

## 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.

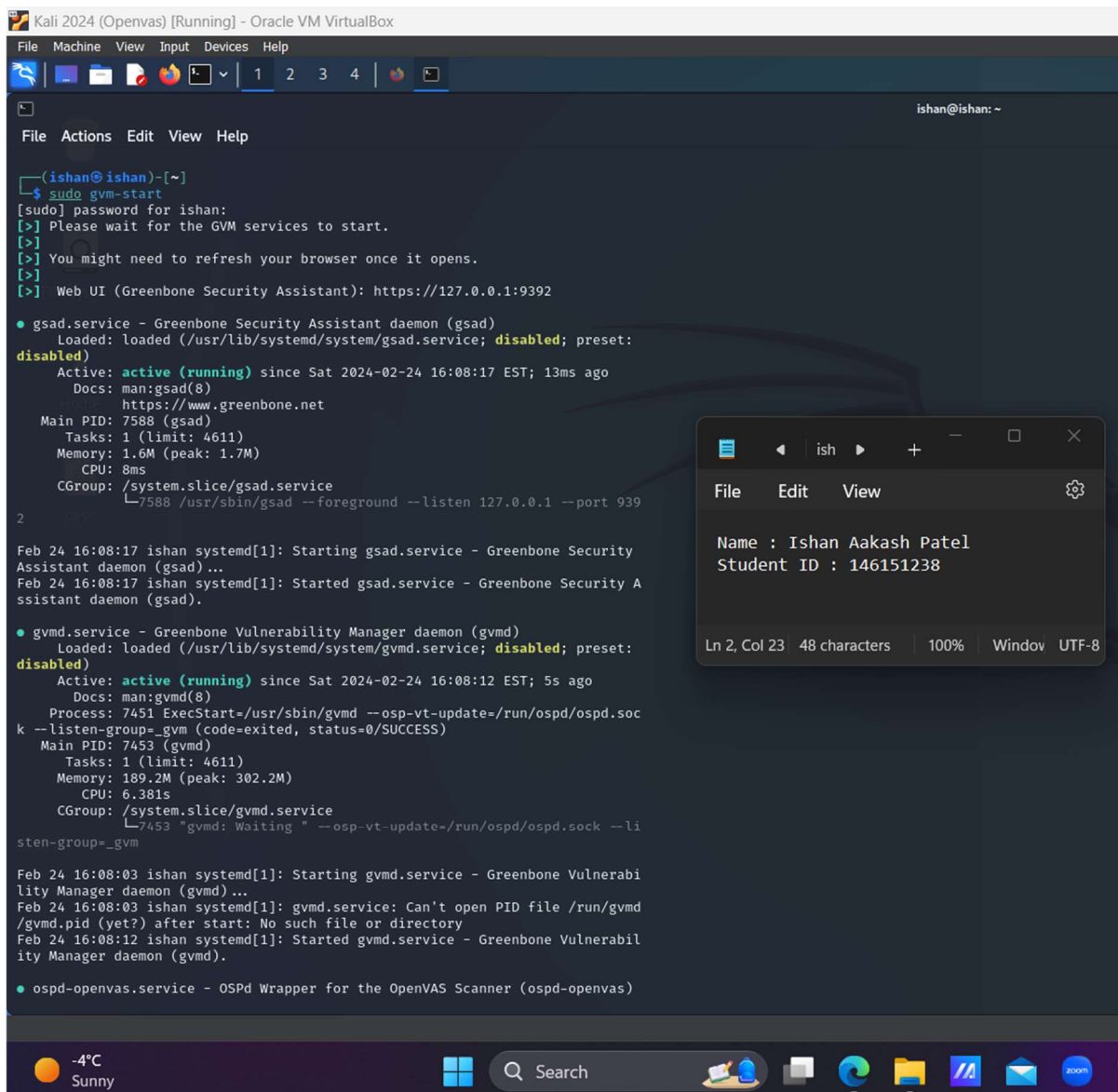
## Part 2: Connecting your Kali machine to the security lab network:

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 itself, not only the output of the command)



```
Kali 2024 (Openvas) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
(ishan@ishan)-[~]
$ sudo gvm-start
[sudo] password for ishan:
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

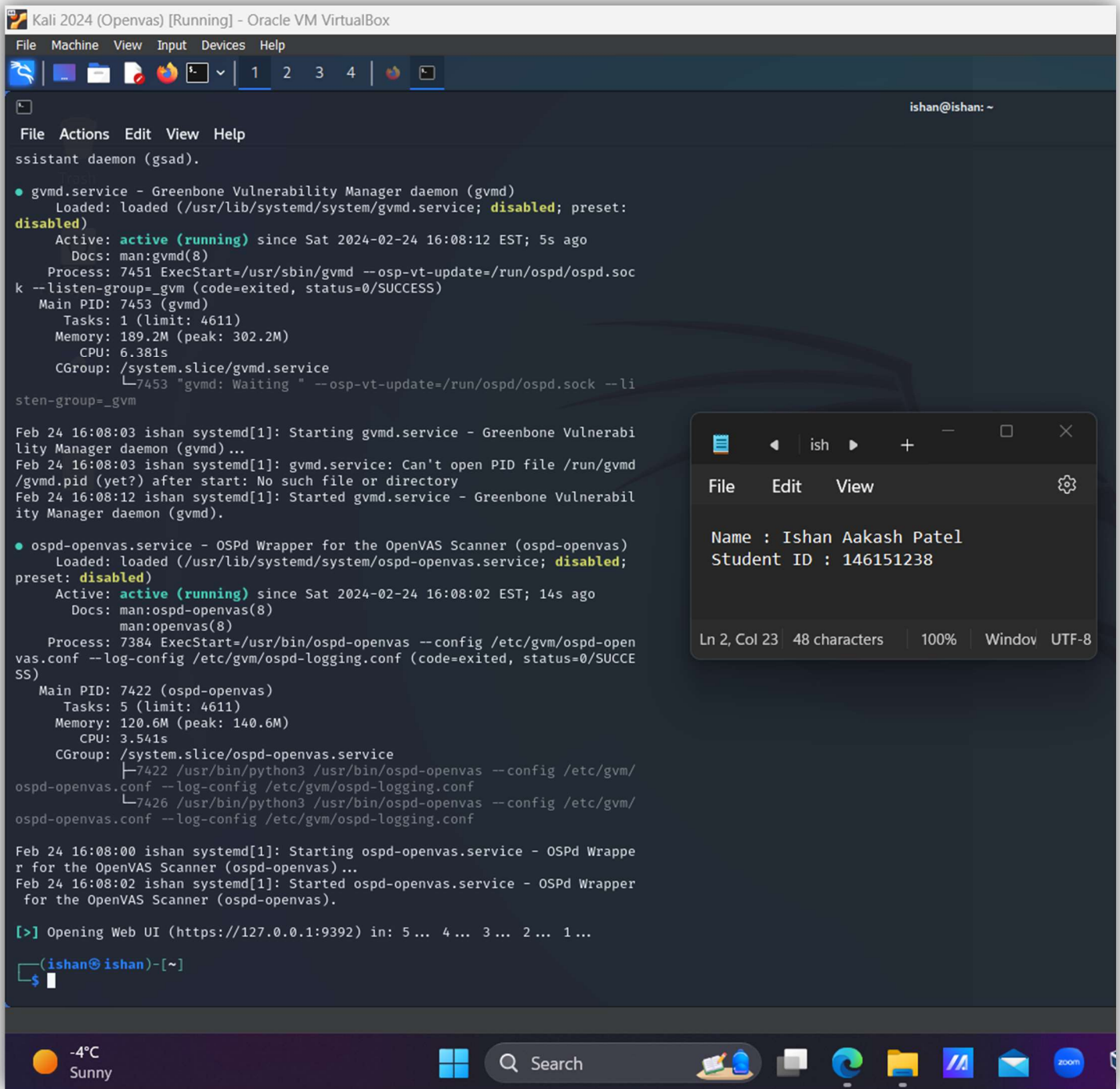
• gsad.service - Greenbone Security Assistant daemon (gsad)
  Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
  Active: active (running) since Sat 2024-02-24 16:08:17 EST; 13ms ago
  Docs: man:gsad(8)
        https://www.greenbone.net
  Main PID: 7588 (gsad)
  Tasks: 1 (limit: 4611)
  Memory: 1.6M (peak: 1.7M)
  CPU: 8ms
  CGroup: /system.slice/gsad.service
          └─7588 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Feb 24 16:08:17 ishan systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Feb 24 16:08:17 ishan systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

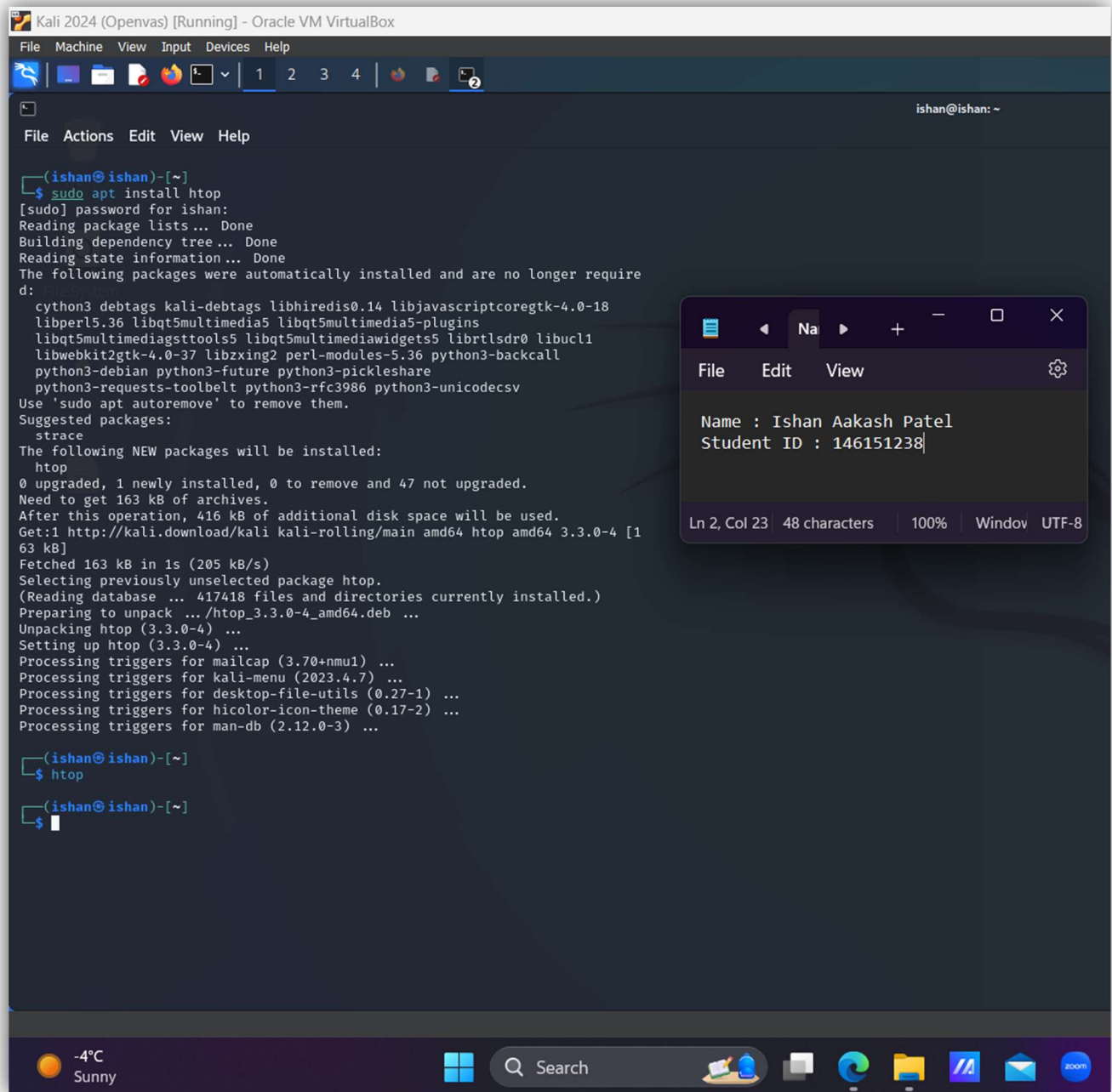
• gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
  Active: active (running) since Sat 2024-02-24 16:08:12 EST; 5s ago
  Docs: man:gvmd(8)
  Process: 7451 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --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 --listen-group=_gvm

Feb 24 16:08:03 ishan systemd[1]: Starting gvmd.service - Greenbone Vulnerability 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 Vulnerability Manager daemon (gvmd).

• ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
```

