Task 15: Vulnerability Assessment & Risk Prioritization

Primary Tool: Nessus Essentials
Alternative Tool: OpenVAS

📌 Aim

To perform a vulnerability assessment using Nessus Essentials, analyze identified vulnerabilities, classify them based on CVE & CVSS scores, and prioritize remediation according to risk level.

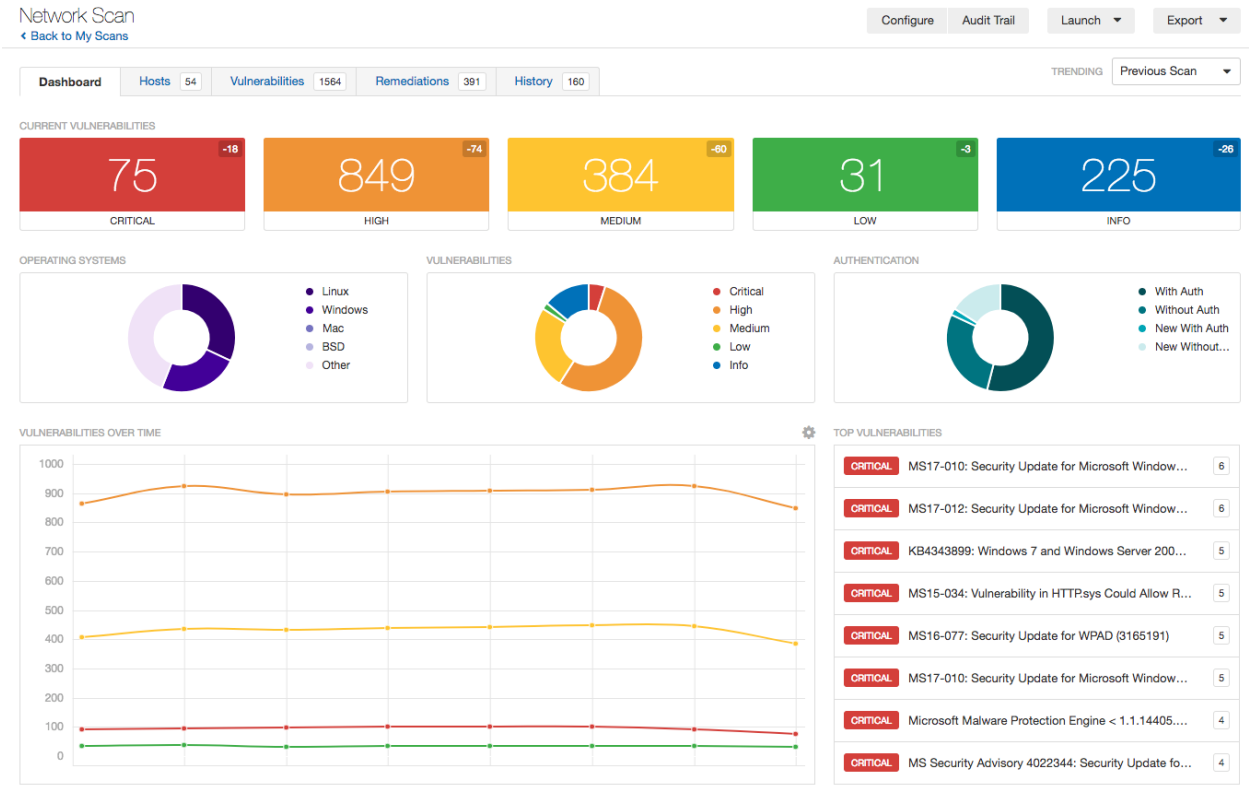
🧰 Tools Required

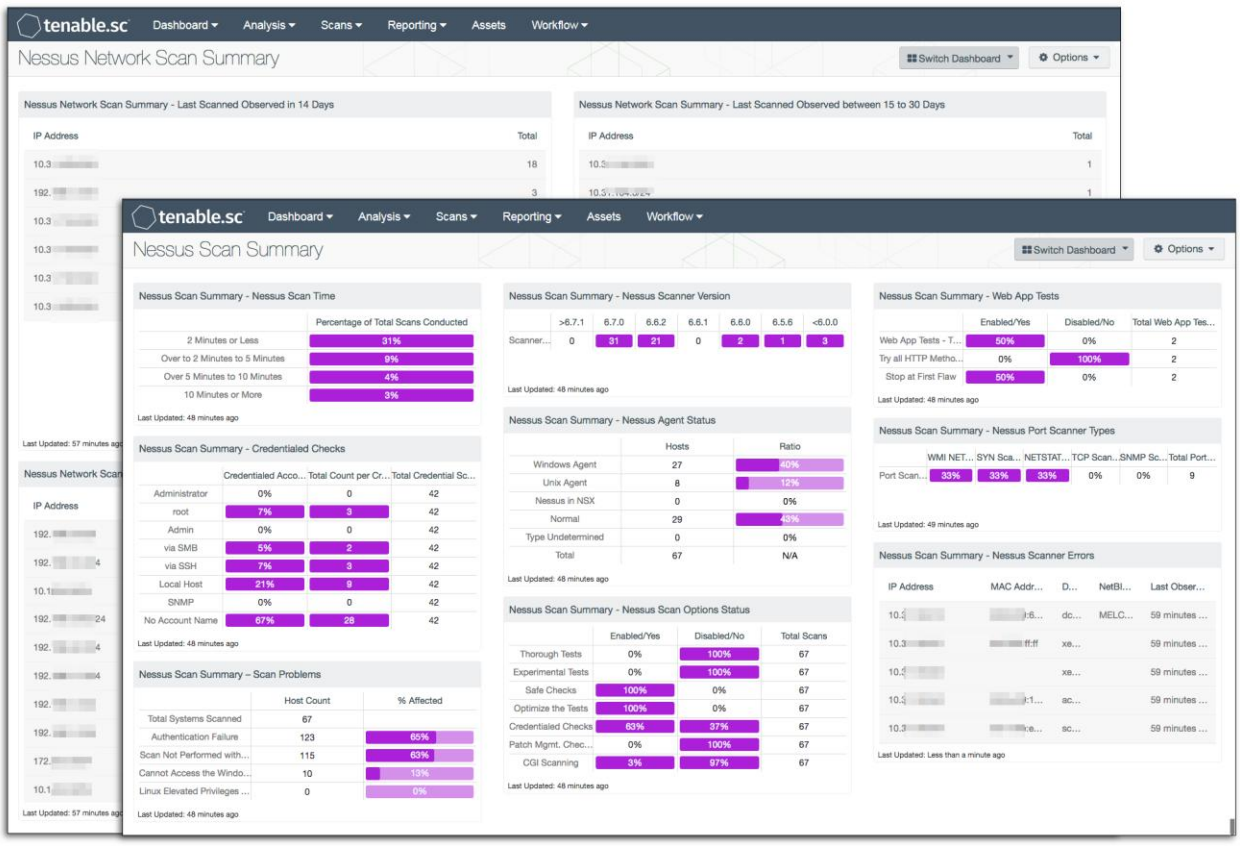
- Nessus Essentials
- Target System (Ubuntu / Windows / Kali)
- Web Browser
- Network Access

