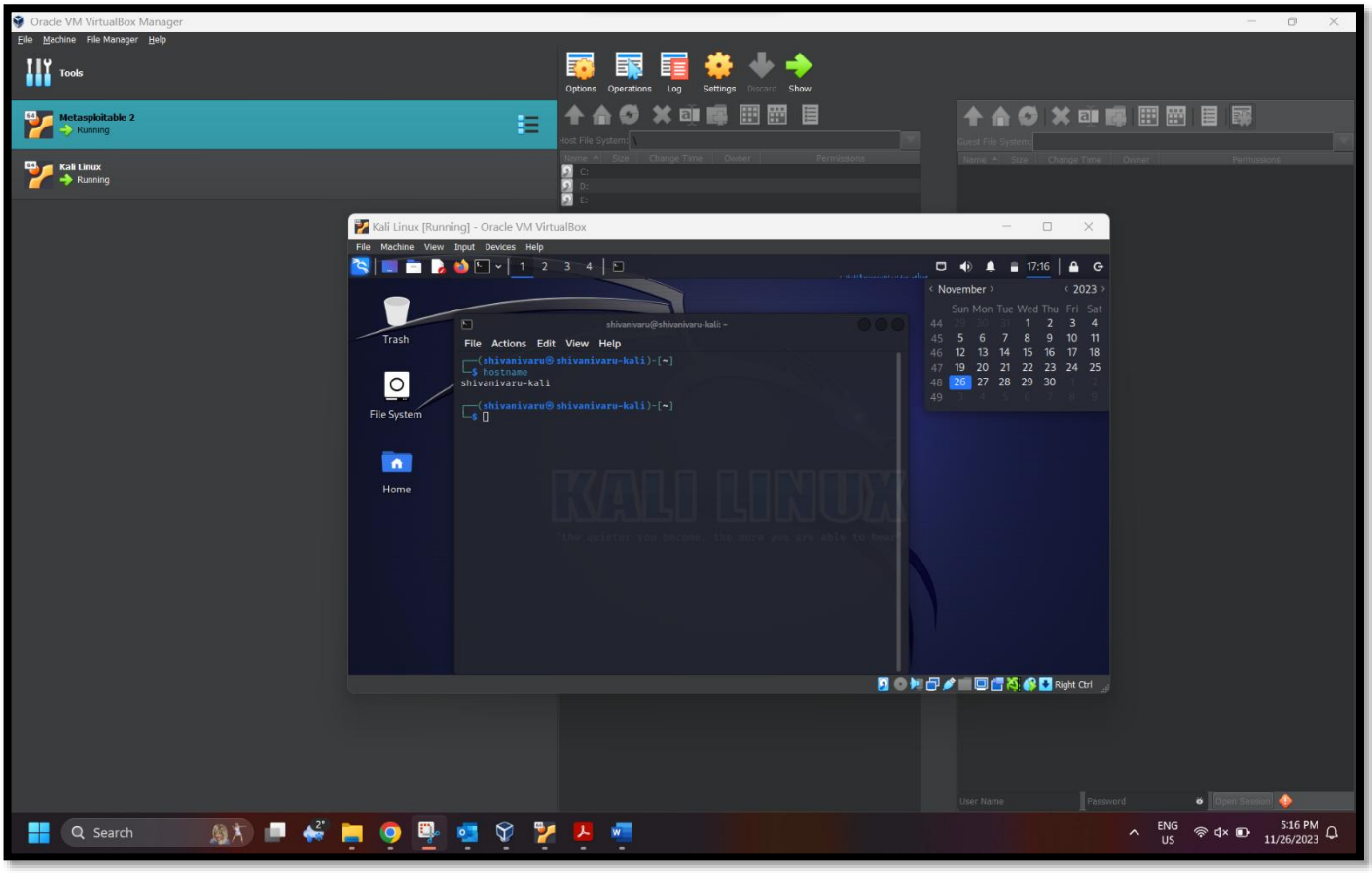
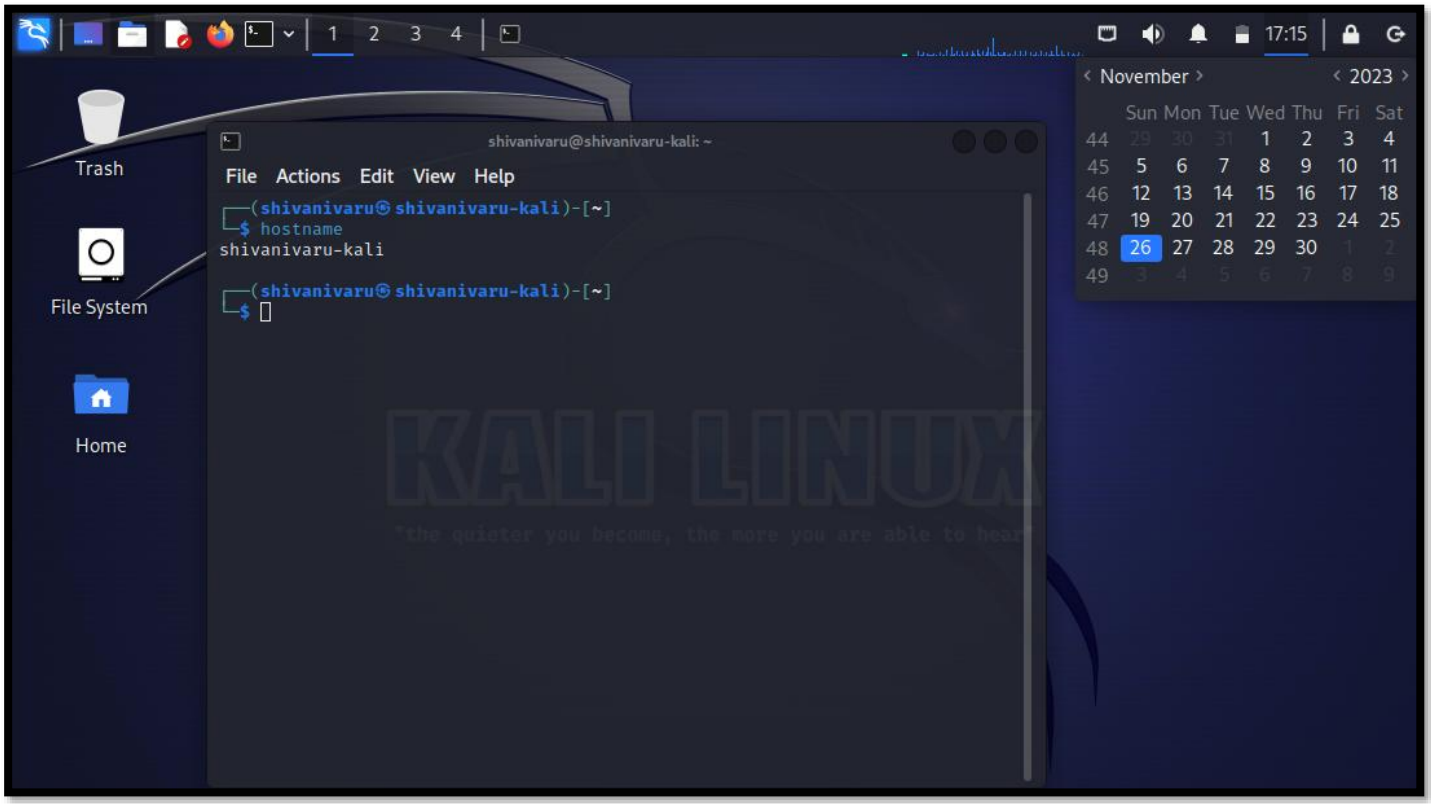
Assignment #4

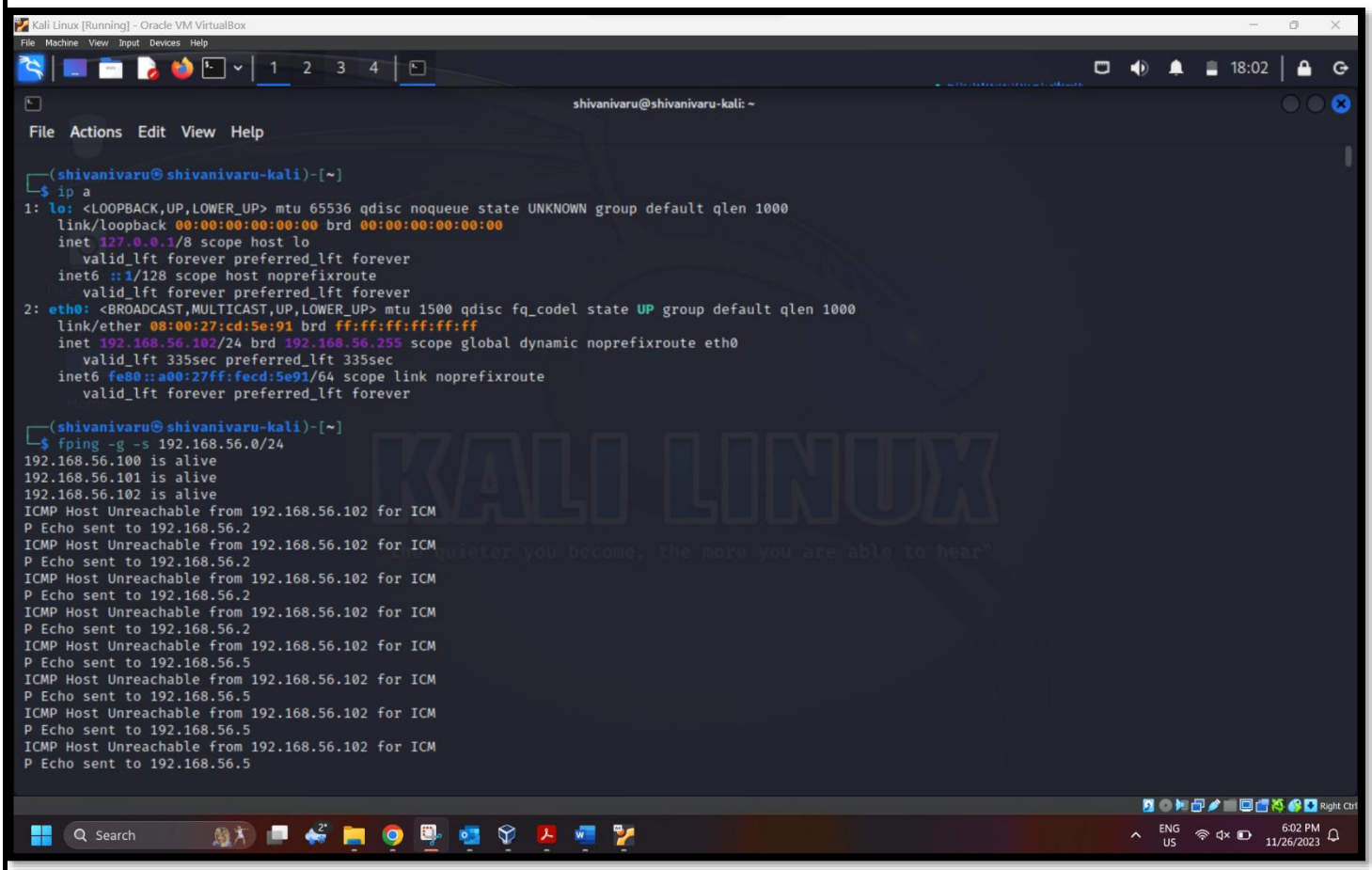
Name: Shivani Shaileshkumar Varu
Student ID: 8941914
Date: 5-12-2023
Section Number: Section – 4

