Shailesh_task3

Nessus Vulnerability Scan Report

Scan Summary

Scan Name: Advanced Scan

Scanner Used: Local Scanner

Scan Policy: Advanced Scan

CVSS Base: v3.0

Status: Completed

Start Time: 5:26 PM

End Time: 5:33 PM

Duration: 6 minutes

Total Hosts Scanned: 2

Total Vulnerabilities Detected: 58

Host: 192.168.153.61

Operating System: Linux Kernel 6.12.25-amd64

MAC Addresses: 58:11:22:81:E6:CD, B4:8C:D9:64:17:E5

Scan Duration: 6 minutes

Vulnerability Distribution:

Info: 68

Medium: 0

Low: 0

High/Critical: 0

Notable Issues:

Multiple informational vulnerabilities in:

SSL (4)

SSH (6)

Apache/HTTP/TLS (multiple)

PostgreSQL, Netstat Portscanner, CPE

LLM/AI report

Device Hostname, Type, Dockerfile presence, and Ethernet detection

---

Host: 192.168.153.248

Operating System: CentOS Linux 7.6, Kernel 3.10

MAC Address: F6:E9:4B:BB:CD:07

Scan Duration: 2 minutes

Vulnerability Distribution:

Info: 13

Low: 2

Medium: 1

High/Critical: 0

Notable Issues:

Medium:

DNS (Multiple Issues)

Low:

DHCP Server Detection (CVSS 3.3)

ICMP Timestamp Disclosure (CVSS 2.1)

Info-Level:

CPE, Device Type, Ethernet MACs

Nessus Scanner Info, mDNS, SYN Scanner

TCP/IP Timestamps, OS Fingerprint/Identification

Overall Vulnerability Breakdown (All Hosts)

Severity	Count	Description
Critical	0	No critical vulnerabilities found
High	0	No high-severity issues identified
Medium	1	Found in DNS configuration
Low	2	Common network disclosures
Info	81	General information and environment fingerprinting

Prioritize Fixes for:

DNS configuration (medium severity).

DHCP and ICMP timestamp disclosures (low severity) as they may leak internal network information.

Informational Checks:

Though not threats, excessive info-level alerts (like exposed services, enumeration data, version banners) may aid attackers in recon.

Consider minimizing unnecessary service exposure.

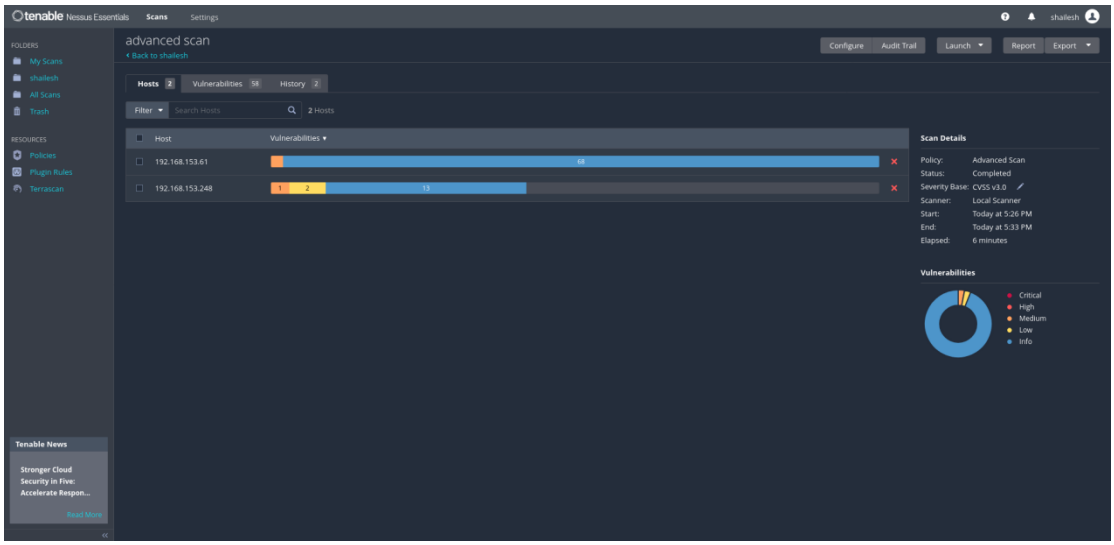
Patch & Harden Systems:

