Title: Task 3: Comprehensive Vulnerability Assessment using Nessus Essentials and NMAP Scripting Engine (NSE)

Prepared by: Nishant Deshmukh

Date: September 25, 2025

Email: nishantdeshmukh996@gmail.com

1. Summary

In this report, I detail the results of a vulnerability assessment I conducted on my local Windows machine. I took a two-pronged approach, using both the Nmap Scripting Engine for a quick scan and Tenable Nessus Essentials for a deeper analysis.

Interestingly, my Nmap scan came back "clean," finding no active software exploits. However, the more in-depth Nessus scan uncovered a **Medium severity vulnerability ("SMB Signing not required")**. This is a security misconfiguration that could expose my machine to Man-in-the-Middle attacks on my network.

This exercise showed me that a system can be fully patched against common exploits but still be vulnerable due to insecure settings. My key recommendation is to fix this misconfiguration by enforcing SMB signing.

2. Objective

My goal for this task was to gain hands-on experience using multiple industry-standard tools to find vulnerabilities on a computer. I wanted to understand how different tools can work together to provide a more complete picture of a system's security.

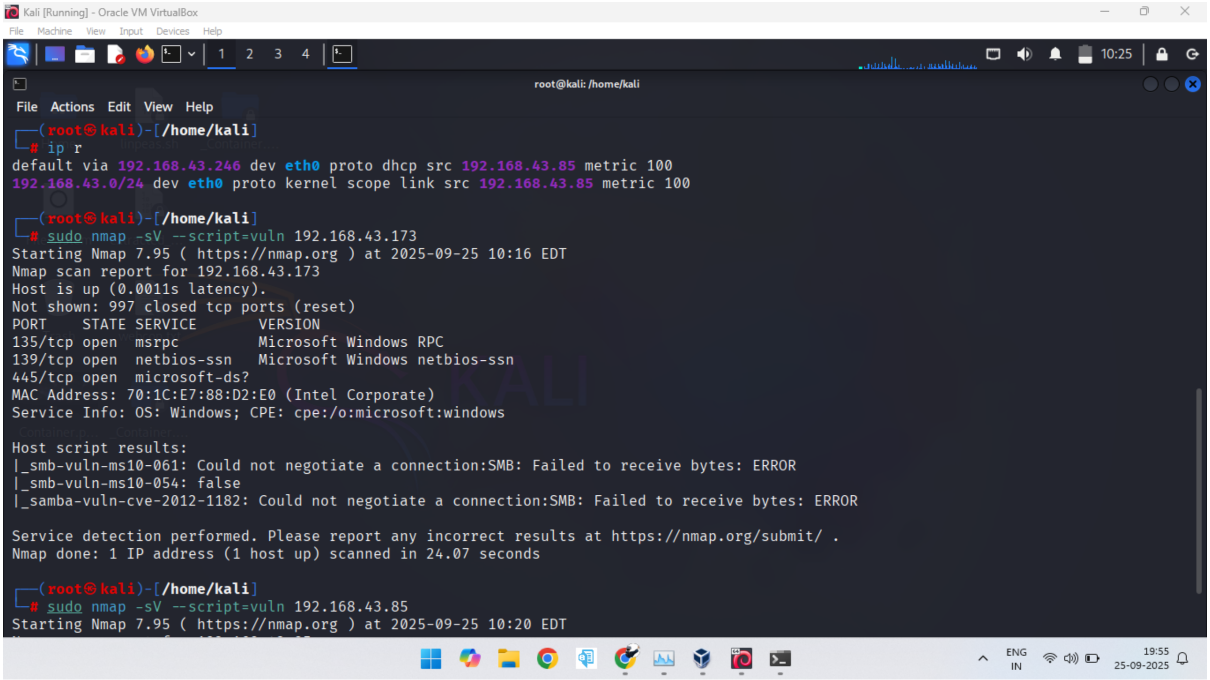
3. Methodology & Tools

I used two different tools to get a comprehensive view of my machine's security.

Tool 1: Nmap Scripting Engine (NSE)

First, I performed a quick scan using Nmap, a tool I was already familiar with. My goal was to check for any common, well-known software vulnerabilities.