Screen Shot of Kali Setup With Time and Date.

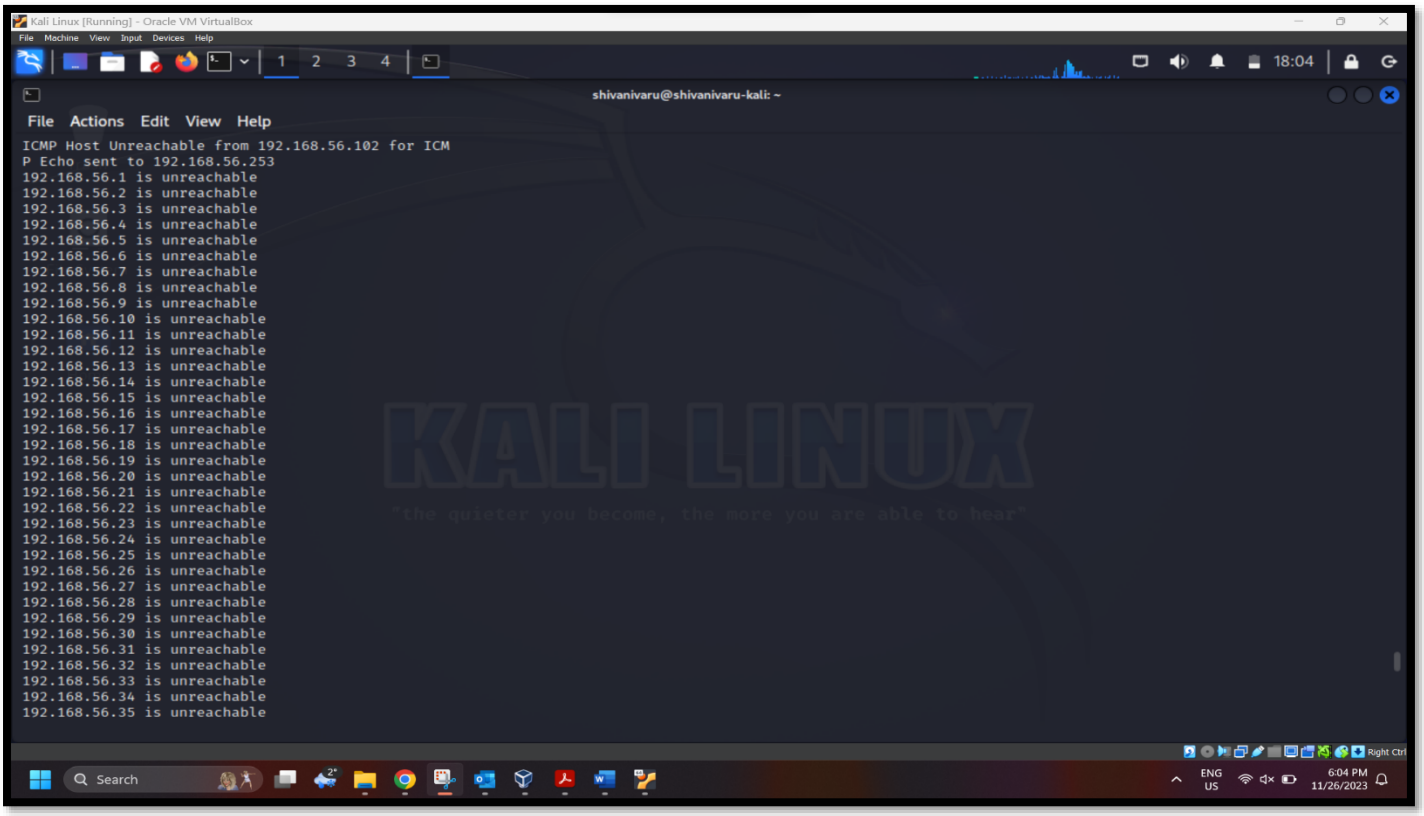


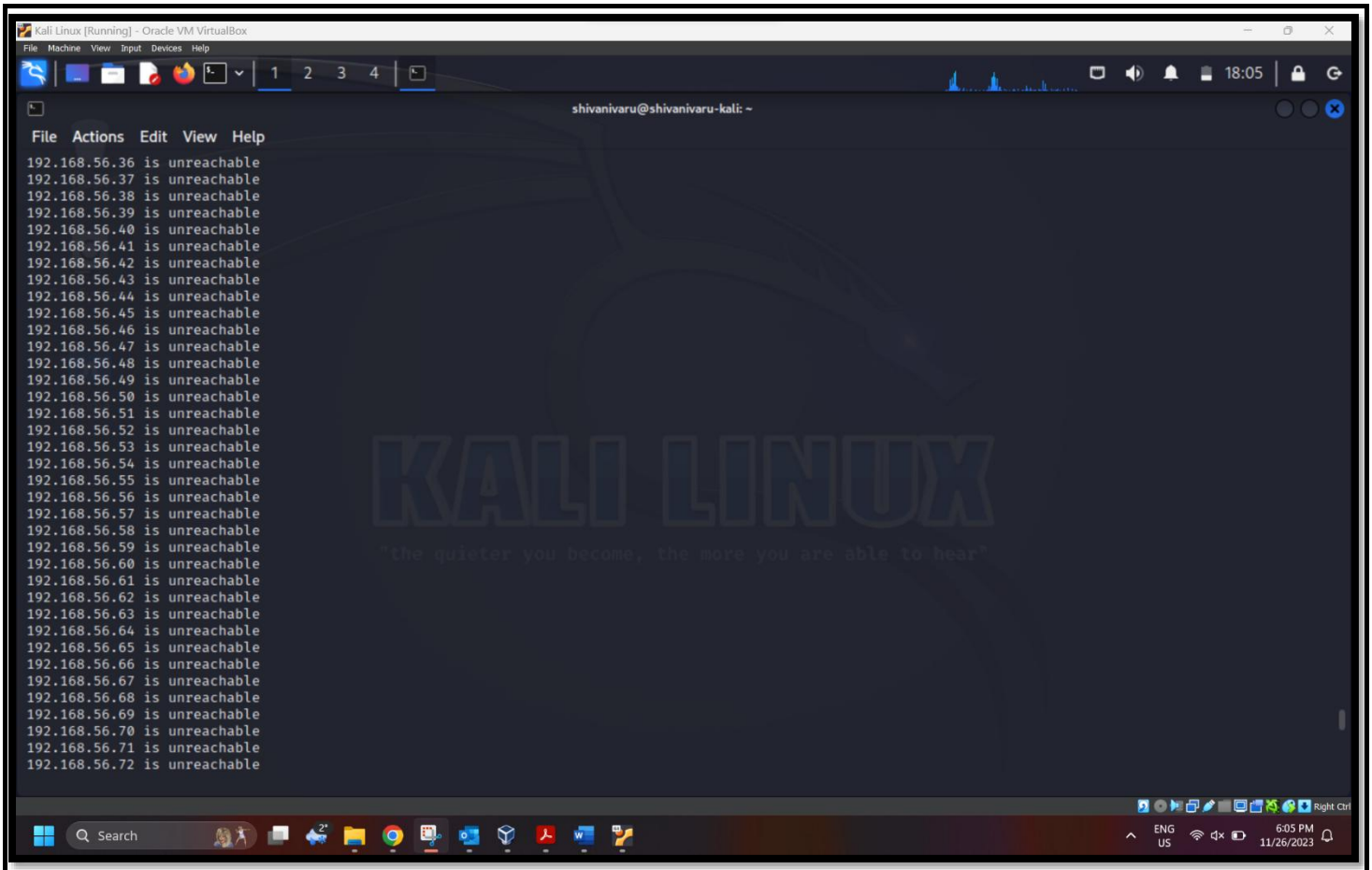


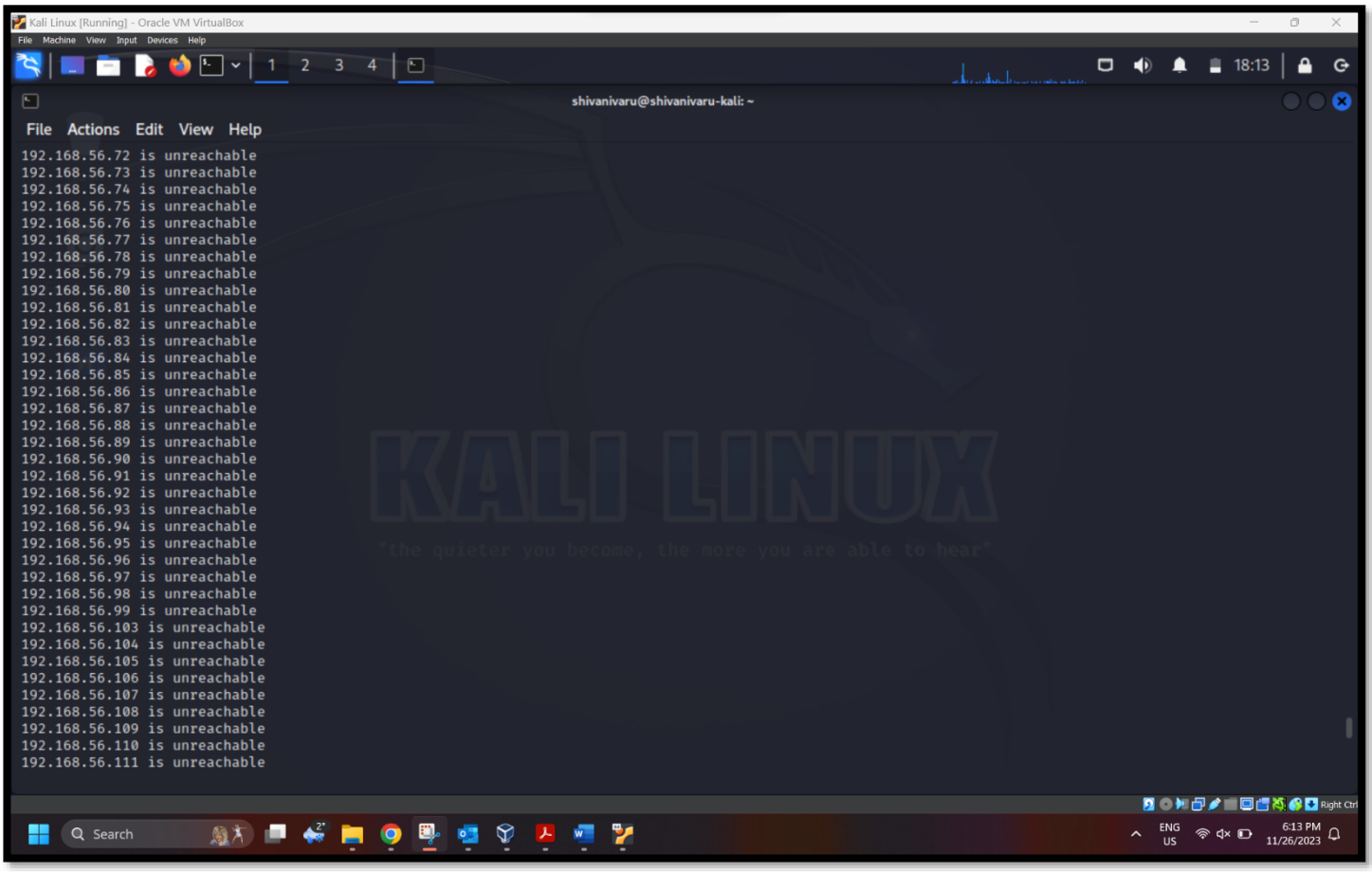
Output From fping:

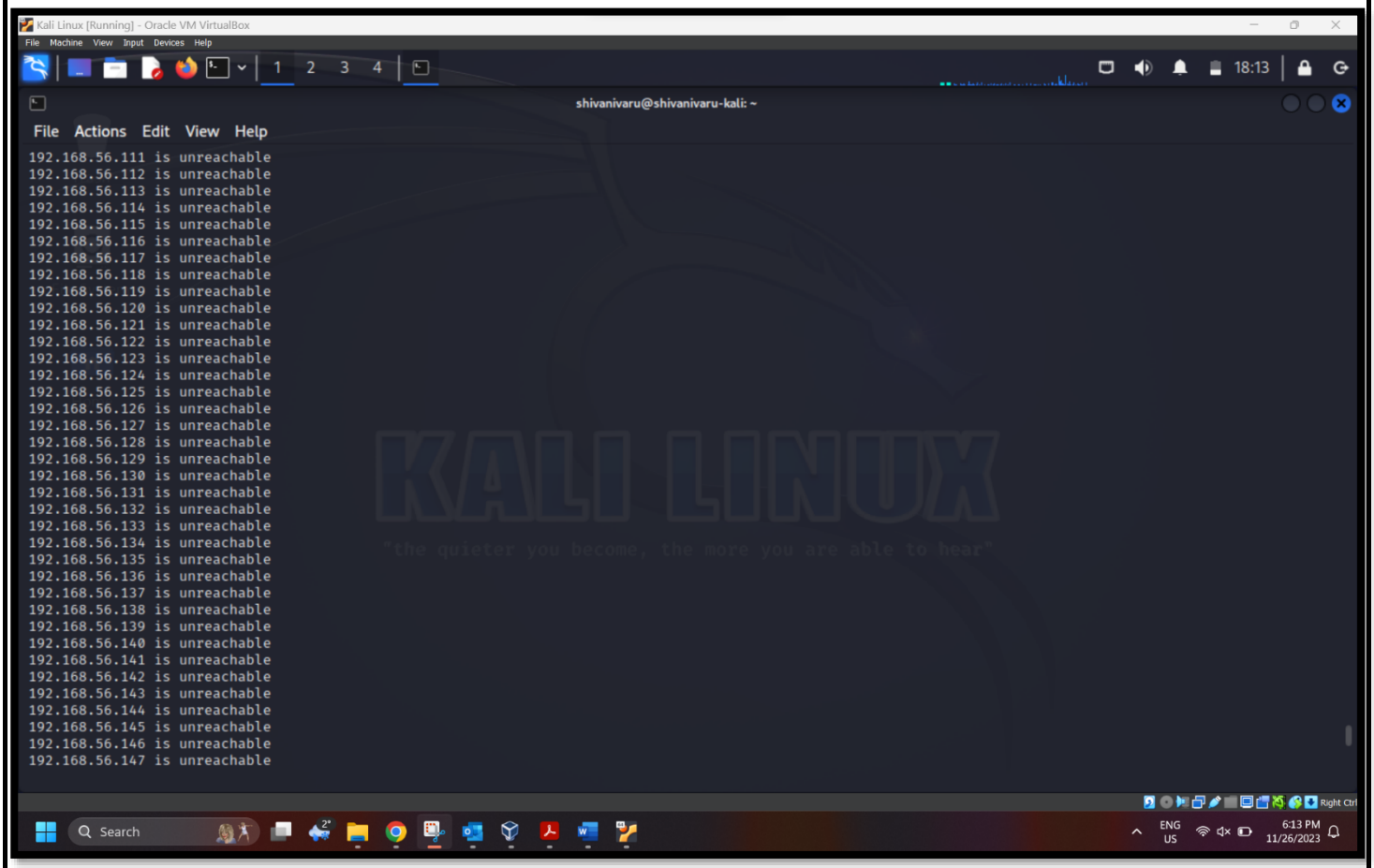


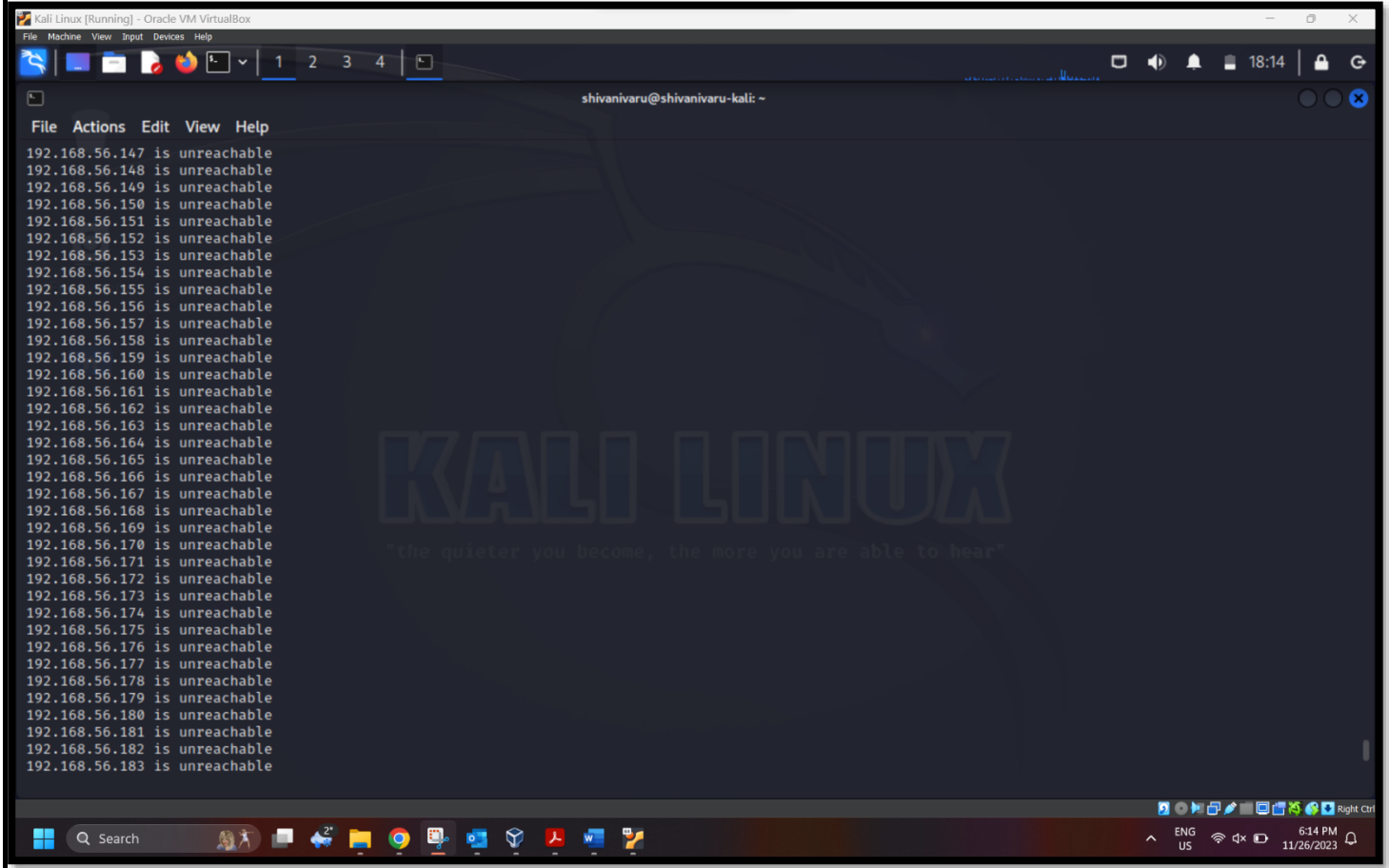
I have three IP addresses alive in the above output and referred to two options from the fping tool, -g to generate and -s to show the stats of all targets.

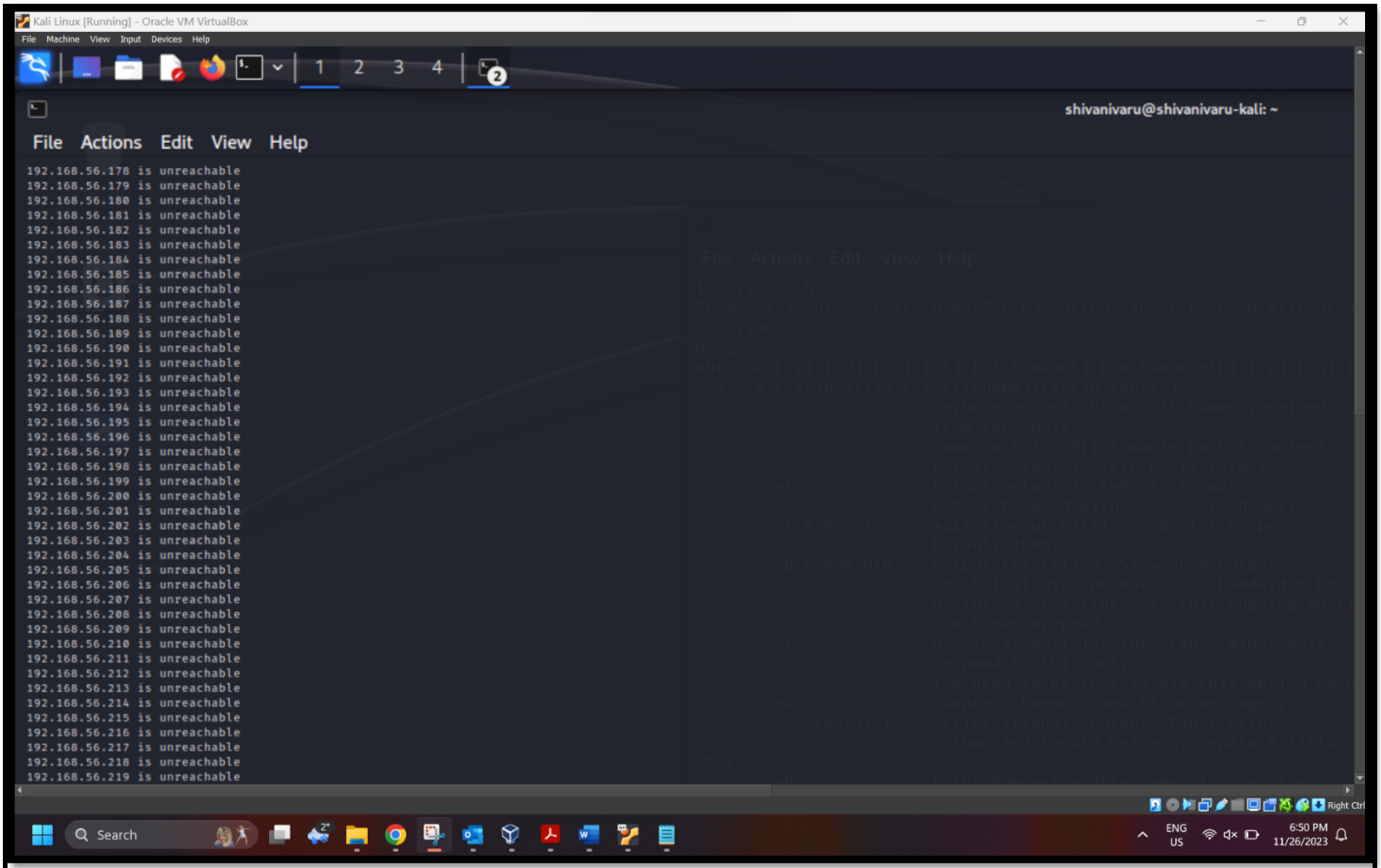



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:05
shivanivaru@shivanivaru-kali: ~
File Actions Edit View Help
192.168.56.36 is unreachable
192.168.56.37 is unreachable
192.168.56.38 is unreachable
192.168.56.39 is unreachable
192.168.56.40 is unreachable
192.168.56.41 is unreachable
192.168.56.42 is unreachable
192.168.56.43 is unreachable
192.168.56.44 is unreachable
192.168.56.45 is unreachable
192.168.56.46 is unreachable
192.168.56.47 is unreachable
192.168.56.48 is unreachable
192.168.56.49 is unreachable
192.168.56.50 is unreachable
192.168.56.51 is unreachable
192.168.56.52 is unreachable
192.168.56.53 is unreachable
192.168.56.54 is unreachable
192.168.56.55 is unreachable
192.168.56.56 is unreachable
192.168.56.57 is unreachable
192.168.56.58 is unreachable
192.168.56.59 is unreachable
192.168.56.60 is unreachable
192.168.56.61 is unreachable
192.168.56.62 is unreachable
192.168.56.63 is unreachable
192.168.56.64 is unreachable
192.168.56.65 is unreachable
192.168.56.66 is unreachable
192.168.56.67 is unreachable
192.168.56.68 is unreachable
192.168.56.69 is unreachable
192.168.56.70 is unreachable
192.168.56.71 is unreachable
192.168.56.72 is unreachable
KALI LINUX
"the quieter you become, the more you are able to hear"
Search
ENG US
6:05 PM 11/26/2023

