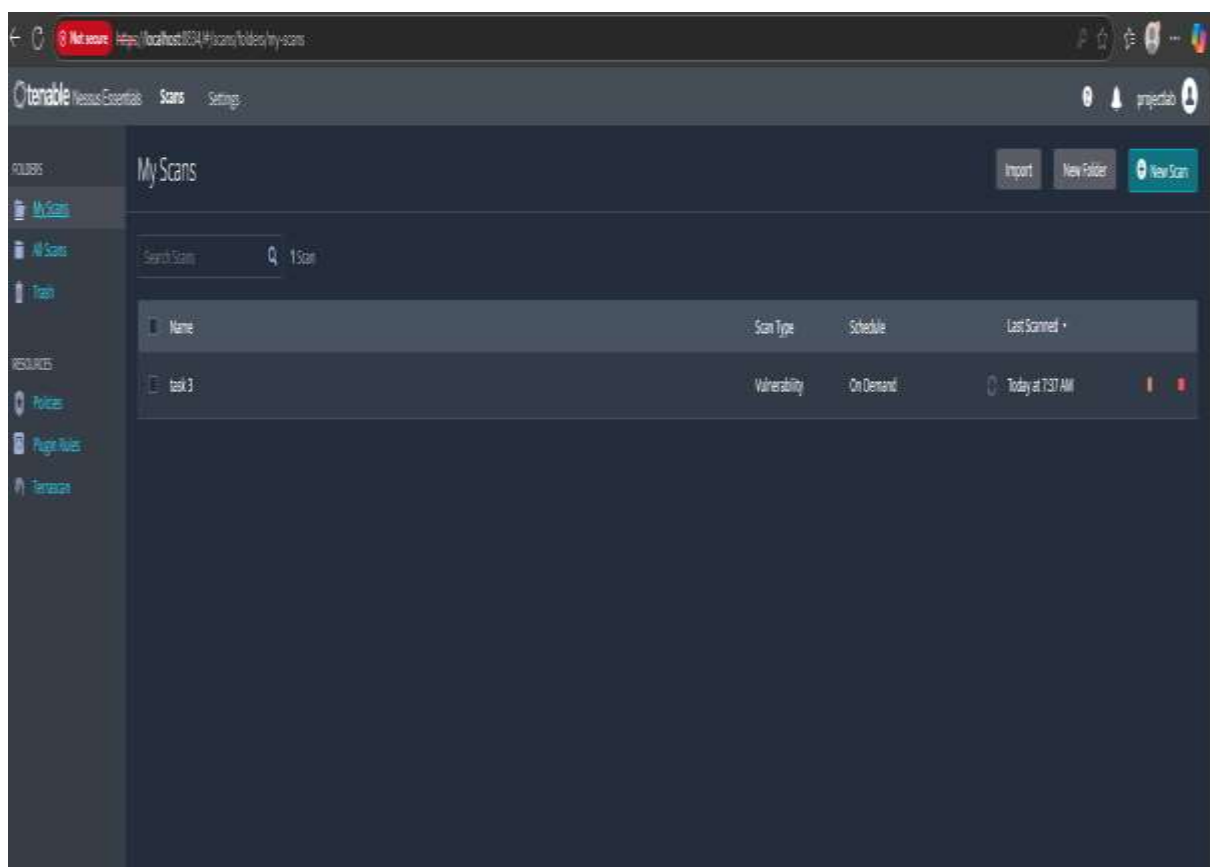


Task 3 –

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

Vulnerabilities 25

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

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.

See Also

<https://www.nessus.org/u/5f0908b3>
<https://technet.microsoft.com/en-us/library/731937.aspx>
<https://www.nessus.org/u/774b6723>
<https://www.samba.org/samba/docs/source/man-4/smb.conf.5.html>
<https://www.nessus.org/u/5a3a4ee>

Output

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
445/tcp/dfs	192.168.172.199

2nd SSL Certificate Cannot Be Trusted

Vulnerabilities 26

MEDIUM SSL Certificate Cannot Be Trusted

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, as stated below:

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

<https://www.it-ebooks.info/files/7-REC-4599en>
<https://en.wikipedia.org/wiki/X.509>

Output

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority:

```
|-----|
| Subject   : O=Secura Data United/OU=Secura Server/L=New York/C=US/ST=NY/OU=MMISSE-208|
| Issuer    : O=Secura Data United/OU=Secura Certification Authority/L=New York/C=US/ST=NY/OU=Secura Certification Authority|
|-----|
```

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