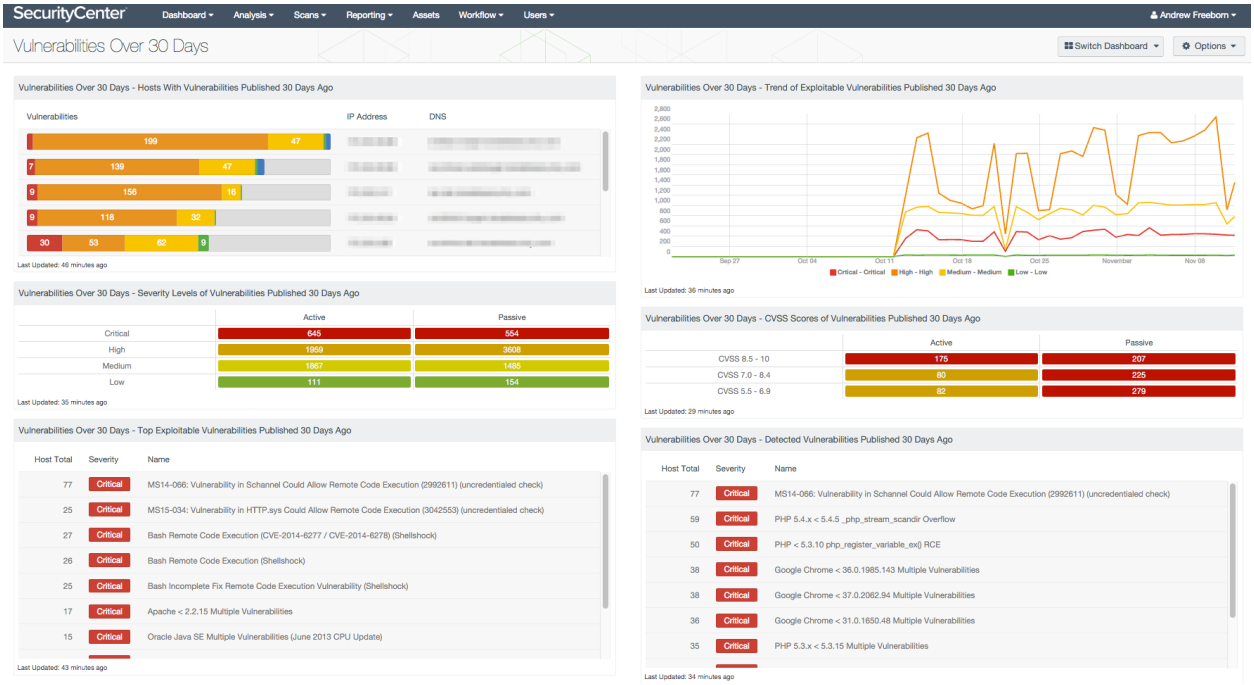
💉 Procedure with Required Screenshots

1️⃣ Install and Open Nessus

- Install Nessus Essentials
- Start Nessus service
- Open in browser: https://localhost:8834
- Login to dashboard


Network Scan
Back to My Scans
Configure
Audit Trail
Launch
Export
Dashboard
Hosts 54
Vulnerabilities 1564
Remediations 391
History 160
TRENDING
Previous Scan
CURRENT VULNERABILITIES
75 -18 CRITICAL
849 -74 HIGH
384 -60 MEDIUM
31 -3 LOW
225 -26 INFO
OPERATING SYSTEMS
Linux
Windows
Mac
BSD
Other
VULNERABILITIES
Critical
High
Medium
Low
Info
AUTHENTICATION
With Auth
Without Auth
New With Auth
New Without...
VULNERABILITIES OVER TIME
1000
900
800
700
600
500
400
300
200
100
0
TOP VULNERABILITIES
CRITICAL MS17-010: Security Update for Microsoft Window... 6
CRITICAL MS17-012: Security Update for Microsoft Window... 6
CRITICAL KB4343899: Windows 7 and Windows Server 200... 5
CRITICAL MS15-034: Vulnerability in HTTP.sys Could Allow R... 5
CRITICAL MS16-077: Security Update for WPAD (3165191) 5
CRITICAL MS17-010: Security Update for Microsoft Window... 5
CRITICAL Microsoft Malware Protection Engine < 1.1.14405.... 4
CRITICAL MS Security Advisory 4022344: Security Update fo... 4

