

## Experiment 14

Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.

Roll No.	19
Name	Manav Jawrani
Class	D15-A
Subject	Security Lab
LO Mapped	LO5: Use open-source tools to scan the network for vulnerabilities and simulate attacks.

**Aim:** Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities

## **Introduction:**

### **Nessus Introduction:**

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

### **Nessus can scan these vulnerabilities and exposures:**

1. Vulnerabilities that could allow unauthorized control or access to sensitive data on the system.
2. Misconfiguration (e.g. open mail relay)
3. Denials of service (Dos) vulnerabilities
4. Default passwords, a few common passwords, and blank/absent passwords on some system accounts.
5. Software flaws, missing patches, malware and misconfiguration errors across a wide range of operating systems, devices and applications are dealt with by Nessus.

The Nessus server is currently available for:

1. Unix
2. Linux
3. FreeBSD

Also, the client is available for:

1. Unix-based operating systems
2. Windows-based operating systems

**Scheduled security audits:**

Detection of security holes in local or remote hosts

Simulated attacks to pinpoint vulnerabilities

**Detection of missing security updates and patches:**

Nessus Professional performs internal network scans as required by the PCI DSS 11.2.1 requirement. The results of the scan can be reported in various formats, such as plain text, XML, and HTML.

You cannot use Nessus on a system with a Host-based Intrusion Prevention System (HIPS) installed. Because during the process of scanning a remote target, Nessus must forge TCP/UDP packets and send probes that are often considered “malicious” by HIPS software. If the HIPS system is configured to block malicious traffic, it will interfere with Nessus and cause the scan results to be incomplete or unreliable.

**Nessus Features:**

1. Vulnerability Scanning
2. Asset Discovery
3. Network Scanning
4. Vulnerability Assessment
5. Prioritization
6. Policy Management
7. Web Scanning

**What is Nessus Agent?**

Nessus Agents provide a flexible way of scanning hosts within your environment without necessarily having to provide credentials to hosts. The agents enable scans to be carried out even when the hosts are offline.

**Nessus Agents provide a subset of the coverage in a traditional network scan:**

Scanning of transient endpoints that are not always connected to the local network.

Scanning assets for which you do not have credentials or could not easily obtain credentials. Improving overall scan performance: With agents, the network scan can be reduced to just remote network checks, speeding scan completion time.

**Nessus Agents currently support a variety of operating systems including:**

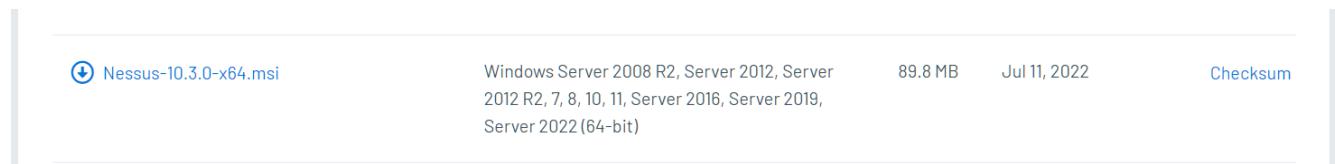
1. Windows Server 2008 and 2012, and Windows 7 and 8
2. Amazon Linux
3. CentOS
4. Debian Linux
5. OS X
6. Red Hat Enterprise Linux
7. Ubuntu Linux