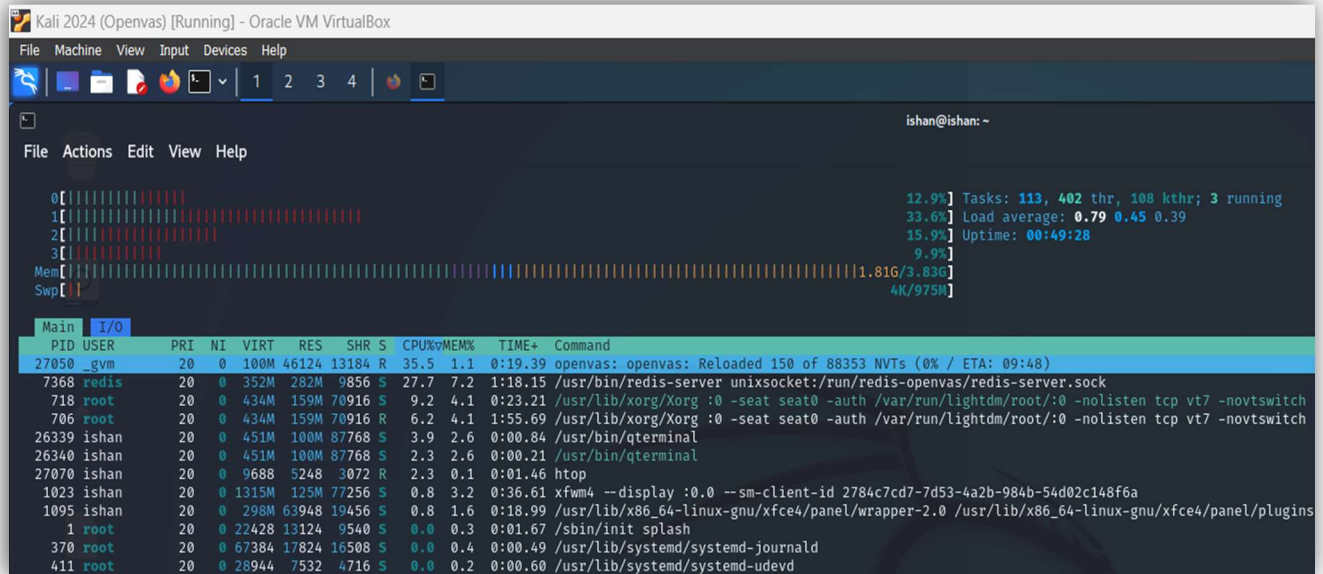
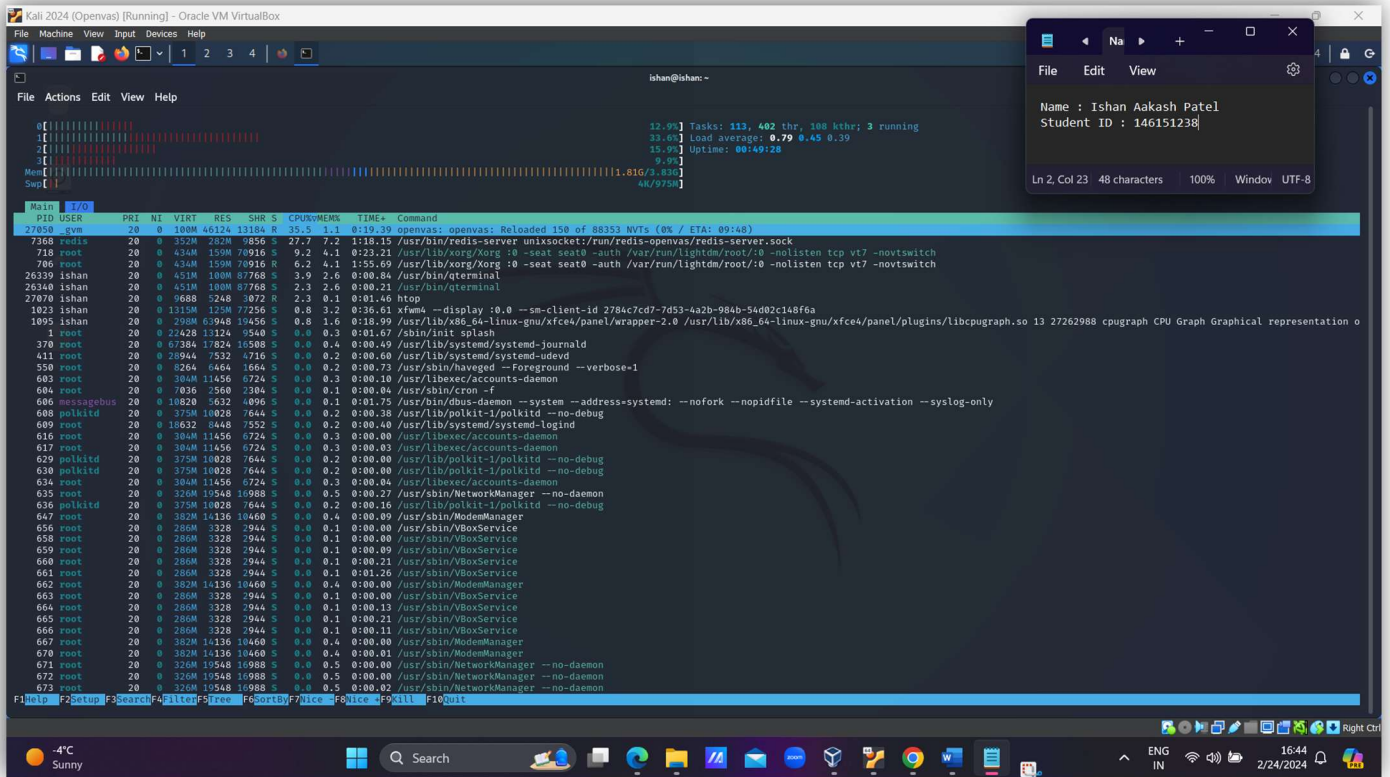


2. Open another terminal window and run the command **htop**. If it is not installed, install it using **sudo apt install htop**.