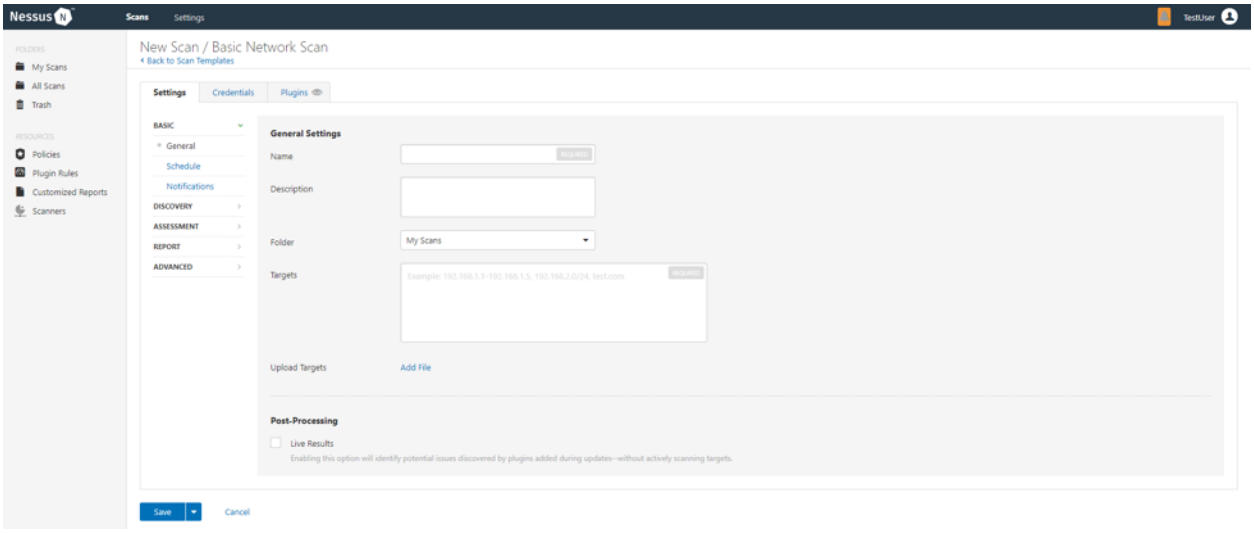

tenable.sc
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Nessus Network Scan Summary
Switch Dashboard
Options
Nessus Network Scan Summary - Last Scanned Observed in 14 Days
IP Address
Total
Nessus Network Scan Summary - Last Scanned Observed between 15 to 30 Days
IP Address
Total
tenable.sc
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Nessus Scan Summary
Switch Dashboard
Options
Nessus Scan Summary - Nessus Scan Time
Percentage of Total Scans Conducted
2 Minutes or Less 31%
Over to 2 Minutes to 5 Minutes 9%
Over 5 Minutes to 10 Minutes 4%
10 Minutes or More 3%
Last Updated: 48 minutes ago
Nessus Scan Summary - Nessus Scanner Version
>6.7.1
6.7.0
6.6.2
6.6.1
6.6.0
6.5.6
<6.0.0
Scanner...
0
31
21
0
2
1
3
Last Updated: 48 minutes ago
Nessus Scan Summary - Web App Tests
Enabled/Yes
Disabled/No
Total Web App Tes...
Web App Tests - T...
50%
0%
2
Try all HTTP Metho...
0%
100%
2
Stop at First Flaw
50%
0%
2
Last Updated: 48 minutes ago
Nessus Scan Summary - Credentialed Checks
Credentialed Acco...
Total Count per Cr...
Total Credential Sc...
Administrator 0% 0 42
root 7% 3 42
Admin 0% 0 42
via SMB 5% 2 42
via SSH 7% 3 42
Local Host 21% 9 42
SNMP 0% 0 42
No Account Name 67% 28 42
Last Updated: 48 minutes ago
Nessus Scan Summary - Nessus Agent Status
Hosts
Ratio
Windows Agent 27 40%
Unix Agent 8 12%
Nessus in NSX 0 0%
Normal 29 43%
Type Undetermined 0 0%
Total 67 N/A
Last Updated: 48 minutes ago
Nessus Scan Summary - Nessus Port Scanner Types
WMI NET...
SYN Sca...
NETSTAT...
TCP Scan...
SNMP Sc...
Total Port...
Port Scan... 33% 33% 33% 0% 0% 9
Last Updated: 49 minutes ago
Nessus Scan Summary – Scan Problems
Host Count
% Affected
Total Systems Scanned 67
Authentication Failure 123 65%
Scan Not Performed with... 115 63%
Cannot Access the Windo... 10 13%
Linux Elevated Privileges ... 0 0%
Last Updated: 48 minutes ago
Nessus Scan Summary - Nessus Scan Options Status
Enabled/Yes
Disabled/No
Total Scans
Thorough Tests 0% 100% 67
Experimental Tests 0% 100% 67
Safe Checks 100% 0% 67
Optimize the Tests 100% 0% 67
Credentialed Checks 63% 37% 67
Patch Mgmt. Chec... 0% 100% 67
CGI Scanning 3% 97% 67
Last Updated: 48 minutes ago
Nessus Scan Summary - Nessus Scanner Errors
IP Address
MAC Addr...
D...
NetBI...
Last Obser...
Last Updated: Less than a minute ago



4

2️⃣ Create New Scan

- Click **New Scan**
- Select **Basic Network Scan**
- Enter:
    - Scan Name
    - Target IP address / range
    - Credentials (if authenticated scan)



