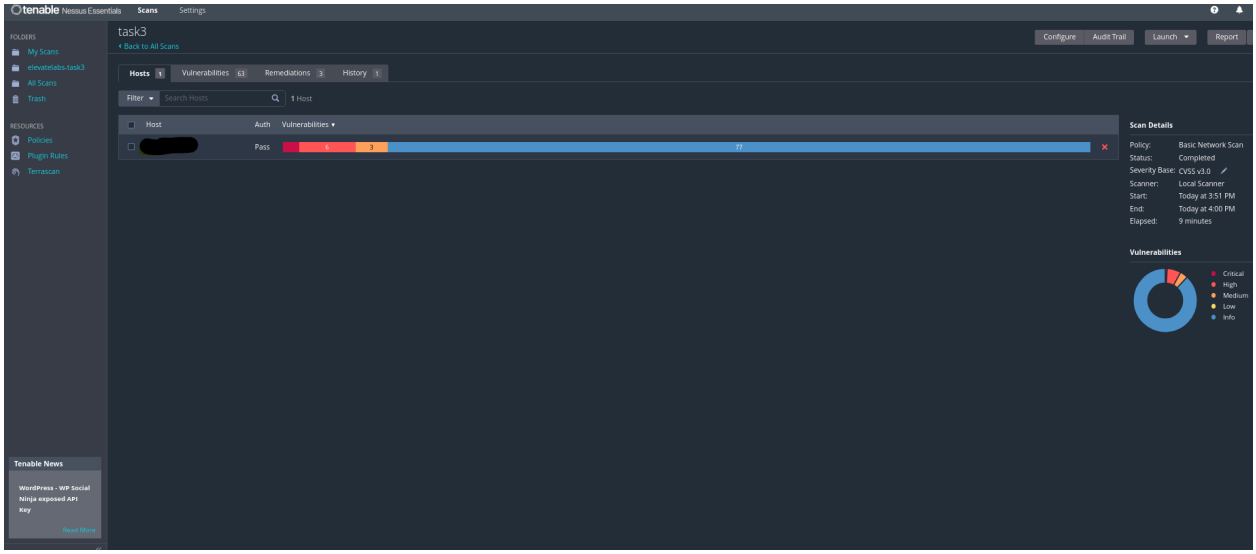
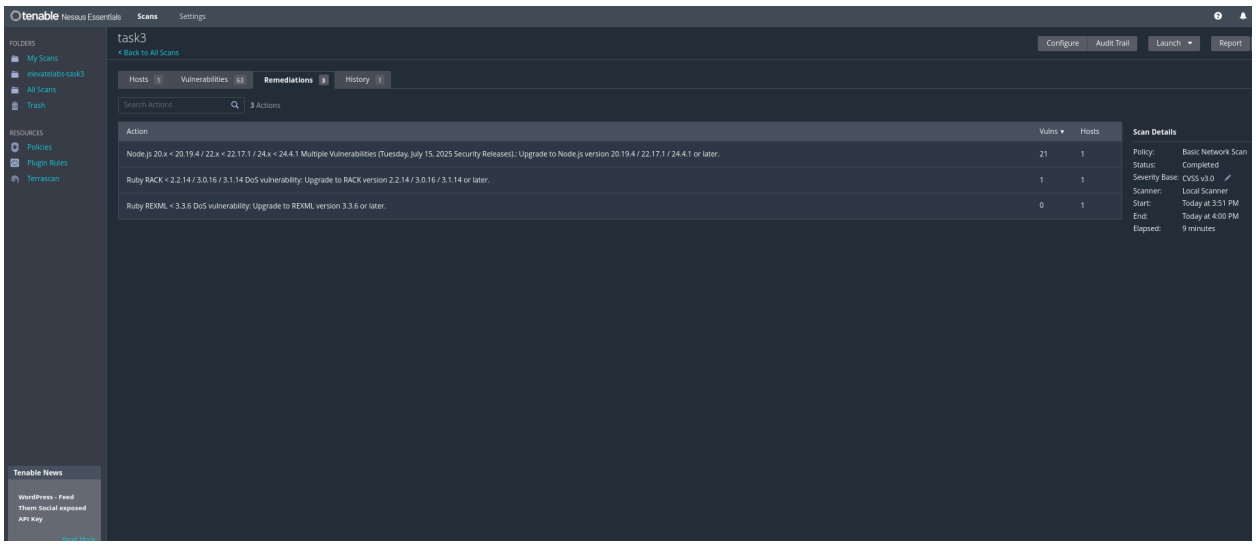
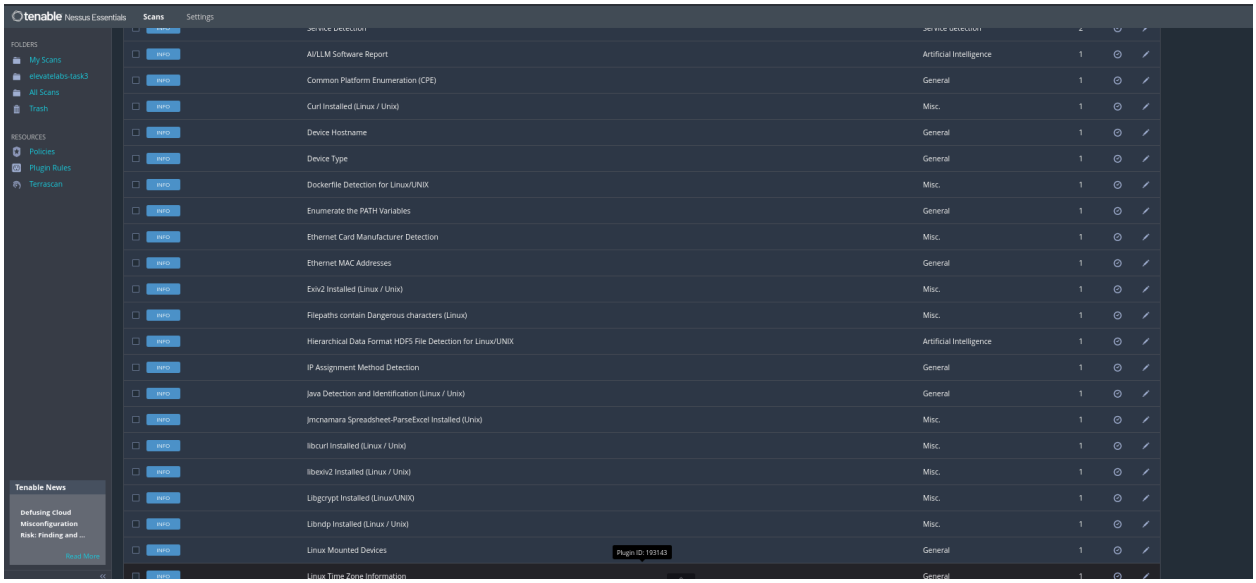
