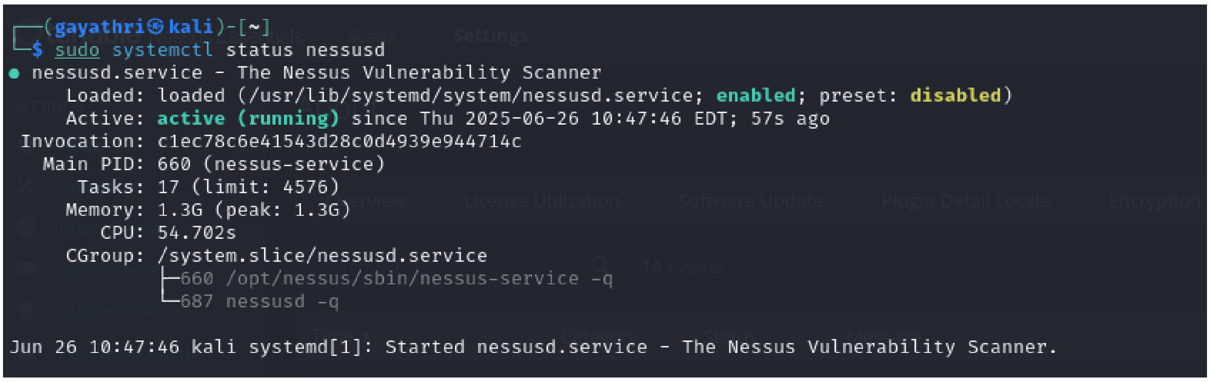
TASK 3 : Perform a Basic Vulnerability Scan on Your PC

1.Install OpenVAS or Nessus Essentials.

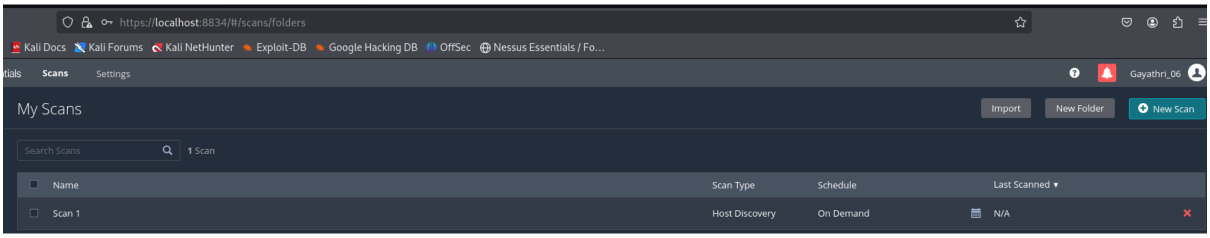


```
┌──(gayathri㉿kali)-[~]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-06-26 10:47:46 EDT; 57s ago
 Invocation: c1ec78c6e41543d28c0d4939e944714c
   Main PID: 660 (nessus-service)
      Tasks: 17 (limit: 4576)
     Memory: 1.3G (peak: 1.3G)
        CPU: 54.702s
     CGroup: /system.slice/nessusd.service
             ├─660 /opt/nessus/sbin/nessus-service -q
             └─687 nessusd -q

Jun 26 10:47:46 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
```

2.Set up scan target as your local machine IP or localhost.

3.Start a full vulnerability scan.



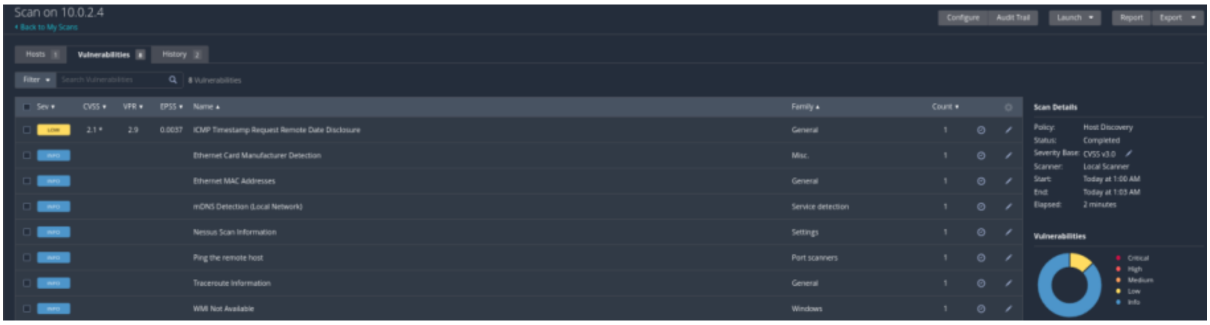
My Scans

1 Scan

Name	Scan Type	Schedule	Last Scanned ▾
Scan 1	Host Discovery	On Demand	N/A

4.Wait for scan to complete (may take 30-60 mins).

5.Review the report for vulnerabilities and severity.