- **Command Used:** nmap -sV --script=vuln 192.168.43.173



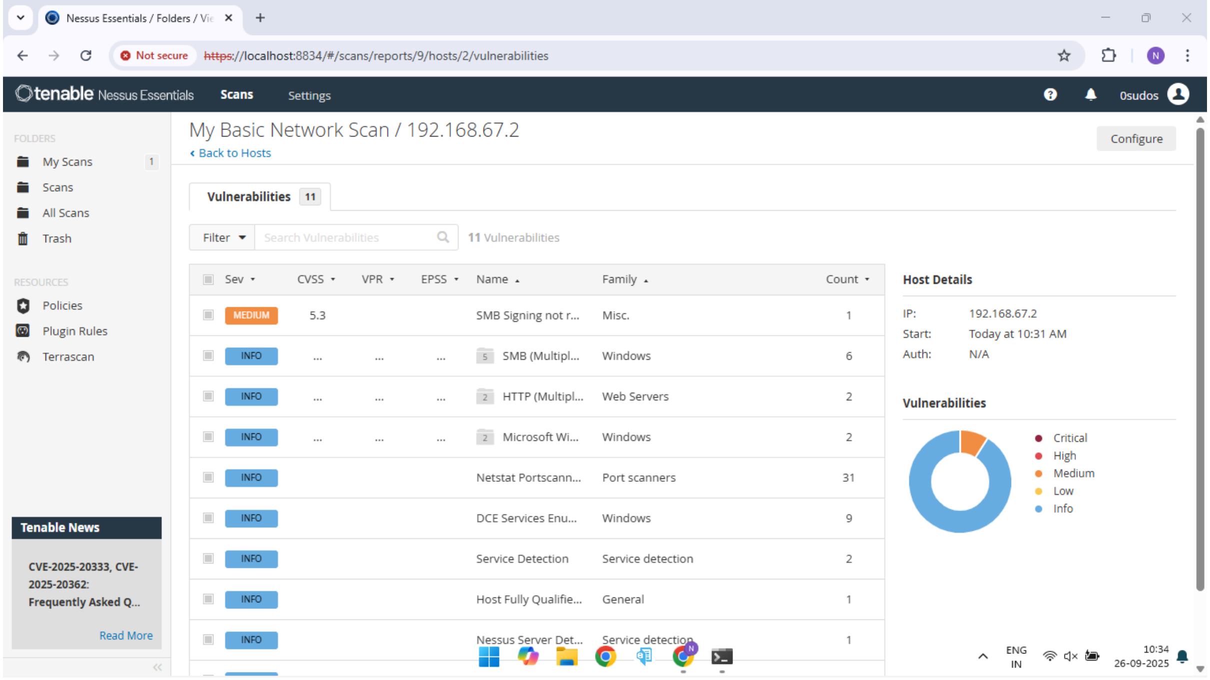
```
┌──(root㉿kali)-[/home/kali]
└─# ip r
default via 192.168.43.246 dev eth0 proto dhcp src 192.168.43.85 metric 100
192.168.43.0/24 dev eth0 proto kernel scope link src 192.168.43.85 metric 100

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV --script=vuln 192.168.43.173
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 10:16 EDT
Nmap scan report for 192.168.43.173
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 70:1C:E7:88:D2:E0 (Intel Corporate)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.07 seconds

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV --script=vuln 192.168.43.85
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 10:20 EDT
```

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
10:25
ENG IN
19:55
25-09-2025

Tool 2: Tenable Nessus Essentials

Next, I used Nessus for a more detailed and in-depth analysis. Nessus checks for thousands of issues, including not just software flaws but also security misconfigurations.

- **Process:** I set up a "Basic Network Scan" in the Nessus web interface and targeted my local machine's IP address (192.168.67.2).



My Basic Network Scan / 192.168.67.2

Vulnerabilities 11

11 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not r...	Misc.	1
INFO	...	...	...	5 SMB (Multipl...	Windows	6
INFO	...	...	...	2 HTTP (Multipl...	Web Servers	2
INFO	...	...	...	2 Microsoft Wi...	Windows	2
INFO				Netstat Portscann...	Port scanners	31
INFO				DCE Services Enu...	Windows	9
INFO				Service Detection	Service detection	2
INFO				Host Fully Qualifie...	General	1
INFO				Nessus Server Det...	Service detection	1

Host Details

IP: 192.168.67.2
Start: Today at 10:31 AM
Auth: N/A

Tenable News

CVE-2025-20333, CVE-2025-20362: Frequently Asked Q...

4. Findings & Analysis

Combining the results from both scans gave me a much clearer understanding of my computer's security.