### **Methods:**

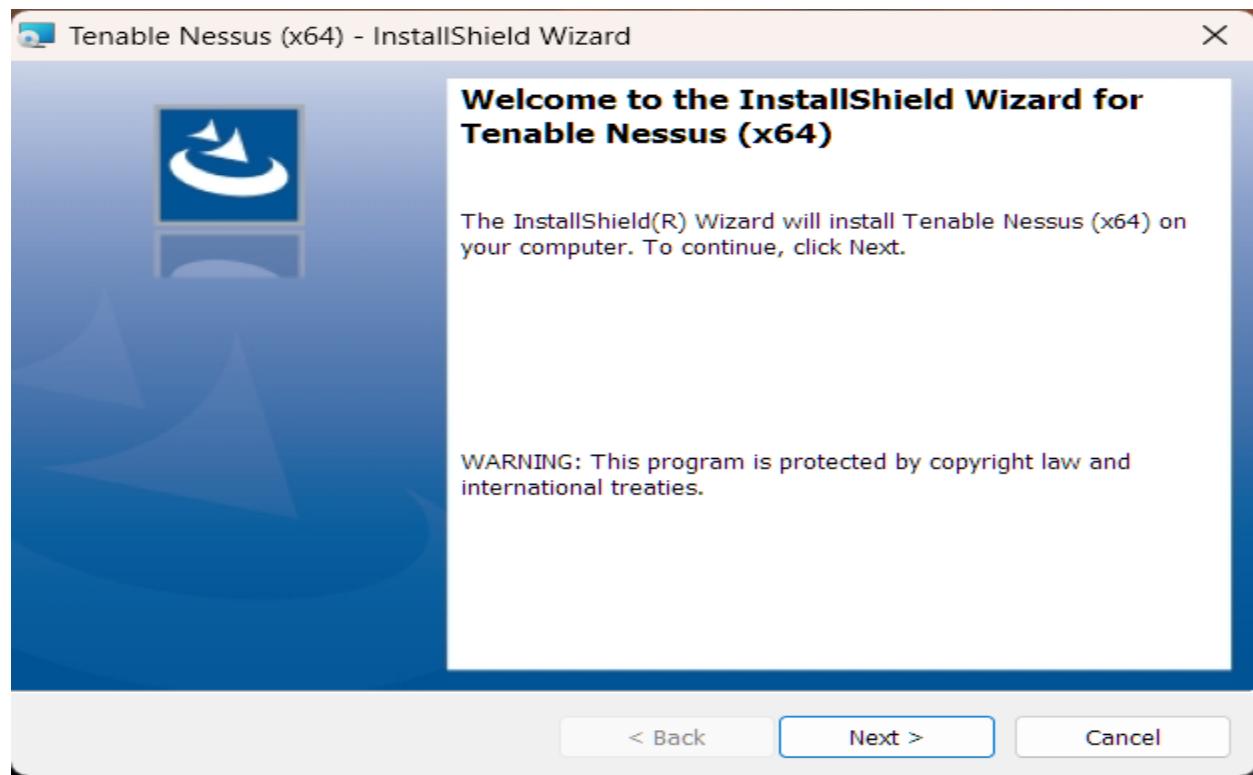
**Step 1:** Go to this website:

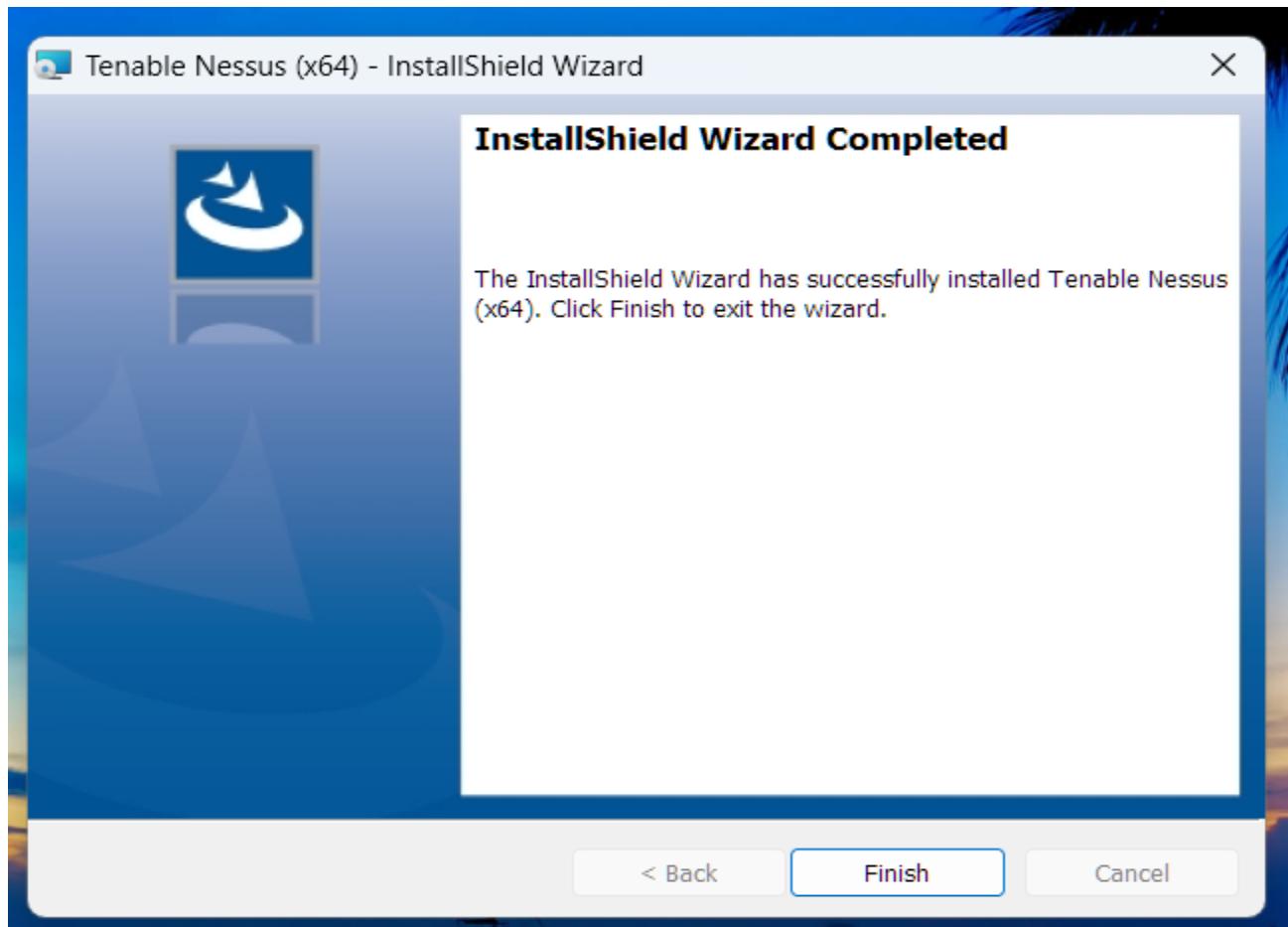
<https://www.tenable.com/downloads/nessus?loginAttempted=true>

