Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Lab 7 – Linux Hacking

NAME – Student ID	COURSE CODE	WEIGHT
Ishan Aakash Patel - 14615238	CYT130	5%

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Become familiar with *OpenVAS and other vulnerability scanners*
- Become familiar with vulnerability scanning reports and how to interpret them

Lab Materials

- Tools and utilities:
  - Product: MSFConsole
    - Installed on Kali: yes
    - Manufacturer: Rapid 7

Lab Materials

- Tools and utilities:
  - Product: OpenVAS
    - Installed on Kali: yes, but needs setup
    - Manufacturer: Greenbone
  - Product: Nikto
    - Installed on Kali: yes
    - Creator: Chris Sullo
    - Web site: https://cirt.net/Nikto2
  - Kali Linux VM

Lab Instructions

- Complete this lab;
- Enter your name and student ID above (Example: Ignatius Michael - Imichael);
- Answer questions and add screenshots into the corresponding textboxes;
- Save the file on your computer for future reference;
- Save the file again as a "`.pdf`" file;
- Submit the PDF file for grading.

Part 1: Setting up OpenVAS (to be done at home before the lab)

No screenshots necessary.

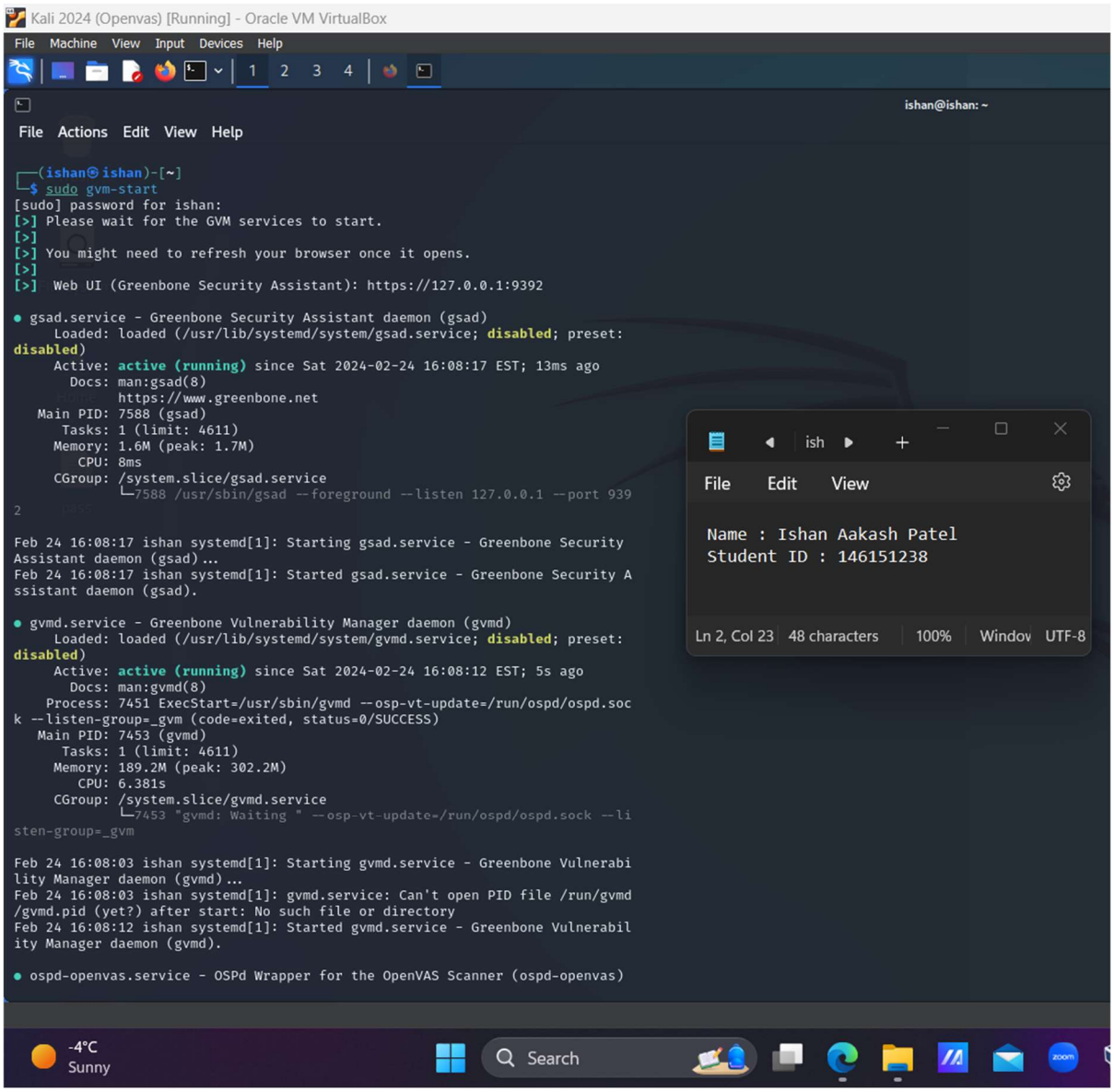
Part 2: Connecting your Kali machine to the security lab network:

Prof, I have performed the scans on my metasploitable 2 which has the IP – 10.0.2.4

I am not able to configure 172.16.0.0/24 inside the nat network so I am using 10.0.2.0/24 natnetwork.