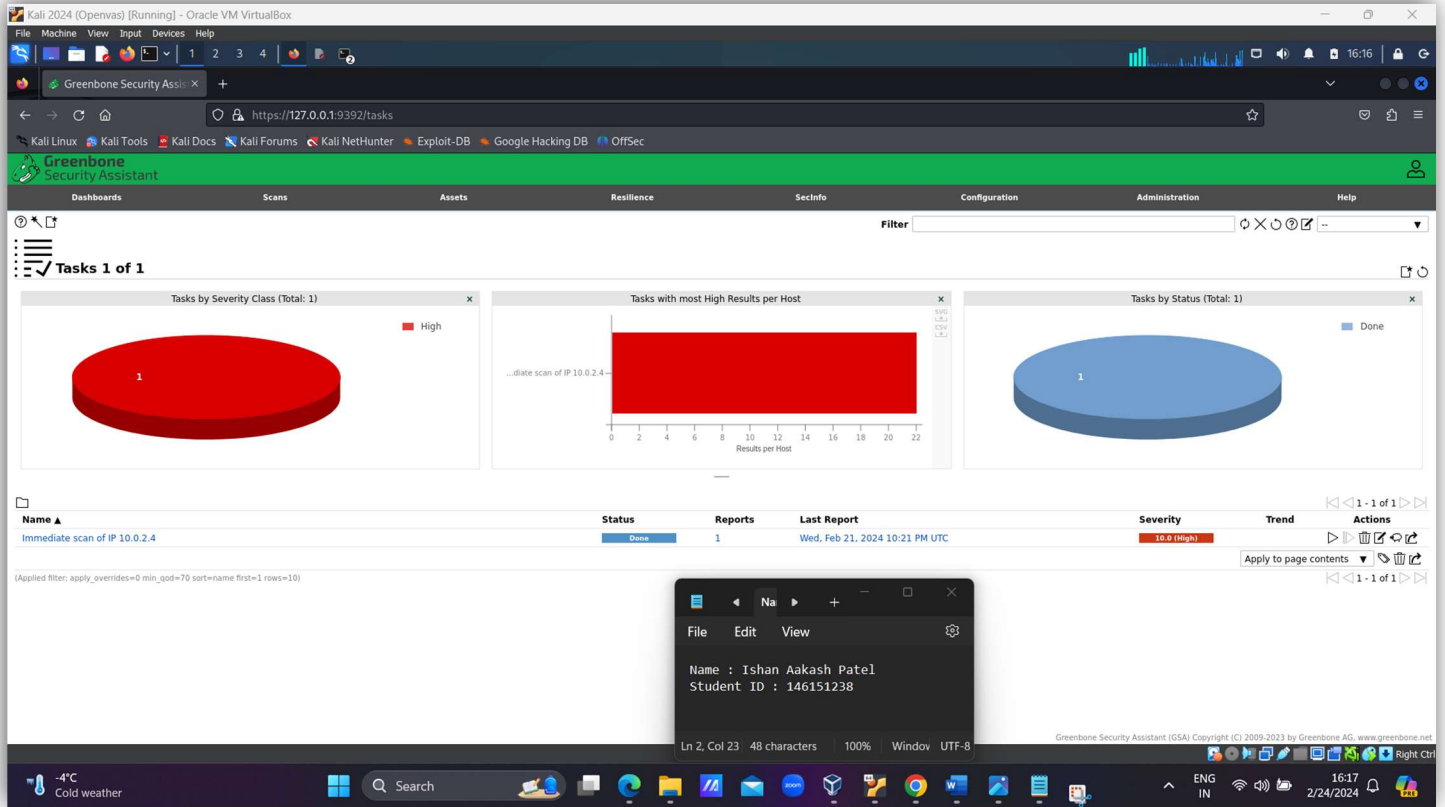




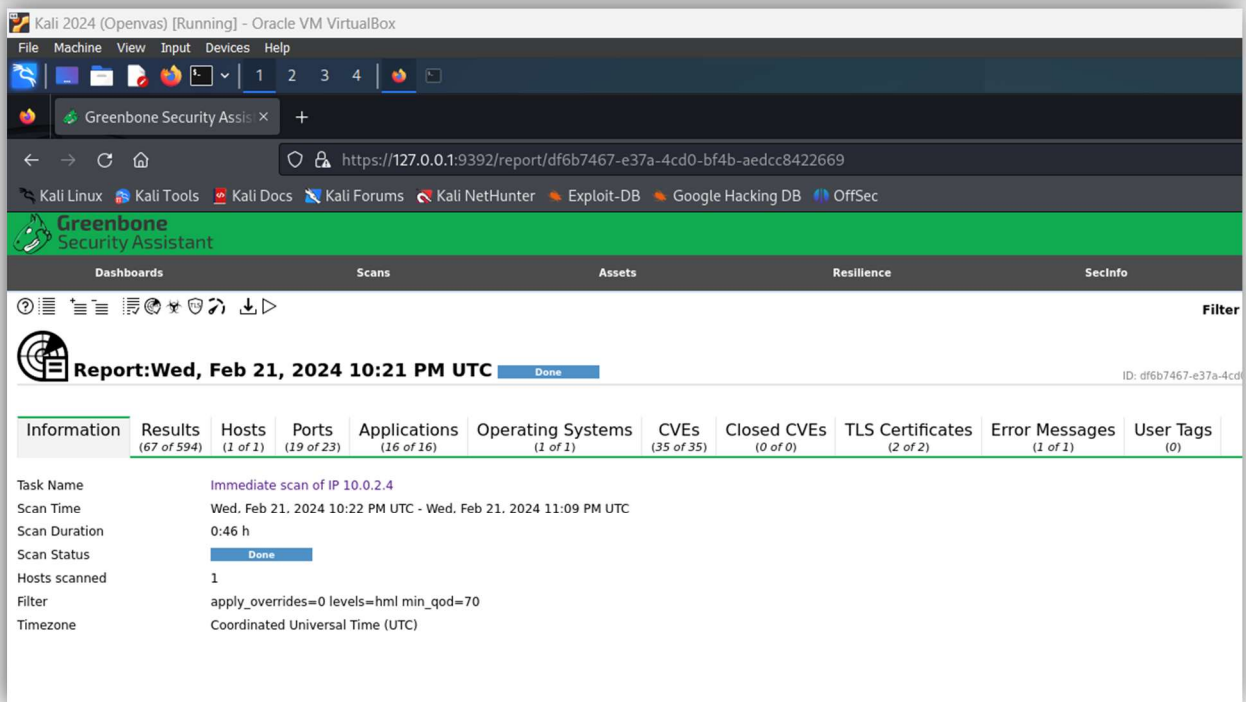
