

IP Scan Report -

tenable

Nessus Essentials

Scans

Settings

My Scans

task_3

All Scans

Trash

Policies

Plugin Rules

Terrascan

Tenable News

Introducing Tenable AI Exposure: Stop Guessing. St...

Read More

My Basic Network Scan / Plugin #35716

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities

5

INFO

Ethernet Card Manufacturer Detection

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

<https://standards.ieee.org/faqs/regauth.html>
<http://www.nessus.org/u7794673b4>

Output

The following card manufacturers were identified :
08:00:27:74:C3:ED : PCS Systemtechnik GmbH

Port

Hosts

N/A

192.168.1.20

Plugin Details

Severity: Info
ID: 35716
Version: 1.15
Type: combined
Family: Misc.
Published: February 19, 2009
Modified: May 13, 2020

Risk Information

Risk Factor: None

tenable

Nessus Essentials

Scans

Settings

My Scans

task_3

All Scans

Trash

Policies

Plugin Rules

Terrascan

Tenable News

Gemini Search Personalization Model - Prompt Injec...

Read More

My Basic Network Scan / Plugin #86420

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities

5

INFO

Ethernet MAC Addresses

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Output

The following is a consolidated list of detected MAC addresses:
- 08:00:27:74:C3:ED

Port

Hosts

N/A

192.168.1.20

Plugin Details

Severity: Info
ID: 86420
Version: 1.8
Type: combined
Family: General
Published: October 16, 2015
Modified: June 10, 2025

Risk Information

Risk Factor: None

tenable

Nessus Essentials

Scans

Settings

My Scans

task_3

All Scans

Trash

Policies

Plugin Rules

Terrascan

Tenable News

CVE-2025-54987, CVE-2025-54948: Trend Micro Apex O...

Read More

My Basic Network Scan / Plugin #10114

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities

5

LOW

ICMP Timestamp Request Remote Date Disclosure

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Output

The remote clock is synchronized with the local clock.

Port

Hosts

0 / icmp

192.168.1.20

Plugin Details

Severity: Low
ID: 10114
Version: 1.56
Type: remote
Family: General
Published: August 1, 1999
Modified: October 7, 2024

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSV3 Impact Score: 1.4
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 2.2