Part 3: Performing vulnerability scan using OpenVAS

1. Run **sudo gvm-start** command, and include a screenshot of the command (include the command itslef, not only the output of the command)



Kali 2024 (Openvas) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

ishan@ishan: ~

File Actions Edit View Help

```
ssistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset:
disabled)
     Active: active (running) since Sat 2024-02-24 16:08:12 EST; 5s ago
       Docs: man:gvmd(8)
    Process: 7451 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.soc
k --listen-group=_gvm (code=exited, status=0/SUCCESS)
   Main PID: 7453 (gvmd)
      Tasks: 1 (limit: 4611)
     Memory: 189.2M (peak: 302.2M)
        CPU: 6.381s
     CGroup: /system.slice/gvmd.service
             └─7453 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --li
sten-group=_gvm

Feb 24 16:08:03 ishan systemd[1]: Starting gvmd.service - Greenbone Vulnerabi
lity Manager daemon (gvmd)...
Feb 24 16:08:03 ishan systemd[1]: gvmd.service: Can't open PID file /run/gvmd
/gvmd.pid (yet?) after start: No such file or directory
Feb 24 16:08:12 ishan systemd[1]: Started gvmd.service - Greenbone Vulnerabil
ity Manager daemon (gvmd).

● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
     Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; disabled;
preset: disabled)
     Active: active (running) since Sat 2024-02-24 16:08:02 EST; 14s ago
       Docs: man:ospd-openvas(8)
             man:openvas(8)
    Process: 7384 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-open
vas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCE
SS)
   Main PID: 7422 (ospd-openvas)
      Tasks: 5 (limit: 4611)
     Memory: 120.6M (peak: 140.6M)
        CPU: 3.541s
     CGroup: /system.slice/ospd-openvas.service
             ├─7422 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/
ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
             └─7426 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/
ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf

Feb 24 16:08:00 ishan systemd[1]: Starting ospd-openvas.service - OSPd Wrappe
r for the OpenVAS Scanner (ospd-openvas)...
Feb 24 16:08:02 ishan systemd[1]: Started ospd-openvas.service - OSPd Wrapper
 for the OpenVAS Scanner (ospd-openvas).

[>] Opening Web UI (https://127.0.0.1:9392) in: 5 ... 4 ... 3 ... 2 ... 1 ...

┌──(ishan㉿ishan)-[~]
└─$
```

ish

File Edit View

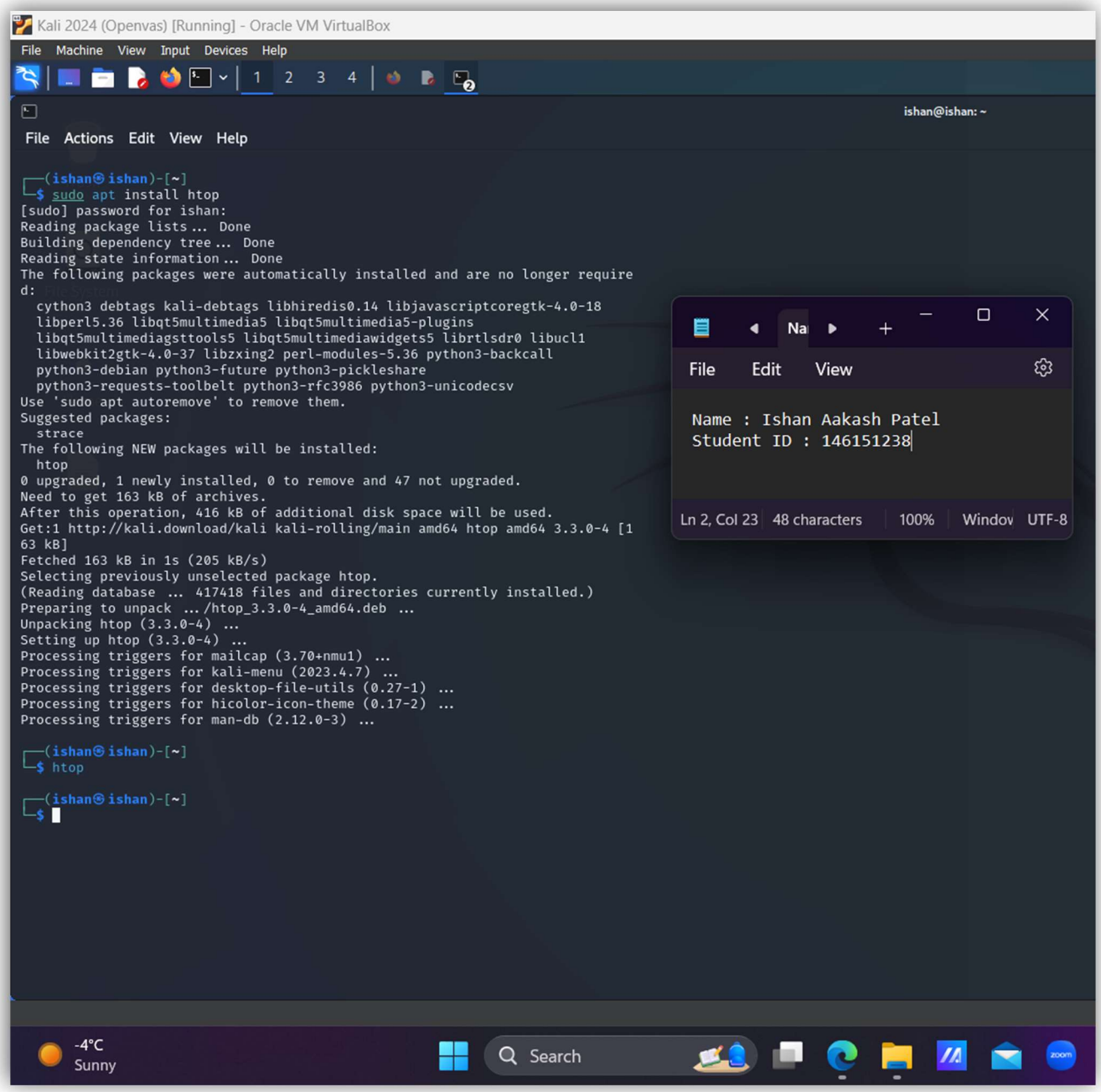
```
Name : Ishan Aakash Patel
Student ID : 146151238
```