Basic Network

‹ Back to My Scans

Configure | Audit Trail | Launch | Export

Hosts 1 | **Vulnerabilities 66** | Remediations 2 | History 1

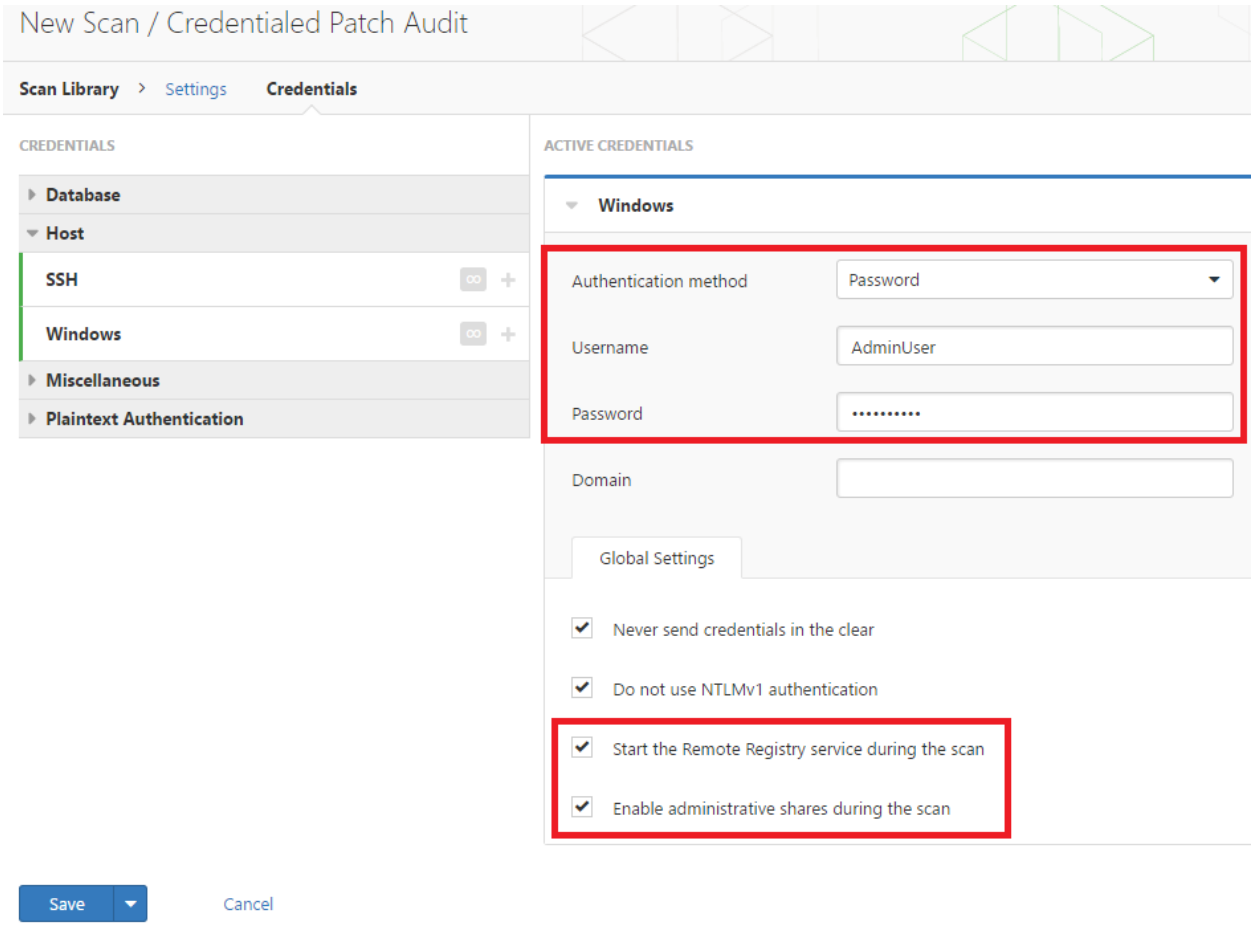
Filter | Search Vulnerabilities | 66 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1
CRITICAL	MS17-010: Security Update f...	Windows	1
HIGH	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1
HIGH	Jenkins < 2.138.4 LTS / 2.150....	CGI abuses	1
HIGH	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1
HIGH	MS12-020: Vulnerabilities in ...	Windows	1
MEDIUM	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1
MEDIUM	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1
MEDIUM	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1
MEDIUM	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1
MEDIUM	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1
MEDIUM	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1
MEDIUM	Microsoft Windows Remote ...	Windows	1

Scan Details

Name:	Basic Network
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Start:	February 25 at 9:03 AM
End:	February 25 at 9:07 AM
Elapsed:	4 minutes