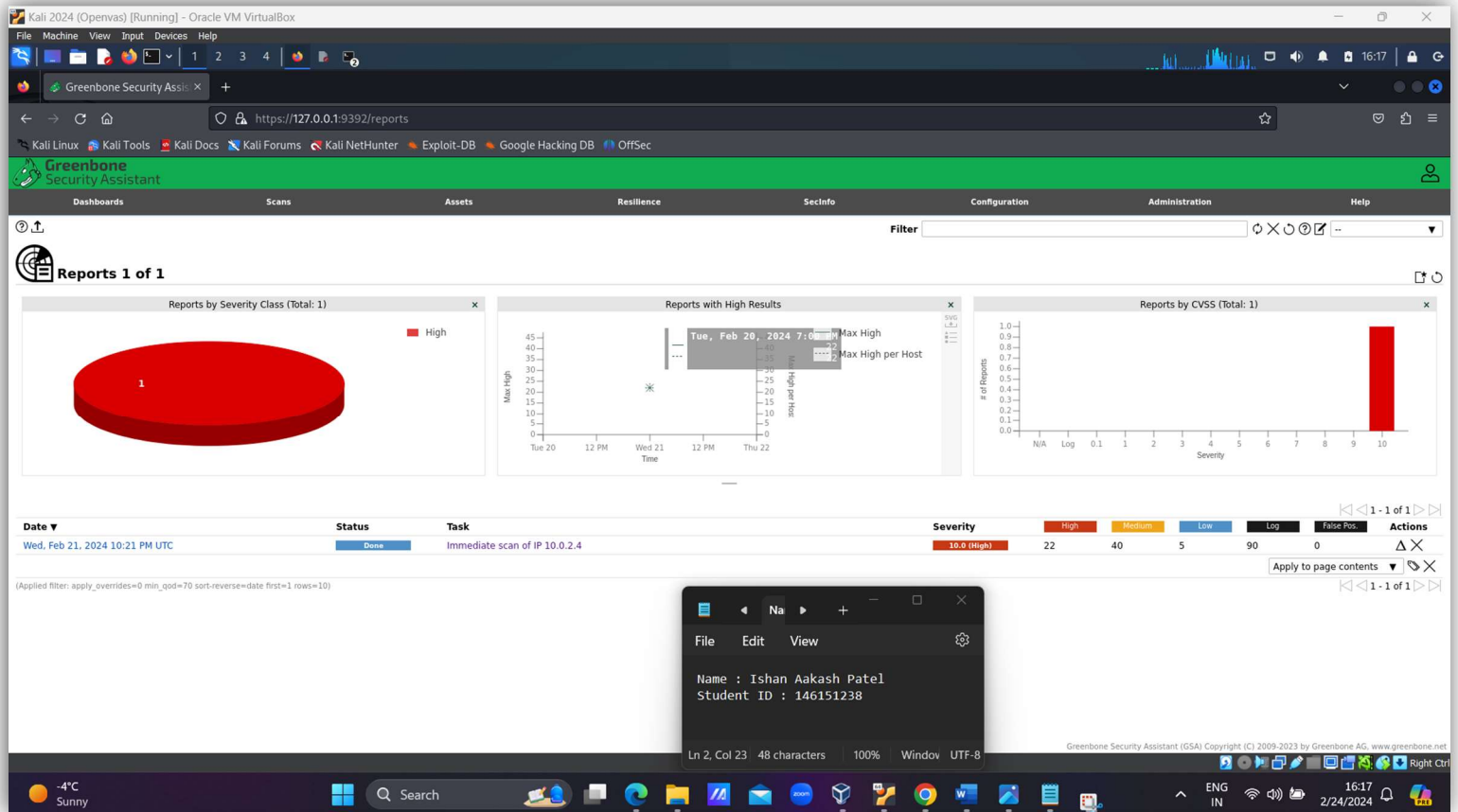
3. Include a screenshot from the result of htop here.



