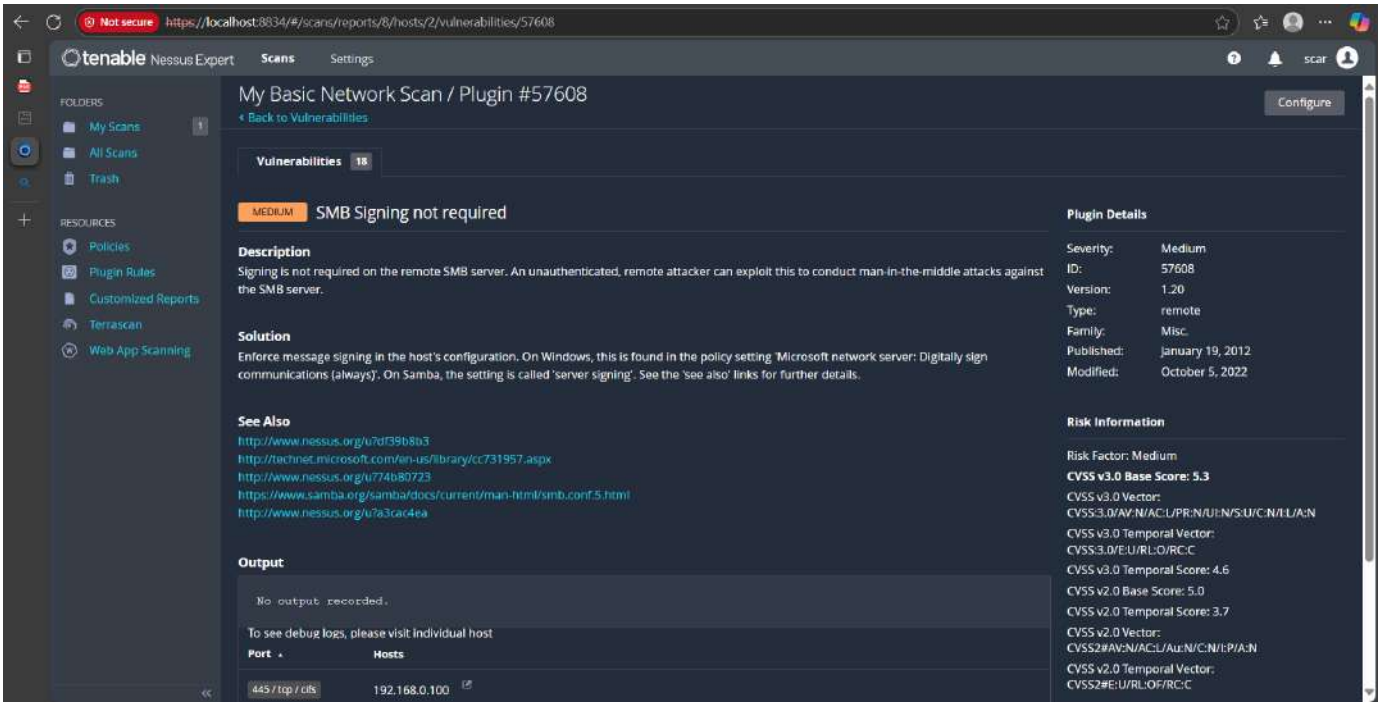
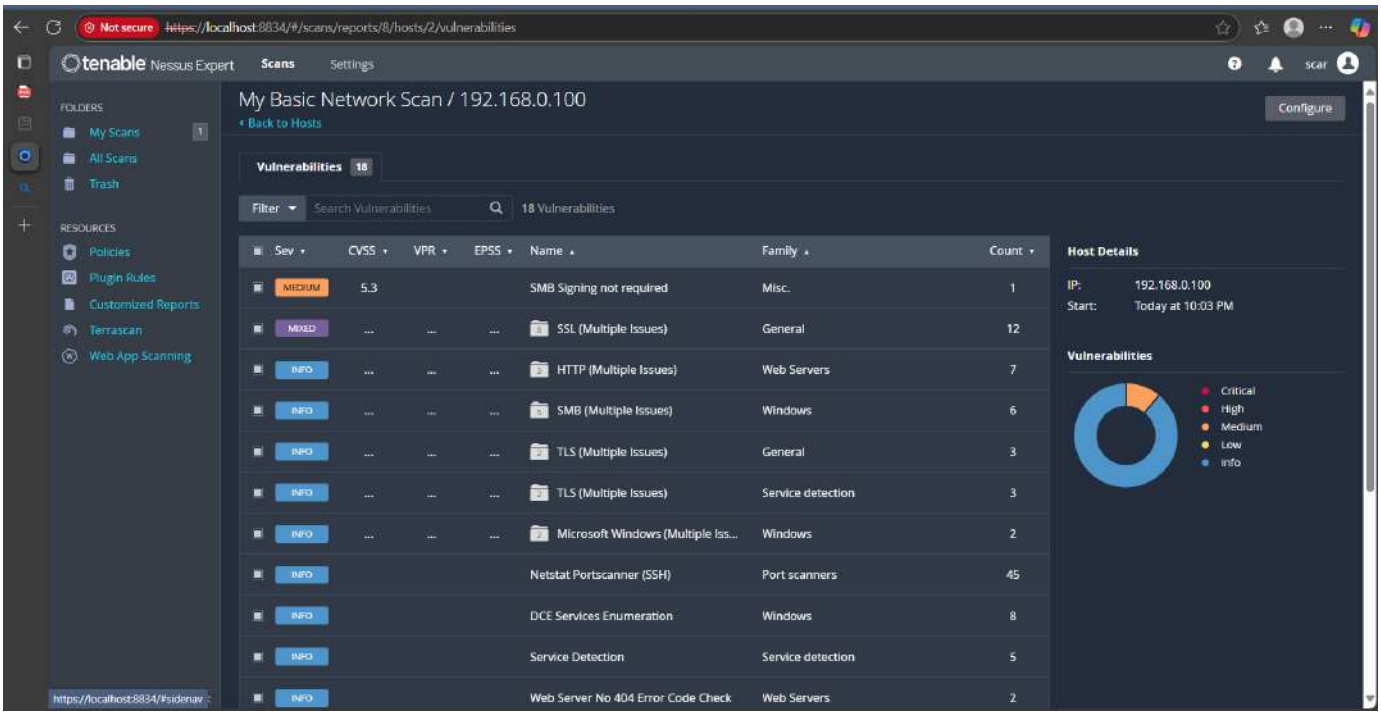

