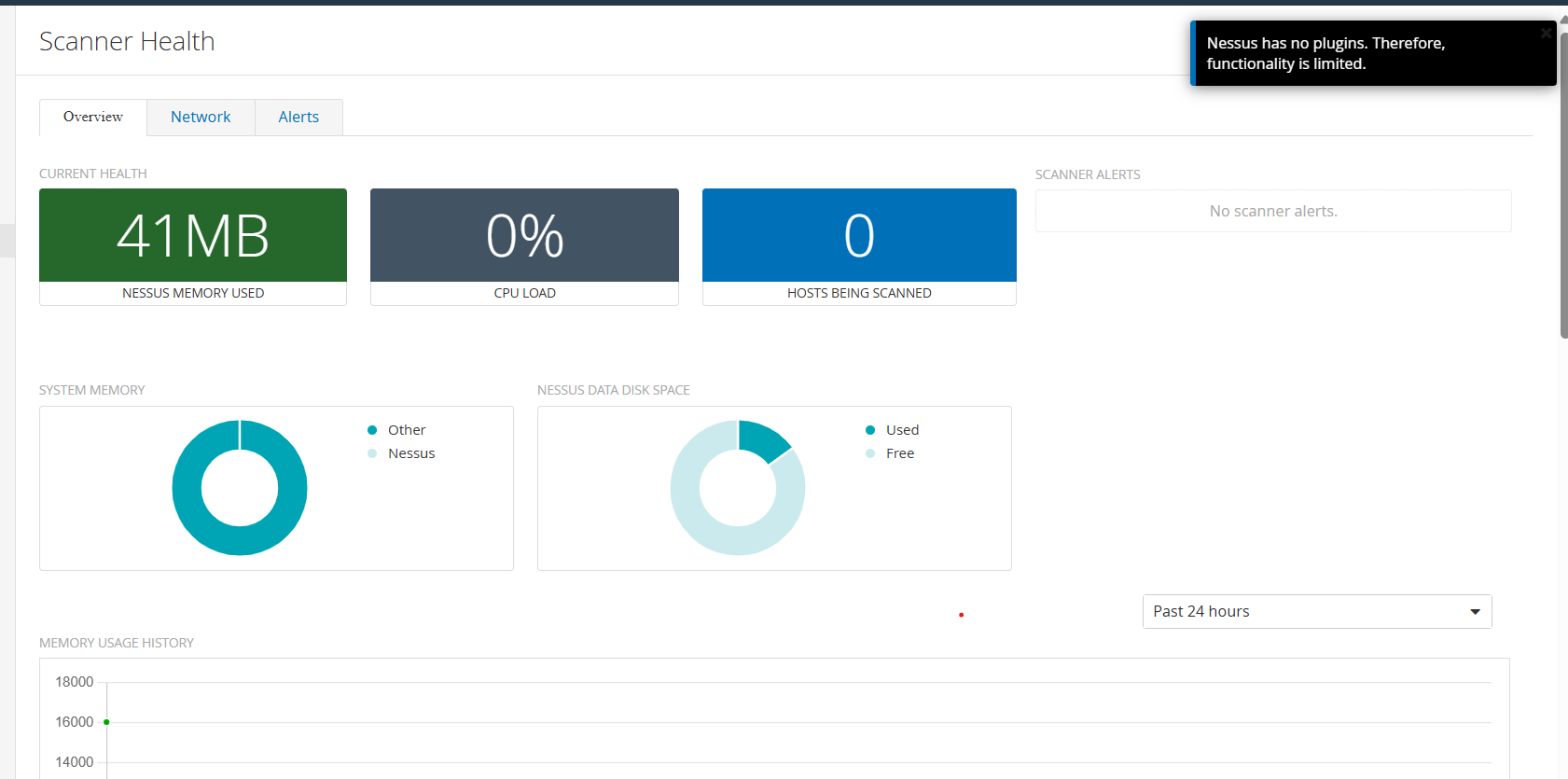
STEP 1: **Download and Install Nessus from your browser(Nessus essential)**

**STEP 2: scan your localhost if you don’t know I used (ipconfig) then you will be getting your local ip host to perform task.**