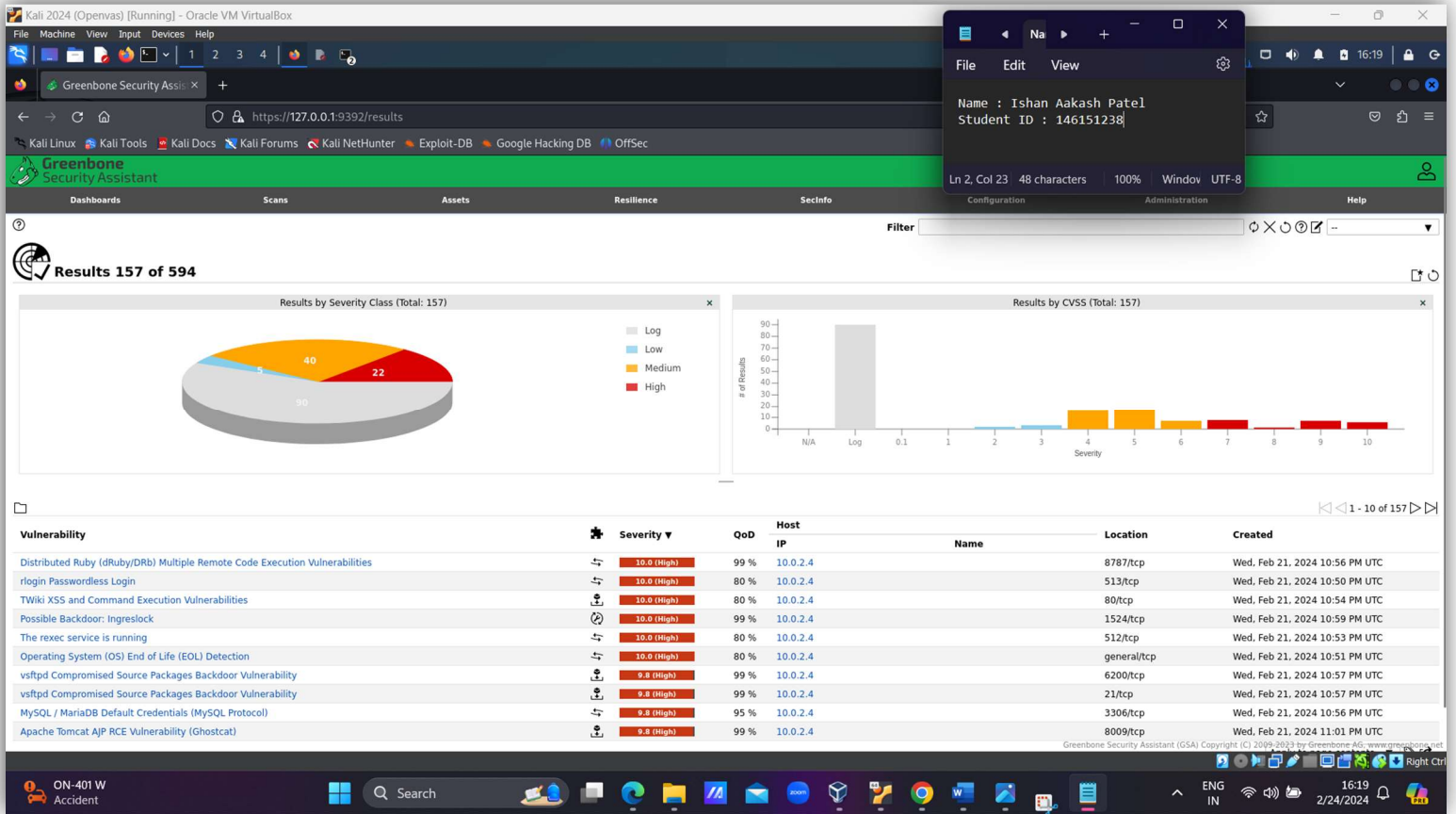
- After the scan of 172.16.11.5 is done, include a screenshot showing the “Tasks” page with the scan marked as “Done”.



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.



Name	Oldest Result	Newest Result	Severity	QoD	Results	Hosts
Possible Backdoor: Ingreslock	Wed, Feb 21, 2024 10:59 PM UTC	Wed, Feb 21, 2024 10:59 PM UTC	10.0 (High)	99 %	1	1
rlogin Passwordless Login	Wed, Feb 21, 2024 10:50 PM UTC	Wed, Feb 21, 2024 10:50 PM UTC	10.0 (High)	80 %	1	1
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	Wed, Feb 21, 2024 10:56 PM UTC	Wed, Feb 21, 2024 10:56 PM UTC	10.0 (High)	99 %	1	1
The rexec service is running	Wed, Feb 21, 2024 10:53 PM UTC	Wed, Feb 21, 2024 10:53 PM UTC	10.0 (High)	80 %	1	1
Operating System (OS) End of Life (EOL) Detection	Wed, Feb 21, 2024 10:51 PM UTC	Wed, Feb 21, 2024 10:51 PM UTC	10.0 (High)	80 %	1	1
TWiki XSS and Command Execution Vulnerabilities	Wed, Feb 21, 2024 10:54 PM UTC	Wed, Feb 21, 2024 10:54 PM UTC	10.0 (High)	80 %	1	1
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	Wed, Feb 21, 2024 11:01 PM UTC	Wed, Feb 21, 2024 11:01 PM UTC	9.8 (High)	99 %	1	1
vsftpd Compromised Source Packages Backdoor Vulnerability	Wed, Feb 21, 2024 10:57 PM UTC	Wed, Feb 21, 2024 10:57 PM UTC	9.8 (High)	99 %	2	1
MySQL / MariaDB Default Credentials (MySQL Protocol)	Wed, Feb 21, 2024 10:56 PM UTC	Wed, Feb 21, 2024 10:56 PM UTC	9.8 (High)	95 %	1	1
DistCC RCE Vulnerability (CVE-2004-2687)	Wed, Feb 21, 2024 10:56 PM UTC	Wed, Feb 21, 2024 10:56 PM UTC	9.3 (High)	99 %	1	1