Not secure
https://localhost:8834/#/scans/reports/8/hosts/2/vulnerabilities/57608
tenable Nessus Expert
Scans
Settings
scar
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web App Scanning
My Basic Network Scan / Plugin #57608
Back to Vulnerabilities
Configure
Vulnerabilities 18
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
http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea
Output
No output recorded.
To see debug logs, please visit individual host
Port
Hosts
445 / tcp / cifs
192.168.0.100
Plugin Details
Severity: Medium
ID: 57608
Version: 1.20
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: October 5, 2022
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C


Not secure
https://localhost:8834/#/scans/reports/8/hosts/2/vulnerabilities
tenable Nessus Expert
Scans
Settings
scar
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web App Scanning
My Basic Network Scan / 192.168.0.100
Back to Hosts
Configure
Vulnerabilities 18
Filter
Search Vulnerabilities
18 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MEDIUM 5.3 SMB Signing not required Misc. 1
MIXED ... ... SSL (Multiple Issues) General 12
INFO ... ... HTTP (Multiple Issues) Web Servers 7
INFO ... ... SMB (Multiple Issues) Windows 6
INFO ... ... TLS (Multiple Issues) General 3
INFO ... ... TLS (Multiple Issues) Service detection 3
INFO ... ... Microsoft Windows (Multiple Iss... Windows 2
INFO Netstat Portscanner (SSH) Port scanners 45
INFO DCE Services Enumeration Windows 8
INFO Service Detection Service detection 5
INFO Web Server No 404 Error Code Check Web Servers 2
Host Details
IP: 192.168.0.100
Start: Today at 10:03 PM
Vulnerabilities
Critical
High
Medium
Low
Info
https://localhost:8834/#sidenav