Vulnerabilities

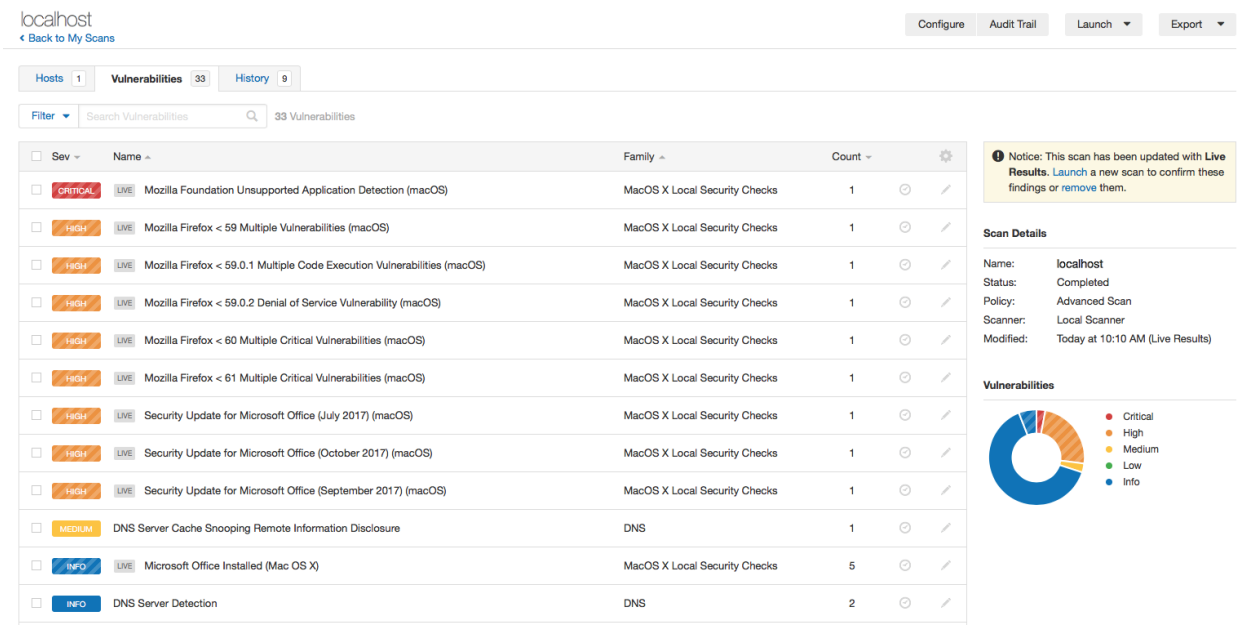


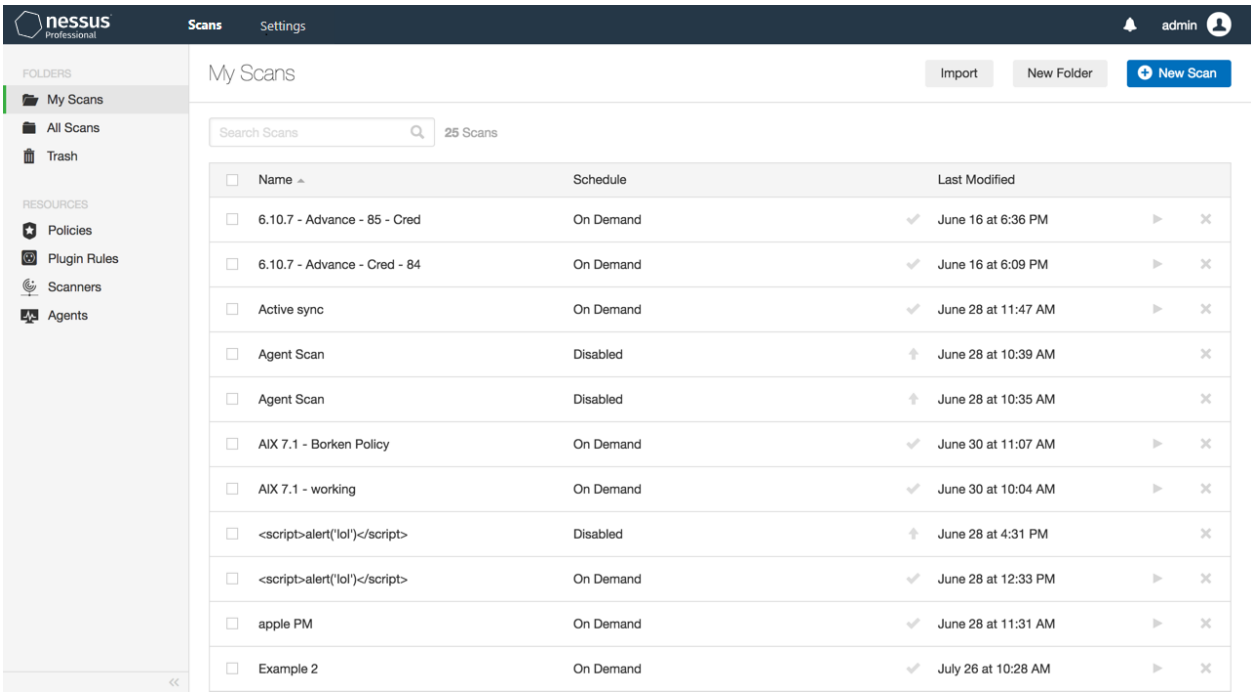
4

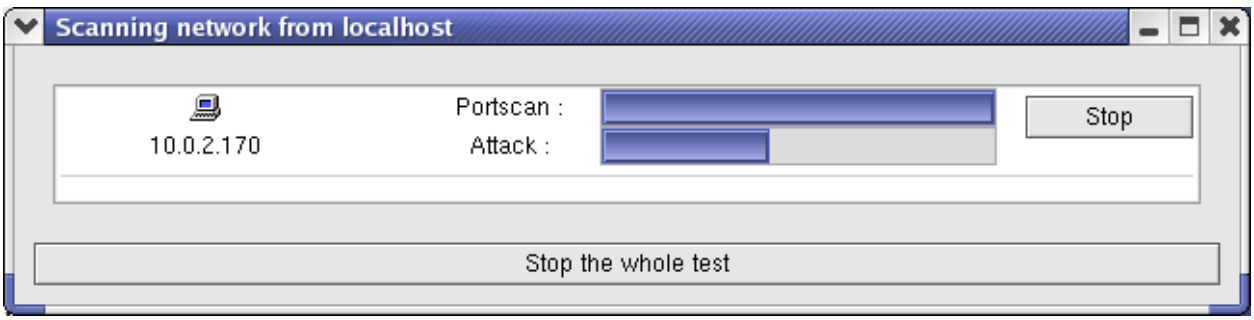
---

3 Launch Scan

- Click **Save**
- Click **Launch**
- Monitor scan progress


localhost
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 33
History 9
Filter
Search Vulnerabilities
33 Vulnerabilities
Sev
Name
Family
Count
CRITICAL LIVE Mozilla Foundation Unsupported Application Detection (macOS) MacOS X Local Security Checks 1
HIGH LIVE Mozilla Firefox < 59 Multiple Vulnerabilities (macOS) MacOS X Local Security Checks 1
HIGH LIVE Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities (macOS) MacOS X Local Security Checks 1
HIGH LIVE Mozilla Firefox < 59.0.2 Denial of Service Vulnerability (macOS) MacOS X Local Security Checks 1
HIGH LIVE Mozilla Firefox < 60 Multiple Critical Vulnerabilities (macOS) MacOS X Local Security Checks 1
HIGH LIVE Mozilla Firefox < 61 Multiple Critical Vulnerabilities (macOS) MacOS X Local Security Checks 1
HIGH LIVE Security Update for Microsoft Office (July 2017) (macOS) MacOS X Local Security Checks 1
HIGH LIVE Security Update for Microsoft Office (October 2017) (macOS) MacOS X Local Security Checks 1
HIGH LIVE Security Update for Microsoft Office (September 2017) (macOS) MacOS X Local Security Checks 1