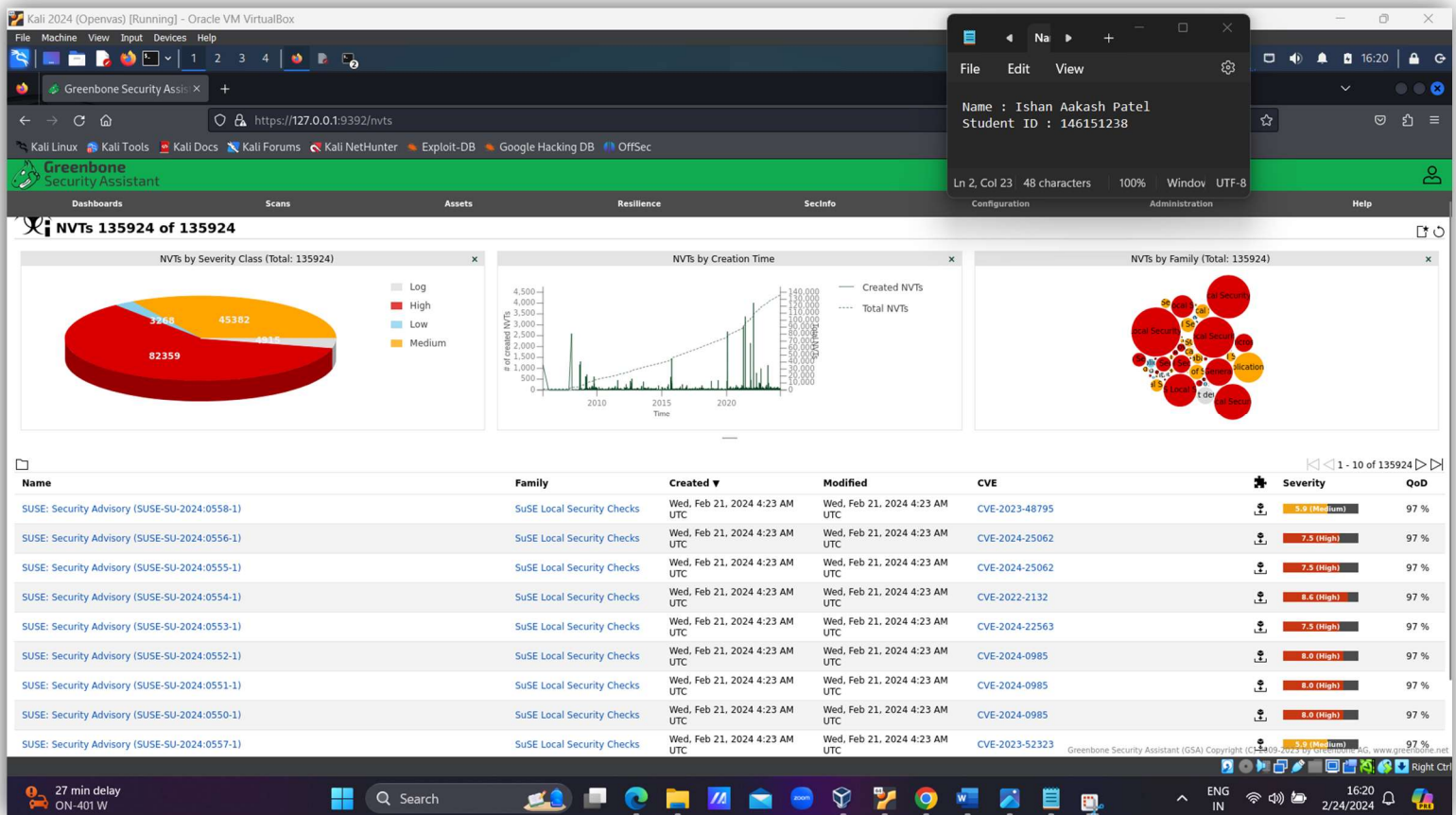


7. What was the vulnerability with the highest severity? Write half a page describing this vulnerability in your own words. Look for information on NVD, and CWE.

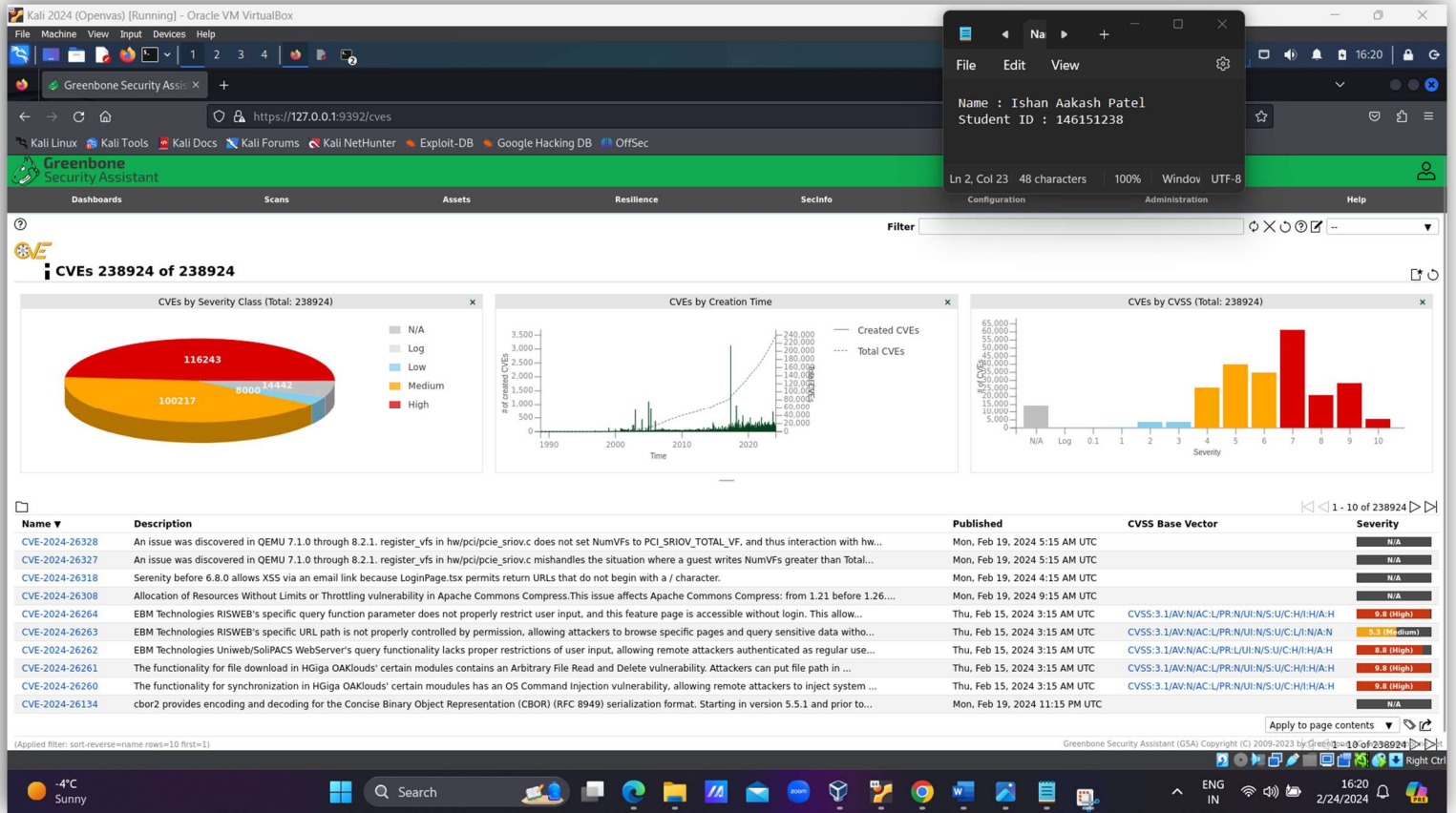
### rlogin passwordless login – (CVE – 2022 – 44589)

