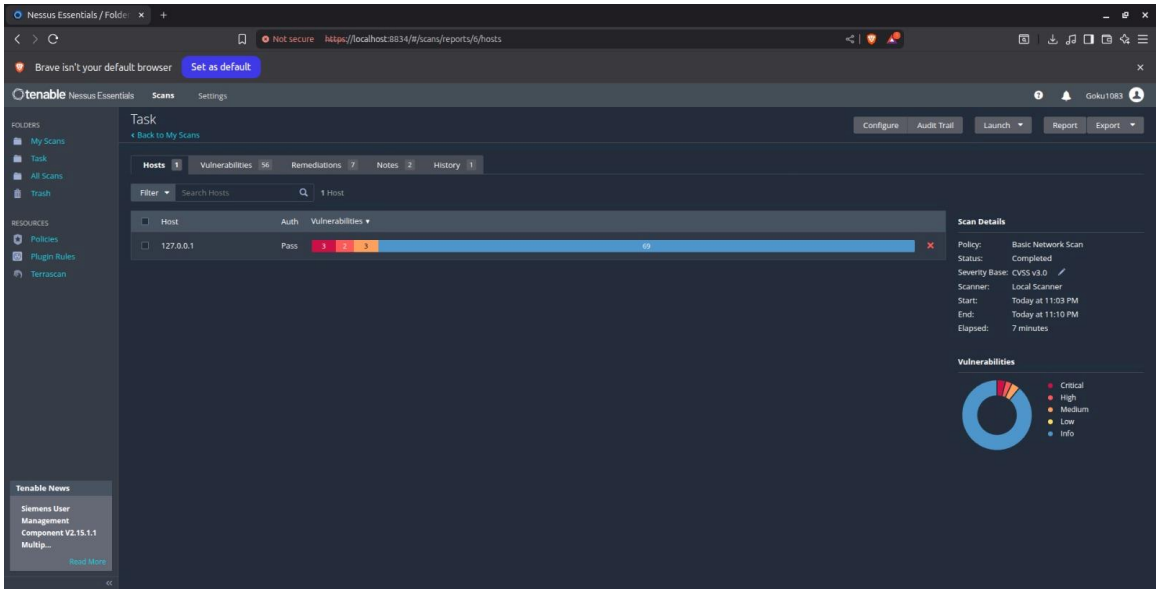

Nessus Essentials / Folder
Not secure https://localhost:8834/#/scans/folders/my-scans
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
Tenable News
Siemens User Management Component V2.15.1.1 Multip...
Read More

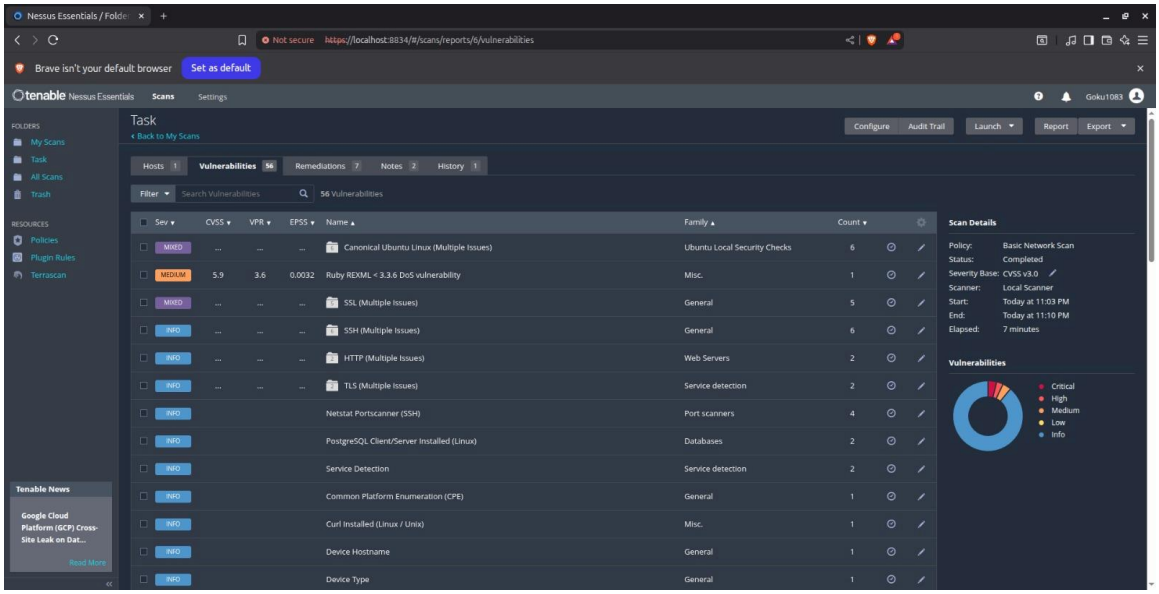

Nessus Essentials / Scans
Not secure https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
REQUIRED
Description
Folder
My Scans
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED
Upload Targets
Add File
Save
Cancel
Tenable News
Cybersecurity Snapshot: Cyber Platforms Are CISOs'...
Read More