Scan Details

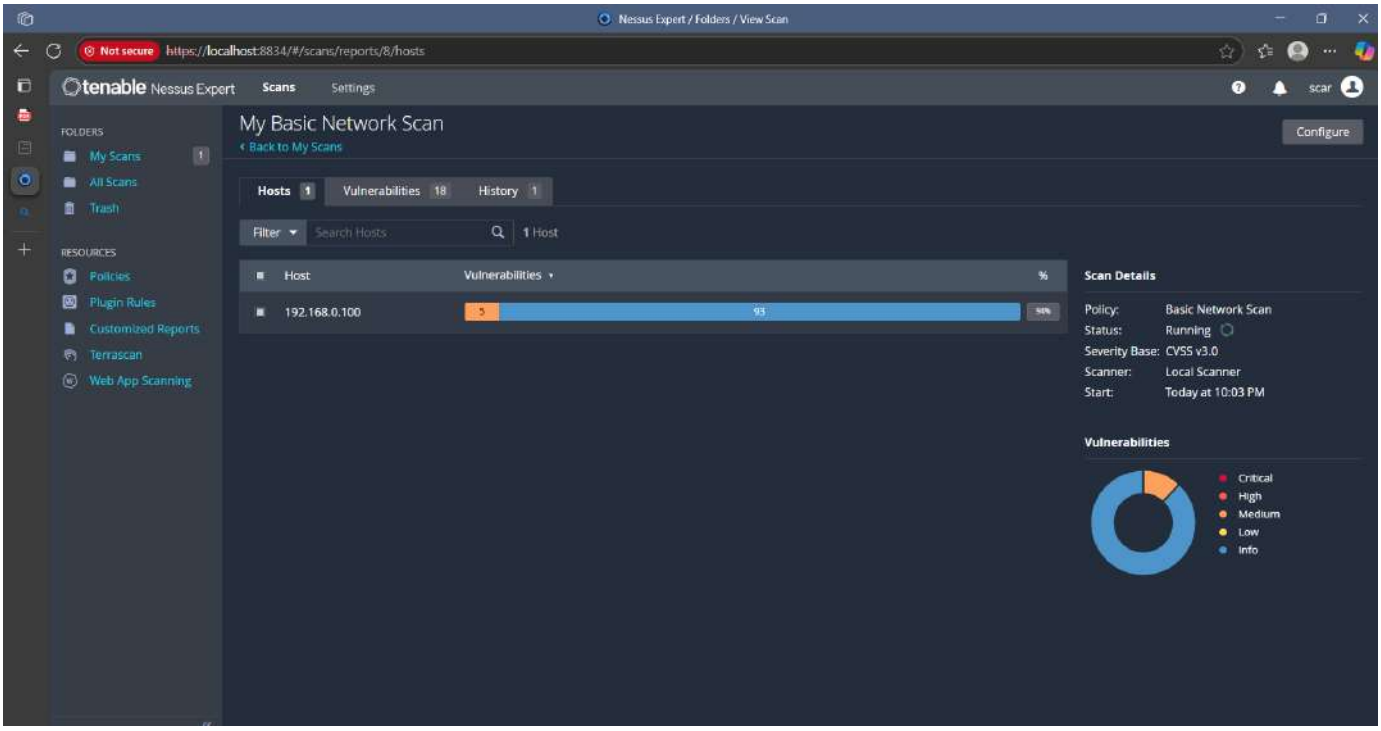
Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:03 PM