and search for the Windows Server 2008 msi installer and Download.

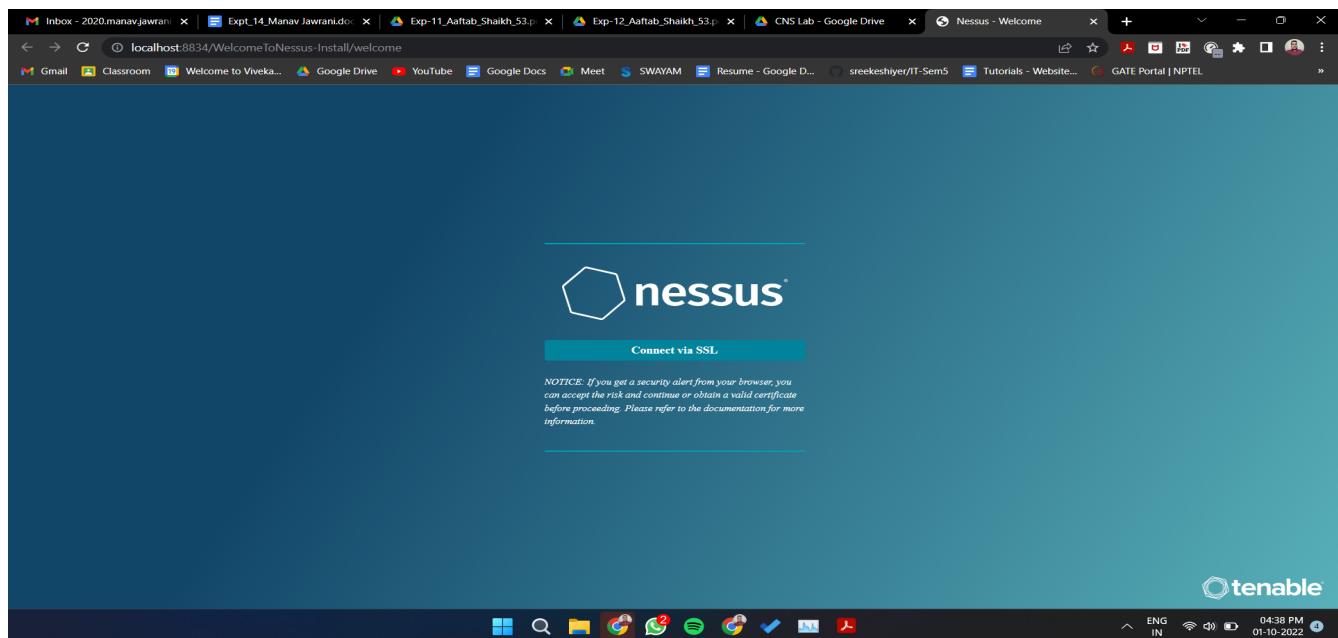


Install Nessus:

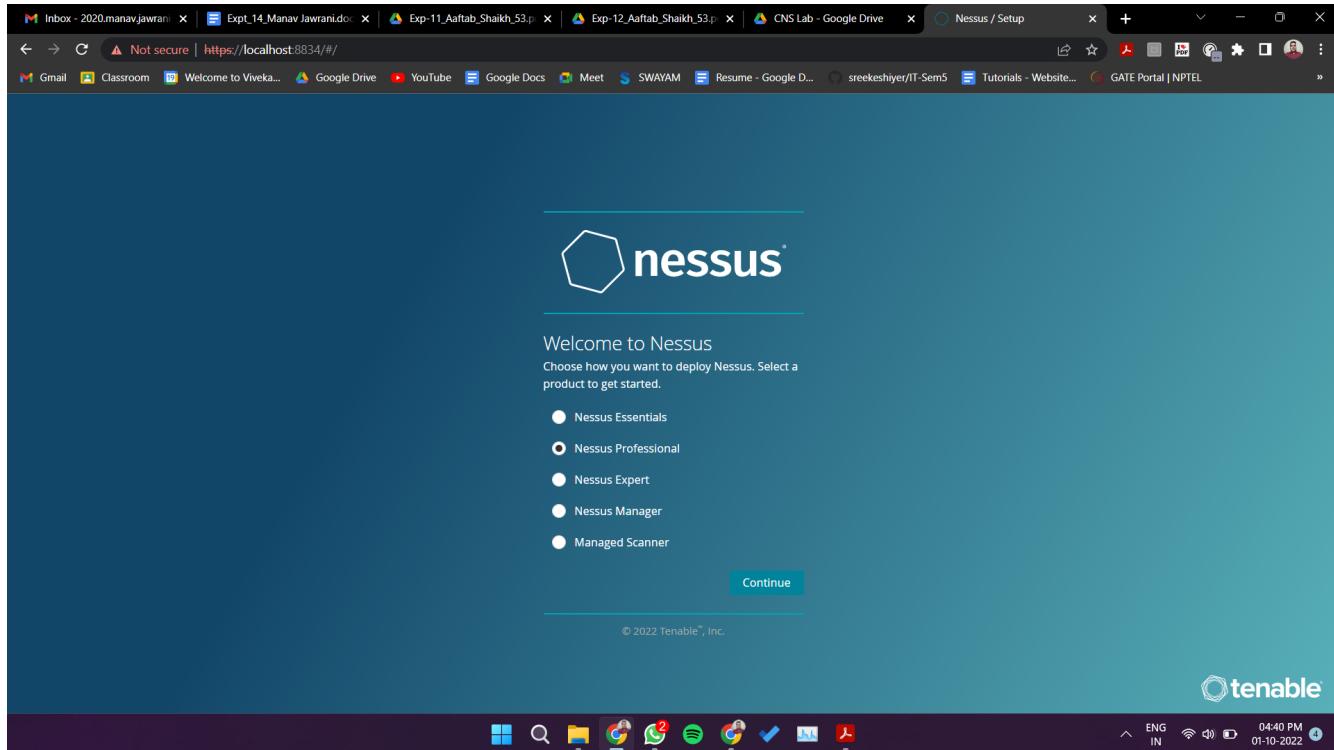




After successfully installing it you will be redirected to this page

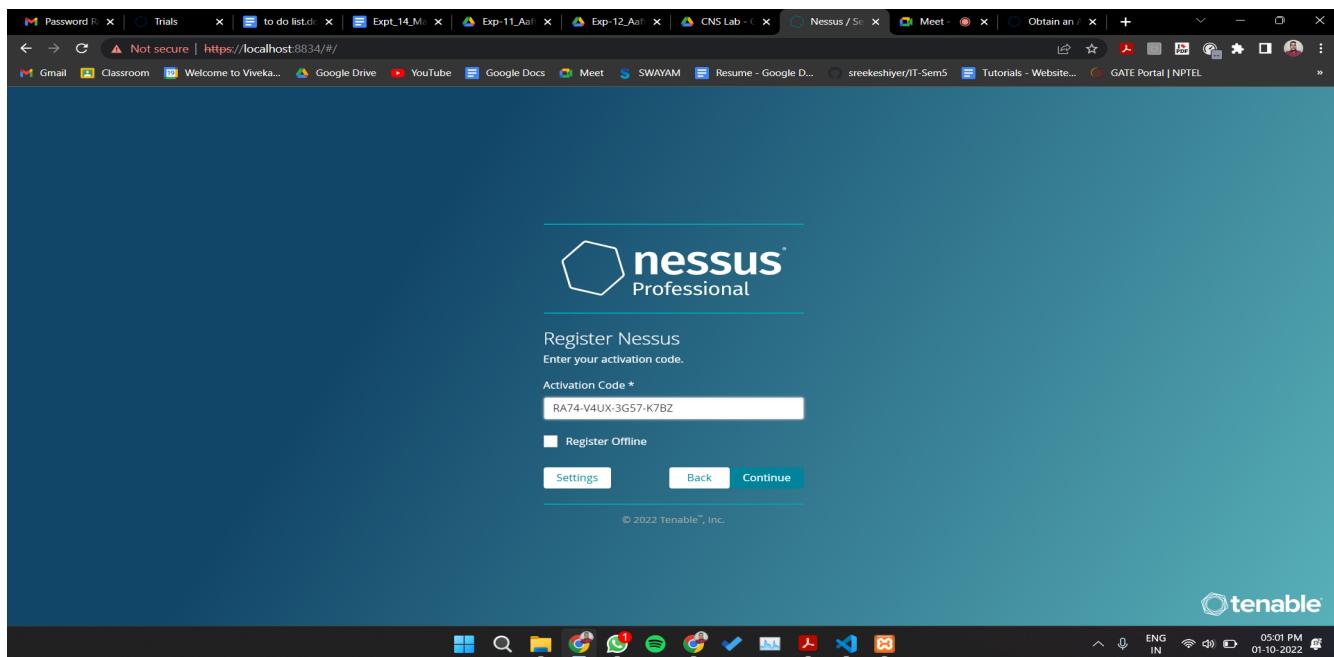


Next it will ask you which version you want to install



Now go to this website <https://www.tenable.com/products/nessus/activation-code> and get an activation code which will be used further.

Copy the activation code and paste it here



Create the username and password

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Create a user account" for Nessus Professional. The page content includes a logo, a title, and a form for entering a username and password. The browser's status bar at the bottom shows the date and time as 01-10-2022.

It will download some plugins

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Initializing" for Nessus. The page content includes a logo, a title, and a message about preparing files for asset scanning. A progress bar indicates the download of plugins. The browser's status bar at the bottom shows the date and time as 01-10-2022.

This will be the Home Page where you will be redirected after installation

The screenshot shows the Nessus Professional web interface. The left sidebar has sections for 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan), and 'Scans' (selected). The main area is titled 'My Scans' with a message: 'This folder is empty. Create a new scan.' There are buttons for 'Import', 'New Folder', and '+ New Scan'. The bottom status bar shows system information like battery level, language (ENG IN), and date (01-10-2022).

Now we will perform a **Basic Network Scan**

The screenshot shows the 'Scan Templates' page in the Nessus Professional interface. The left sidebar is identical to the previous screenshot. The main area is titled 'Scan Templates' with a 'Scanner' tab selected. It shows various scan templates categorized under 'DISCOVERY' and 'VULNERABILITIES'. Under 'DISCOVERY', there is 'Host Discovery'. Under 'VULNERABILITIES', there are several options: 'Basic Network Scan' (a full system scan suitable for any host), 'Advanced Scan' (configure a scan without using any recommendations), 'Advanced Dynamic Scan' (configure a dynamic plugin scan without recommendations), 'Malware Scan' (scan for malware on Windows and Unix systems), 'Mobile Device Scan' (assess mobile devices via Microsoft Exchange or an MDM, with an 'UPGRADE' banner), 'Web Application Tests' (scan for published and unknown web vulnerabilities using Nessus Scanner), 'Credentialed Patch Audit' (authenticate to hosts and enumerate missing updates), 'Intel AMT Security Bypass' (remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754), 'Spectre and Meltdown' (remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754), and 'WannaCry Ransomware' (remote and local checks for MS17-010). The bottom status bar shows system information like battery level, language (ENG IN), and date (01-10-2022).