MEDIUM DNS Server Cache Snooping Remote Information Disclosure DNS 1
INFO LIVE Microsoft Office Installed (Mac OS X) MacOS X Local Security Checks 5
INFO DNS Server Detection DNS 2
Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them.
Scan Details
Name: localhost
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Modified: Today at 10:10 AM (Live Results)
Vulnerabilities
Critical
High
Medium
Low
Info


nessus Professional
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Agents
My Scans
Import
New Folder
New Scan
Search Scans
25 Scans
Name
Schedule
Last Modified
6.10.7 - Advance - 85 - Cred On Demand June 16 at 6:36 PM
6.10.7 - Advance - Cred - 84 On Demand June 16 at 6:09 PM
Active sync On Demand June 28 at 11:47 AM
Agent Scan Disabled June 28 at 10:39 AM
Agent Scan Disabled June 28 at 10:35 AM
AIX 7.1 - Borken Policy On Demand June 30 at 11:07 AM
AIX 7.1 - working On Demand June 30 at 10:04 AM
<script>alert('lol')</script> Disabled June 28 at 4:31 PM
<script>alert('lol')</script> On Demand June 28 at 12:33 PM
apple PM On Demand June 28 at 11:31 AM
Example 2 On Demand July 26 at 10:28 AM


Scanning network from localhost
10.0.2.170
Portscan :
Attack :
Stop
Stop the whole test