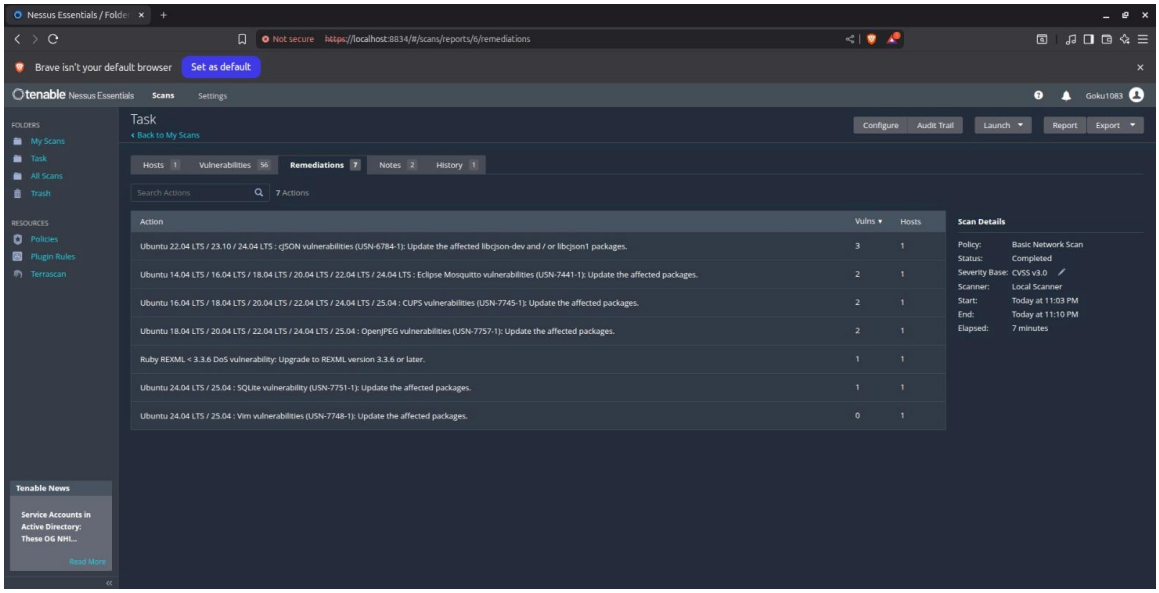

Nessus Essentials / Scans
Not secure https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Task
Description
Basic network scan on localhost
Folder
My Scans
Targets
127.0.0.1
Upload Targets
Add File
Save
Cancel
Tenable News
WordPress - Feed Them Social exposed API Key
Read More