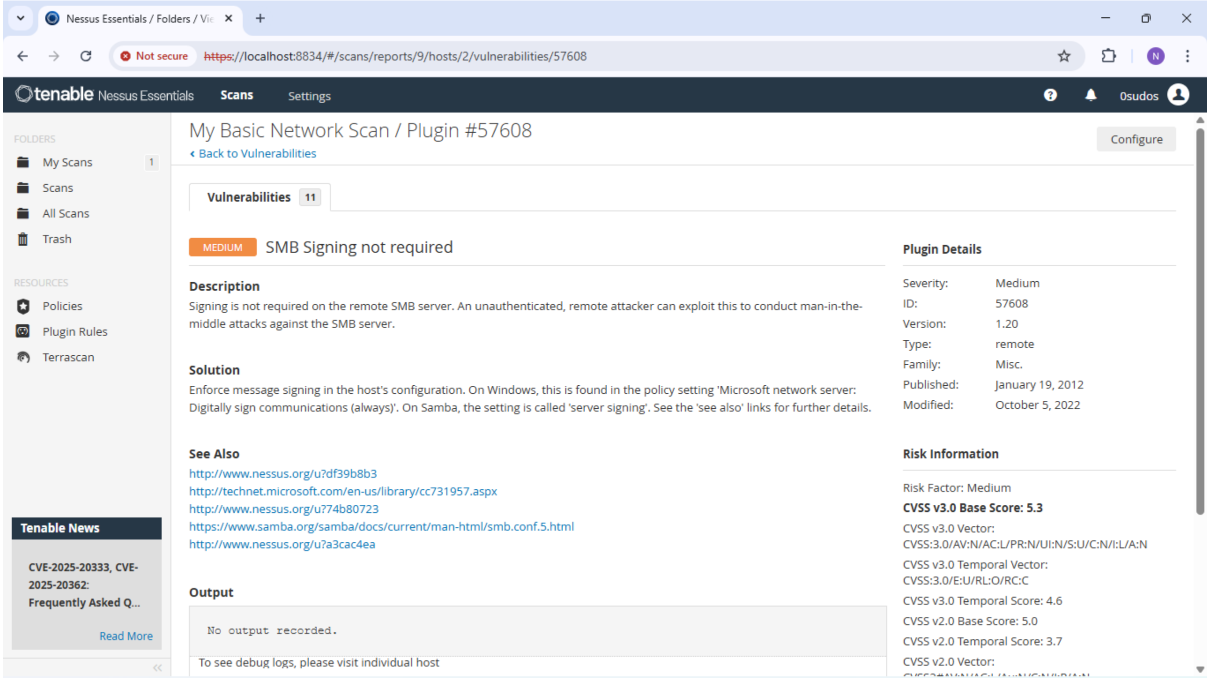
Finding 1: No Active Software Exploits Found (Nmap)

My Nmap scan did not find any of the common vulnerabilities it was checking for. For example, the check for smb-vuln-ms10-054 came back as false. This is a positive result, as it suggests my computer's software is up-to-date and patched against those specific threats.

Finding 2: SMB Signing Not Required (Nessus - Medium Severity)

The Nessus scan, however, found a security misconfiguration that Nmap missed.

- **Severity: Medium**
- **CVSS v3.0 Score: 5.3**
- **Description:** My computer's file sharing service (SMB) doesn't require a digital "signature" on its communications. This is risky because it opens the door to a **Man-in-the-Middle (MitM) attack**. An attacker on my Wi-Fi network could potentially intercept the connection between my PC and another device, and then read or even alter the data without me knowing.


Nessus Essentials / Folders / Vie
Not secure
https://localhost:8834/#/scans/reports/9/hosts/2/vulnerabilities/57608
tenable Nessus Essentials
Scans
Settings
0sudos
FOLDERS
My Scans 1
Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
CVE-2025-20333, CVE-2025-20362: Frequently Asked Q...
Read More
Configure
‹ Back to Vulnerabilities
Vulnerabilities 11
MEDIUM

My Basic Network Scan / Plugin #57608

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

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:

5. My Remediation Plan

Based on the findings, my top priority is to fix the Medium severity issue discovered by Nessus.