Enter the details

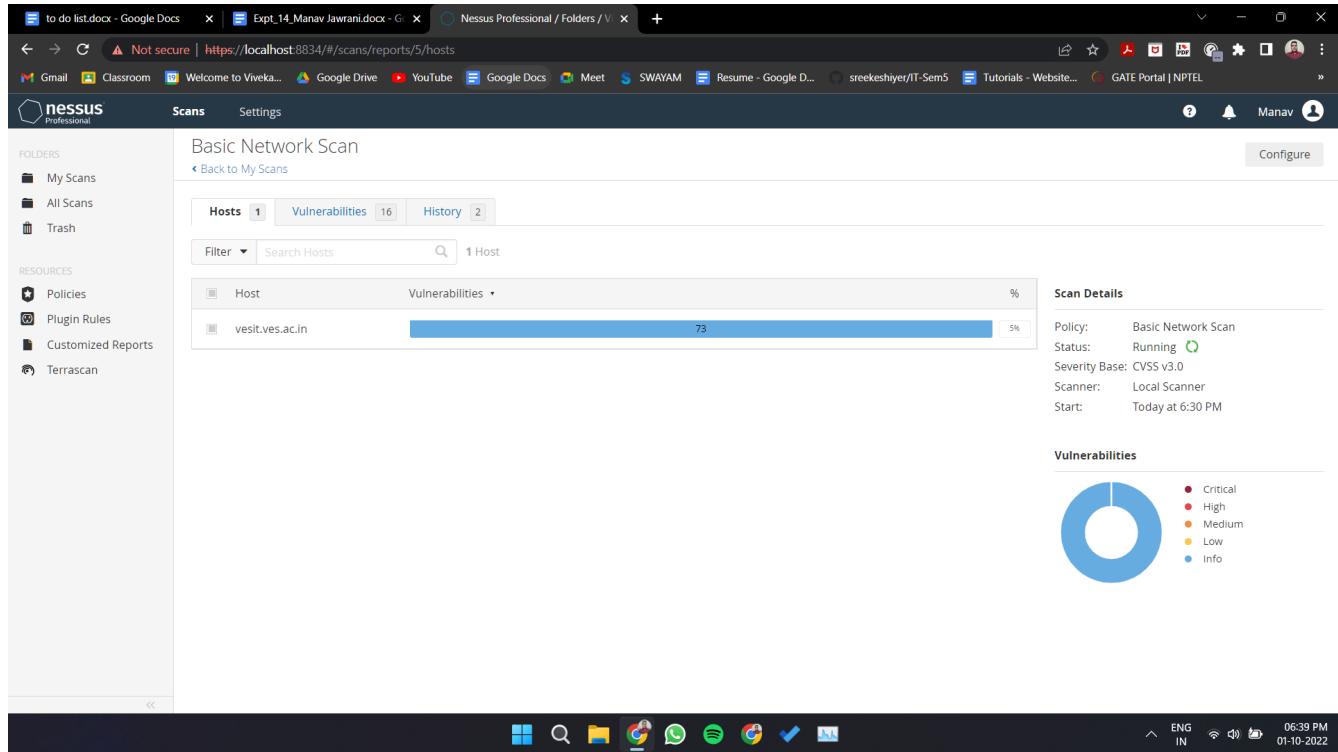
The screenshot shows the Nessus Professional web interface. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans', 'All Scans', and 'Trash'. Under 'RESOURCES', there are 'Policies', 'Plugin Rules', 'Customized Reports', and 'Terrascan'. The main area has tabs for 'Scans', 'Settings', 'Credentials', and 'Plugins'. The 'Settings' tab is active, showing the 'BASIC' section with 'General' selected. Under 'General Settings', the 'Name' is 'Basic Network Scan' and the 'Description' is also 'Basic Network Scan'. The 'Folder' is set to 'My Scans'. In the 'Targets' field, the value is 'vesit.ves.ac.in'. Below this, there's an 'Upload Targets' section with a 'Add File' button. Under 'Post-Processing', there's a checkbox for 'Live Results' with a descriptive note. At the bottom, there are 'Save' and 'Cancel' buttons.

Our targeted website for scan in [www.vesit.ves.ac.in](http://www.vesit.ves.ac.in)

Now Launch the scan

The screenshot shows the 'My Scans' page. At the top, there's a search bar with 'Search Scans' and a 'Clear Selected Item' link. To the right are buttons for 'More', 'Import', 'New Folder', and '+ New Scan'. Below is a table with columns for 'Name', 'Schedule', 'Last Modified', and 'Launch'. There are two rows: one for 'Basic Network Scan' (which is checked) and another for 'On Demand' (which is unchecked). The 'Launch' button is highlighted with a red arrow.

## Scan is running



## Results

After scanning these are the results

**Scan Details**

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:30 PM
- End: Today at 7:56 PM
- Elapsed: an hour