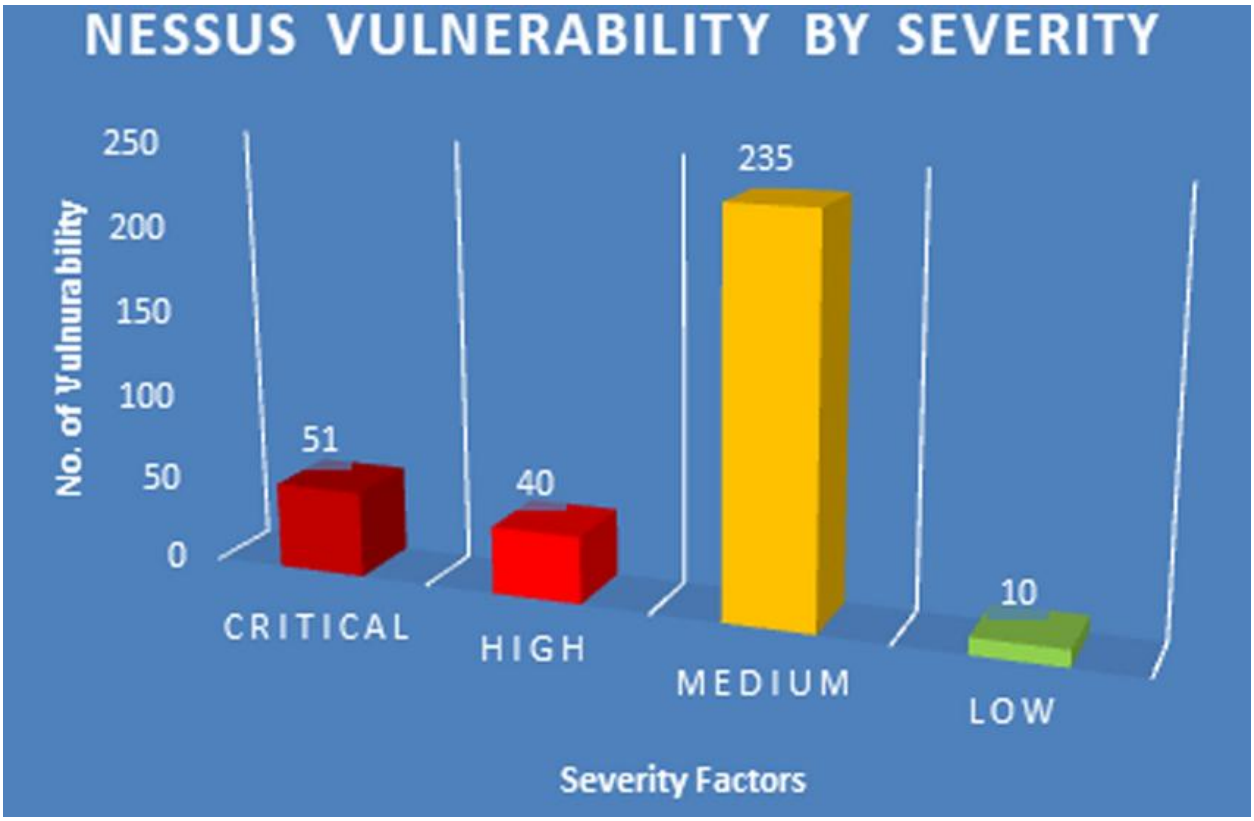
4️⃣ Review Scan Results

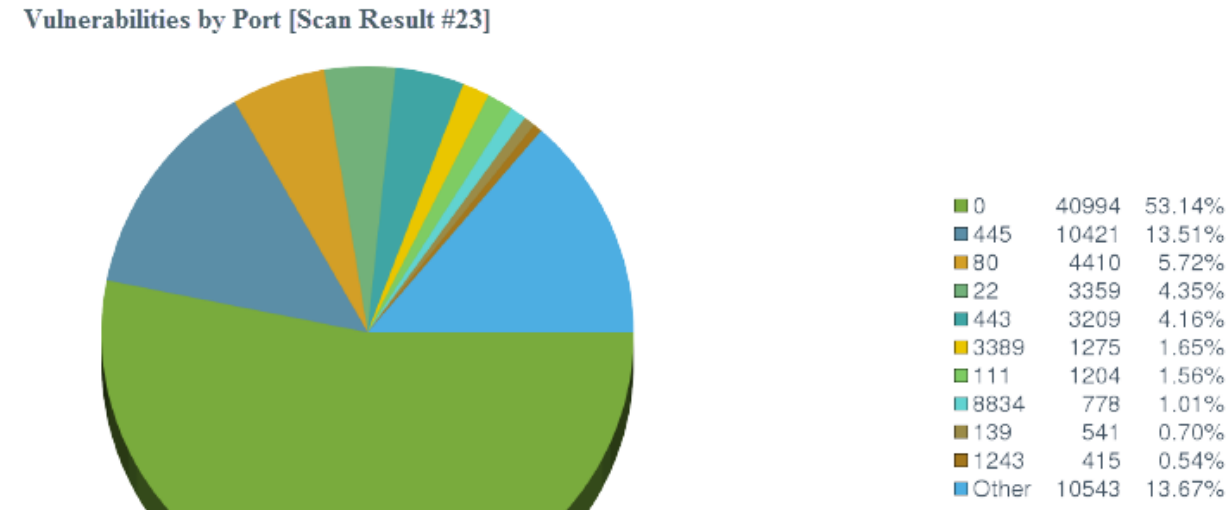
After scan completion:

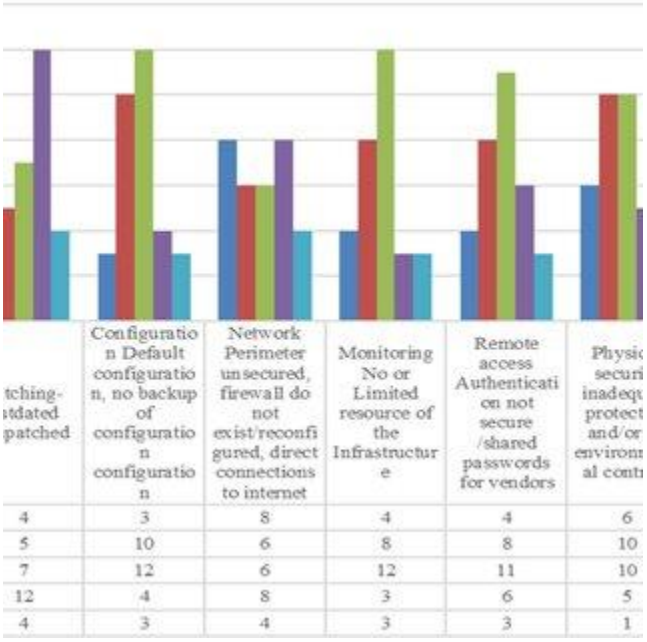
- Click on scan name
- View vulnerabilities by severity

Severity Levels:

- 🔴 Critical
- 🟠 High
- 🟡 Medium
- 🔵 Low
- ℹ️ Informational







tching- tdated patched	Configuration Default configuration, no backup of configuration configuration	Network Perimeter unsecured, firewall do not exist/reconfigured, direct connections to internet	Monitoring No or Limited resource of the Infrastructure	Remote access Authentication not secure /shared passwords for vendors	Physi securi inadeq protect and/or environ al cont
4	3	8	4	4	6
5	10	6	8	8	10
7	12	6	12	11	10
12	4	8	3	6	5
4	3	4	3	3	1