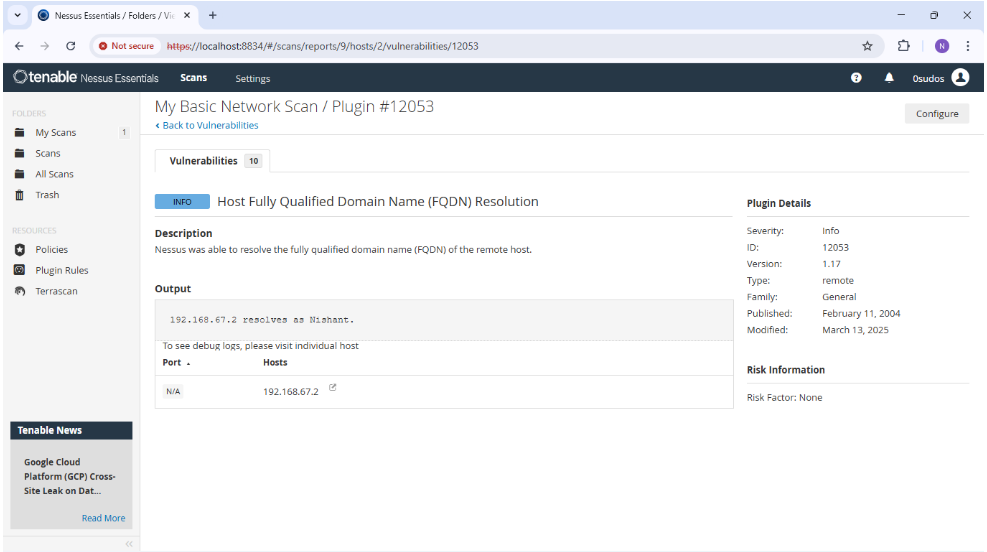
- **Primary Recommendation: Enforce SMB Message Signing**
  - **My Action Plan:** The solution is to change a security policy on my Windows machine to always require SMB signing. This setting can be found in the Group Policy Editor.

- **Why This Works:** Forcing all file-sharing traffic to be digitally signed acts like a tamper-proof seal, which effectively prevents Man-in-the-Middle attacks against this service.

6. Conclusion

This was a very successful assessment. It taught me a valuable lesson: a system might be fully patched against old exploits (which is why Nmap found nothing), but still be vulnerable due to an insecure setting. Using both a quick scanner like Nmap and a detailed tool like Nessus gave me a much more accurate view of my machine's real security posture. By enforcing SMB signing, I can significantly improve my system's security.

7. Additional Scan Evidence


Nessus Essentials / Folders / Vi
Not secure
https://localhost:8834/#/scans/reports/9/hosts/2/vulnerabilities/12053
tenable Nessus Essentials
Scans
Settings
0sudos
FOLDERS
My Scans 1
Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Google Cloud Platform (GCP) Cross-Site Leak on Dat...
Read More
Configure

My Basic Network Scan / Plugin #12053

‹ Back to Vulnerabilities

Vulnerabilities 10

INFO Host Fully Qualified Domain Name (FQDN) Resolution

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Output

```
192.168.67.2 resolves as Nishant.
```

To see debug logs, please visit individual host

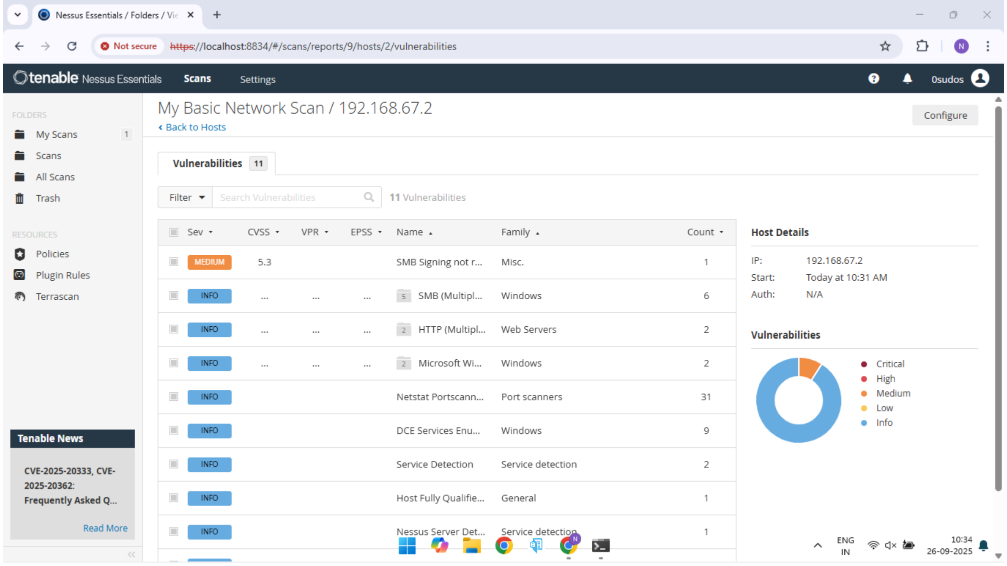
Port	Hosts
N/A	192.168.67.2

Plugin Details

Severity:	Info
ID:	12053
Version:	1.17
Type:	remote
Family:	General
Published:	February 11, 2004
Modified:	March 13, 2025