Ln 2, Col 23 | 48 characters | 100% | Windov | UTF-8

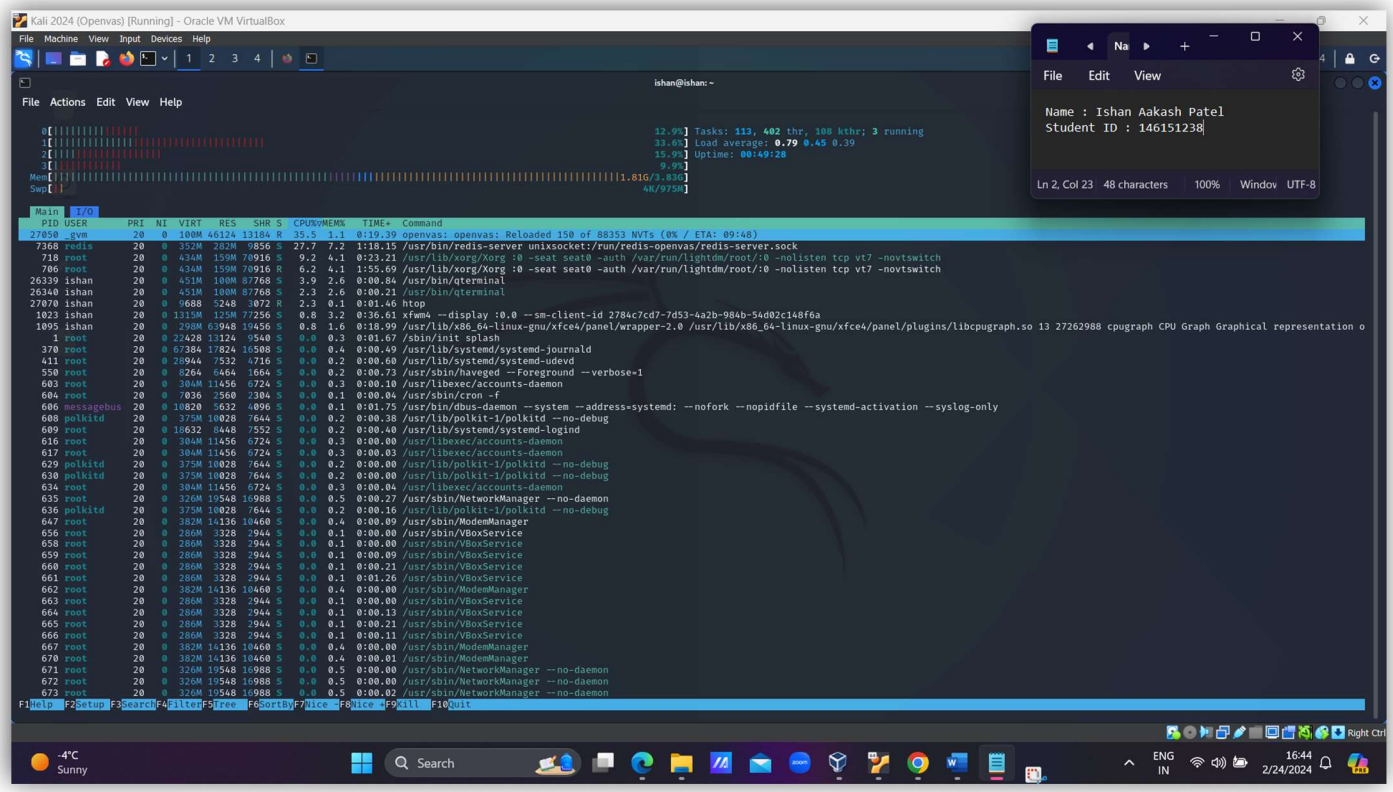
-4°C Sunny

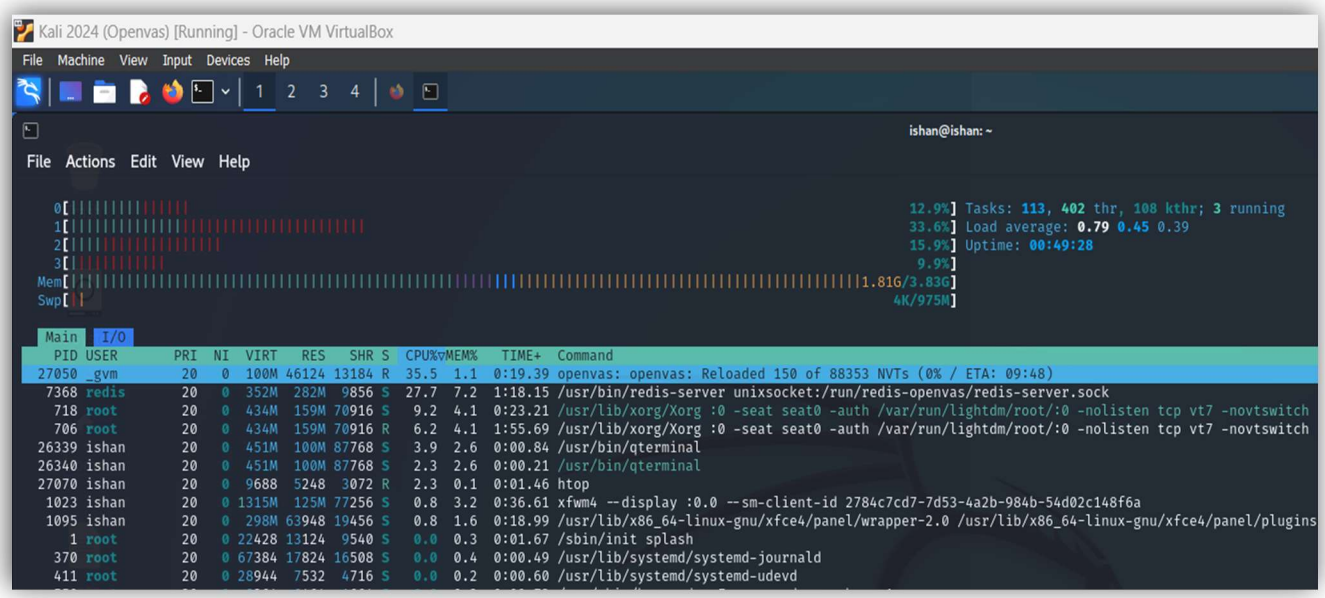
Search

2. Open another terminal window and run the command **htop**. If it is not installed, install it using **sudo apt install htop**.

