1. Provision a **Linux Virtual Machine** (Take note of which one it was!) — **Do not use labuser/Cyberlab123! for credentials (or any other easy password). Your VM will most certainly get breached by a bad actor if it's on long enough. This has already happened once.**
2. Create an Agent Group if one doesn't already exist (Settings -> Sensors -> Nessus Agents -> Agent Groups -> +Add Agent Group (name it what you want, but don't use spaces)
3. Create another scan: Triggered: Basic Agent Scan (take note of the name)
    a. Select the group you created in Step 2.
    b. Take note of the filename you choose for the trigger (For Example: dishsoap.lol)
4. Log into the **Linux Virtual Machine** with the new username and password.
    a. You may have to delete your known hosts file on mac: /Users/nnamdimadakor/.ssh/known_hosts
5. Login to the Tenable Portal https://cloud.tenable.com/
6. Start Provisioning a Tenable Agent (settings -> Sensors -> Nessus Agents -> +Add Nessus Agent)
7. Copy the bash command within the browser. It looks like this:
    a. curl -H 'X-Key: xxx'
    'https://sensor.cloud.tenable.com/install/agent?name=agent-name&groups=agent-group' | bash
        i. In notepad, EDIT the line so it fits what you want to do
        ii. Copy the line
8. In your Linux Virtual Machine (still connected by SSH), enter an administrative command line by running:
    a. sudo -i
    b. Next, paste/run the edited command from above. It will look like this as it installs:

```
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Agent Core Components...
Created symlink /etc/systemd/system/nessusagent.service → /lib/systemd/s
Created symlink /etc/systemd/system/multi-user.target.wants/nessusagent
 - First, start Nessus Agent by typing /bin/systemctl start nessusagent
 - To link this agent, use the '/opt/nessus_agent/sbin/nessuscli agent'
   Type '/opt/nessus_agent/sbin/nessuscli agent help' for more info.
Applying auto-configuration.
Starting Nessus Agent.
Waiting for Nessus Agent to start and link...
....................
```

9. It should finish installing and look like this (see below). If there is an error, re-check all the steps to try to find out what's wrong. Ask in the community

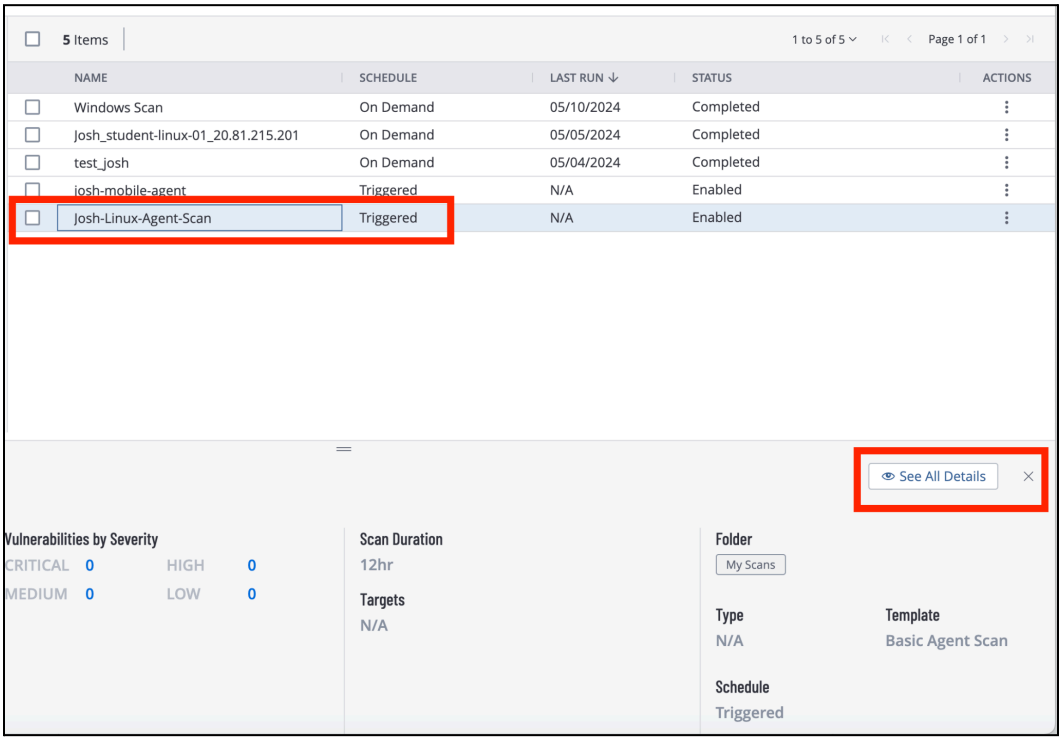
```
Waiting for Nessus Agent to start and link...
.........................
Auto-configuration complete.
The Nessus Agent is now linked to sensor.cloud.tenable.com:443
root@student-linux-01:~#
```

