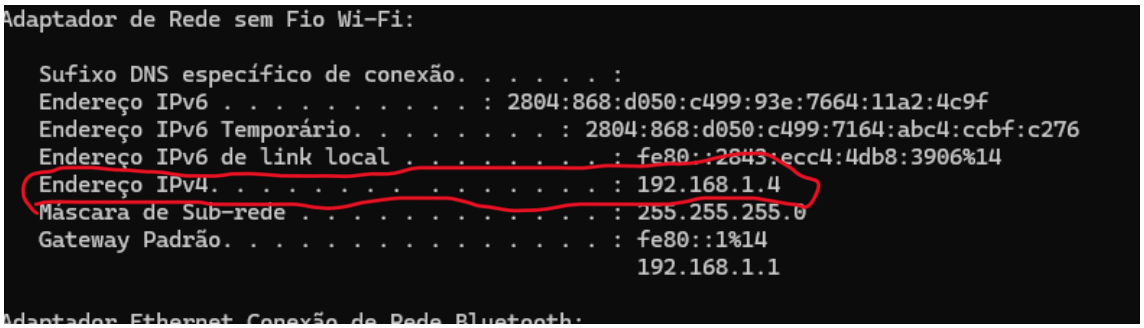
Name: Ruan Saure 26/06/2025

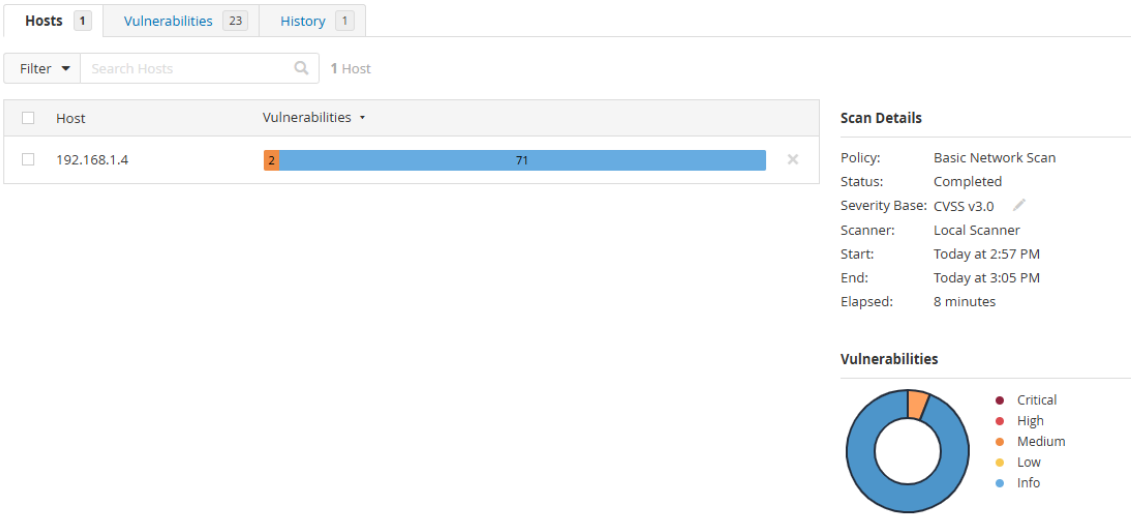
Summer Intership – Task 3

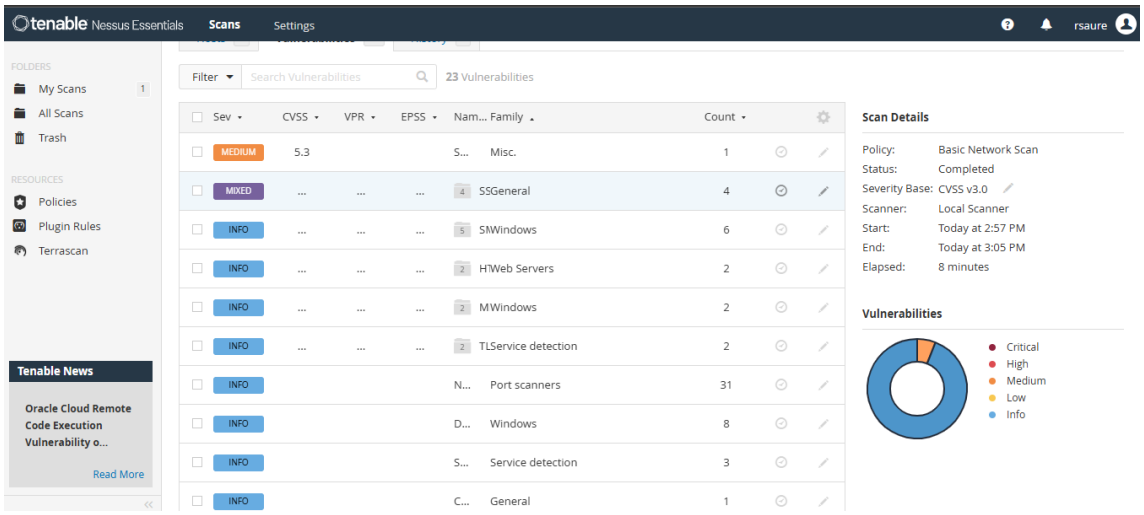
First of all, I had to Discover my own IP before send it to Nessus, so, I entered in cmd and execute the “ipconfig” command and had the results below:

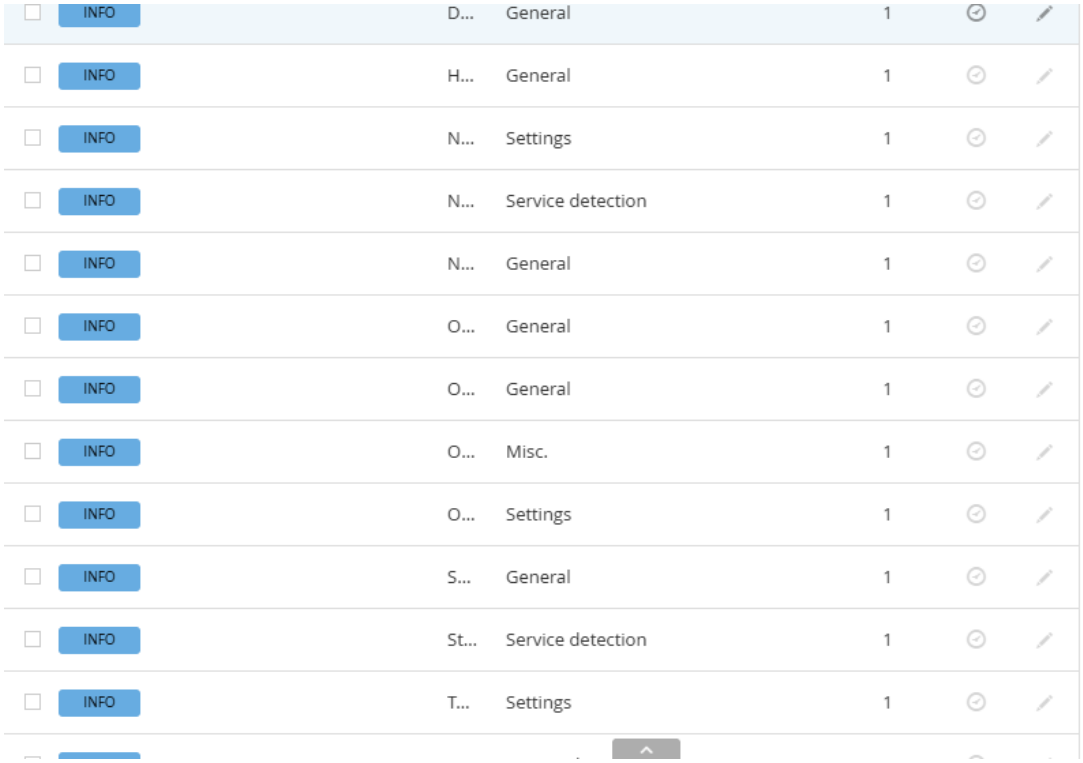


(Sorry, I don’t change my PC’s language yet)

After Discover my IP, I copied it into Nessus and started the scan.







Description of the most critical vulnerabilities:

Medium → SMB signing not required

Description → When SMB signing is not required, an attacker on the same network can intercept or alter communications between a client and the server, because messages are not cryptographically signed to ensure their integrity.

Solution → 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'. See the 'see also' links for further details.

Step-by-step: Enable SMB Signing

1. Open Local Security Policy

- Press Win + R, type secpol.msc, hit **Enter**.

If you get an error that secpol.msc doesn't exist (it happens on Windows Home), let me know — I'll give you the Registry method instead.

2. Navigate to:

   Local Policies → Security Options

3. Enable the following policies:

Policy Name	Set to
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Then, restart the PC.

Option 2:

Press Win + R, type regedit, and press Enter

Click **Yes** if prompted for permission.

2. Navigate to the following path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters

Create or edit these DWORD (32-bit) values:

Name	Type	Value
EnableSecuritySignature	DWORD	1
RequireSecuritySignature	DWORD	1

If they don't exist:

- Right-click on the right panel → New → DWORD (32-bit) Value
- Name it exactly as shown above
- Double-click to set the value to 1

4. Navigate to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters this second path:

Name	Type	Value
EnableSecuritySignature	DWORD	1
RequireSecuritySignature	DWORD	1

Then, restart the PC

Medium → SSL Certificate Cannot Be Trusted(That's the Nessus in my PC)

Description → The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken

Solution → Purchase or generate a proper SSL certificate for this service.

The other results in the list are just information on my PC, like PC's name, running services, etc...

Open a PowerShell terminal and run:

netstat -ano | findstr :443

It will show you the PID of the process using port 443.

Then:

tasklist /FI "PID eq <PID from above>"

This will tell you what app is using HTTPS.
If it's something unexpected — like a local test environment or malware — you can disable or uninstall it.