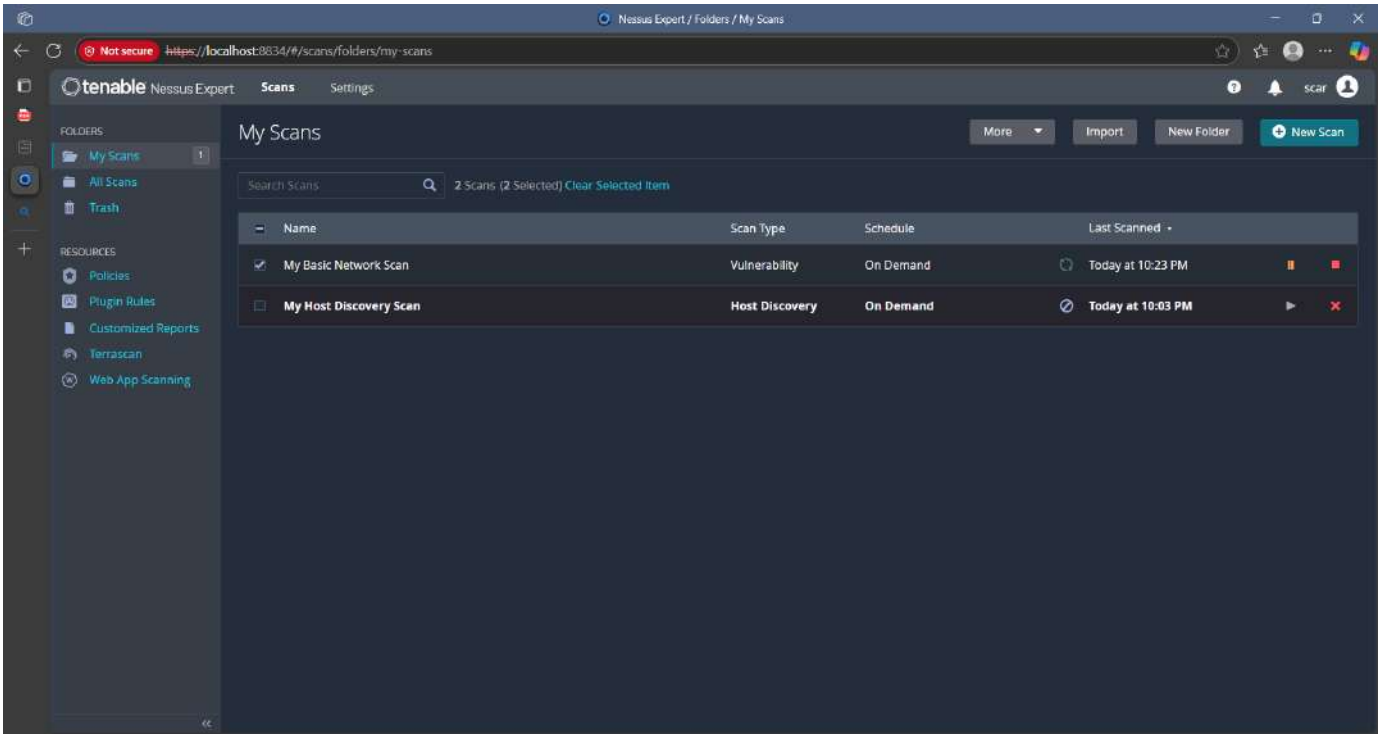
Vulnerabilities

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:03 PM

Vulnerabilities


Nessus Expert / Folders / View Scan
Not secure
https://localhost:8834/#/scans/reports/8/hosts
tenable Nessus Expert
Scans
Settings
scar
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web App Scanning
My Basic Network Scan
Back to My Scans
Configure
Hosts 1
Vulnerabilities 18
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
192.168.0.100
5
93
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:03 PM
Vulnerabilities
Critical
High
Medium
Low
Info


Nessus Expert / Folders / My Scans
Not secure
https://localhost:8834/#/scans/folders/my-scans
tenable Nessus Expert
Scans
Settings
scar
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web App Scanning
My Scans
More
Import
New Folder
New Scan
Search Scans
2 Scans (2 Selected) Clear Selected Item
Name
Scan Type
Schedule
Last Scanned
My Basic Network Scan
Vulnerability
On Demand
Today at 10:23 PM
My Host Discovery Scan
Host Discovery
On Demand
Today at 10:03 PM