4

---

5 View Detailed Vulnerability

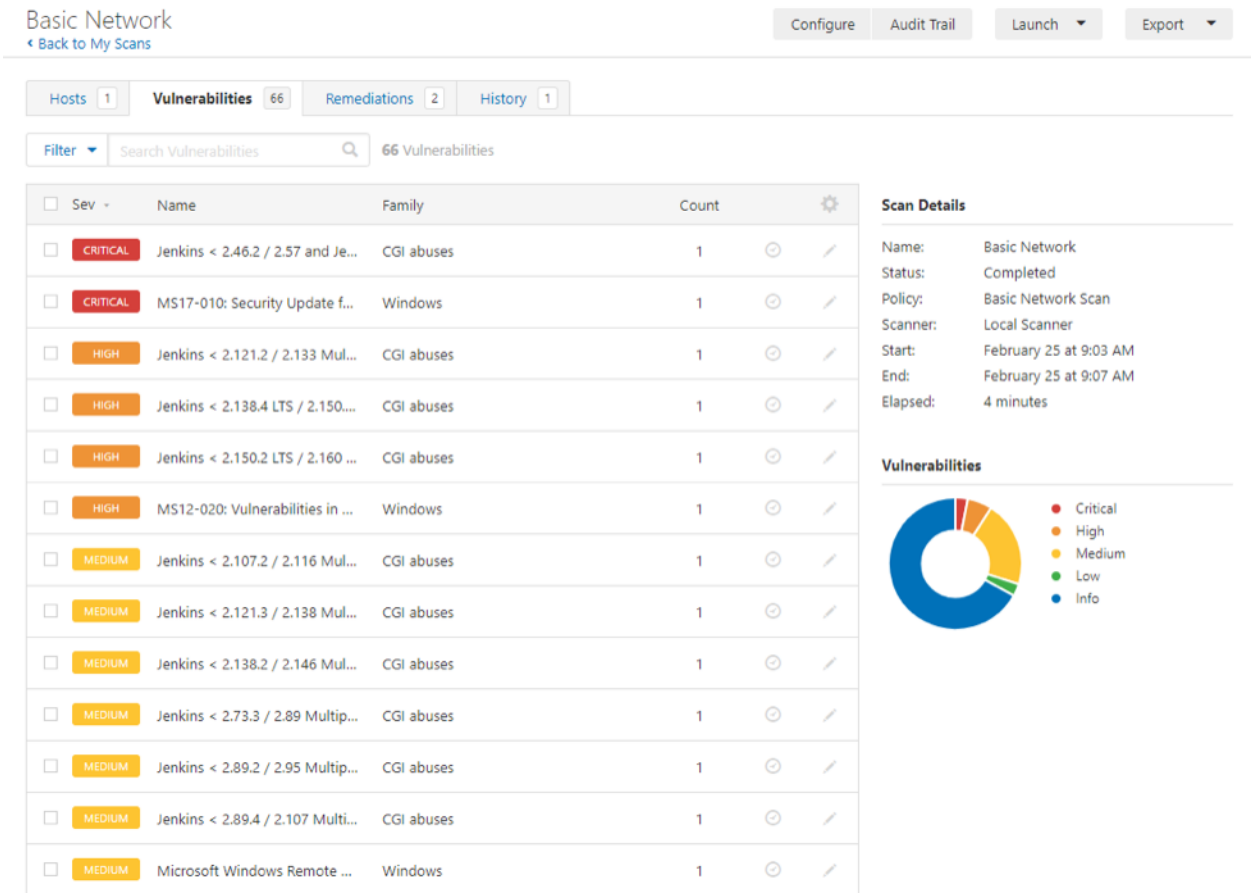
Click any **Critical vulnerability**

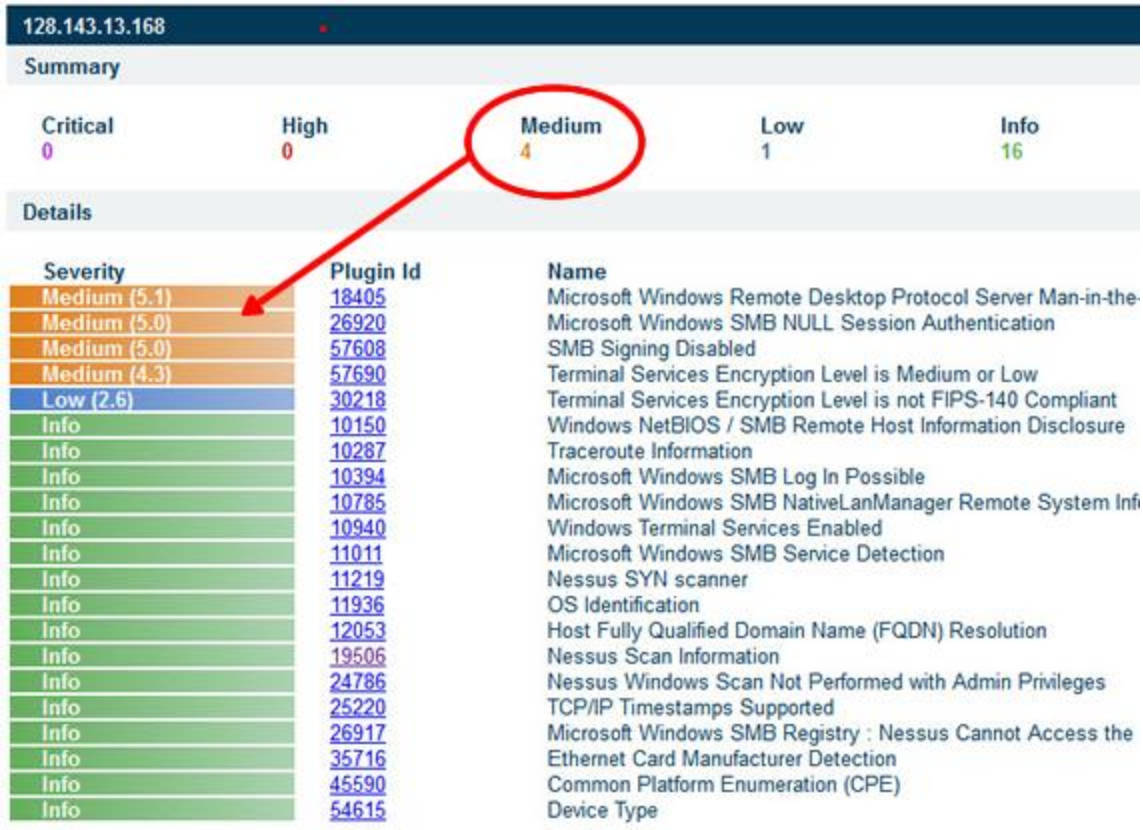
Check:

- CVE ID
- CVSS Score
- Description
- Affected Host
- Remediation Steps

📸 **Screenshot 5 Required:**

✓ Vulnerability Details Page
✓ CVE and CVSS visible





4

🔎 CVE & CVSS Explanation

CVE (Common Vulnerabilities and Exposures) is a unique identifier assigned to publicly known vulnerabilities.

Maintained by: MITRE Corporation

Example: CVE-2023-XXXX

CVSS (Common Vulnerability Scoring System) measures severity from 0 to 10:

9.0 – 10.0 → Critical
7.0 – 8.9 → High
4.0 – 6.9 → Medium
0.1 – 3.9 → Low

Higher score means higher risk.

📊 Risk Classification & Prioritization

Prioritize based on:

- CVSS score
- Business impact
- Asset importance
- Exploit availability
- Exposure (Internal / External)

Example Priority List:

1. Remote Code Execution (CVSS 9.8) – Immediate Patch
2. SMB Vulnerability (CVSS 8.5) – Disable SMBv1
3. Weak TLS Configuration (CVSS 6.5) – Update Cipher Suites