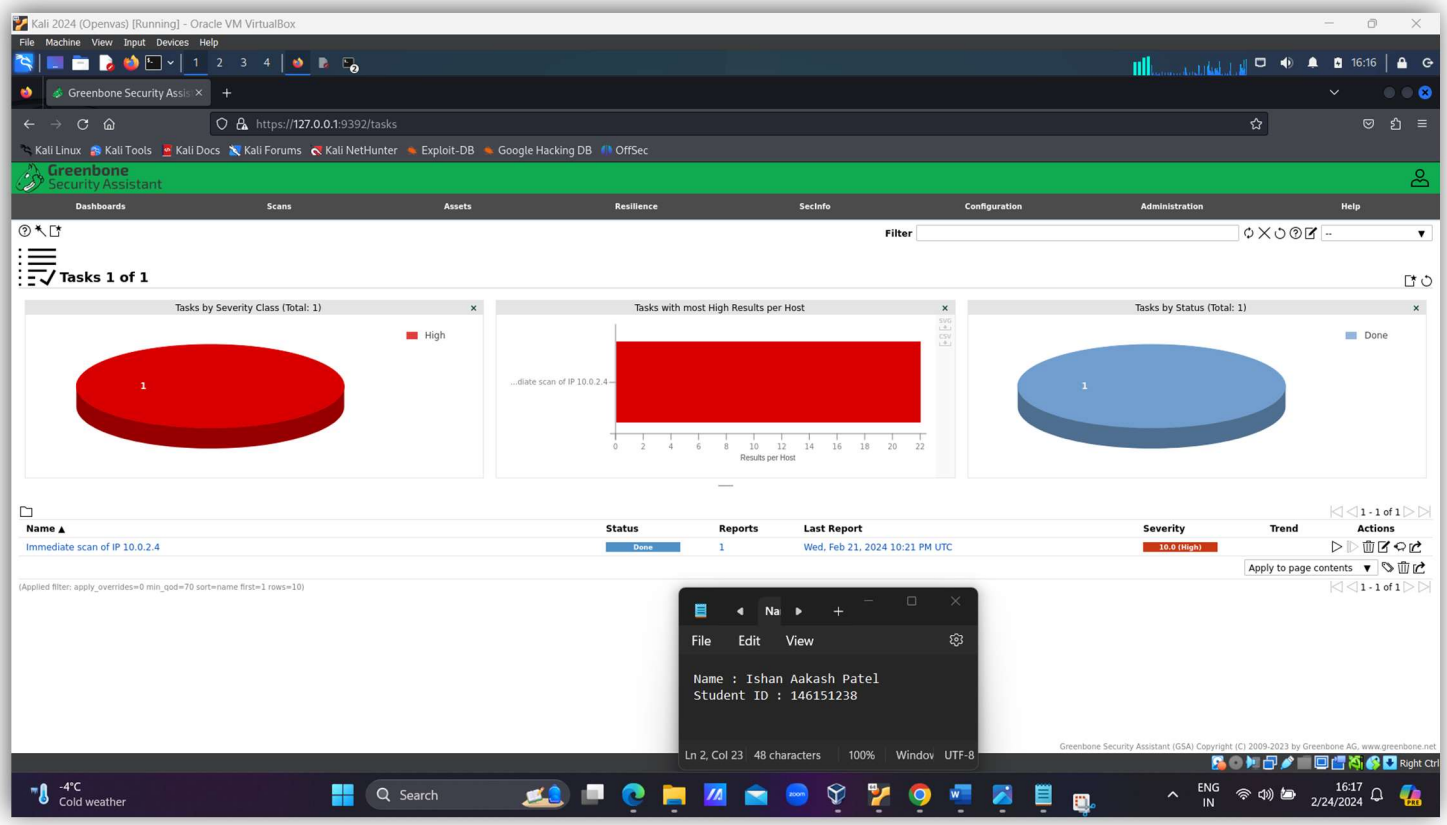


3. Include a screenshot from the result of htop here.

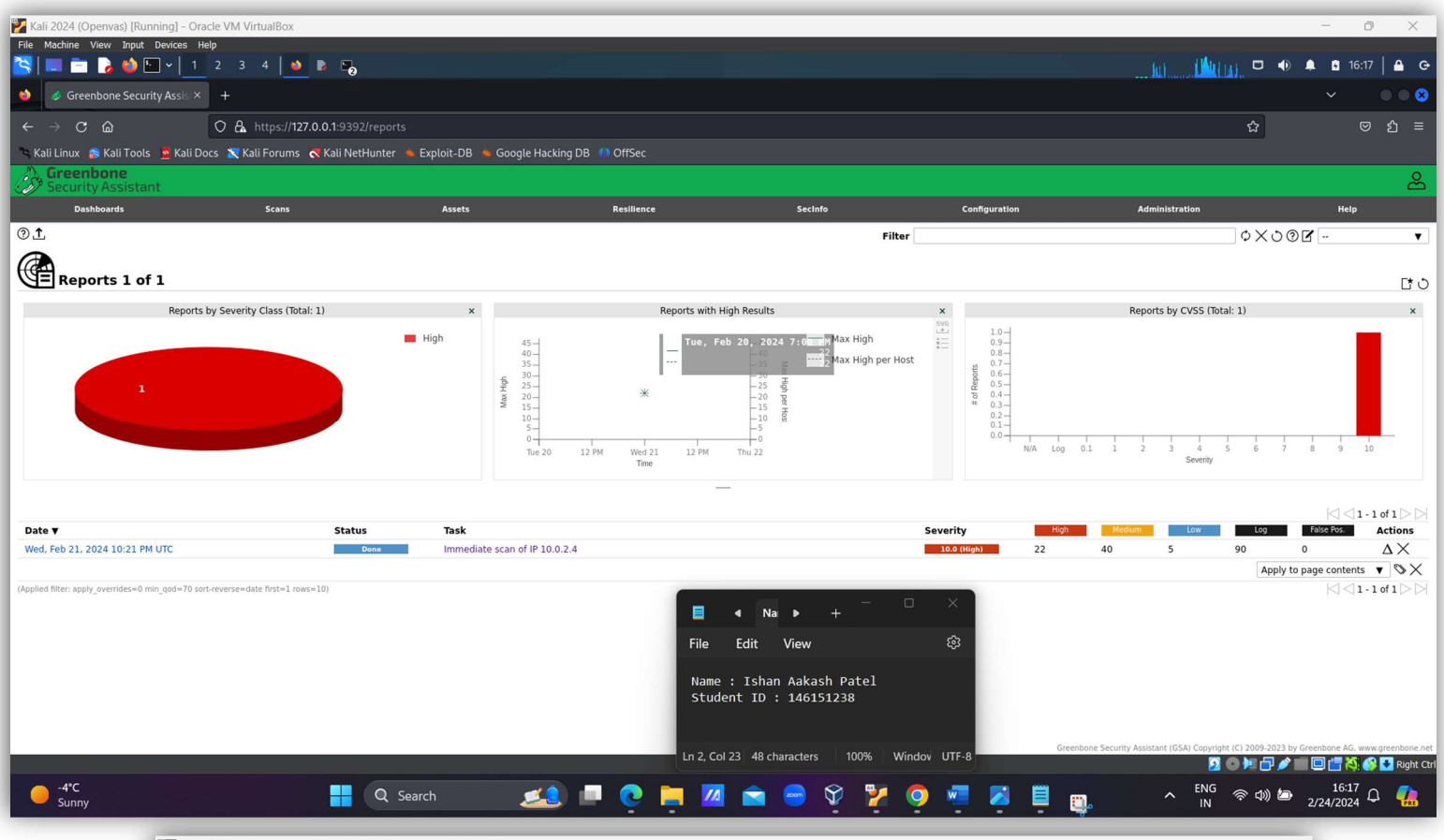


