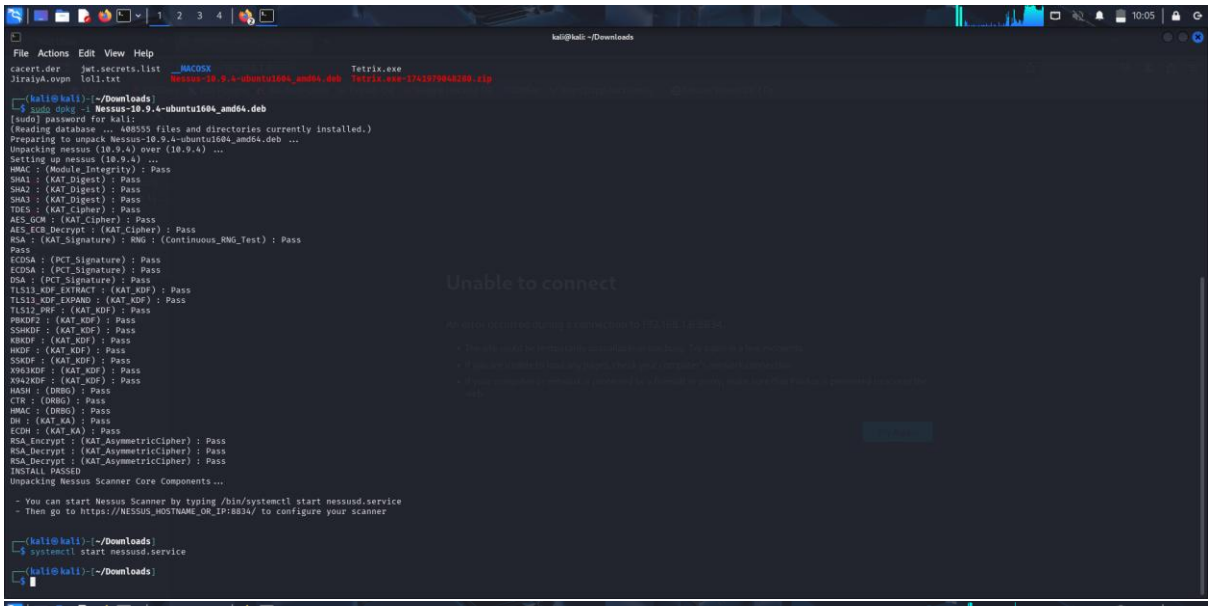
Elevate labs Taks-3

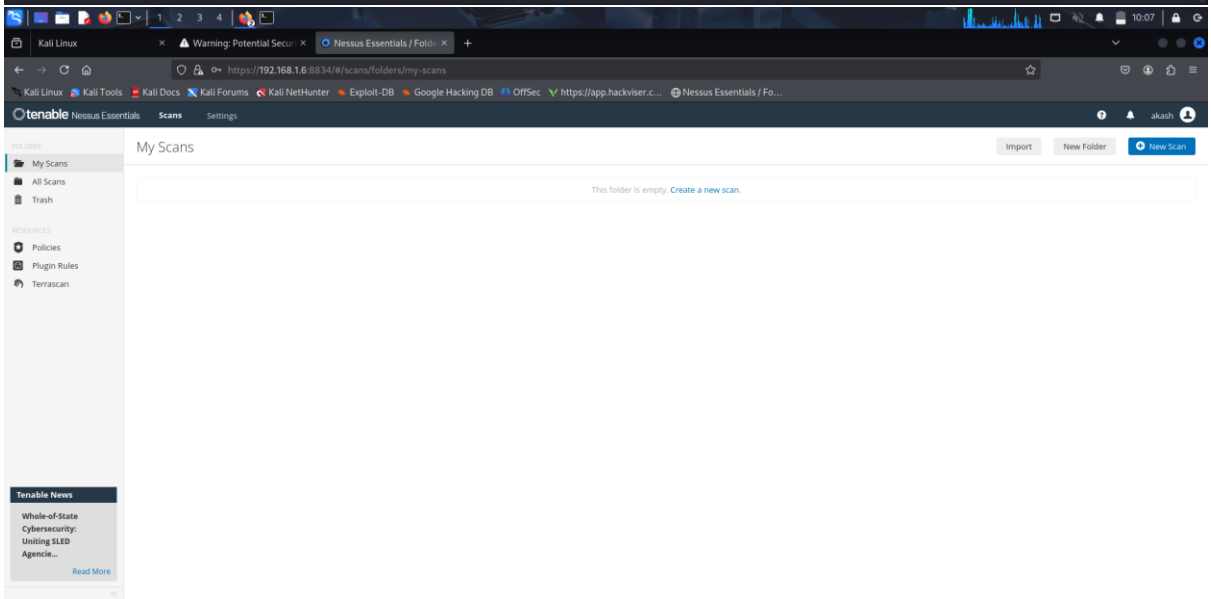
Task 3 : Perform a Basic Vulnerability Scan on Your PC.

