Cyber Security Internship

Task 3 – Perform a Basic Vulnerability Scan on PC

Executive Summary:

A vulnerability assessment was performed on the target system on 17 November 2025. The scan identified multiple vulnerabilities of varying severity. This report summarizes key findings and recommend mitigation steps.

Scope:

Target System: 192.168.x.x

Tool Used: Nessus Essentials

Scan Type: Basic Network Scan (non-credentialed)

Summary of Findings:

Severity	Count
Critical	0
High	0
Medium	1
Low	0
Mixed	1

Detailed Findings:

- **SMB signing not required**

  Severity: Medium

  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.

  Evidence: port 445/tcp/cifs, exploits are available

  Recommendation: Enforce message signing in the host's configuration. On windows, this is found in setting 'Microsoft network server: Digitally sign communications.'

- **SSL Certificate cannot be trusted, SSL self-signed certificate:**

Severity: Mixed

Description: The server's X.509 certificate cannot be trusted. 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

Evidence: 8089/tcp/www, 8191/tcp, 8834/tcp/www – splunk ports

Recommendation: Purchase or generate a proper SSL certificate for the server

- **SSL certificate with wrong Hostname:**

  Severity: Medium

  Description: The 'CommonName' CN attribute of the SSL certificate presented for this service is for a different machine.

  Evidence: 8191/tcp, splunkserverdefaultcert

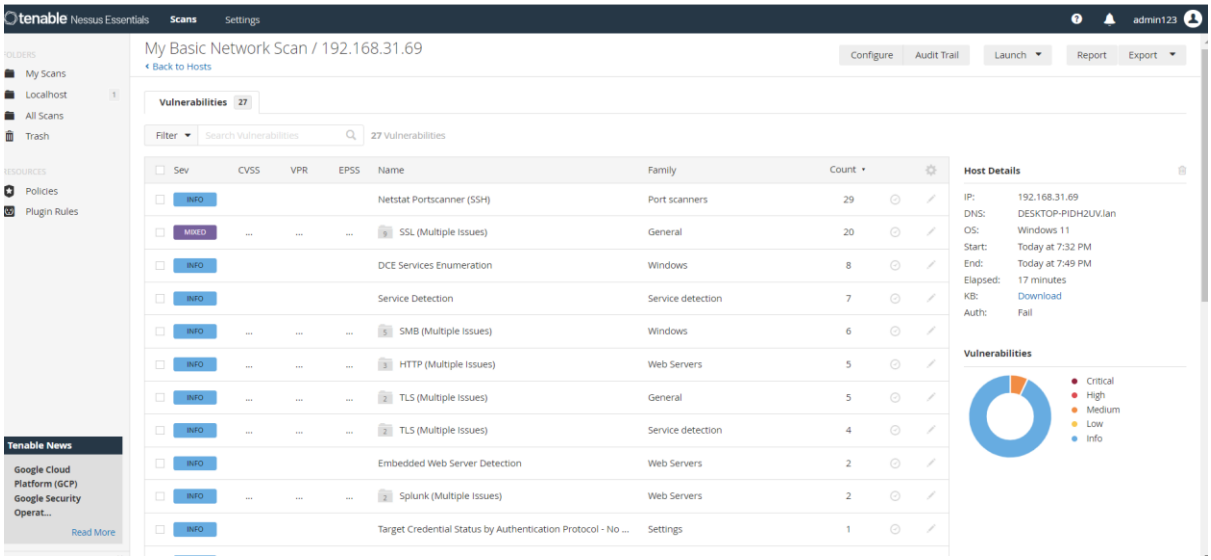
  Recommendation: generate a proper SSL certificate for this service.

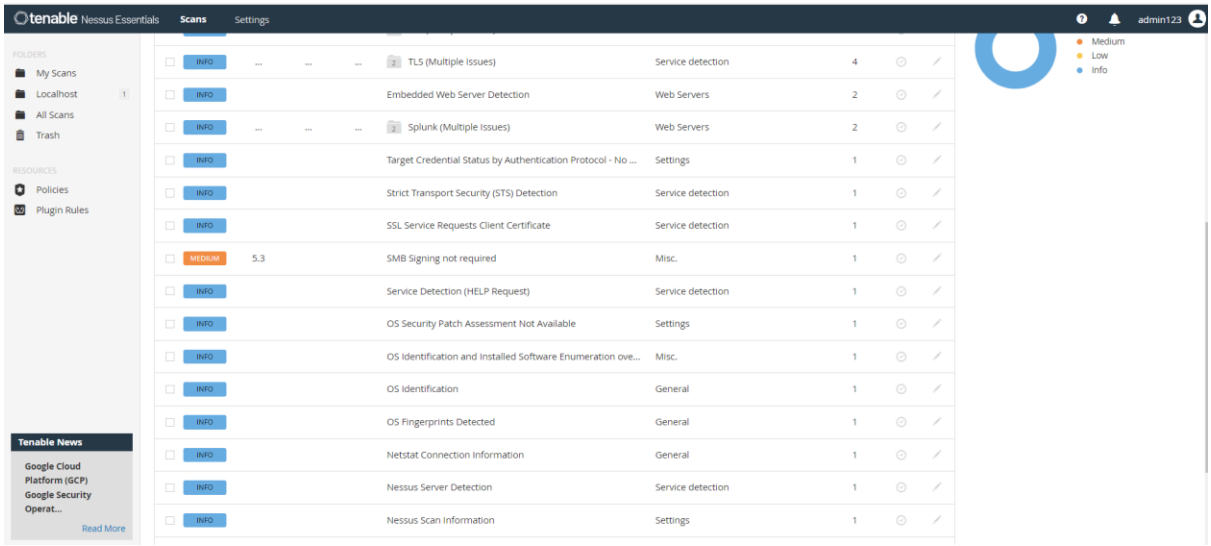
Recommendation Summary

- Apply all pending windows updates.
- Proper SSL certification
- Microsoft network server digital scanning enable

Conclusion

The vulnerability scan identified several issues that could be exploited to compromise the system. Timely remediation is recommended.




tenable Nessus Essentials
Scans
Settings
admin123
FOLDERS
My Scans
Localhost
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Google Cloud Platform (GCP) Google Security Operat...
Read More
INFO TLS (Multiple Issues) Service detection 4
INFO Embedded Web Server Detection Web Servers 2
INFO Splunk (Multiple Issues) Web Servers 2
INFO Target Credential Status by Authentication Protocol - No ... Settings 1
INFO Strict Transport Security (STS) Detection Service detection 1
INFO SSL Service Requests Client Certificate Service detection 1
MEDIUM 5.3 SMB Signing not required Misc. 1
INFO Service Detection (HELP Request) Service detection 1
INFO OS Security Patch Assessment Not Available Settings 1
INFO OS Identification and Installed Software Enumeration ove... Misc. 1
INFO OS Identification General 1
INFO OS Fingerprints Detected General 1
INFO Netstat Connection Information General 1
INFO Nessus Server Detection Service detection 1
INFO Nessus Scan Information Settings 1
Medium
Low
Info