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.

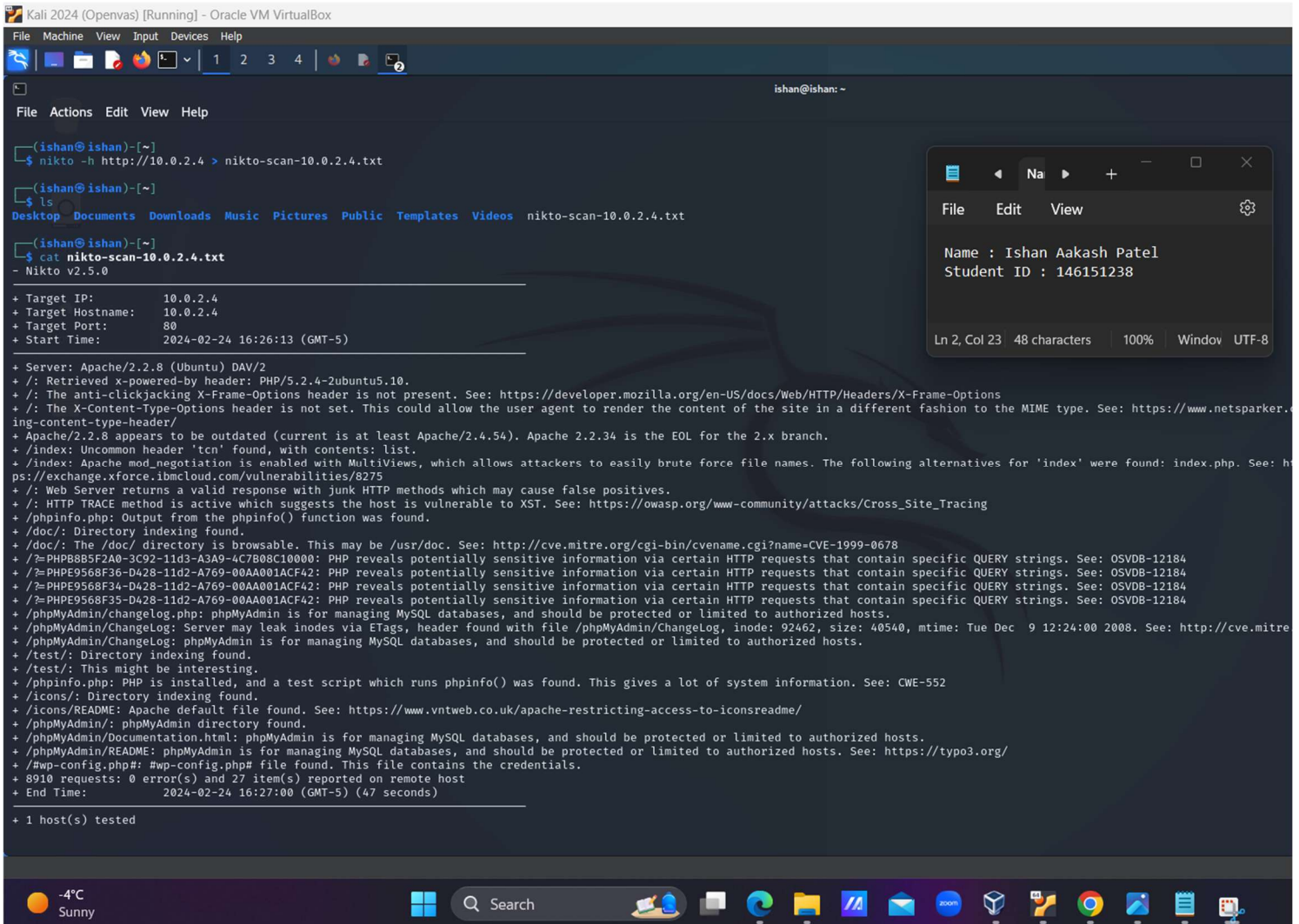
If the rlogin service supports passwordless login, an attacker who gets access to the client system may be able to connect to the remote machine without entering a password. Relying only on passwordless logins may compromise the overall security posture. Without adequate authentication, an attacker might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



```
(ishan@ ishan)-[~]
$ nikto -h http://10.0.2.4 > nikto-scan-10.0.2.4.txt

(ishan@ ishan)-[~]
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  nikto-scan-10.0.2.4.txt

(ishan@ ishan)-[~]
$ cat nikto-scan-10.0.2.4.txt
- Nikto v2.5.0

+ Target IP: 10.0.2.4
+ Target Hostname: 10.0.2.4
+ Target Port: 80
+ Start Time: 2024-02-24 16:26:13 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/blog/content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4615
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2024-02-24 16:27:00 (GMT-5) (47 seconds)

+ 1 host(s) tested
```

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.