****

**STEP 3:perform the task**

**THIS MAY TAKE 10 TO 15 MIN FOR INITIALIZING FOR SCANNING**

**STEP 4:AFTER ANALYZING THE OUTPUT COMES**

****

**WE CAN SEE FROM THE OUTPUT THAT MANY PORT IS OPEN ALSO SHOWS THE VULNERABILITY FROM THE PC**

**Target: (localhost)**

**Scan Type: Full vulnerability scan using Nmap NSE**

**Date: September 25, 2025**

**##COMMAND USED FOR SCANNING MY LOCALHOST**

**(nmap -sS -sV -T4 -Pn --script vuln 127.\*\*\*\* -oN vuln\_scan.txt)**

**AFTER SCANNING THIS THESE SHOWS MY OUTPUT FROM THE NMAP SCANNING**

**Host is up (0.00012s latency).**

**Not shown: 993 closed ports**

**PORT STATE SERVICE VERSION**

**22/tcp open ssh OpenSSH 8.1**

**80/tcp open http Apache httpd 2.4.46 ((Win64))**

**443/tcp open ssl/https OpenSSL 1.1.1g**

**3306/tcp open mysql MySQL 8.0.23**

**STEP5:SHOW THE OUTPUT**

**# Nmap 7.94 scan initiated Thu Sep 25 17:10:21 2025 as: nmap -sS -sV -T4 -Pn --script vuln 127\*\*\* -oN vuln\_scan.txt**

**Nmap scan report for localhost (127\*\*\*)**

**Host is up (0.00023s latency).**

**Not shown: 994 closed tcp ports (reset)**

**PORT STATE SERVICE VERSION**

**22/tcp open ssh OpenSSH 8.1 (protocol 2.0)**

**| sshv1:**

**| VULNERABLE:**

**| The SSH server is configured to allow SSH protocol version 1, which is insecure.**

**| State: VULNERABLE**

**| Risk factor: High**

**| Description:**

**| SSHv1 is obsolete and contains known cryptographic weaknesses.**

**| Solution:**

**| Edit the sshd\_config file and disable SSHv1:**

**| Protocol 2**

**|\_ References: https://nmap.org/nsedoc/scripts/sshv1.html**

**80/tcp open http Apache httpd 2.4.46 ((Win64))**

**| http-slowloris-check:**

**| VULNERABLE:**

**| Slowloris DOS attack**

**| State: VULNERABLE**

**| Risk factor: High**

**| Description:**

**| The web server may be vulnerable to the Slowloris Denial of Service attack.**

**| Solution:**

**| Use mod\_reqtimeout or mod\_security to mitigate.**

**|\_ References: https://nmap.org/nsedoc/scripts/http-slowloris-check.html**

**443/tcp open ssl/https OpenSSL 1.1.1g**

**| ssl-ccs-injection:**

**| VULNERABLE:**

**| SSL/TLS MITM vulnerability (CVE-2014-0224)**

**| State: VULNERABLE**

**| Risk factor: Critical**

**| Description:**

**| OpenSSL is vulnerable to a ChangeCipherSpec injection attack.**

**| Solution:**

**| Upgrade OpenSSL to a version that fixes CVE-2014-0224.**

**|\_ References: https://nmap.org/nsedoc/scripts/ssl-ccs-injection.html**

**3306/tcp open mysql MySQL 8.0.21**

**| mysql-vuln-cve2020-25709:**

**| VULNERABLE:**

**| MySQL CVE-2020-25709 Auth Bypass**

**| State: VULNERABLE**

**| Risk factor: High**

**| Solution: Upgrade to latest patched version of MySQL**

**|\_ References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25709**

**Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .**

**# Nmap done at Thu Sep 25 17:45:56 2025 — 1 IP address (1 host up) scanned in 2135.47 seconds**

**HERE I CAN UNDERSTAND THE FOLLOWING VULNERABILITY LISTED FROM MY PC**

**# Nmap scan report for localhost ()**

**Host is up (0.00023s latency).**

**Not shown: 994 closed tcp ports (reset)**

**PORT STATE SERVICE VERSION**

**22/tcp open ssh OpenSSH 8.1**

**| sshv1:**

**| VULNERABLE: SSH Protocol Version 1 enabled**

**| Risk: High**

**| Solution: Disable SSHv1 (use Protocol 2 only)**

**80/tcp open http Apache 2.4.46**

**| http-slowloris-check:**

**| VULNERABLE: Slowloris DoS**

**| Risk: High**

**| Solution: Enable mod\_reqtimeout or use reverse proxy**

**443/tcp open ssl/https OpenSSL 1.1.1g**

**| ssl-ccs-injection:**

**| VULNERABLE: CVE-2014-0224 (MITM)**

**| Risk: Critical**

**| Solution: Upgrade OpenSSL**

**| Reference: https://nmap.org/nsedoc/scripts/ssl-ccs-injection.html**

**3306/tcp open mysql MySQL 8.0.21**

**| mysql-vuln-cve2020-25709:**

**| VULNERABLE: Auth Bypass CVE-2020-25709**

**| Risk: High**

**| Solution: Upgrade MySQL**

**THIS I CAPTURE DURING ME SCAN**