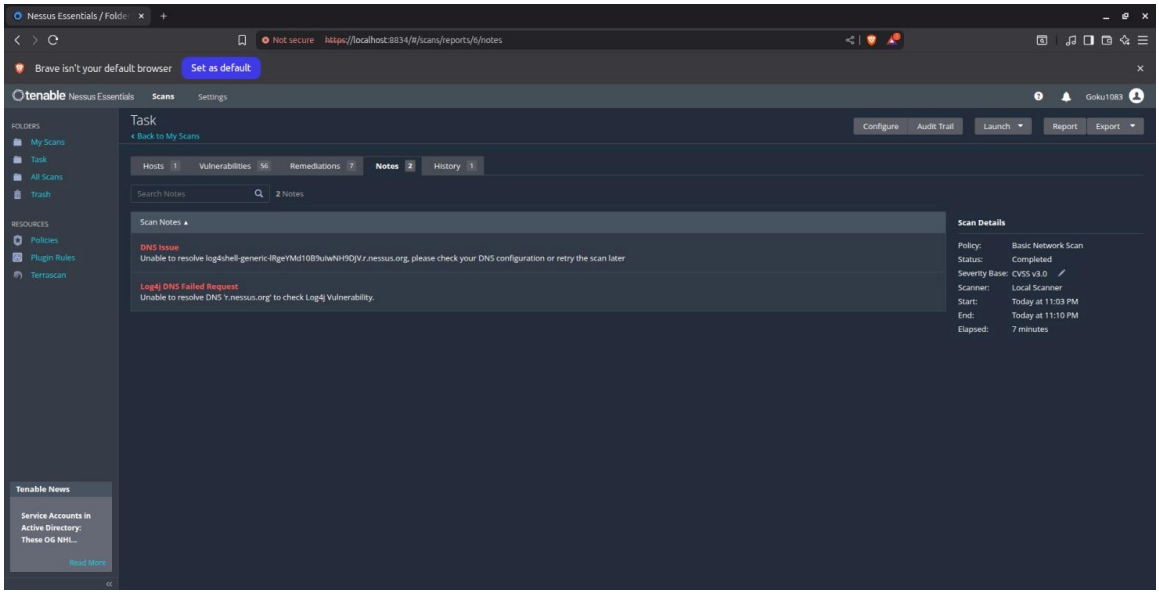

Nessus Essentials / Folders
Not secure https://localhost:8834/#/scans/folders
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
Task
Vulnerability
On Demand
Today at 11:03 PM
Tenable News
Google Cloud Platform (GCP) Cross-Site Leak on Dat...
Read More


Nessus Essentials / Folder
Not secure https://localhost:8834/#/scans/folders
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
Task
Vulnerability
On Demand
Today at 11:10 PM
Tenable News
What's New in Tenable Cloud Security: A More Perso...
Read More


Nessus Essentials / Folder
Not secure https://localhost:8834/#/scans/reports/6/hosts
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Task
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 56
Remediations 7
Notes 2
History 1
Filter
Search Hosts
1 Host
Host
Auth
Vulnerabilities
127.0.0.1
Pass
3
2
3
69
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:03 PM
End: Today at 11:10 PM
Elapsed: 7 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Siemens User Management Component V2.15.1.1 Multip...
Read More


Nessus Essentials / Folder
Not secure https://localhost:8834/#/scans/reports/6/vulnerabilities
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Task
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 56
Remediations 7
Notes 2
History 1
Filter
Search Vulnerabilities
56 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MIXED Canonical Ubuntu Linux (Multiple Issues) Ubuntu Local Security Checks 6
MEDIUM 5.9 3.6 0.0032 Ruby REXML < 3.3.6 DoS vulnerability Misc. 1
MIXED SSL (Multiple Issues) General 5
INFO SSH (Multiple Issues) General 6
INFO HTTP (Multiple Issues) Web Servers 2
INFO TLS (Multiple Issues) Service detection 2
INFO Netstat Portscanner (SSH) Port scanners 4
INFO PostgreSQL Client/Server Installed (Linux) Databases 2
INFO Service Detection Service detection 2
INFO Common Platform Enumeration (CPE) General 1
INFO Curl Installed (Linux / Unix) Misc. 1
INFO Device Hostname General 1
INFO Device Type General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:03 PM
End: Today at 11:10 PM
Elapsed: 7 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Google Cloud Platform (GCP) Cross-Site Leak on Dat...
Read More


Nessus Essentials / Folder
Not secure https://localhost:8834/#/scans/reports/6/remediations
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Task
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 56
Remediations 7
Notes 2
History 1
Search Actions
7 Actions
Action
Vulns
Hosts
Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : cJSON vulnerabilities (USN-6784-1): Update the affected libcjson-dev and / or libcjson1 packages. 3 1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Eclipse Mosquitto vulnerabilities (USN-7441-1): Update the affected packages. 2 1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : CUPS vulnerabilities (USN-7745-1): Update the affected packages. 2 1
Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : OpenJPEG vulnerabilities (USN-7757-1): Update the affected packages. 2 1
Ruby REXML < 3.3.6 DoS vulnerability: Upgrade to REXML version 3.3.6 or later. 1 1
Ubuntu 24.04 LTS / 25.04 : SQLite vulnerability (USN-7751-1): Update the affected packages. 1 1
Ubuntu 24.04 LTS / 25.04 : Vim vulnerabilities (USN-7748-1): Update the affected packages. 0 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:03 PM
End: Today at 11:10 PM
Elapsed: 7 minutes
Tenable News
Service Accounts in Active Directory: These OG NHI...
Read More


Nessus Essentials / Folder
Not secure https://localhost:8834/#/scans/reports/6/notes
Brave isn't your default browser
Set as default
tenable Nessus Essentials
Scans
Settings
Goku1083
FOLDERS
My Scans
Task
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Service Accounts in Active Directory: These OG NHI...
Read More
Task
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 56
Remediations 7
Notes 2
History 1
Search Notes
2 Notes
Scan Notes
DNS Issue
Unable to resolve log4shell-generic-IRgeYMd10B9ulwNH9DJV.r.nessus.org, please check your DNS configuration or retry the scan later
Log4j DNS Failed Request
Unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability.
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:03 PM
End: Today at 11:10 PM
Elapsed: 7 minutes