**Vulnerabilities**

Critical: 1, High: 1, Medium: 33, Low: 235, Info: 6

Host	Vulnerabilities
visit.ves.ac.in	6 Critical, 33 Medium, 235 Low, 6 Info

## Vulnerabilities:

**Scan Details**

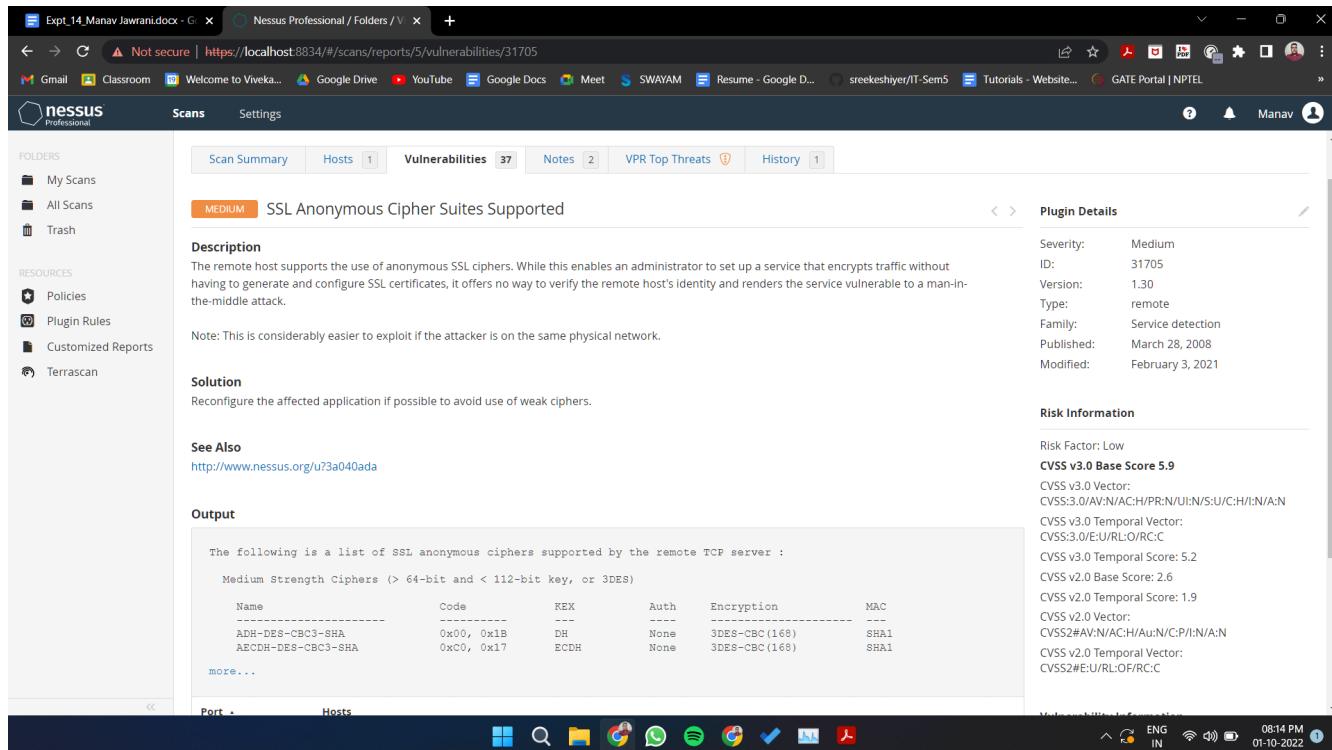
- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:30 PM
- End: Today at 7:56 PM
- Elapsed: an hour

**Vulnerabilities**

Critical: 1, High: 1, Medium: 33, Low: 235, Info: 6

Sev	Score	Name	Family	Count
MIXED	...	SSL (Multiple Issues)	Plugin ID: 31705 General	63
MEDIUM	5.9	SSL Anonymous Cipher Suites Supported	Service detection	1
MIXED	...	TLS (Multiple Issues)	Service detection	39
MIXED	...	HTTP (Multiple Issues)	Web Servers	27
INFO	...	TLS (Multiple Issues)	General	22
INFO	...	IETF Md5 (Multiple Issues)	General	10
INFO	...	Web Server (Multiple Issues)	Web Servers	8
INFO	...	DNS (Multiple Issues)	DNS	4
INFO	...	TLS (Multiple Issues)	Misc.	3
INFO	...	ISC Bind (Multiple Issues)	DNS	2