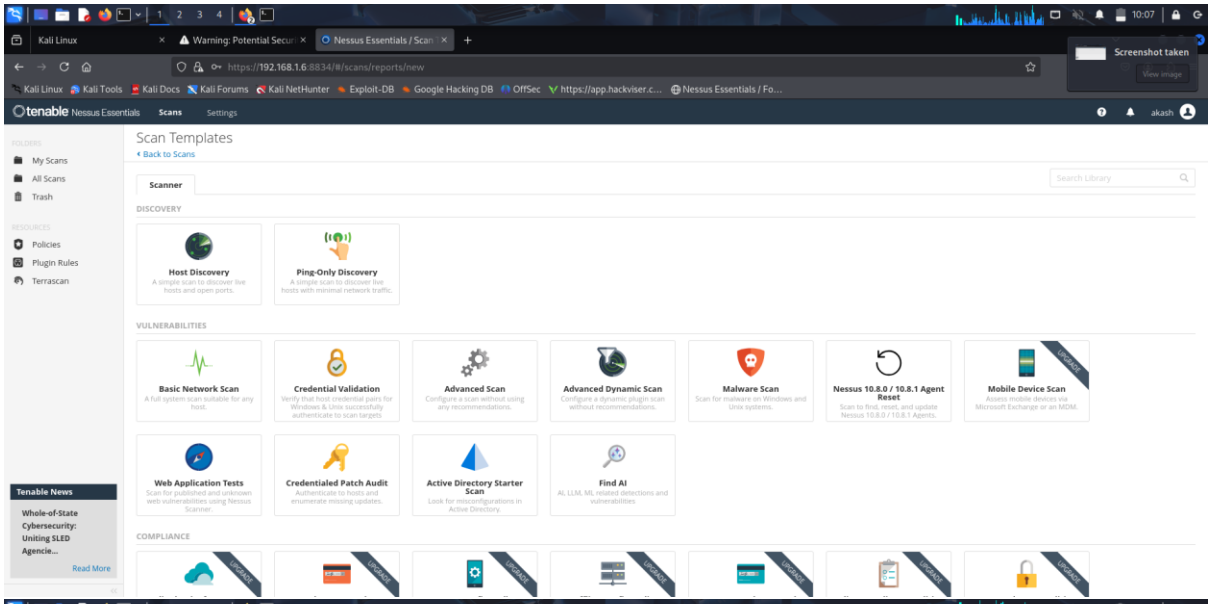
First we have to download any one of theose software like Nessus or OpenVAS

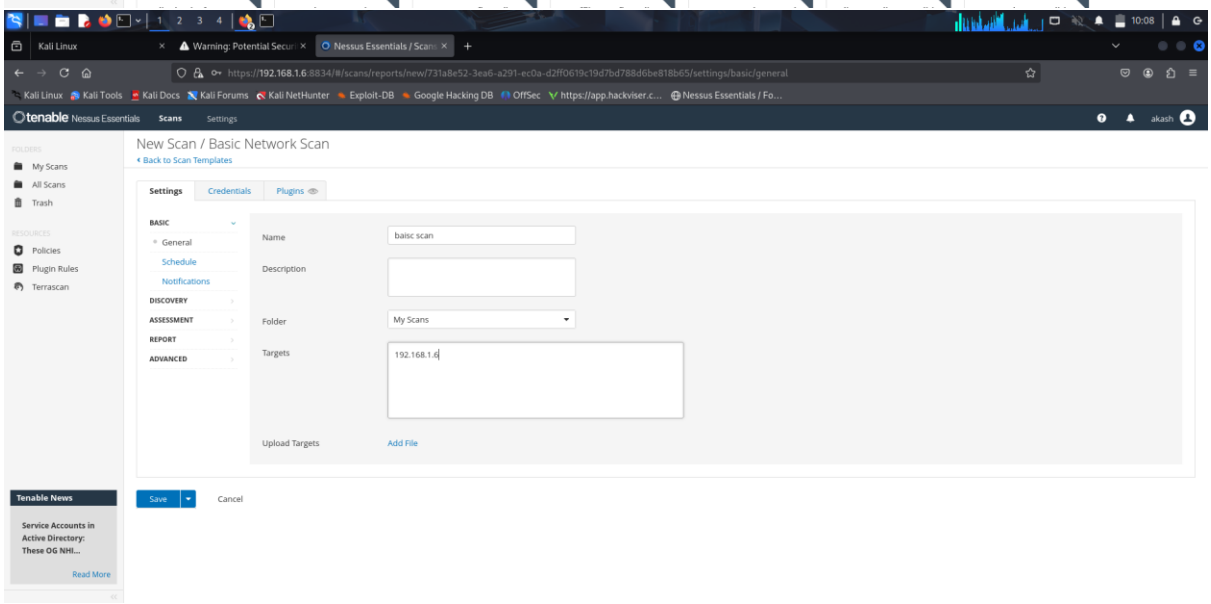
I have selected Nessus for this task
we can get how to download Nessus from youtube

