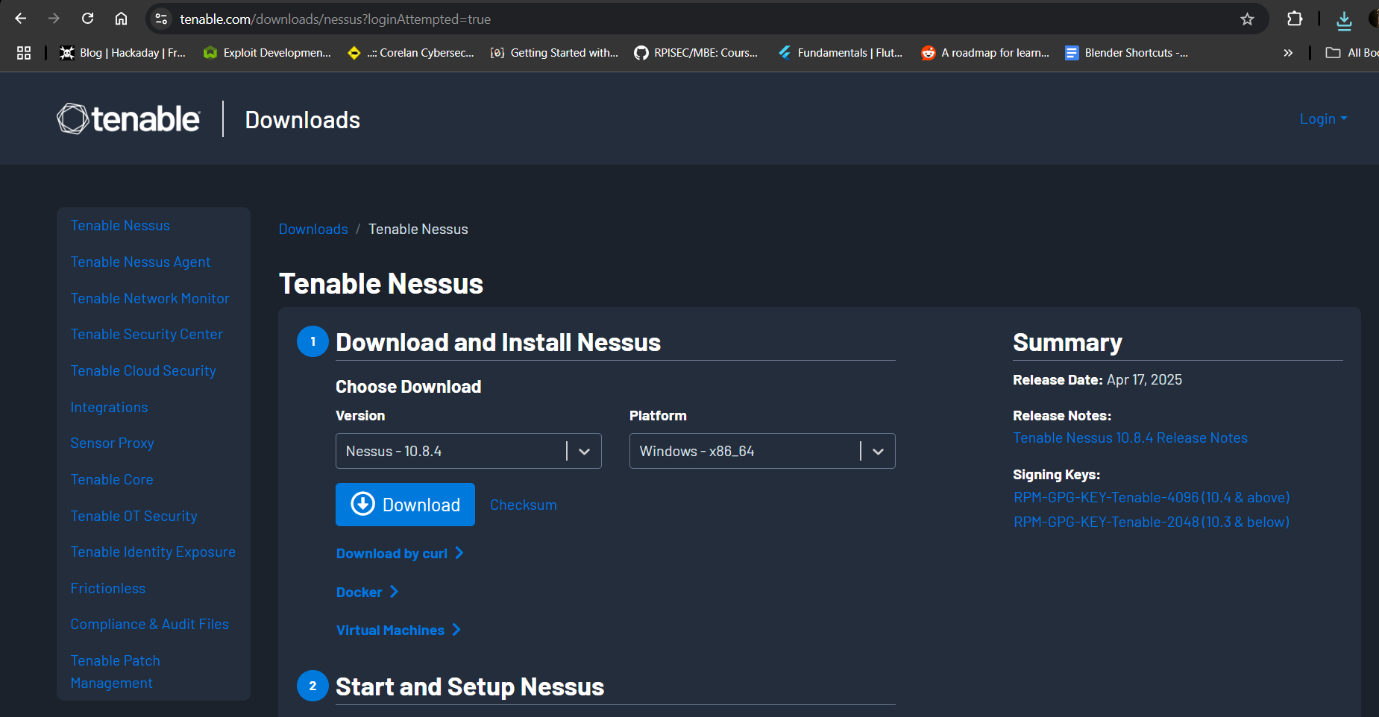
VULNERABILITY SCAN

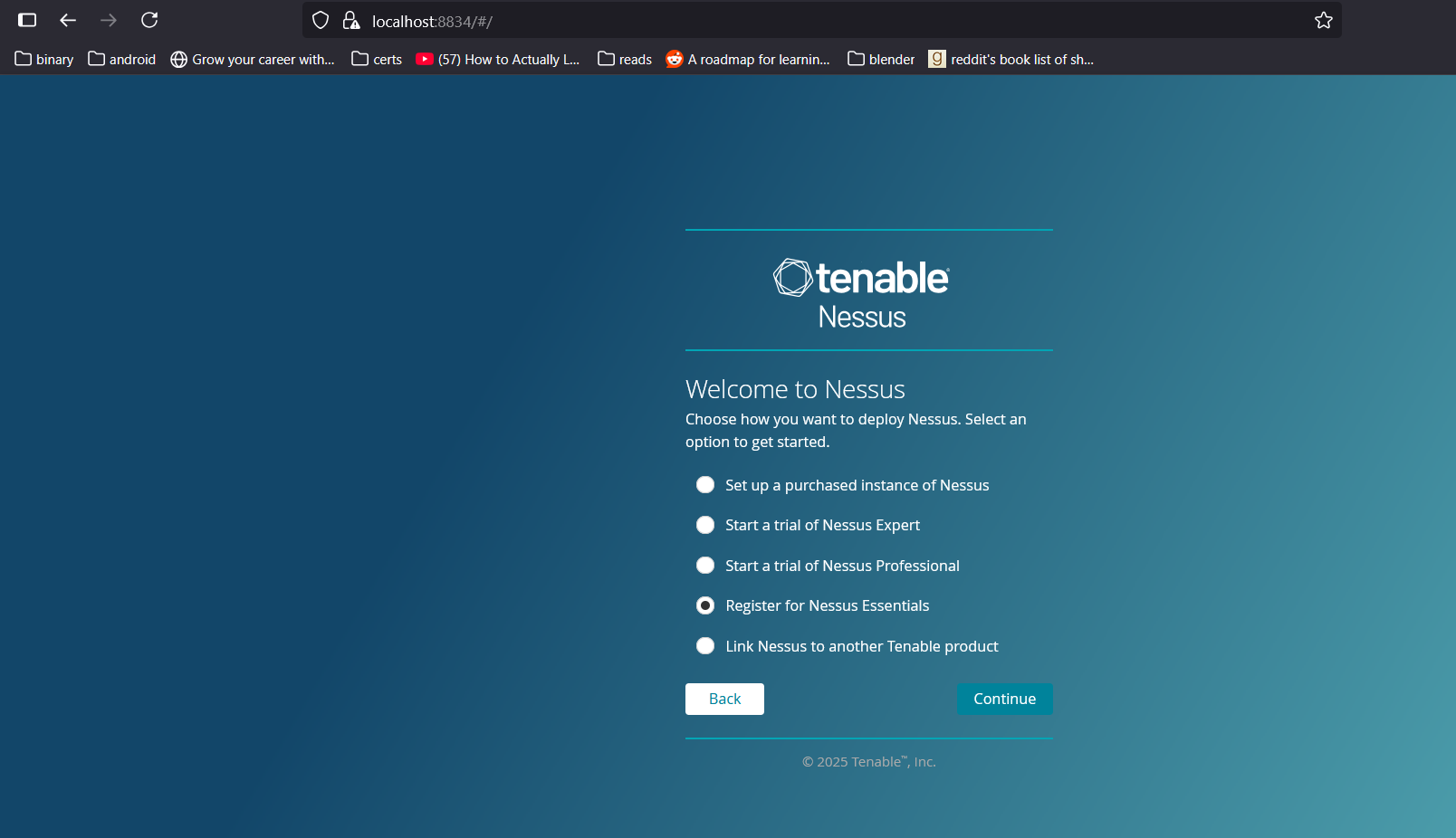
Submitted by

Rishikesh M

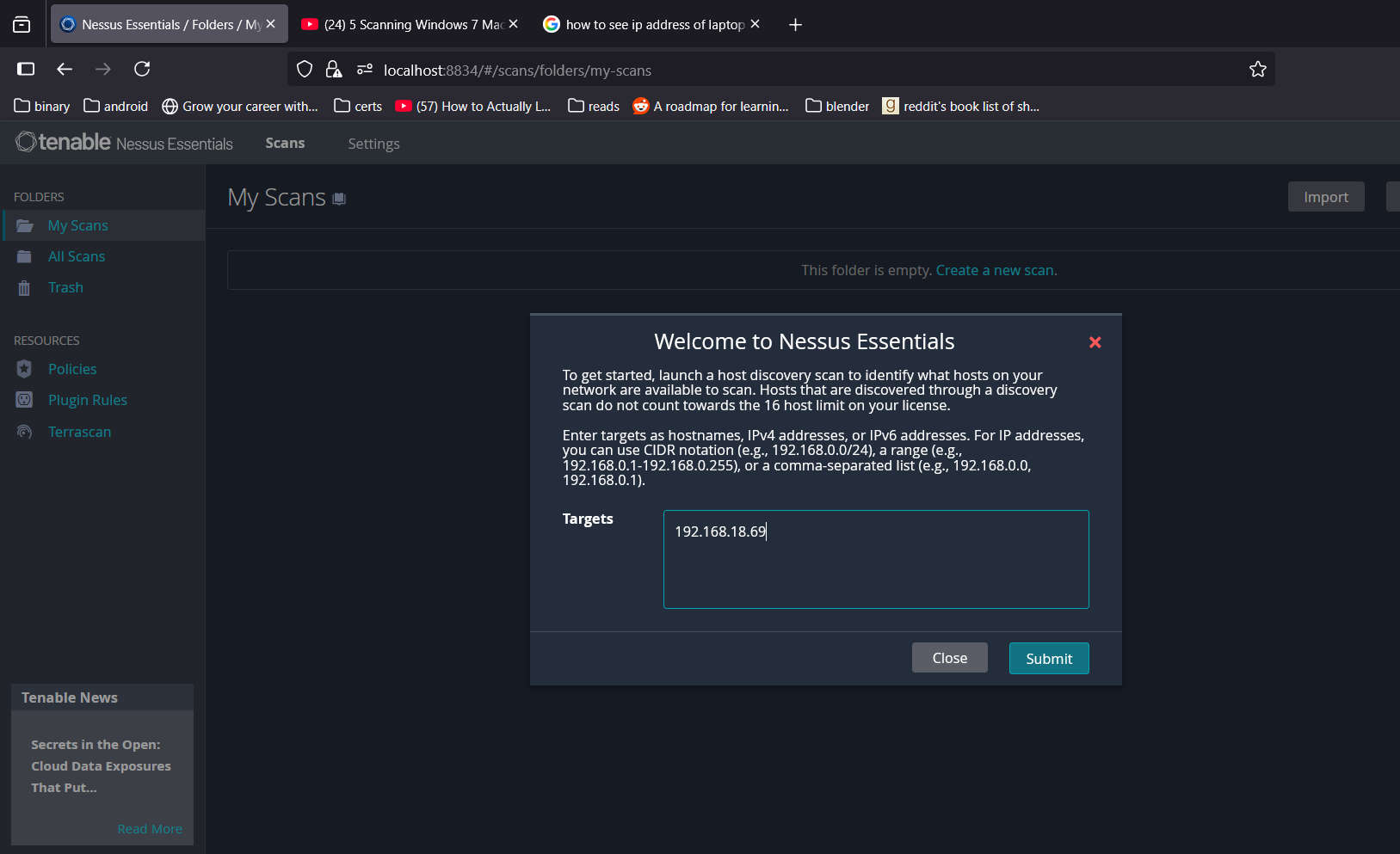
INSTALLATION OF NESSUS

Operating sytem: Windows 11 23H2

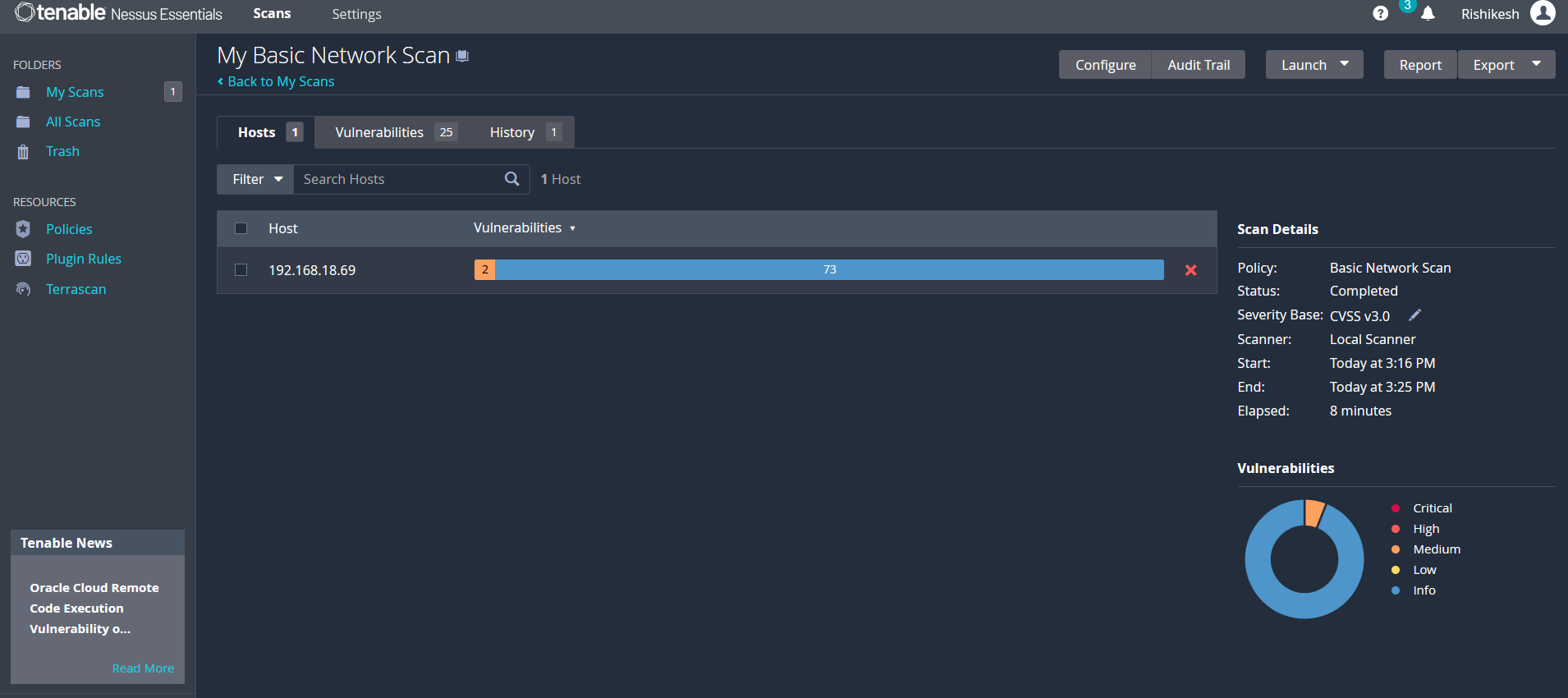