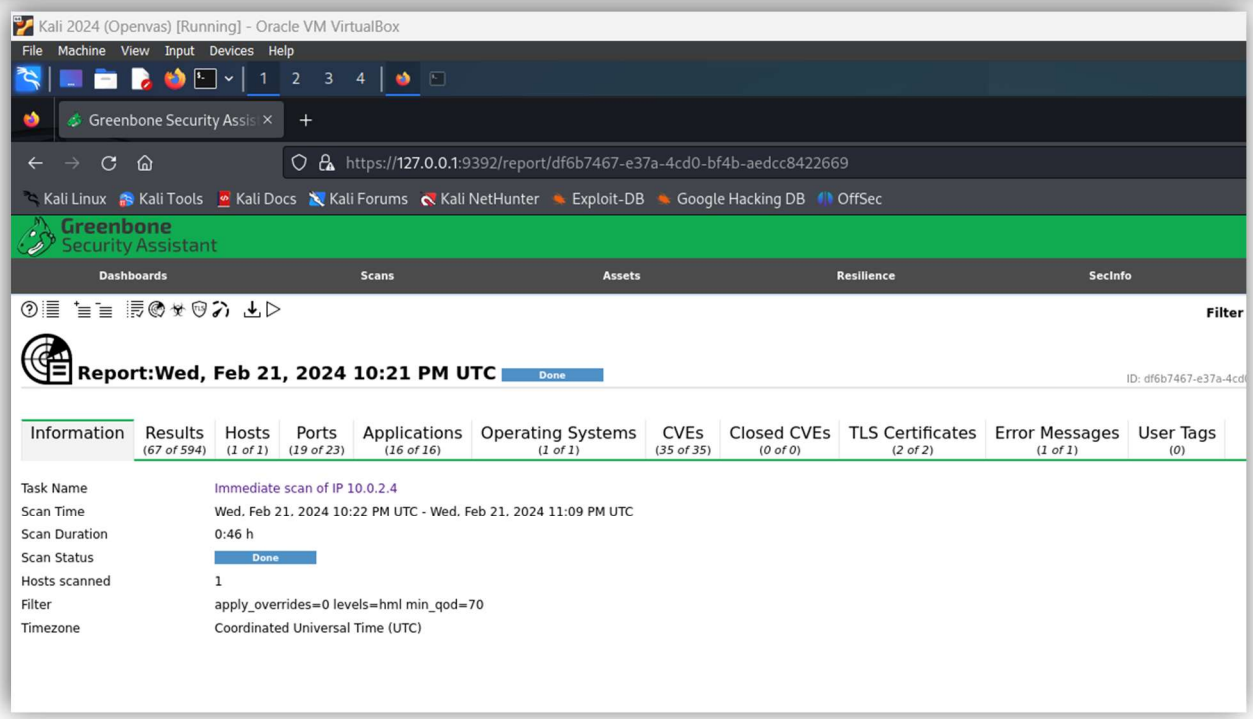


4. After the scan of 172.16.11.5 is done, include a screenshot showing the “Tasks” page with the scan marked as “Done”.