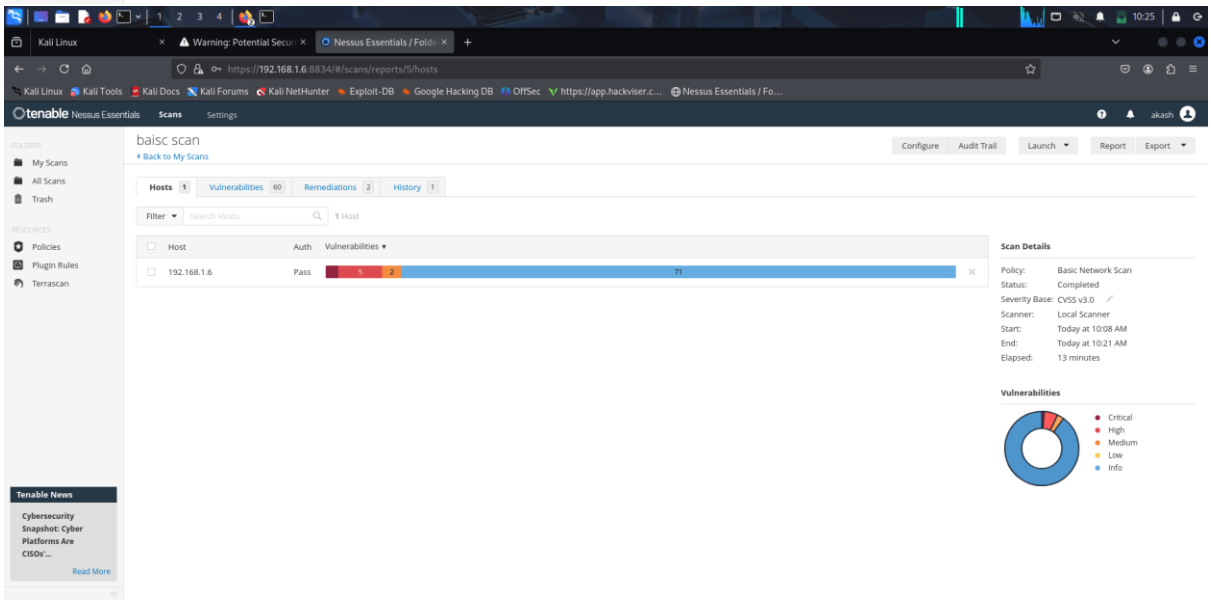
From Nessus we need to to port scan and we need to keep our IP address

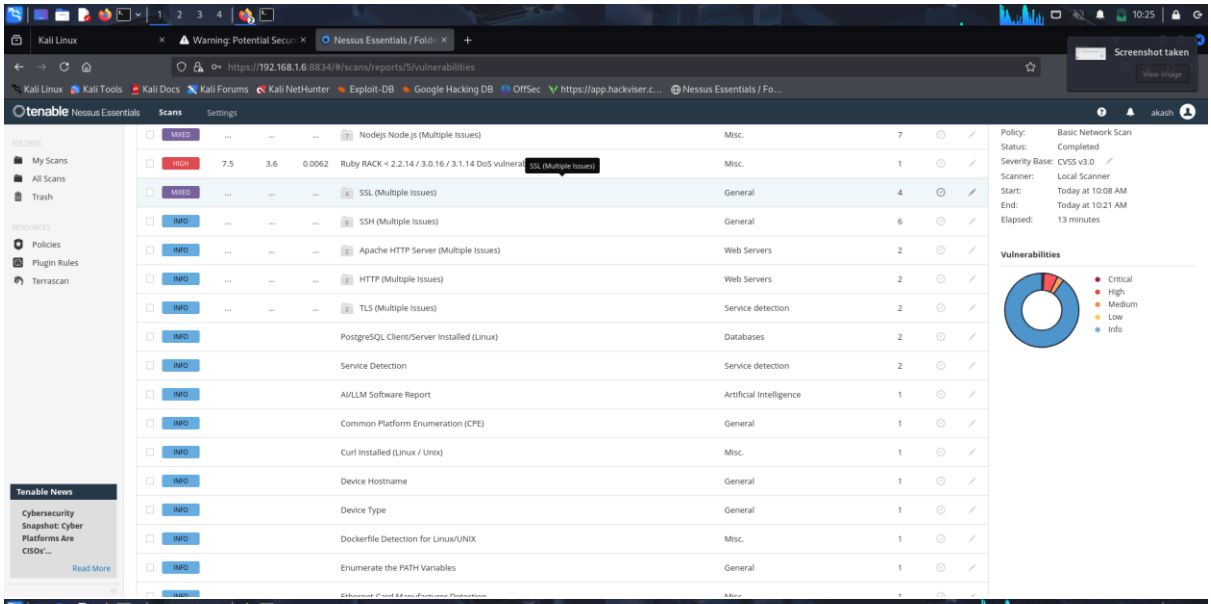


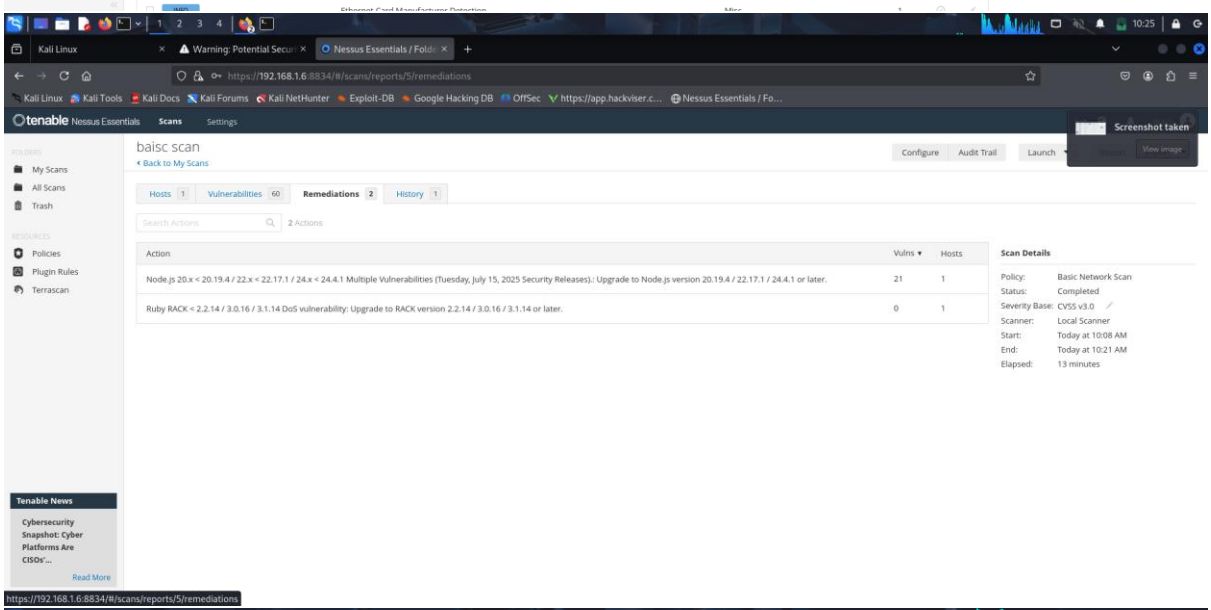


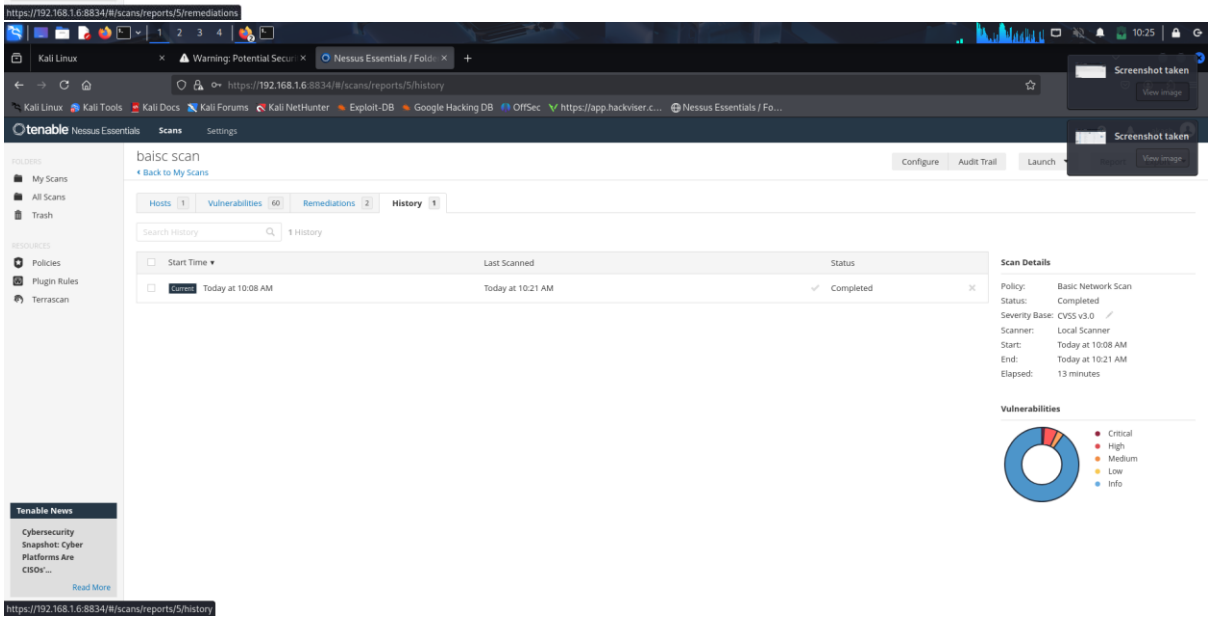

Kali Linux
Warning: Potential Secur
Nessus Essentials / Scan
https://192.168.1.6:8834/#/scans/reports/new
Screenshot taken
tenable Nessus Essentials
Scans
Settings
akash
Scan Templates
Back to Scans
Scanner
DISCOVERY
Host Discovery
Ping-Only Discovery
VULNERABILITIES
Basic Network Scan
Credential Validation
Advanced Scan
Advanced Dynamic Scan
Malware Scan
Nessus 10.8.0 / 10.8.1 Agent Reset
Mobile Device Scan
Web Application Tests
Credentialed Patch Audit
Active Directory Starter Scan
Find AI
COMPLIANCE
My Scans
All Scans
Trash
Policies
Plugin Rules
Terrascan
Tenable News
Whole-of-State Cybersecurity: Uniting SLED Agencie...
Read More


Kali Linux
Warning: Potential Secur
Nessus Essentials / Scan
https://192.168.1.6:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
tenable Nessus Essentials
Scans
Settings
akash
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
baisc scan
Description
Folder
My Scans
Targets
192.168.1.6
Upload Targets
Add File
Save
Cancel
My Scans
All Scans
Trash
Policies
Plugin Rules
Terrascan
Tenable News
Service Accounts in Active Directory: These OG NHI...
Read More


Kali Linux
Warning: Potential Secur
Nessus Essentials / Folde
https://192.168.1.6:8834/#/scans/reports/5/hosts
tenable Nessus Essentials
Scans
Settings
akash
baisc scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 60
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Auth
Vulnerabilities
192.168.1.6
Pass
5
2
71
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:08 AM
End: Today at 10:21 AM
Elapsed: 13 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
My Scans
All Scans
Trash
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Cyber Platforms Are CISOs'...
Read More