10. To trigger the scan, create the trigger file (dishsoap.lol) in the trigger directory (may need to use sudo first):
    `touch /opt/nessus_agent/var/nessus/triggers/dishsoap.lol`

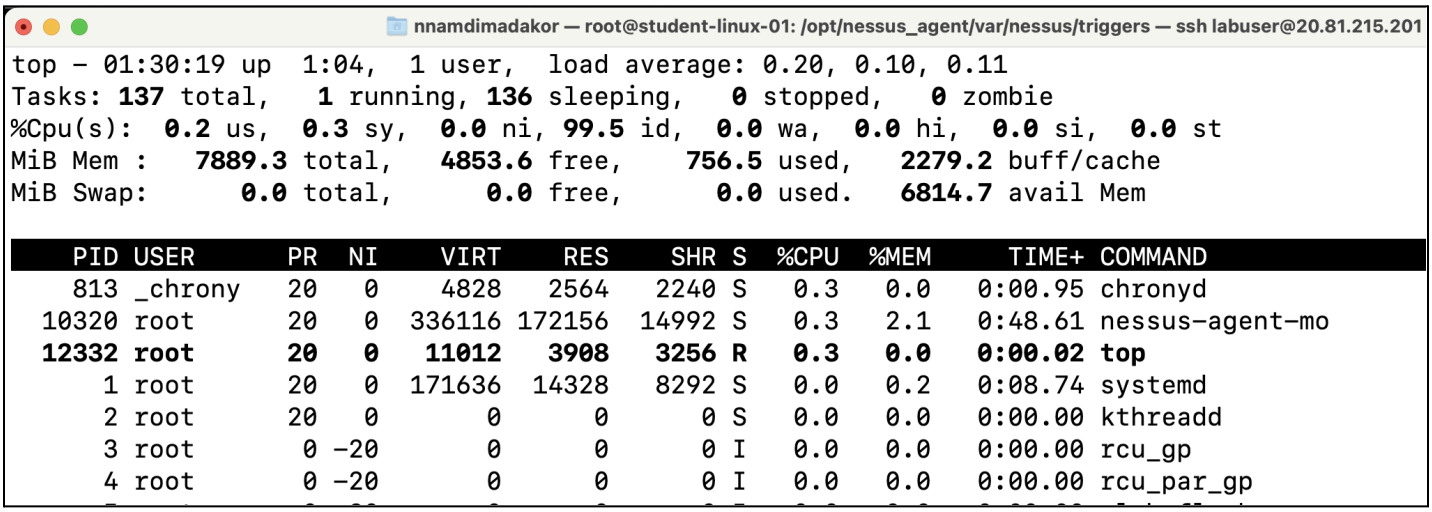
You can also view your agent trigger information in the agent trigger directory:

Operating System	Location
Windows	`C:\ProgramData\Tenable\Nessus Agent\nessus\triggers`
macOS	`/Library/NessusAgent/run/var/nessus/triggers`
Linux	`/opt/nessus_agent/var/nessus/triggers`

11. Change directories and look inside until it goes away:
    ```
    cd /opt/nessus_agent/var/nessus/triggers
    ls -lasht
    ```
12. OPTIONAL: You can try to restart the nessus service once to get it to trigger/read the file:
    ```
    sudo systemctl restart nessusagent.service
    ```
13. OPTIONAL: You can view the status of the service:
    ```
    sudo systemctl status nessusagent.service
    ```
14. Then keep checking for the file to disappear
    ```
    cd /opt/nessus_agent/var/nessus/triggers
    ls -lasht
    ```
15. Watch until the file disappears. This signifies the local agent scan has begun. (if it takes time, skip to the next step to see if the agent is showing up
16. Go back to the Tenable Portal (https://cloud.tenable.com/) and observe your nessus agent should be showing up in: (settings -> Sensors -> Nessus Agents)
    a. Ensure YOURS is in there; there could be some in there already from other people. See “LINKED ON” date and name to find yours. If it’s not there, you may have to wait a bit longer. If it still doesn’t show up after like 30 minutes, ask in the community 🙂
17. Once your agent shows up, it will still take time for the vulnerabilities to be populated
18. To check the scan/discovered vulnerabilities, navigate to “Scans” and then select the triggered scan you created for the linux virtual machine. Then click “See all details”



19. Keep looking at/reloading this until the vulnerabilities populate
    a. You can monitor the nessus scan process on the linux machine by typing:
       top



20. When the local agent scan finishes, export the results if you want
21. Delete your scan (if you want)
22. Delete your agent group
23. Unlink your agents
24. Delete the Virtual Machine

Troubleshooting steps:

- Re-image vm
- Delete the scan and re-create it
- Create a new scan group (you can delete the old one if noone is using it)
- Hard delete asset from Tenable