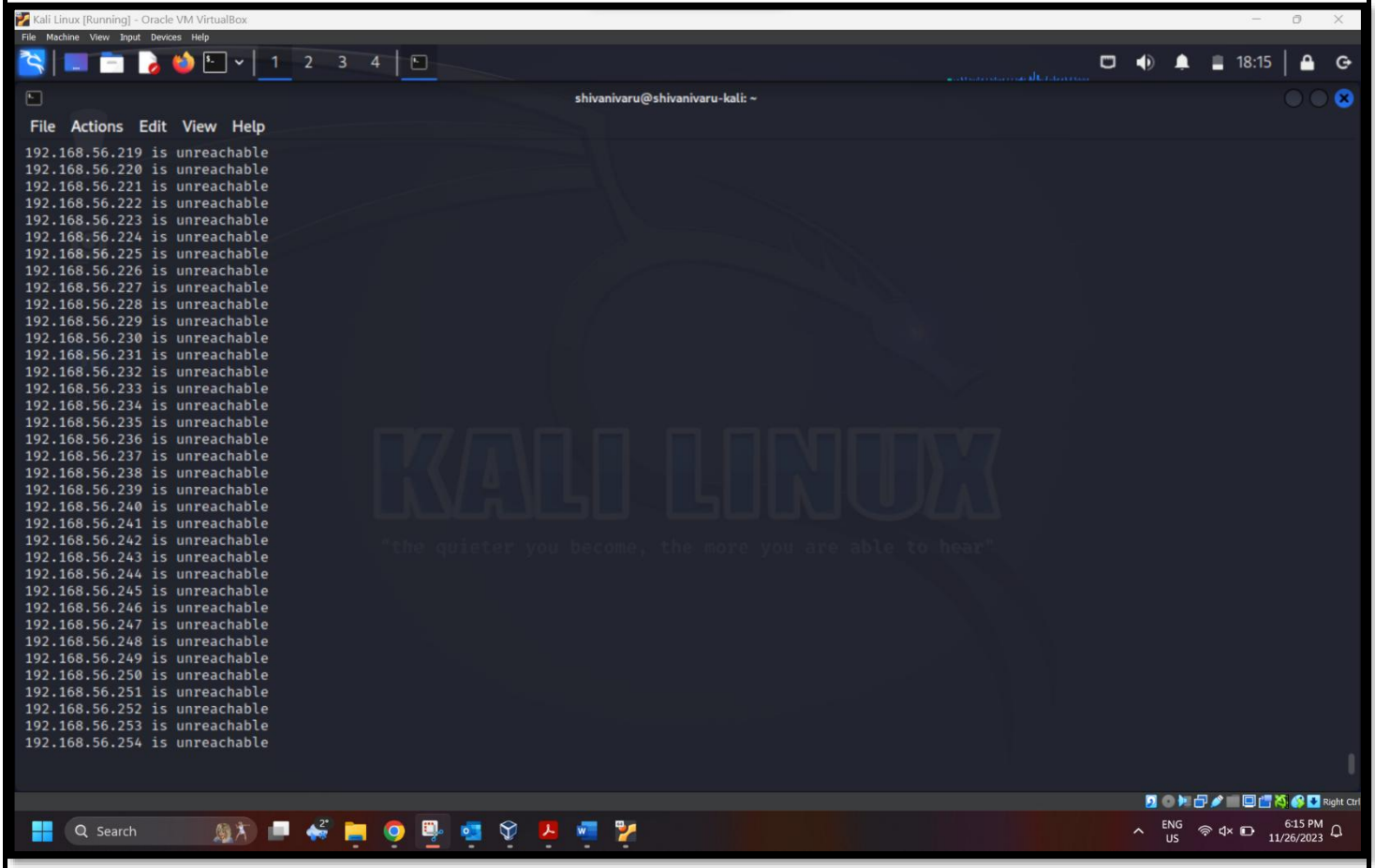

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:13
shivanivaru@shivanivaru-kali: ~
File Actions Edit View Help
192.168.56.72 is unreachable
192.168.56.73 is unreachable
192.168.56.74 is unreachable
192.168.56.75 is unreachable
192.168.56.76 is unreachable
192.168.56.77 is unreachable
192.168.56.78 is unreachable
192.168.56.79 is unreachable
192.168.56.80 is unreachable
192.168.56.81 is unreachable
192.168.56.82 is unreachable
192.168.56.83 is unreachable
192.168.56.84 is unreachable
192.168.56.85 is unreachable
192.168.56.86 is unreachable
192.168.56.87 is unreachable
192.168.56.88 is unreachable
192.168.56.89 is unreachable
192.168.56.90 is unreachable
192.168.56.91 is unreachable
192.168.56.92 is unreachable
192.168.56.93 is unreachable
192.168.56.94 is unreachable
192.168.56.95 is unreachable
192.168.56.96 is unreachable
192.168.56.97 is unreachable
192.168.56.98 is unreachable
192.168.56.99 is unreachable
192.168.56.103 is unreachable
192.168.56.104 is unreachable
192.168.56.105 is unreachable
192.168.56.106 is unreachable
192.168.56.107 is unreachable
192.168.56.108 is unreachable
192.168.56.109 is unreachable
192.168.56.110 is unreachable
192.168.56.111 is unreachable
KALI LINUX
"the quieter you become, the more you are able to hear"
Search
ENG US
6:13 PM 11/26/2023

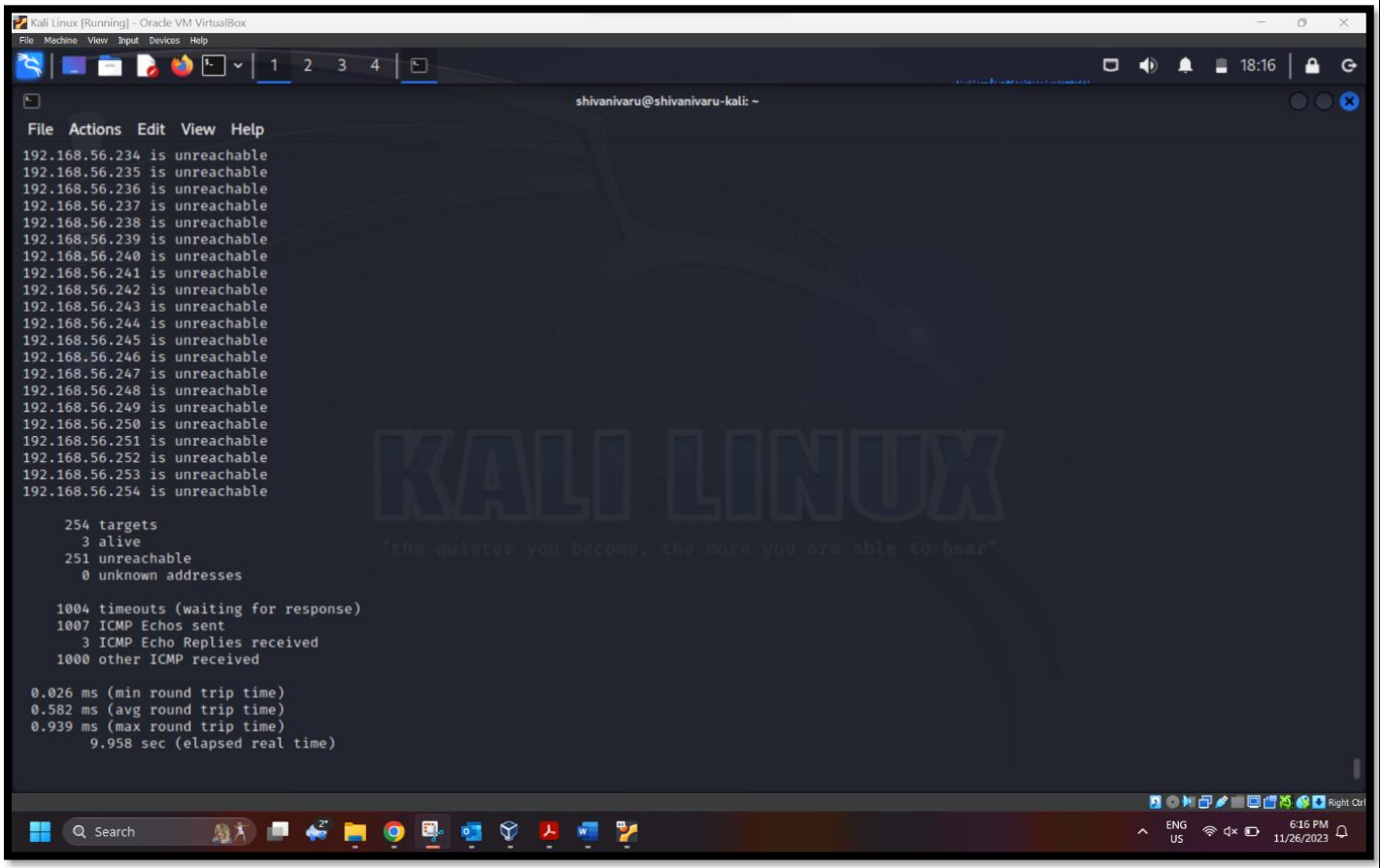

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:13
shivanivaru@shivanivaru-kali: ~
File Actions Edit View Help
192.168.56.111 is unreachable
192.168.56.112 is unreachable
192.168.56.113 is unreachable
192.168.56.114 is unreachable
192.168.56.115 is unreachable
192.168.56.116 is unreachable
192.168.56.117 is unreachable
192.168.56.118 is unreachable
192.168.56.119 is unreachable
192.168.56.120 is unreachable
192.168.56.121 is unreachable
192.168.56.122 is unreachable
192.168.56.123 is unreachable
192.168.56.124 is unreachable
192.168.56.125 is unreachable
192.168.56.126 is unreachable
192.168.56.127 is unreachable
192.168.56.128 is unreachable
192.168.56.129 is unreachable
192.168.56.130 is unreachable
192.168.56.131 is unreachable
192.168.56.132 is unreachable
192.168.56.133 is unreachable
192.168.56.134 is unreachable
192.168.56.135 is unreachable
192.168.56.136 is unreachable
192.168.56.137 is unreachable
192.168.56.138 is unreachable
192.168.56.139 is unreachable
192.168.56.140 is unreachable
192.168.56.141 is unreachable
192.168.56.142 is unreachable
192.168.56.143 is unreachable
192.168.56.144 is unreachable
192.168.56.145 is unreachable
192.168.56.146 is unreachable
192.168.56.147 is unreachable
KALI LINUX
"the quieter you become, the more you are able to hear"
Search
ENG US
6:13 PM 11/26/2023


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:14
shivanivaru@shivanivaru-kali: ~
File Actions Edit View Help
192.168.56.147 is unreachable
192.168.56.148 is unreachable
192.168.56.149 is unreachable
192.168.56.150 is unreachable
192.168.56.151 is unreachable
192.168.56.152 is unreachable
192.168.56.153 is unreachable
192.168.56.154 is unreachable
192.168.56.155 is unreachable
192.168.56.156 is unreachable
192.168.56.157 is unreachable
192.168.56.158 is unreachable
192.168.56.159 is unreachable
192.168.56.160 is unreachable
192.168.56.161 is unreachable
192.168.56.162 is unreachable
192.168.56.163 is unreachable
192.168.56.164 is unreachable
192.168.56.165 is unreachable
192.168.56.166 is unreachable
192.168.56.167 is unreachable
192.168.56.168 is unreachable
192.168.56.169 is unreachable
192.168.56.170 is unreachable
192.168.56.171 is unreachable
192.168.56.172 is unreachable
192.168.56.173 is unreachable
192.168.56.174 is unreachable
192.168.56.175 is unreachable
192.168.56.176 is unreachable
192.168.56.177 is unreachable
192.168.56.178 is unreachable
192.168.56.179 is unreachable
192.168.56.180 is unreachable
192.168.56.181 is unreachable
192.168.56.182 is unreachable
192.168.56.183 is unreachable
KALI LINUX
"the quieter you become, the more you are able to hear"
Search
ENG US
6:14 PM 11/26/2023

