MIT World Peace University

Vulnerability Identification and Penetration Testing
Third Year B. Tech, Semester 6

Gathering Network Information from Attackers Perspective

Assignment 3

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

April 20, 2024

Contents

1 Aim

To use various tools to gather network information from an attackers perspective.

2 Objectives

1. To understand the importance of gathering network information.
2. To use various tools to gather network information.
3. To understand the importance of network information in penetration testing.
4. To understand the importance of network information in vulnerability identification.

3 Theory

4 Network Information Gathering

4.1 nmap

nmap is a network scanning tool that is used to discover hosts and services on a computer network. It is used to create a "map" of the network by sending specially crafted packets to the target host and analyzing the responses.

4.2 Uses

- Discovering hosts on a network.
- Identifying open ports and services running on target systems.
- Detecting operating systems and software versions.
- Performing security audits and vulnerability assessments.
- Monitoring network performance and availability.
- Troubleshooting network connectivity issues.
- Investigating suspicious or malicious activities.

4.3 Advantages

- Comprehensive scanning capabilities for discovering hosts, open ports, and services running on target systems.
- Flexible and customizable scanning options, allowing users to tailor scans according to their specific requirements.
- Support for scripting and automation, enabling efficient and repeatable scanning processes.
- Active development and community support, ensuring continuous improvement and updates to the tool.
- Cross-platform compatibility, making it available for use on various operating systems.

4.4 Disadvantages

- Requires expertise to interpret scan results accurately and effectively identify vulnerabilities.
- Scanning can be resource-intensive and may lead to network congestion or disruptions if not managed properly.
- Limited effectiveness against well-configured and hardened systems that actively block or disguise scanning attempts.
- Possibility of triggering intrusion detection and prevention systems or being flagged as suspicious activity by network administrators.
- Legal considerations and potential ethical concerns related to unauthorized scanning of networks without proper authorization.

4.5 Metasploit

Metasploit is a penetration testing framework that simplifies hacking. It is an open-source tool used for developing, testing, and executing exploit code against remote target machines to exploit vulnerabilities in a network.

4.6 Uses

- Identifying and exploiting vulnerabilities in target systems for penetration testing purposes.
- Developing and testing custom exploits for known vulnerabilities in software and systems.
- Post-exploitation activities, such as privilege escalation, lateral movement, and data exfiltration.
- Generating and delivering payloads to compromised systems for remote access and control.
- Conducting security assessments, red teaming exercises, and ethical hacking engagements.
- Researching and analyzing security vulnerabilities and attack techniques to improve defense strategies.
- Collaborating with other security tools and frameworks to enhance testing capabilities and coverage.
- Training and education in offensive security techniques and methodologies for security professionals.
- Contributing to the security community through the development and sharing of exploit code and research.
- Supporting incident response and forensic investigations by simulating real-world attack scenarios.
- Demonstrating the impact of security vulnerabilities and the importance of proactive defense measures.

4.7 Advantages

- Extensive library of exploit modules and payloads for targeting a wide range of vulnerabilities across different systems and applications.
- User-friendly interface with intuitive features and workflows, suitable for both beginners and experienced penetration testers.
- Integration with other security tools and frameworks, enhancing its capabilities and interoperability in complex testing scenarios.
- Active community and regular updates, providing access to new exploits, features, and improvements.
- Extensibility through custom scripting and module development, allowing users to extend its functionality according to their needs.

4.8 Disadvantages

- Requires caution and ethical considerations due to the potential for causing harm or damage if used maliciously or irresponsibly.
- Complexity of exploit development and usage may pose challenges for inexperienced users, requiring a steep learning curve.
- Reliance on publicly available exploit code may lead to detection by security solutions or failure to exploit patched vulnerabilities.
- Limited effectiveness against well-defended networks with robust security measures and up-to-date patching practices.
- Legal implications and regulatory compliance considerations, particularly when conducting penetration testing without proper authorization or consent.