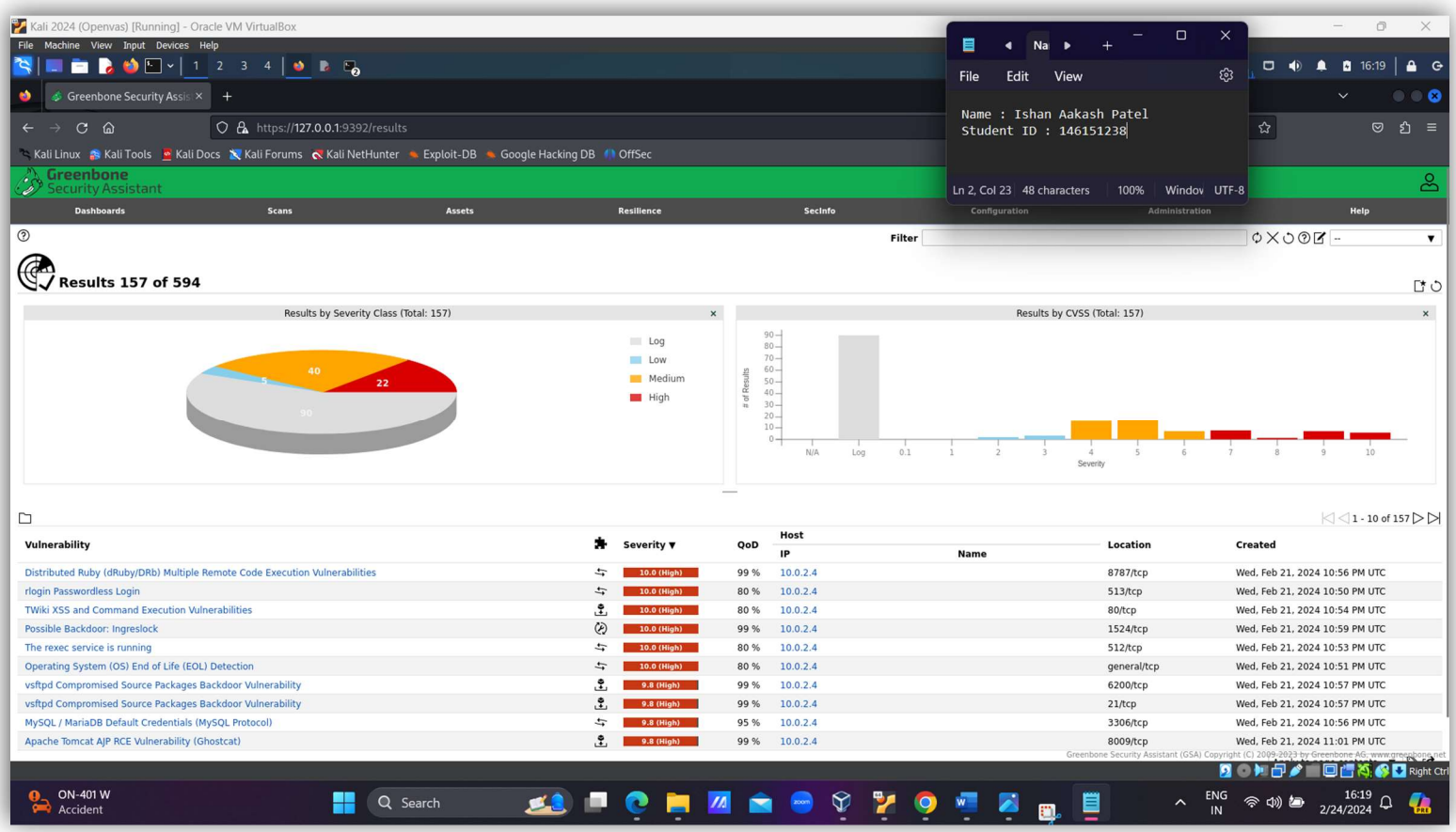


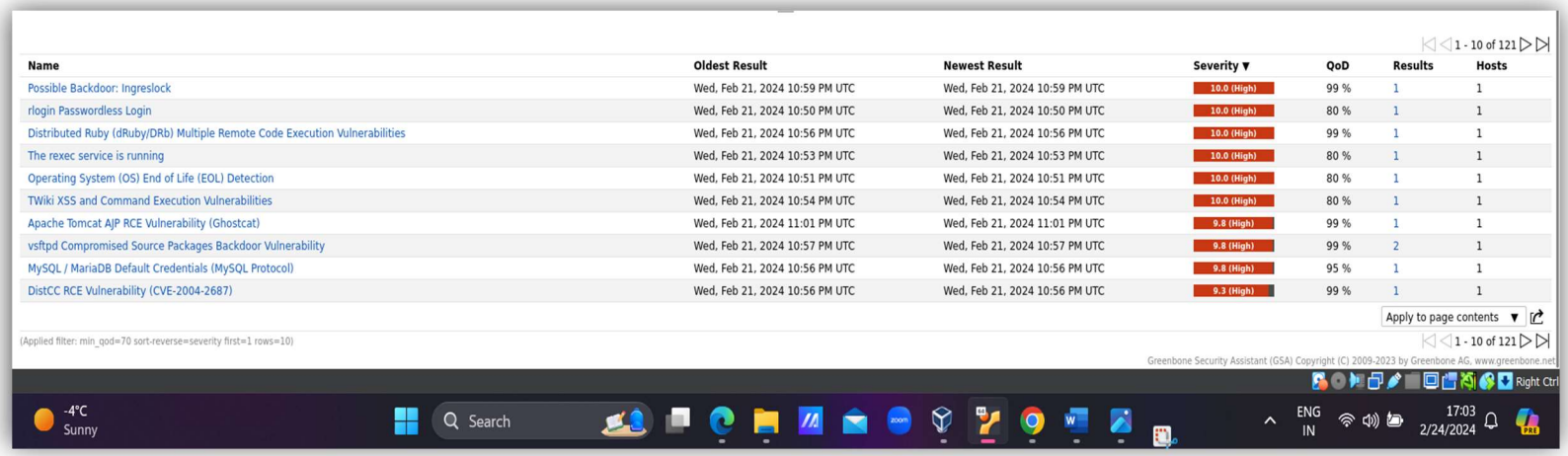
5. Include a screenshot showing the “Scans” > “Reports” main page.