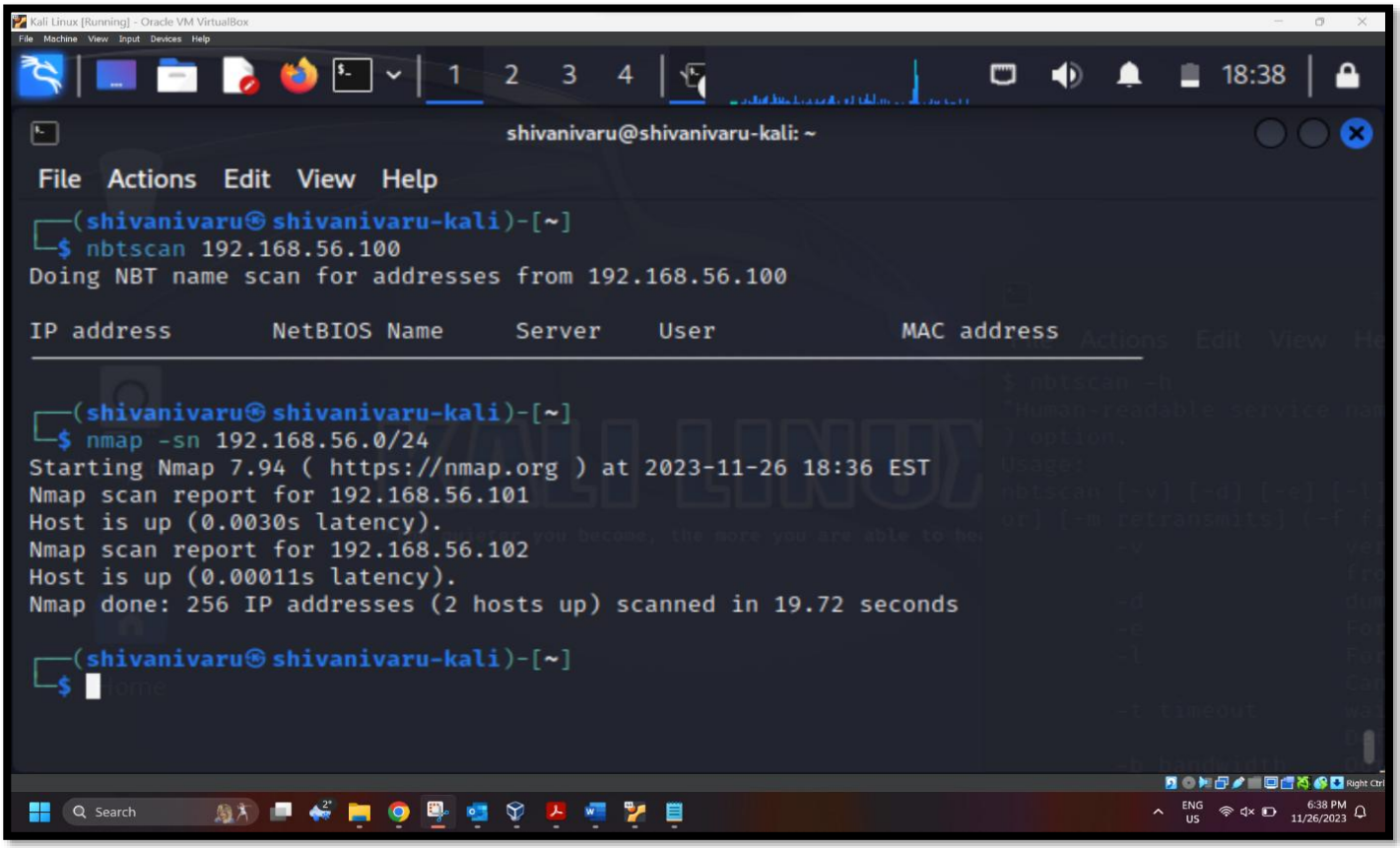


In the above screenshots, the list of IP addresses unreachable is displayed.



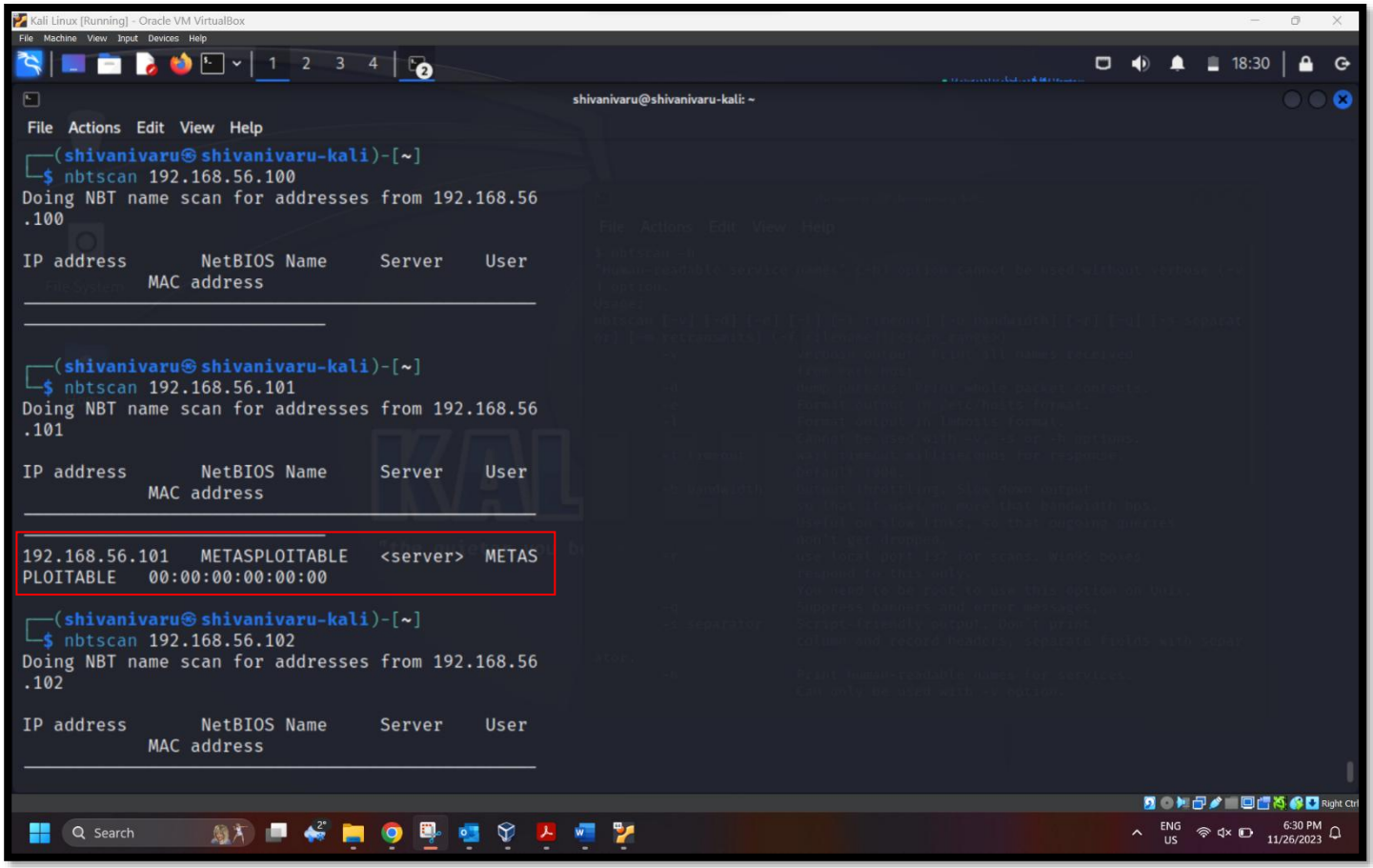


The above screenshot shows the final stats with **254 targets** out of which **3** are alive and **251 targets** are **unreachable**.



To find the exact IP address, I have referred to using the **-sn** command from the Nmap tool to find only the available host. This option helps in the reconnaissance of the target. This can be used to find available machines