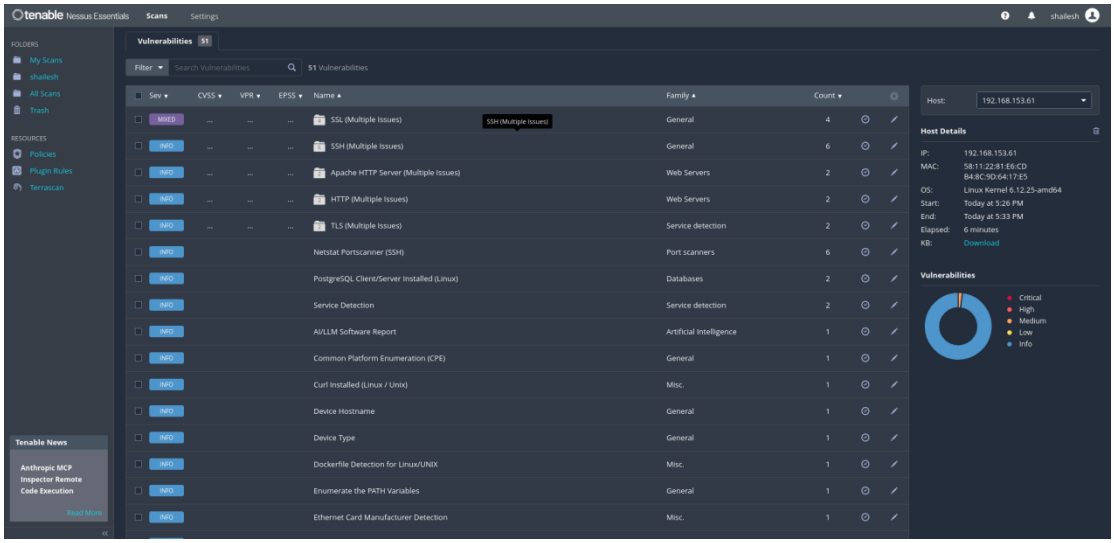
Keep OS and services updated.

Restrict unnecessary services (e.g., mDNS, ICMP timestamping).

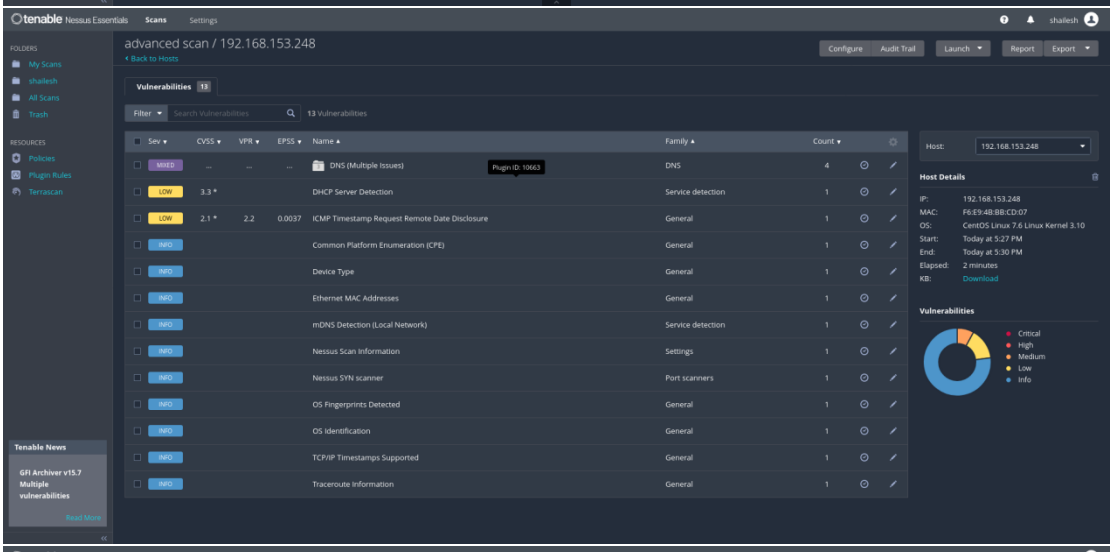
Use firewalls and network segmentation.