Scan on 10.0.2.4

8 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
LOW	2.1 *	2.9	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				mDNS Detection (Local Network)	Service detection	1
INFO				Nessus Scan Information	Settings	1
INFO				Ping the remote host	Port scanners	1
INFO				Traceroute Information	General	1
INFO				WMI Not Available	Windows	1

Scan Details

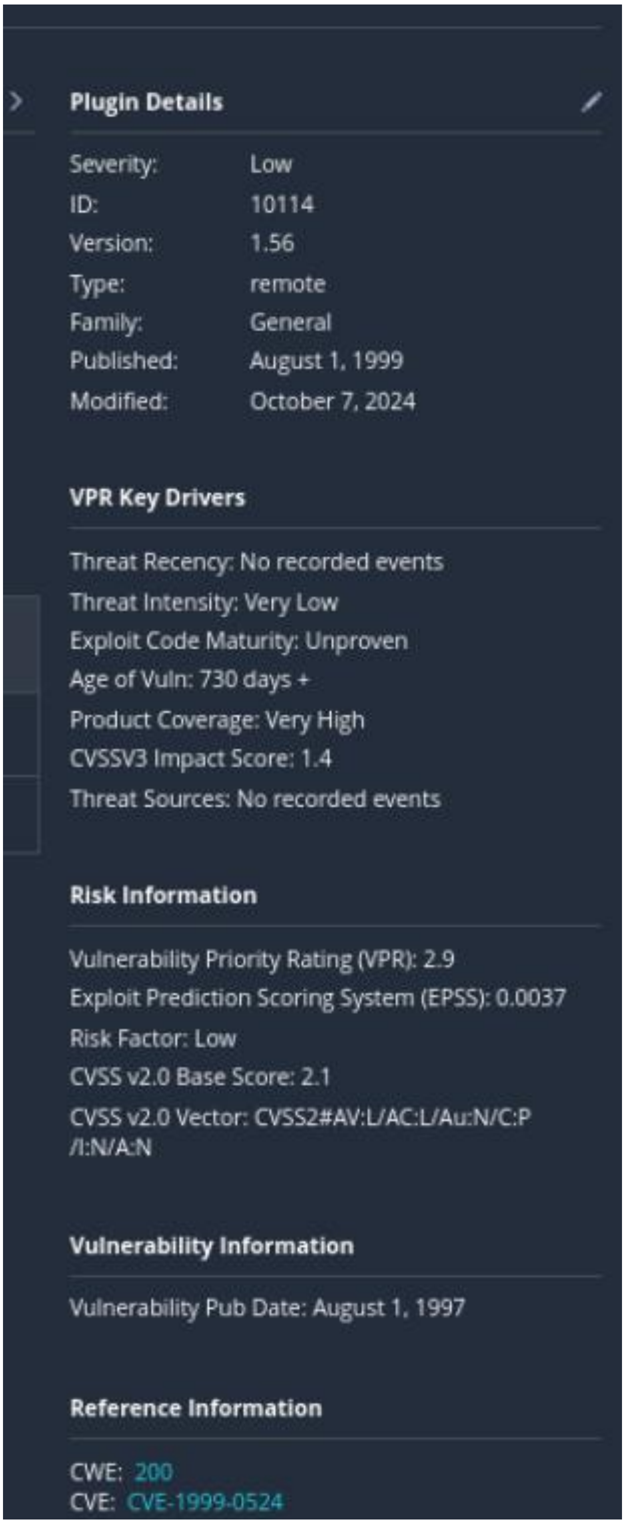
Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:00 AM
End: Today at 1:03 AM
Elapsed: 2 minutes

Vulnerabilities

6.Research simple fixes or mitigations for found vulnerabilities.

➔ In the victim system, the vulnerability found is the “ICMP Timestamp Request Remote Date Disclosure”. CVSS score is 2.1 (low), VPR is 2.9

7.Document the most critical vulnerabilities.



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: Unproven
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): 2.9
Exploit Prediction Scoring System (EPSS): 0.0037
Risk Factor: Low
CVSS v2.0 Base Score: 2.1
CVSS v2.0 Vector: CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

Vulnerability Pub Date: August 1, 1997

Reference Information

CWE: 200
CVE: CVE-1999-0524

The Nessus plugin with ID 10114, classified under the *General* family, reports a low-severity remote vulnerability. The vulnerability is associated with CVE-1999-0524, which involves information exposure (CWE-200). According to the report, this issue has a CVSS v2.0 base score of 2.1, indicating limited impact, primarily affecting confidentiality with no significant impact on integrity or availability.

The Vulnerability Priority Rating (VPR) is 2.9, reflecting a low risk, and the Exploit Prediction Scoring System (EPSS) is 0.0037, suggesting very low probability of exploitation. There have been no recent threat events or sources recorded, and the exploit code maturity is unproven.

Remedy:

To remediate CVE-1999-0524, ensure that systems do not expose whether a username is valid during login attempts. Configure all authentication mechanisms to return generic error messages such as "Invalid credentials." Disable or restrict unused user accounts and enforce strong password policies. Additionally, keep all services up to date and monitor authentication logs for suspicious activity.