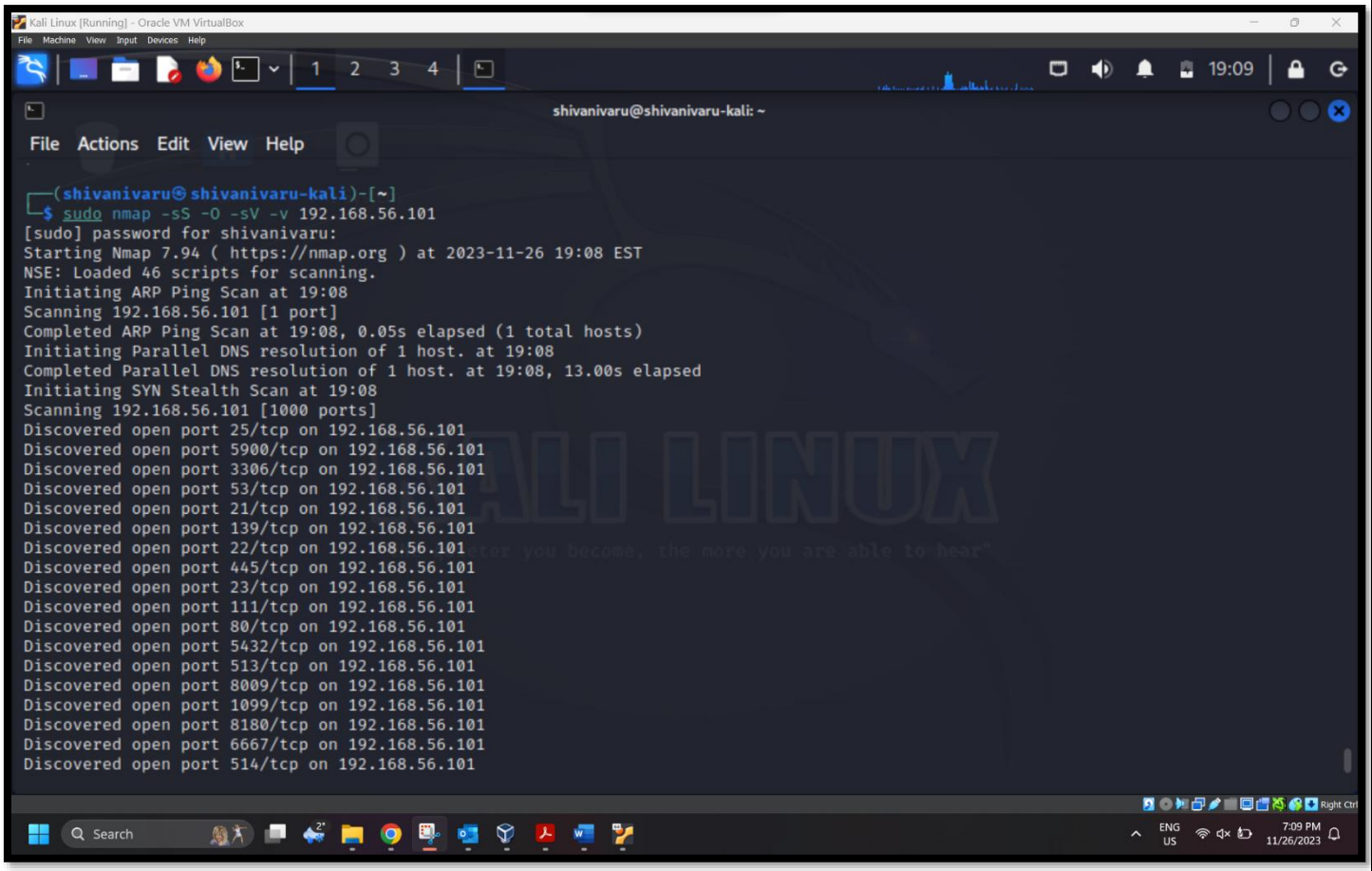
Output from NBTSCAN :



The above output shows the execution of the nbtscan tool on the list of 3 IP addresses that I have found**. The IP address for Metaspoitable is 192.168.56.101 which I have highlighted with red box.**

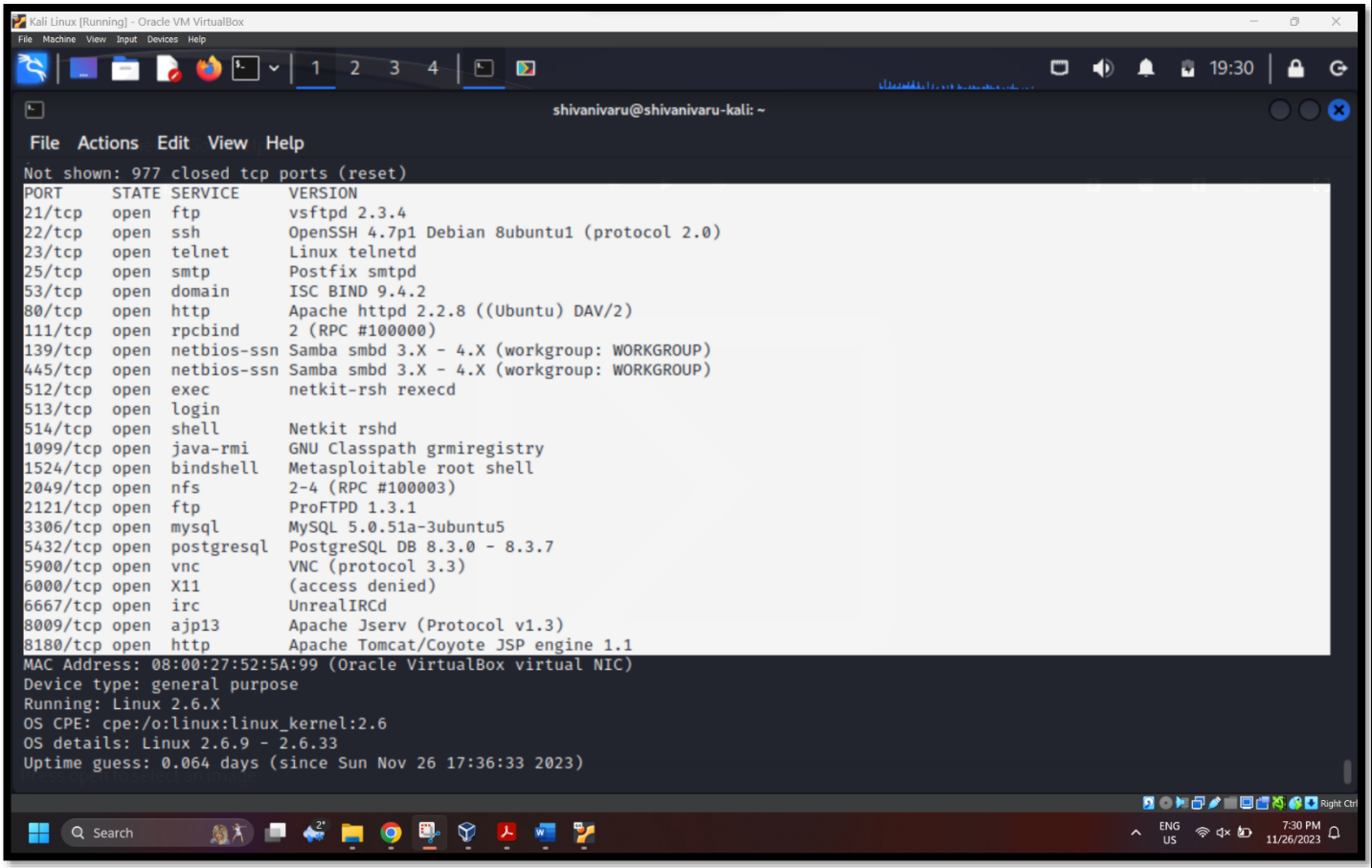
.

Nmap for Detailed Scanning:

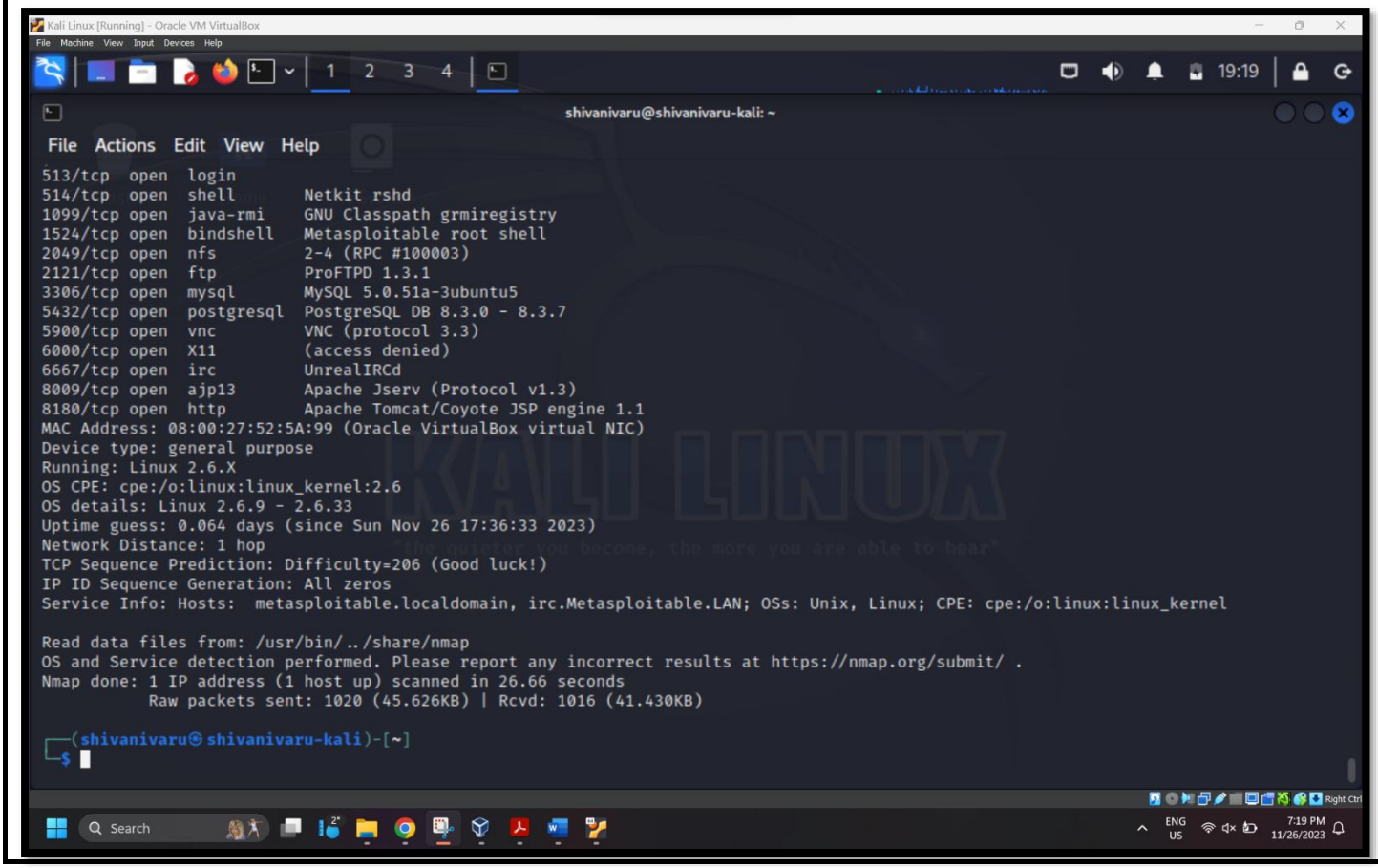


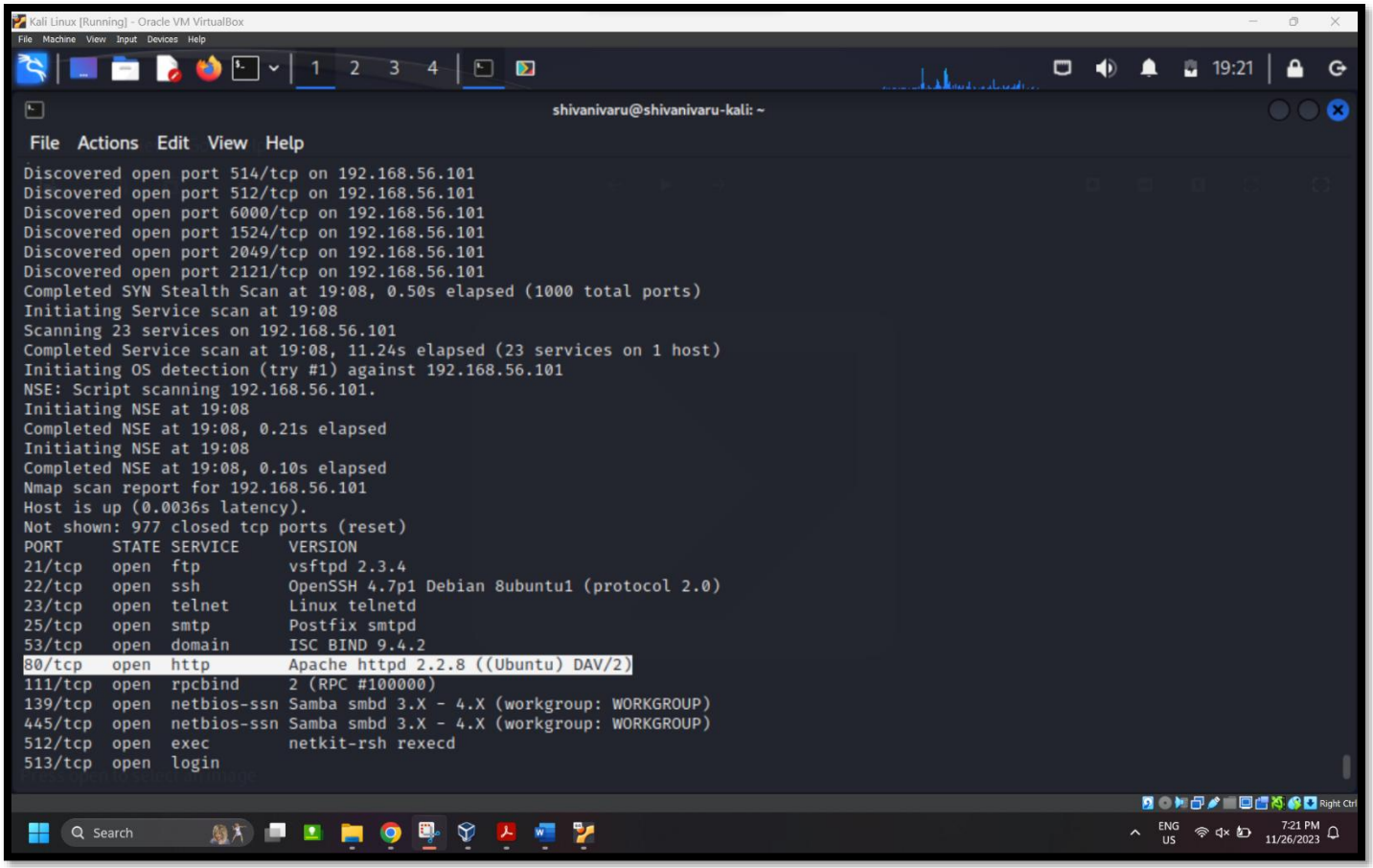
I have highlighted the Nmap command with all the correct options below:

1. -sS is used to check if the host is up, and also Nmap attempts the TCP SYN connection.
2. -O helps in OS Scanning.
3. -sV helps in version detection
4. -v helps with more information about scanning progress, and it also provides an estimation of completion time.



In the above screenshot, I have highlighted all the open ports and services.





In the above output, I have highlighted the service name Apache httpd 2.2.8 that I will conduct.

Answer for research on Apache HTTPD server 2.2.8:

The Apache HTTP Server, a critical component of web hosting, has gone through various versions. Version 1.3, released on June 6, 1998, remained in use until its final release, 1.3.42, on February 3, 2010. Versions 2.0 (April 6, 2002), 2.2 (December 1, 2005), and 2.4 (February 21, 2012) followed. The most recent, 2.4.57, released on April 6, 2023, reflects continual improvements. The first initial release began on April 27, 1995, with version 0.6.2, which marked the beginning of Apache's impact on web hosting.

However, there are numerous known vulnerabilities in Apache HTTP Server version 2.2.8.

Optionsbleed is one of the vulnerabilities that lets remote attackers access confidential information from process memory. This might happen if there are certain misconfigurations in httpd.conf or if the Limit directive is set in a user.htaccess file. To access the secret data, the attacker might submit an unauthenticated OPTIONS HTTP request.

As a penetration tester, the information about the Optionsbleed vulnerability would be crucial in assessing the security of a system. Here's how I would proceed: Here's how I would proceed:

Step 1: Defining Scope and Goals

Defining the goals and scope of the test is the first stage in every penetration test. This involves identifying the systems to be tested, the processes to be followed, and agreeing on the format for reporting the results.

Step 2: Reconnaissance

Next, I would gather as much information as possible about the target system. This could include identifying the version of Apache being used, the configuration of the .htaccess file, and any other relevant details.

Step 3: Scanning and Exploitation

After getting sufficient details, I'd would use Kali Linux's penetration testing tools to check the target system for the Optionsbleed vulnerability. This might include sending an OPTIONS HTTP request to the server without authentication and examining the response for indications of memory leakage.

Here is an example of a command that could be used in Kali Linux to send an OPTIONS request:

curl -X OPTIONS http://target-server.com

If the server is vulnerable to Optionsbleed, the response could contain confidential information from the server's memory.

Step 4: Reporting

After the test, I would compile a report detailing the findings. This would include information about the vulnerability, the potential impact, and recommended mitigation strategies.

❖ **To safeguard systems from the Optionsbleed vulnerability,**

I can suggest some points that clients should do: -

- Apply the patch for Optionsbleed available from the Apache source code servers. This is a critical step to address the vulnerability and prevent potential data leakage.
- Review the httpd.conf and .htaccess files to ensure that they are properly configured. Avoid misconfigurations that could trigger the Optionsbleed vulnerability.
- Conduct regular security audits and penetration tests to identify and address vulnerabilities, including Optionsbleed. This will help in proactively identifying and mitigating any potential risks.
- Stay informed about the latest security vulnerabilities and patches. Subscribe to security advisories and news sources to stay updated on emerging threats and mitigation strategies.

End users can, however, stay informed about the security of the systems they use and report any unusual or suspicious activity to their IT department or system administrators.

❖ References

1. *Apache HTTP server*. Wikidata. (n.d.). https://www.wikidata.org/wiki/Q11354
2. Chauhan, B. (2023, October 26). *3 most critical Apache vulnerabilities found*. Astra Security Blog. https://www.getastra.com/blog/911/top-3-most-critical-apache-vulnerabilities-found/
3. Apache < 2.2.8 multiple vulnerabilities. Tenable. (n.d.). https://www.tenable.com/plugins/lce/800581
4. *10 apache web server security and hardening tips*. Online Tutorials, Courses, and eBooks Library. (n.d.). https://www.tutorialspoint.com/10-apache-web-server-security-and-hardening-tips
5. *Apache HTTP server version 2.2.8 : Security vulnerabilities, CVES*. Apache Http Server version 2.2.8 : Security vulnerabilities, CVEs. (n.d.). https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-416233/Apache-Http-Server 2.2.8.html?page=2&order=1&trc=67&sha=614e10502c7f37a061f7932cc90f7534419090d
6. Ducklin. (2017, September 19). *Apache "Optionsbleed" vulnerability – what you need to know*. Sophos News. https://news.sophos.com/en-us/2017/09/19/apache-optionsbleed-vulnerability-what-you-need-to-know/
7. Maury, J. (2023, October 10). *Kali Linux penetration testing tutorial: How to use Kali linux*. eSecurity Planet. https://www.esecurityplanet.com/networks/kali-linux-tutorial/
8. Thorat, B. P., Authors, Pavan Thorat Vulnerability Researcher William Gamazo Sanchez Sr. Threat Researcher, Researcher, P. T. V., Thorat, P., Researcher, V., Researcher, W. G. S. Sr. T., Sanchez, W. G., Researcher, Sr. T., Us, C., & Subscribe. (2017, September 22). *OptionsBleed – the apache HTTP server now bleeds*. Trend Micro. https://www.trendmicro.com/en_ph/research/17/i/optionsbleed-apache-http-server-now-bleeds.html
9. Sanders, C. (2017, September 20). *Chaim sanders*. OWASP ModSecurity Core Rule Set. https://coreruleset.org/20170920/optionsbleed/