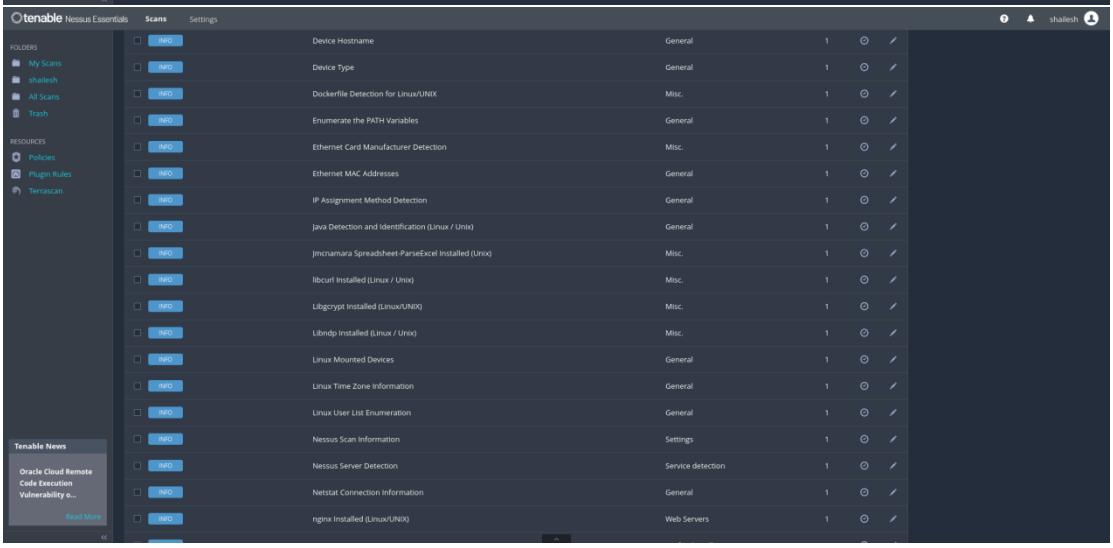
Screenshots:






tenable Nessus Essentials
Scans
Settings
shailesh
FOLDERS
My Scans
shailesh
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
mySCADA PRO Manager Password Disclosure
Read More
INFO
OpenSSL Installed (Linux)
Misc.
OpenVPN Installed (Linux)
OS Fingerprints Detected
General
OS Identification
OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
OS Security Patch Assessment Available
Settings
Package Manager Packages Report (nix)
PHP Scripting Language Installed (Unix)
Reachable IPv6 address
Ruby Programming Language Installed (Linux)
SSL / TLS Versions Supported
Strict Transport Security (STS) Detection
Service detection
Target Credential Issues by Authentication Protocol - No Issues Found
Target Credential Status by Authentication Protocol - Valid Credentials Provided
Tenable Nessus Installed (Linux)
Tukaani XZ Utils Installed (Linux / Unix)
Unix / Linux Running Processes Information
Unix Software Discovery Commands Available
Results per page 50
Showing: 1 to 50 of 51


tenable Nessus Essentials
Scans
Settings
shailesh
advanced scan / 192.168.153.248
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 13
Filter
Search Vulnerabilities
13 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MIXED
DNS (Multiple Issues)
Plugin ID: 10663
DNS
4
LOW
3.3 *
DHCP Server Detection
Service detection
2.1 *
2.2
0.0037
ICMP Timestamp Request Remote Date Disclosure
General
INFO
Common Platform Enumeration (CPE)
Device Type
Ethernet MAC Addresses
mDNS Detection (Local Network)
Nessus Scan Information
Settings
Nessus SYN scanner
Port scanners
OS Fingerprints Detected
OS Identification
TCP/IP Timestamps Supported
Traceroute Information
Host:
192.168.153.248
Host Details
IP: 192.168.153.248
MAC: F6:E9:4B:BB:CD:07
OS: CentOS Linux 7.6 Linux Kernel 3.10
Start: Today at 5:27 PM
End: Today at 5:30 PM
Elapsed: 2 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
GFI Archiver v15.7 Multiple vulnerabilities
Read More


tenable Nessus Essentials
Scans
Settings
shailesh
FOLDERS
My Scans
shailesh
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle Cloud Remote Code Execution Vulnerability o...
Read More
INFO
Device Hostname
General
Device Type
Dockerfile Detection for Linux/UNIX
Misc.
Enumerate the PATH Variables
Ethernet Card Manufacturer Detection
Ethernet MAC Addresses
IP Assignment Method Detection
Java Detection and Identification (Linux / Unix)
Jmcnamara Spreadsheet-ParseExcel Installed (Unix)
libcurl Installed (Linux / Unix)
Libgcrypt Installed (Linux/UNIX)
Libndp Installed (Linux / Unix)
Linux Mounted Devices
Linux Time Zone Information
Linux User List Enumeration
Nessus Scan Information
Settings
Nessus Server Detection
Service detection
Netstat Connection Information
General
nginx Installed (Linux/UNIX)
Web Servers