————————————————————Nessus SOP ————————————————————

Nessus Installation and Configuration (WINDOWS)

1. Download and Install Nessus from the official website.

2. Run Task Manager as Administrator *-> More Details -> Services -> Stop Tenable Nessus.*

3. Run Command

Prompt as Administrator -> **cd Files**.

For Help -> **nessuscli.exe –help**

4.Activate Nessus License -> **nessuscli.exe fetch –register (Activation Code)**

5. Once all plugins are installed, run the following commands:

1.nessuscli.exe adduser [username]

2. nessuscli.exe password [password]

6.Run Task Manager *as Administrator -> More Details -> Services -> Start Tenable Nessus.*

7. On Browser, go to: *https://127.0.0.1:8834*

Nessus Installation and Configuration (LINUX)

1. Download and Install Nessus from the official website.

2. Go to Terminal -> **cd ~/Downloads**

3.To Install, run -> **sudo dpkg -i Nessus.deb**

a. If proxy required, run **-> sudo /opt/nessus/sbin/nessuscli fix –secure –set proxy=IP_Address**

b. If port required, run **-> sudo /opt/nessus/sbin/nessuscli fix –secure –set port=Port_Number**

4. To set up Nessus, run **-> sudo /opt/nessus/sbin/nessuscli fetch –register (Activation Code)**

5. Once all plugins are installed, run the following commands:

1. nessuscli adduser [username]

2. nessuscli password [password]

6. On Browser, go to: *https://127.0.0.1:8834*

Set Up Nessus (Main Configuration) Before performing any scanning,

select the *'Main' Scan -> More -> Copy to My Scans*. Just change the IP address with the one provided.

1. Login on Nessus using username and password created earlier. Allow plugins to finish installation.
2. Once done, *go to New Scan -> Select Advanced Scan. Configure as follows:*

A. Basic -> General:

- Name: Main
- Target: 10.10.10.1

B. Discovery -> Host Discovery:

- Ping the Remote Host: Off

C. Discovery -> Port Scanning:

- Consider Unscanned Ports as Closed: Enabled
- Port Scan Range: 0-65535
- Verify open TCP ports found by local port enumerators: Enabled

D. Assessment -> Windows:

- Request information about SMB Domain: Enabled
- RID Brute Forcing: On

E. Assessment -> Malware:

- Scan for malware: On

F. Report:

- Designate hosts by their DNS name: Enabled
- Display hosts that respond to ping: Enabled
- Display unreachable hosts: Enabled

G. Plugins:

- Denial of Service: Disabled

All other settings should remain as default.

3. Internal Scanning (if credentials are provided):

- For Windows: Enter Username & Password in Credentials tab.
- For Linux: Select SSH -> Authentication Method: Password ->

  Enter Username & Password -> Elevate Privileges using su or sudo

  (verify with client).

4. External Scanning:

- No credentials required.

Downloading Nessus Reports

1. Go to the specific Nessus scan -> **Export -> Download the .nessus file.**

2. Then go to Report -> **Select CSV ->Generate Report.**

3. Create folders for each project and save both files there.