Kali Linux
Warning: Potential Secur
Nessus Essentials / Folde
https://192.168.1.6:8834/#/scans/reports/5/vulnerabilities
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec https://app.hackviser.c... Nessus Essentials / Fo...
tenable Nessus Essentials
Scans
Settings
akash
Screenshot taken
View image
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Cyber Platforms Are CISOs'...
Read More
MIXED Nodejs Node.js (Multiple Issues) Misc. 7
HIGH 7.5 3.6 0.0062 Ruby RACK < 2.2.14 / 3.0.16 / 3.1.14 DoS vulnerabil SSL (Multiple Issues) Misc. 1
MIXED SSL (Multiple Issues) General 4
INFO SSH (Multiple Issues) General 6
INFO Apache HTTP Server (Multiple Issues) Web Servers 2
INFO HTTP (Multiple Issues) Web Servers 2
INFO TLS (Multiple Issues) Service detection 2
INFO PostgreSQL Client/Server Installed (Linux) Databases 2
INFO Service Detection Service detection 2
INFO AI/LLM Software Report Artificial Intelligence 1
INFO Common Platform Enumeration (CPE) General 1
INFO Curl Installed (Linux / Unix) Misc. 1
INFO Device Hostname General 1
INFO Device Type General 1
INFO Dockerfile Detection for Linux/UNIX Misc. 1
INFO Enumerate the PATH Variables General 1
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:08 AM
End: Today at 10:21 AM
Elapsed: 13 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Kali Linux
Warning: Potential Secur
Nessus Essentials / Folde
https://192.168.1.6:8834/#/scans/reports/5/remediations
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec https://app.hackviser.c... Nessus Essentials / Fo...
tenable Nessus Essentials
Scans
Settings
Screenshot taken
View image
baisc scan
Back to My Scans
Configure
Audit Trail
Launch
Hosts 1
Vulnerabilities 60
Remediations 2
History 1
Search Actions
2 Actions
Action
Vulns
Hosts
Node.js 20.x < 20.19.4 / 22.x < 22.17.1 / 24.x < 24.4.1 Multiple Vulnerabilities (Tuesday, July 15, 2025 Security Releases).: Upgrade to Node.js version 20.19.4 / 22.17.1 / 24.4.1 or later.
21
1
Ruby RACK < 2.2.14 / 3.0.16 / 3.1.14 DoS vulnerability: Upgrade to RACK version 2.2.14 / 3.0.16 / 3.1.14 or later.
0
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:08 AM
End: Today at 10:21 AM
Elapsed: 13 minutes
Tenable News
Cybersecurity Snapshot: Cyber Platforms Are CISOs'...
Read More
https://192.168.1.6:8834/#/scans/reports/5/remediations


Kali Linux
Warning: Potential Secur
Nessus Essentials / Folde
https://192.168.1.6:8834/#/scans/reports/5/history
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec https://app.hackviser.c... Nessus Essentials / Fo...
tenable Nessus Essentials
Scans
Settings
Screenshot taken
View image
baisc scan
Back to My Scans
Configure
Audit Trail
Launch
Hosts 1
Vulnerabilities 60
Remediations 2
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 10:08 AM
Today at 10:21 AM
Completed
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:08 AM
End: Today at 10:21 AM
Elapsed: 13 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Cybersecurity Snapshot: Cyber Platforms Are CISOs'...
Read More
https://192.168.1.6:8834/#/scans/reports/5/history

Here is the description of the task

- **Task Focus:** This document is about performing a basic vulnerability scan on your PC using Nessus, a widely-used vulnerability scanner. The procedure starts with downloading Nessus (with a mention of OpenVAS as an alternative), and then guides you through the installation process specifically on Kali Linux, detailing the steps and commands required for setup.
- **Installation Steps:** It includes examples of terminal commands like sudo dpkg -i Nessus-10.9.4-ubuntu1604 amd64.deb for installation, and the use of systemctl start nessusd.service to start the Nessus service. After installation, configuration is done via the browser interface at https://<hostname or IP>:8834.
- **Scanning Workflow:** Once Nessus is active, the PDF walks through creating a "Basic Network Scan." It describes accessing the interface, setting scan templates, adding targets (IP addresses), and launching the scan. The interface features, such as folders, scan settings, plugin rules, and policies, are briefly mentioned.
- **Finding Vulnerabilities:** After running the scan, the report includes a breakdown of vulnerabilities found on the host, categorized by severity (Critical, High, Medium, Low, Info). The example report shows details for vulnerabilities like those in Node.js and Ruby RACK, with recommendations for upgrading to secure versions.
- **Key Results:** The scan summary lists vulnerabilities (including critical ones), remediation steps, history of scans, and the elapsed time for scanning. There are references to screenshots (not displayed here) showing the Nessus web interface and scan results.
- **Contextual Details:** The document makes reference to cybersecurity platforms, threat databases (Exploit-DB, Google Hacking DB), and tools within Kali Linux. It also touches upon audit trails, scan export options, configuration, and the importance of keeping systems updated with security patches.
- **Overall Purpose:** The PDF is instructional, targeted at beginners in cybersecurity or students learning to use vulnerability scanning tools in real-world environments. It emphasizes practical steps, results interpretation, and remediation advice for discovered vulnerabilities.