Risk Information

Risk Factor: None



My Basic Network Scan / 192.168.67.2

‹ Back to Hosts

Vulnerabilities 11

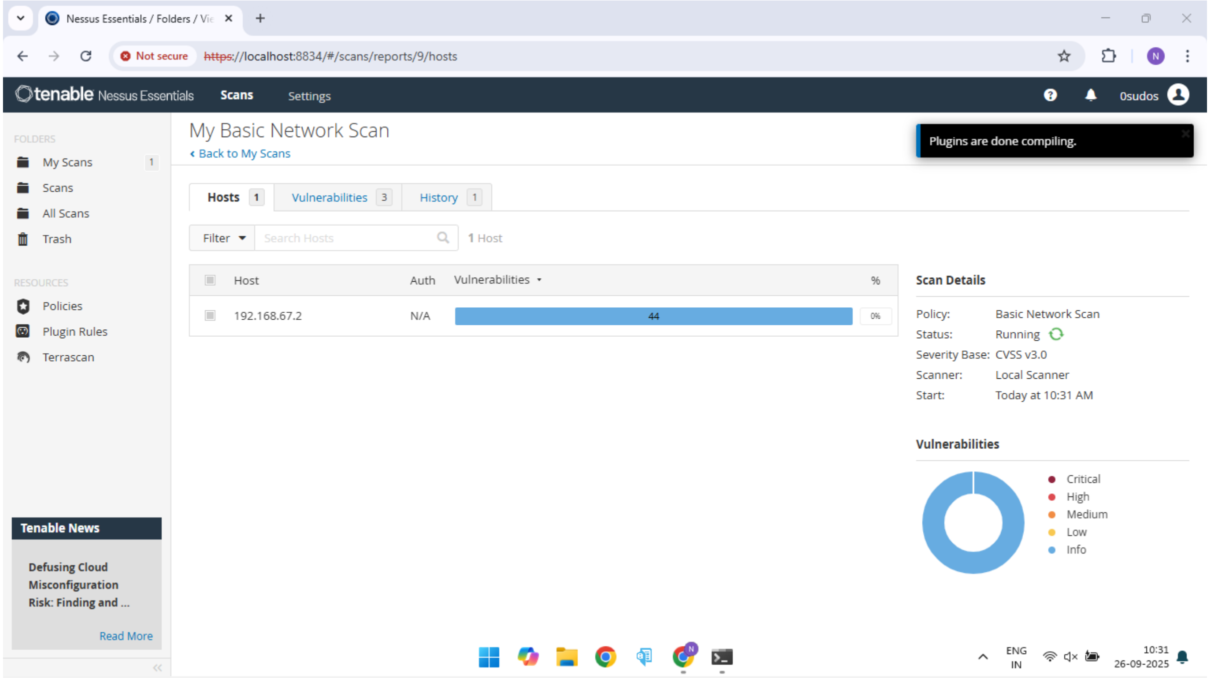
11 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not r...	Misc.	1
INFO	...	...	...	5 SMB (Multipl...	Windows	6
INFO	...	...	...	2 HTTP (Multipl...	Web Servers	2
INFO	...	...	...	2 Microsoft Wi...	Windows	2
INFO				Netstat Portscann...	Port scanners	31
INFO				DCE Services Enu...	Windows	9
INFO				Service Detection	Service detection	2
INFO				Host Fully Qualifie...	General	1
INFO				Nessus Server Det...	Service detection	1

Host Details

IP:	192.168.67.2
Start:	Today at 10:31 AM
Auth:	N/A

Vulnerabilities



My Basic Network Scan

‹ Back to My Scans

Plugins are done compiling.

Host	Auth	Vulnerabilities	%
192.168.67.2	N/A	44	0%

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:31 AM

8. References

1. The "SMB Signing not required" Vulnerability

    - Microsoft's Official Guide on SMB Signing: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always

2. Man-in-the-Middle (MitM) Attacks

    - What is a Man-in-the-Middle Attack?: https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/

3. Comparing Nmap and Nessus

    - Nmap vs Nessus: A Detailed Comparison: https://www.upguard.com/blog/nmap-vs-nessus

4. Understanding Vulnerability Assessment

    - What is Vulnerability Assessment?: https://www.tenable.com/vulnerability-management/vulnerability-assessment