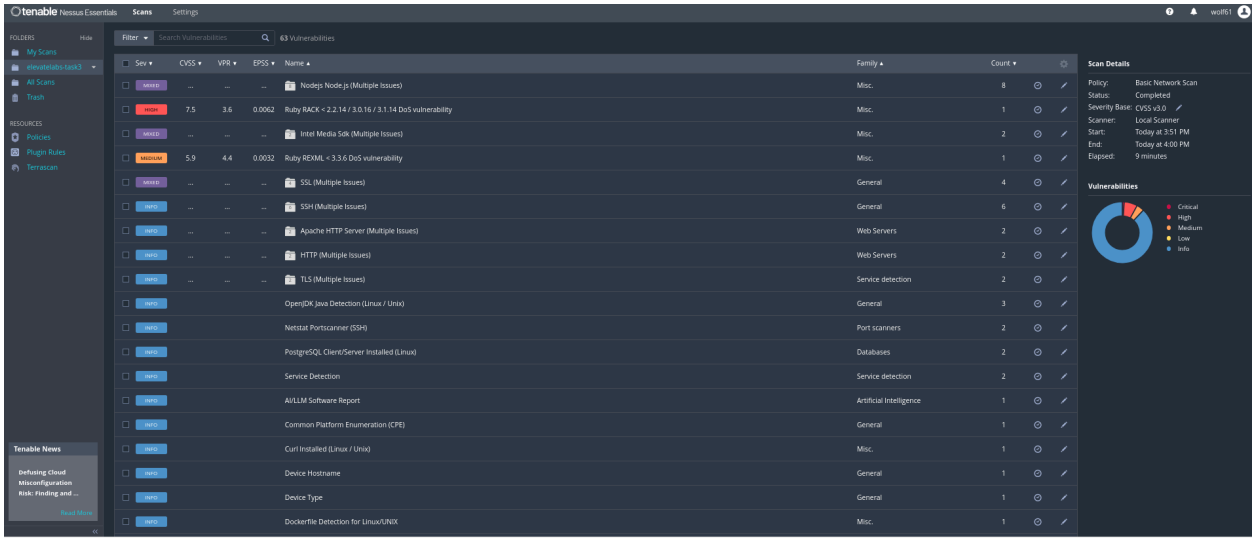
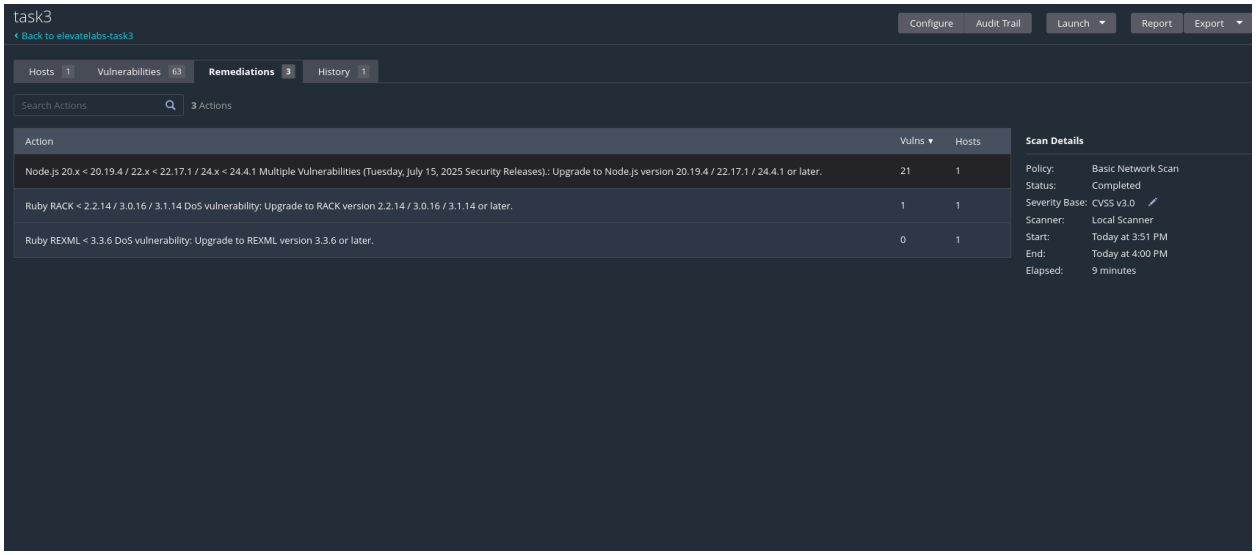

tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
elevatelabs-task3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
task3
Back to All Scans
Configure
Audit Trail
Launch
Report
Hosts 1
Vulnerabilities 63
Remediations 3
History 1
Filter
Search Hosts
1 Host
Host
Auth
Vulnerabilities
Pass
6
3
77
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:51 PM
End: Today at 4:00 PM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
WordPress - WP Social Ninja exposed API Key
Read More


tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
elevatelabs-task3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
task3
Back to All Scans
Configure
Audit Trail
Launch
Report
Hosts 1
Vulnerabilities 63
Remediations 3
History 1
Search Actions
3 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.
1
1
Ruby REXML < 3.3.6 DoS vulnerability: Upgrade to REXML version 3.3.6 or later.
0
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:51 PM
End: Today at 4:00 PM
Elapsed: 9 minutes
Tenable News
WordPress - Feed Them Social exposed API Key
Read More


tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
elevatelabs-task3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
INFO
AI/LLM Software Report
Artificial Intelligence
Common Platform Enumeration (CPE)
General
Curl Installed (Linux / Unix)
Misc.
Device Hostname
Device Type
Dockerfile Detection for Linux/UNIX
Enumerate the PATH Variables
Ethernet Card Manufacturer Detection
Ethernet MAC Addresses
Exiv2 Installed (Linux / Unix)
Filepaths contain Dangerous characters (Linux)
Hierarchical Data Format HDF5 File Detection for Linux/UNIX
IP Assignment Method Detection
Java Detection and Identification (Linux / Unix)
Jmcnamara Spreadsheet-ParseExcel Installed (Unix)
libcurl Installed (Linux / Unix)
libexiv2 Installed (Linux / Unix)
Libgcrypt Installed (Linux/UNIX)
Libndp Installed (Linux / Unix)
Linux Mounted Devices
Plugin ID: 193143
Linux Time Zone Information
Tenable News
Defusing Cloud Misconfiguration Risk: Finding and ...
Read More


tenable Nessus Essentials
Scans
Settings
wolf61
FOLDERS
Hide
My Scans
elevatelabs-task3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Defusing Cloud Misconfiguration Risk: Finding and ...
Read More
Filter
Search Vulnerabilities
63 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MIXED
Nodejs Node.js (Multiple Issues)
Misc.
8
HIGH
7.5
3.6
0.0062
Ruby RACK < 2.2.14 / 3.0.16 / 3.1.14 DoS vulnerability
Misc.
1
MIXED
Intel Media Sdk (Multiple Issues)
Misc.
2
MEDIUM
5.9
4.4
0.0032
Ruby REXML < 3.3.6 DoS vulnerability
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
OpenJDK Java Detection (Linux / Unix)
General
3
INFO
Netstat Portscanner (SSH)
Port scanners
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
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:51 PM
End: Today at 4:00 PM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


task3
Back to elevatelabs-task3
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 63
Remediations 3
History 1
Search Actions
3 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.
1
1
Ruby REXML < 3.3.6 DoS vulnerability: Upgrade to REXML version 3.3.6 or later.
0
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:51 PM
End: Today at 4:00 PM
Elapsed: 9 minutes