## Analyzing one of the vulnerabilities:



The screenshot shows the Nessus Professional interface with a vulnerability report. The title is "SSL Anonymous Cipher Suites Supported" (Severity: MEDIUM). The "Description" section states: "The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack." The "Note" section says: "Note: This is considerably easier to exploit if the attacker is on the same physical network." The "Solution" section advises: "Reconfigure the affected application if possible to avoid use of weak ciphers." The "See Also" section provides a link: <http://www.nessus.org/u?3a040ada>. The "Output" section lists supported ciphers:

```

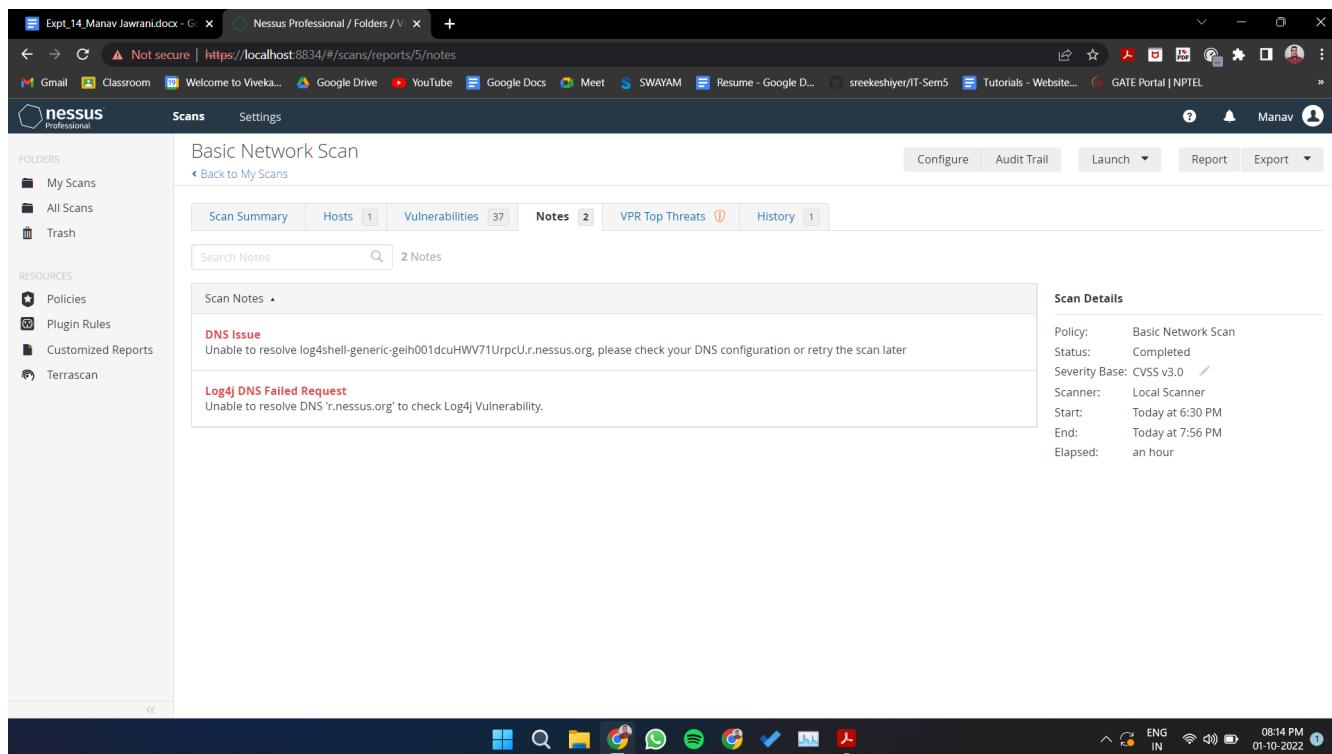
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name          Code      KEX      Auth      Encryption      MAC
-----        -----    ----     ---       -----        ---
ADH-DES-CBC3-SHA   0x00, 0x1B  DH        None      3DES-CBC(168)  SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH     None      3DES-CBC(168)  SHA1
more...
  
```

On the right side, there are sections for "Plugin Details" and "Risk Information". "Plugin Details" includes fields like Severity: Medium, ID: 31705, Version: 1.30, Type: remote, Family: Service detection, Published: March 28, 2008, and Modified: February 3, 2021. "Risk Information" shows Risk Factor: Low, CVSS v3.0 Base Score: 5.9, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N, and CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C.

## Notes:



The screenshot shows the Nessus Professional interface with a notes report for a "Basic Network Scan". The title is "Basic Network Scan". The "Scan Notes" section contains two entries:

- DNS Issue**: Unable to resolve log4shell-generic-geih001dcuHWV71UrpcU.r.nessus.org, please check your DNS configuration or retry the scan later.
- Log4j DNS Failed Request**: Unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability.

On the right side, there is a "Scan Details" panel with the following information:

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:30 PM
End:	Today at 7:56 PM
Elapsed:	an hour

## Top Threats:

The screenshot shows the Nessus Professional interface with a 'Basic Network Scan' report. The report details three vulnerabilities:

VPR Severity	Name	Reasons	VPR Score	Hosts
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	No recorded events	5.1	1
MEDIUM	SSL Anonymous Cipher Suites Supported	No recorded events	4.4	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	No recorded events	3.6	1

**Scan Details:**

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:30 PM
- End: Today at 7:56 PM
- Elapsed: an hour

## Conclusion:

Thus we have successfully downloaded, installed and configured the Nessus tool on Windows.