6. Include a screenshot showing the results tab inside the scan report, and shoing the top vulnerabilities.



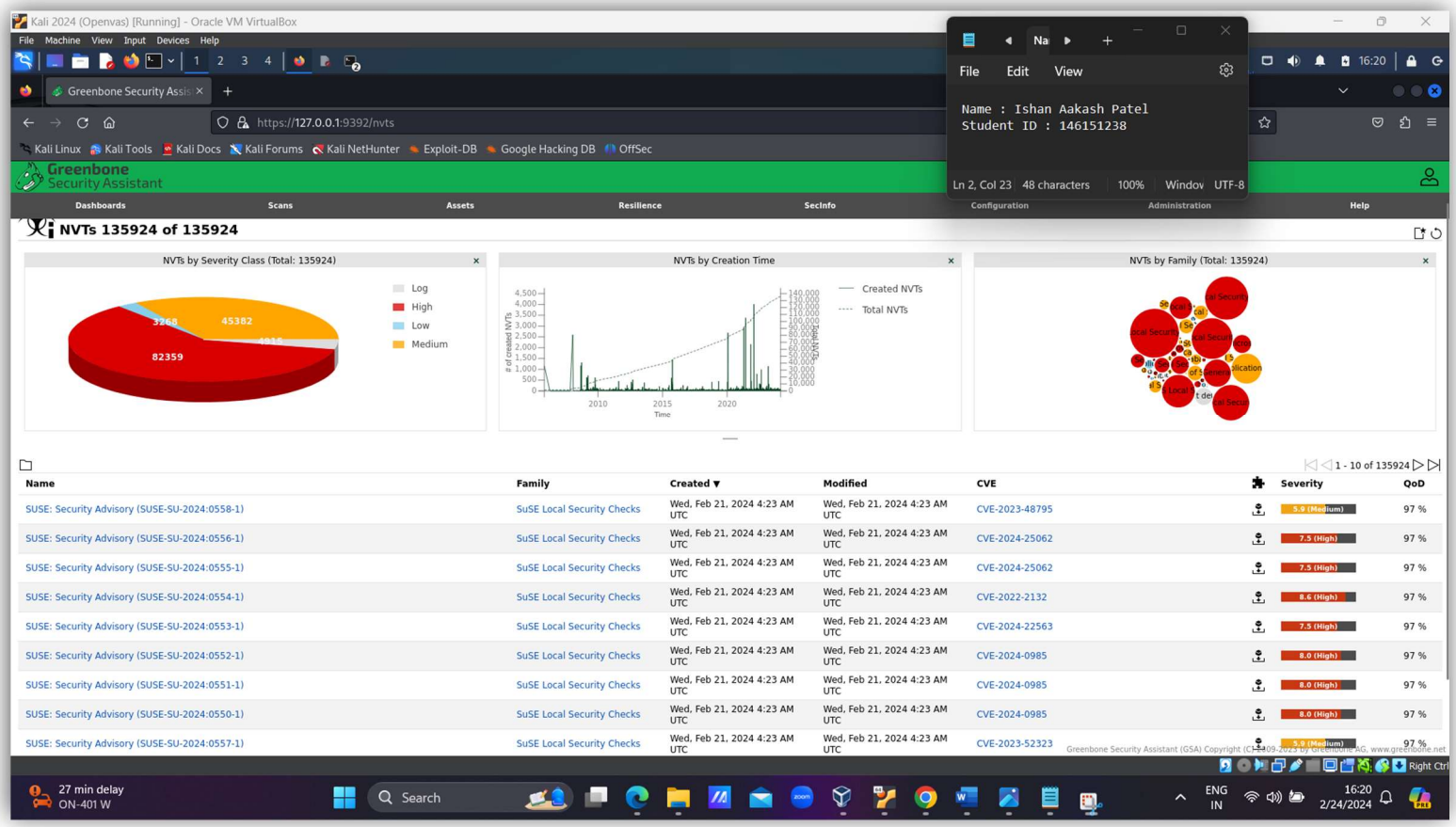


7. What was the vulnerability with the highest severity? Write half a page describing this vulnerability in your own words. Look for information on NVD, and CWE.

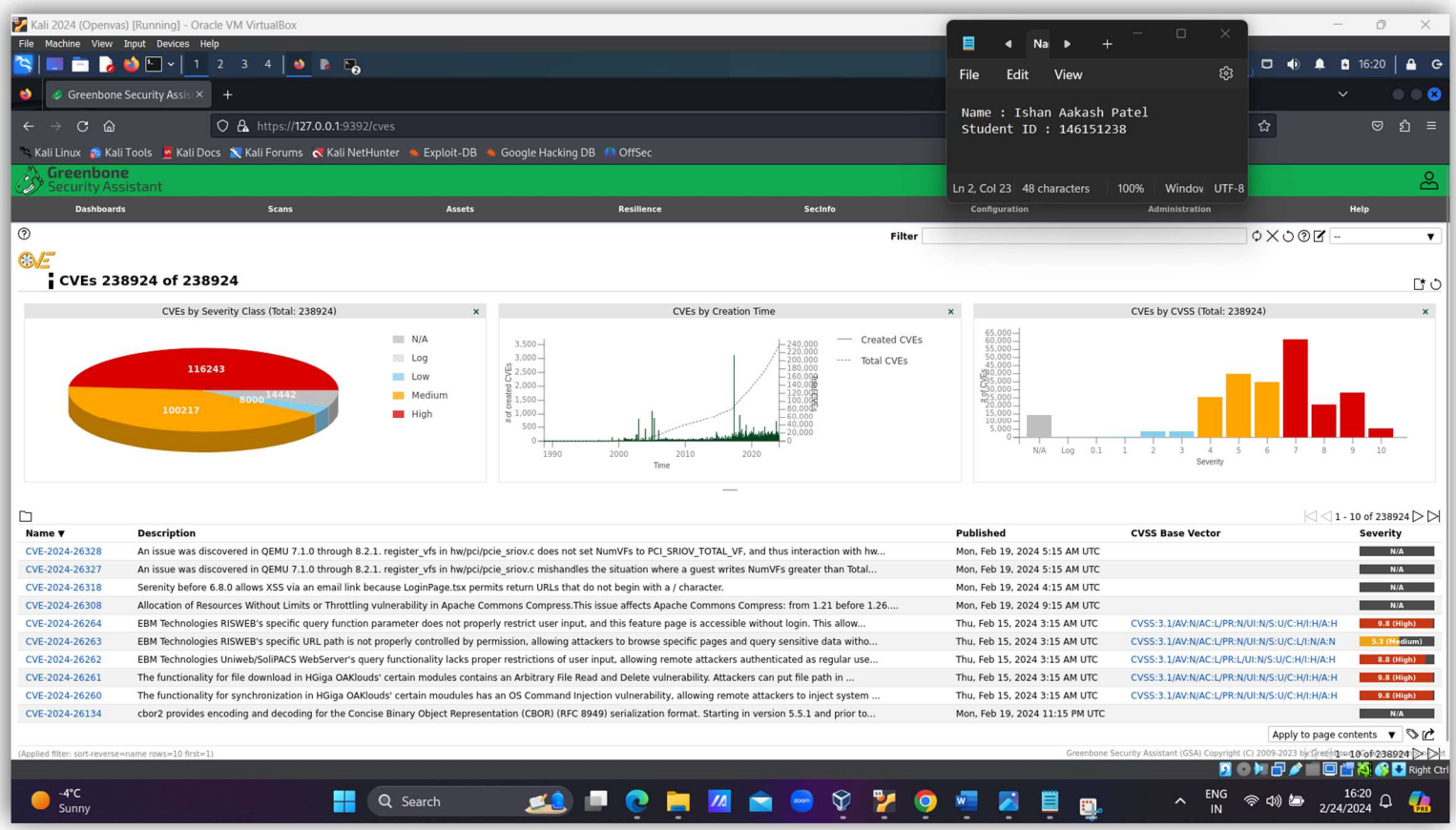
<u>rlogin passwordless login – (CVE – 2022 – 44589)</u>