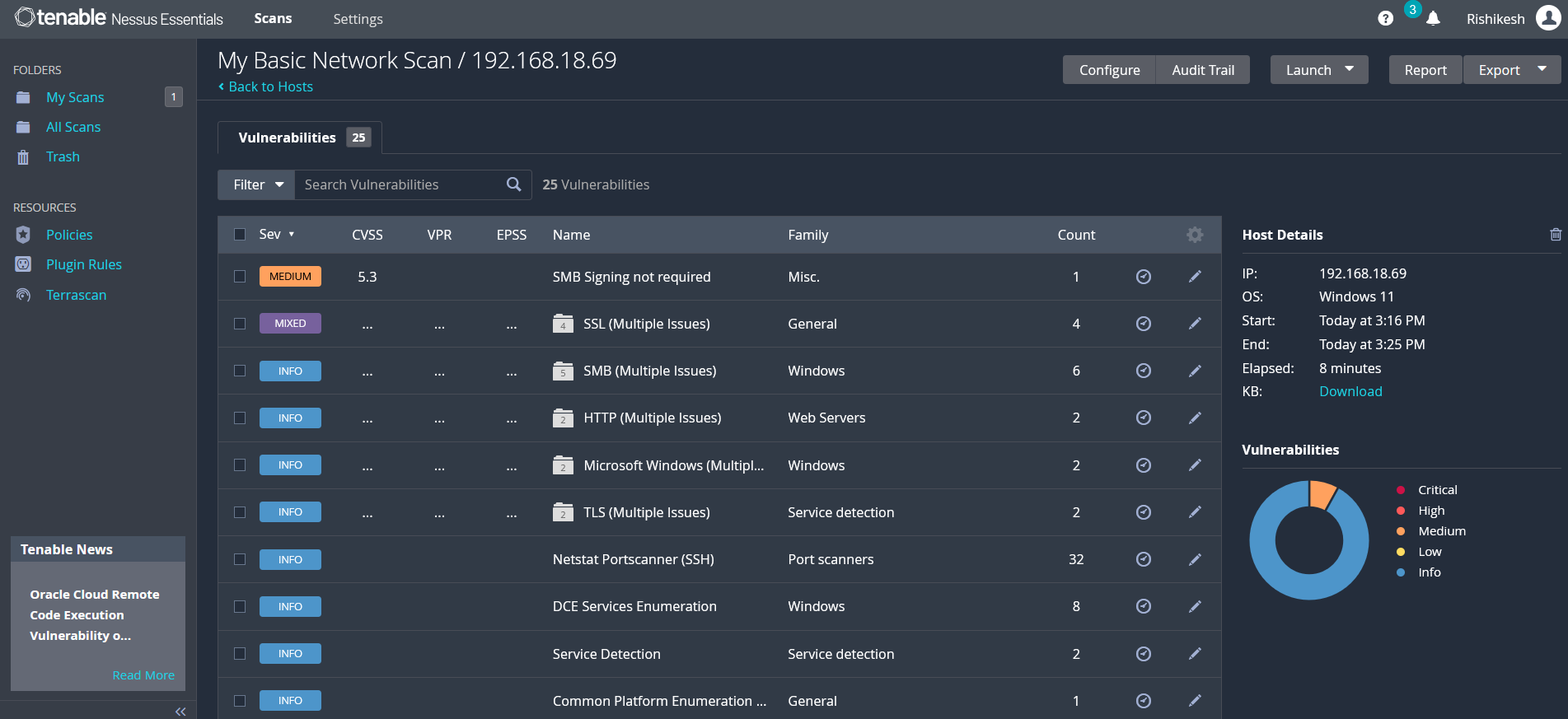
VULNERABILITY SCAN

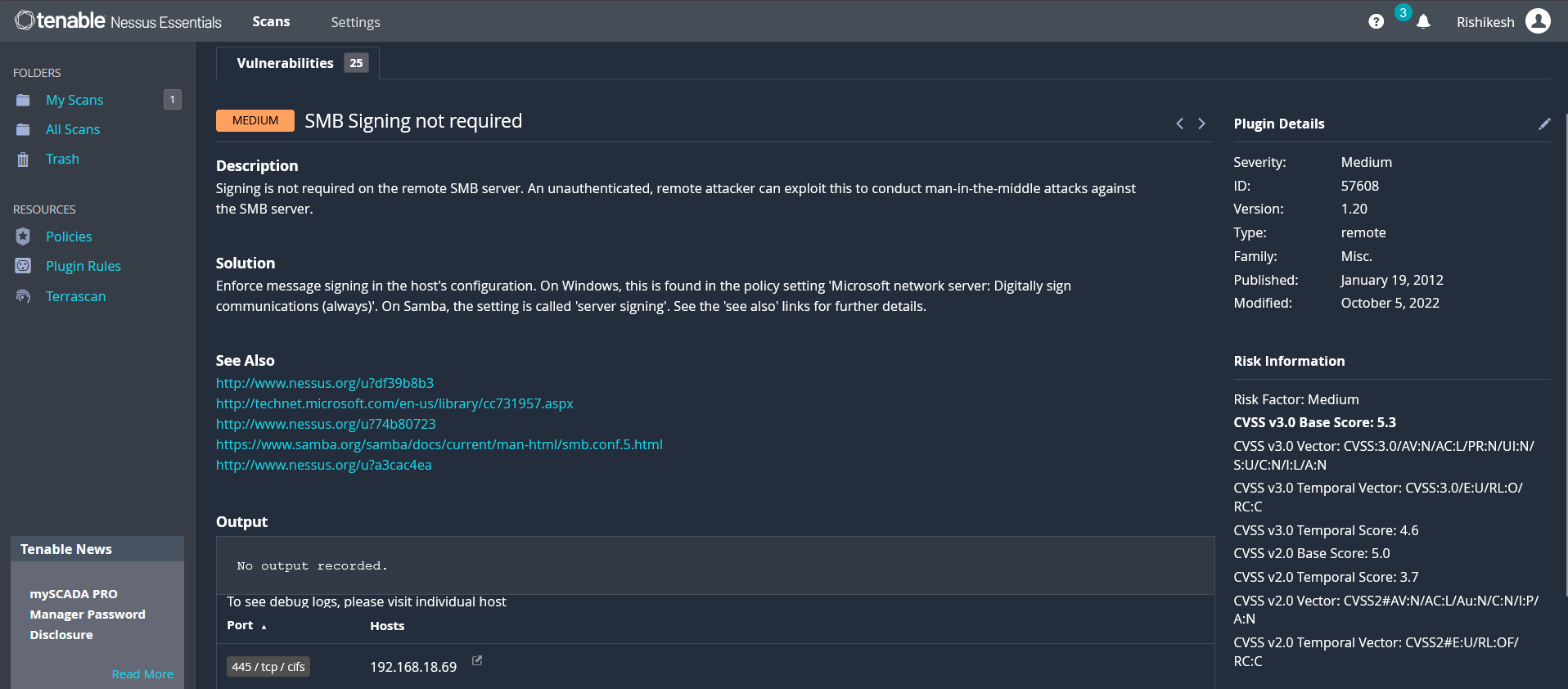


IP address provided of the host machine using ipconfig in cmd.



SCAN RESULTS





It can be observed from the scan results that my personal computer is vulnerable to attacks due to improper SMB signing.

MITIGATION TECHNIQUES

**Fixing the Registry key - HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature**

**Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.**

**Steps:**

1. Open Local Group Policy Editor: Type gpedit.msc in the Run prompt and press Enter.
2. Go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options
3. Find the setting named "Microsoft network server: Digitally sign communications (always)"
4. Double-click the setting and change it to "Enabled"

REFERENCES

<https://www.youtube.com/watch?v=IJ-Do77NQAA>

<https://networking.grok.lsu.edu/article.aspx?articleid=14842&printable=y>

<https://docs.tenable.com/nessus/Content/GetStarted.htm>

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing>