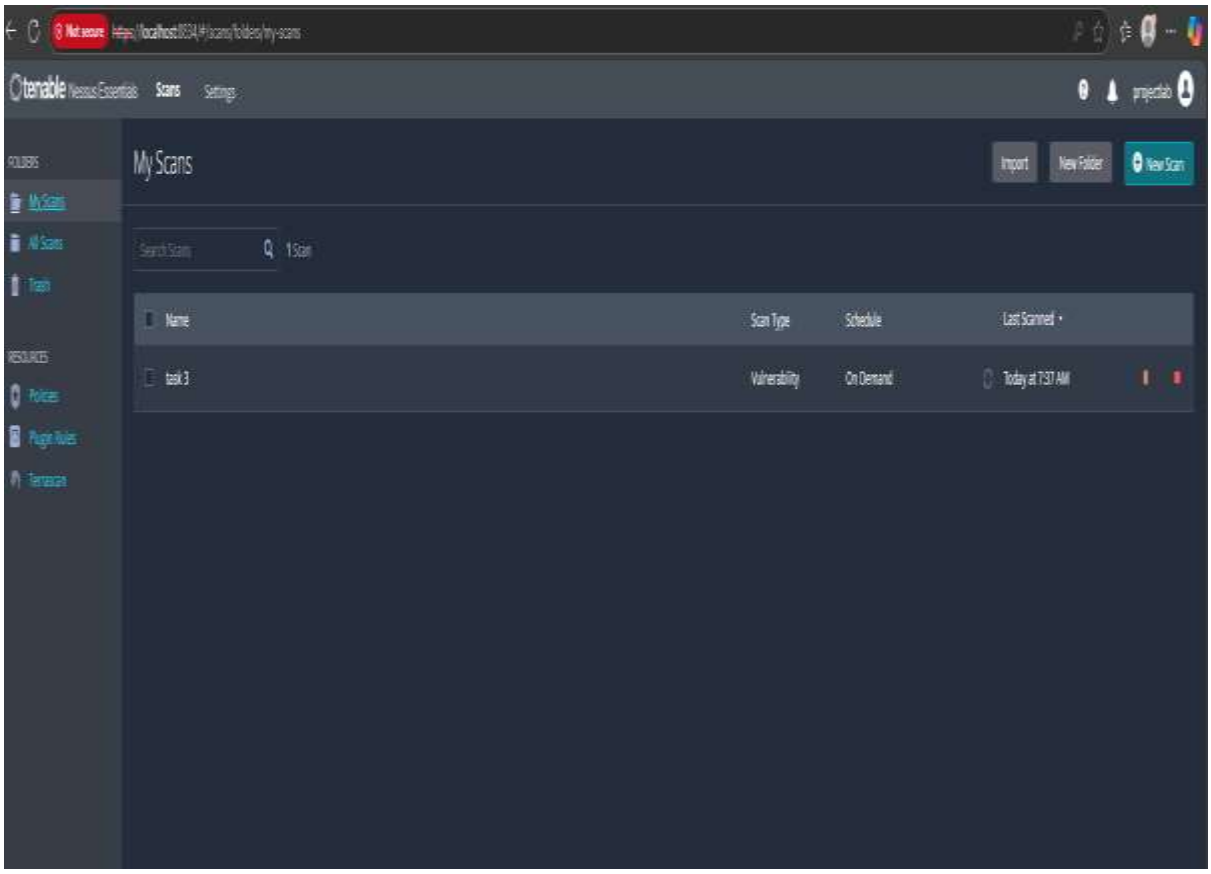
Task 3 –

Download Nessus Essentials:

- Go to the Tenable website: https://www.tenable.com/
- Navigate to the Nessus product page.
- Look for a "Download" or "Get Started" section. You'll likely need to register for a Nessus Essentials license (which is free for home use and up to 16 IP addresses).
- Once registered, you'll be able to download the appropriate Nessus installer package for your operating system.

I am using it in my windows os on edge browser web client.

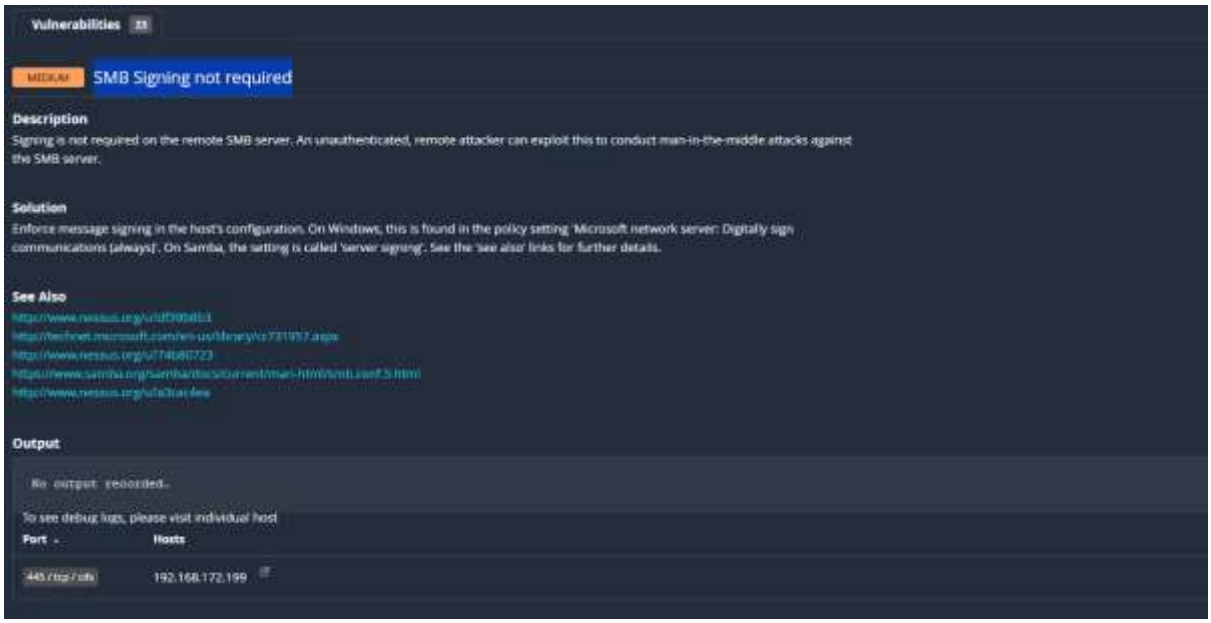


All plugins downloaded as per requirement

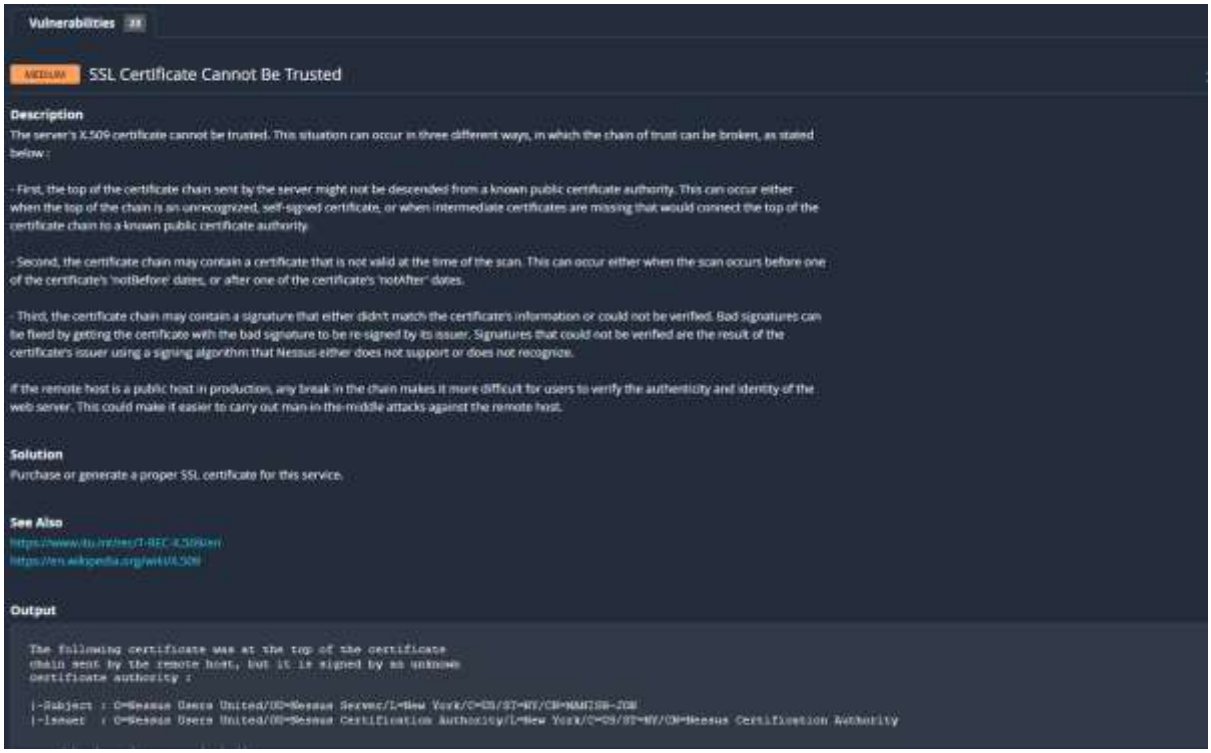
2 vulnerability findout in my system.

Let’s explore

1st **SMB Signing not required**



2nd **SSL Certificate Cannot Be Trusted**



Document of most critical vulnerability

Vulnerability Name: Remote Code Execution (RCE)

Severity: Critical

Description:
Remote Code Execution (RCE) is a vulnerability that allows an attacker to execute arbitrary code on a target system or server remotely. This can lead to full system compromise, data theft, or disruption of services.

Affected System:
Specify the application, version, or system where the vulnerability was found.

Vulnerability Details:
The vulnerability occurs due to improper input validation or unsafe deserialization, allowing an attacker to inject and execute malicious code remotely.

Impact:

- Complete control over the affected system
- Data breach or data loss
- Service disruption or denial of service
- Potential pivot to internal networks

Proof of Concept (PoC):
Provide a minimal example or steps to reproduce the vulnerability, e.g., sending a crafted payload to a vulnerable endpoint that executes a command.

Mitigation:

- Apply vendor patches or updates immediately
- Implement strict input validation and sanitization
- Use secure coding practices to avoid unsafe deserialization
- Employ runtime application self-protection (RASP) or web application firewalls (WAF)

References:

- CVE entries related to the vulnerability
- Vendor security advisories
- OWASP guidelines on RCE