The term "rlogin" refers to the remote login protocol used on Unix and Unix-like systems that allows users to log into a different system and execute commands as if they were directly logged in. Passwordless login, on the other hand, frequently involves implementing authentication measures that enable users to access a system without providing a password. However, enabling passwordless login, particularly using the rlogin protocol, might cause security weaknesses by exposing systems to unauthorized access.

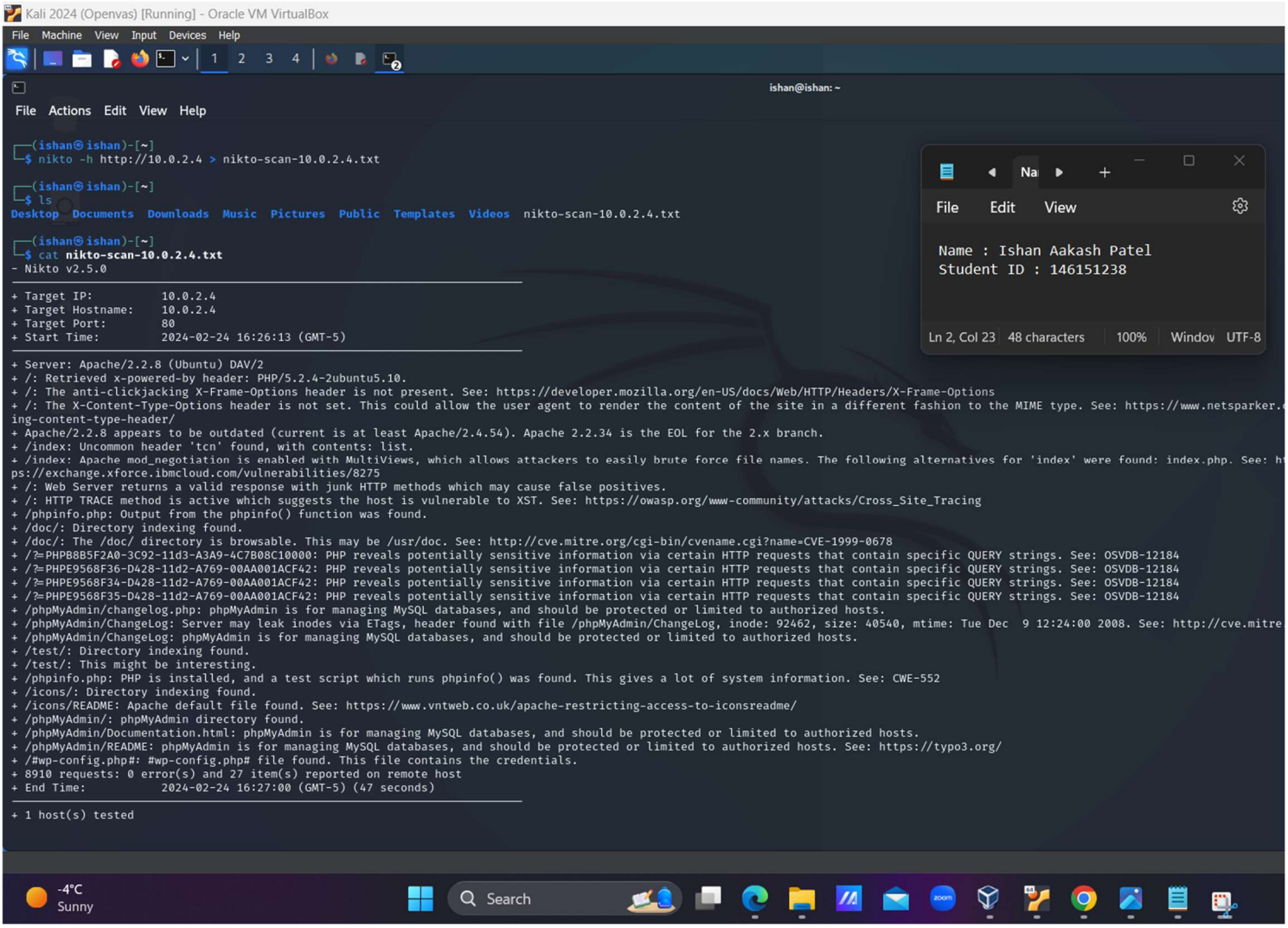
If the rlogin service supports passwordless login, an attacker who gets access to the client system may be able to connect to the remote machine without entering a password. Relying only on passwordless logins may compromise the overall security posture. Without adequate authentication, an attacker might use this to carry out harmful operations on the remote machine.



8. Include a screenshots of the CVEs tab from your scan report page.



9. Include a screenshot showing the results of “nikto” scan on the same target.



10. Identify the results that were found in nikto scan that were not detected in the openvas scan.

    1) Outdated Apache server
    2) XST – HTTP trace method is active which is vulnerable to XST – Cross site tracing
    3) PHP – Path disclosure
    4) Open Files

Submit your lab

- **Doublecheck all your answers.**
- **Save the file on your computer for future reference.**
- **Save the file again as a "`.pdf`" file.**
- **Submit the PDF file for grading.**