5 Implementation

5.1

Syntax

```
$
```

Command

```
$
```

Purpose

Output

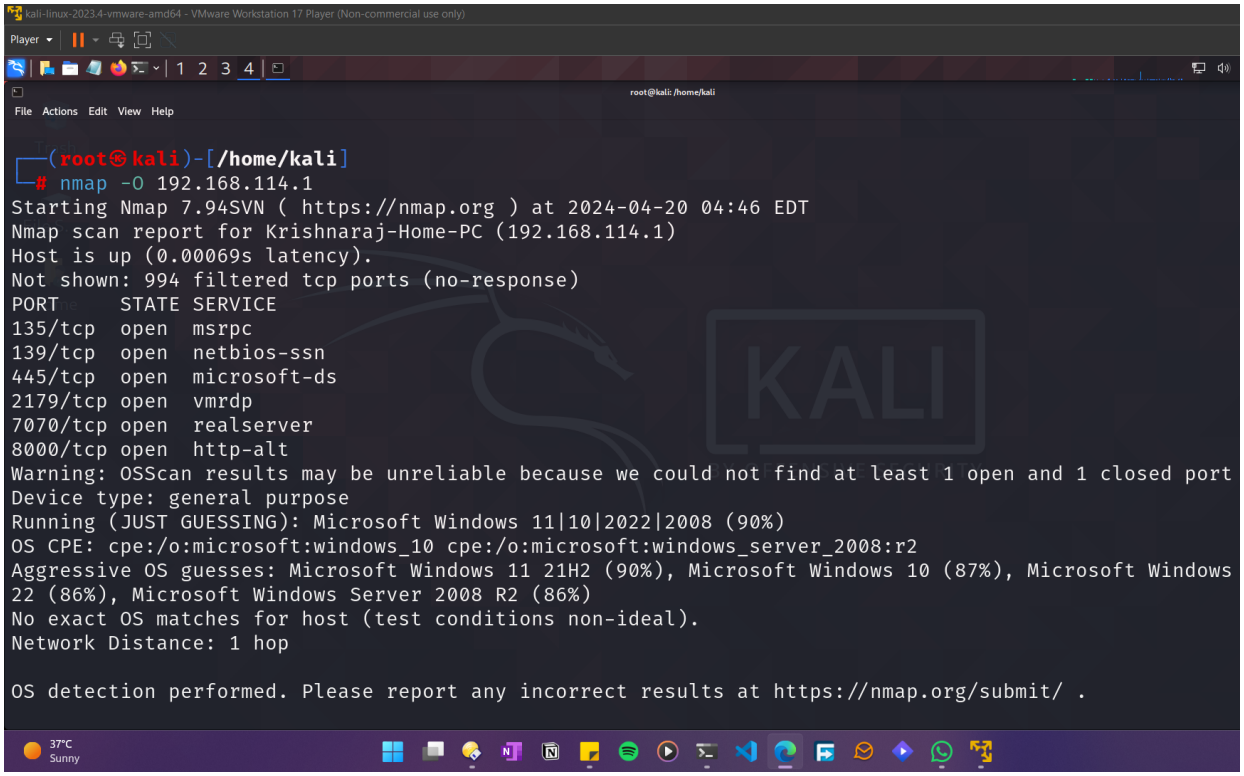

Figure 1: Get IP Address

5.2

Syntax

$

Command

$

Purpose

Output

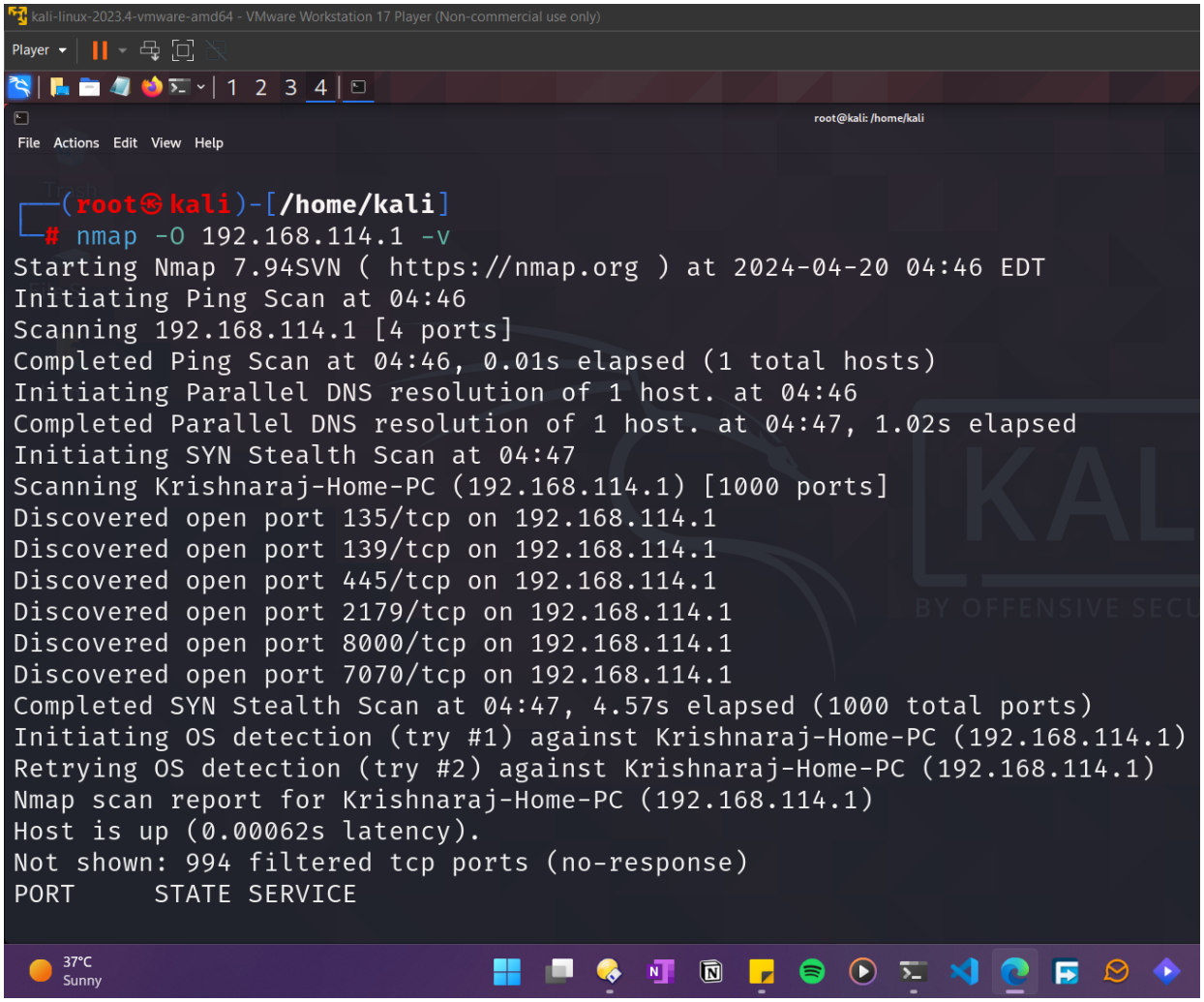

Figure 2: Get IP Address

5.3

Syntax

$

Command

$

Purpose

Output

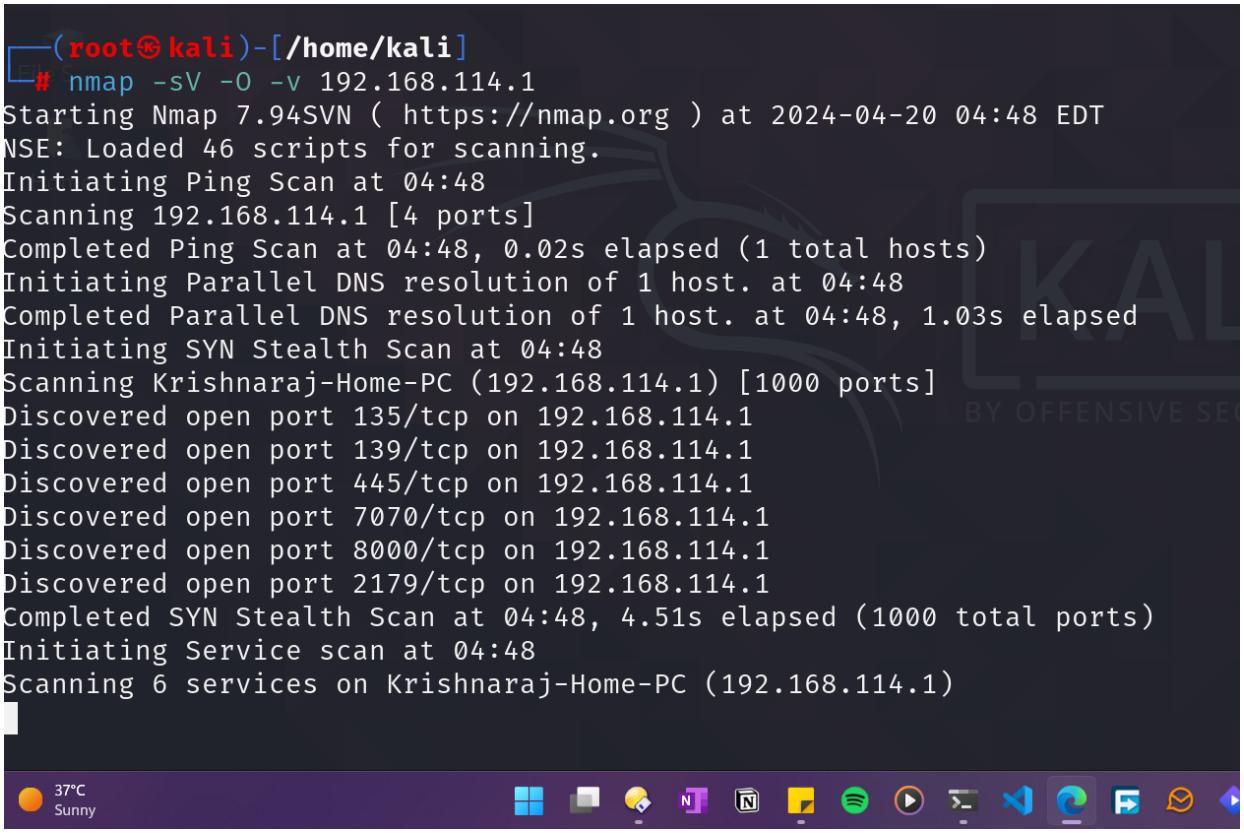

Figure 3: Get IP Address

5.4

Syntax

$

Command

$

Purpose

Output

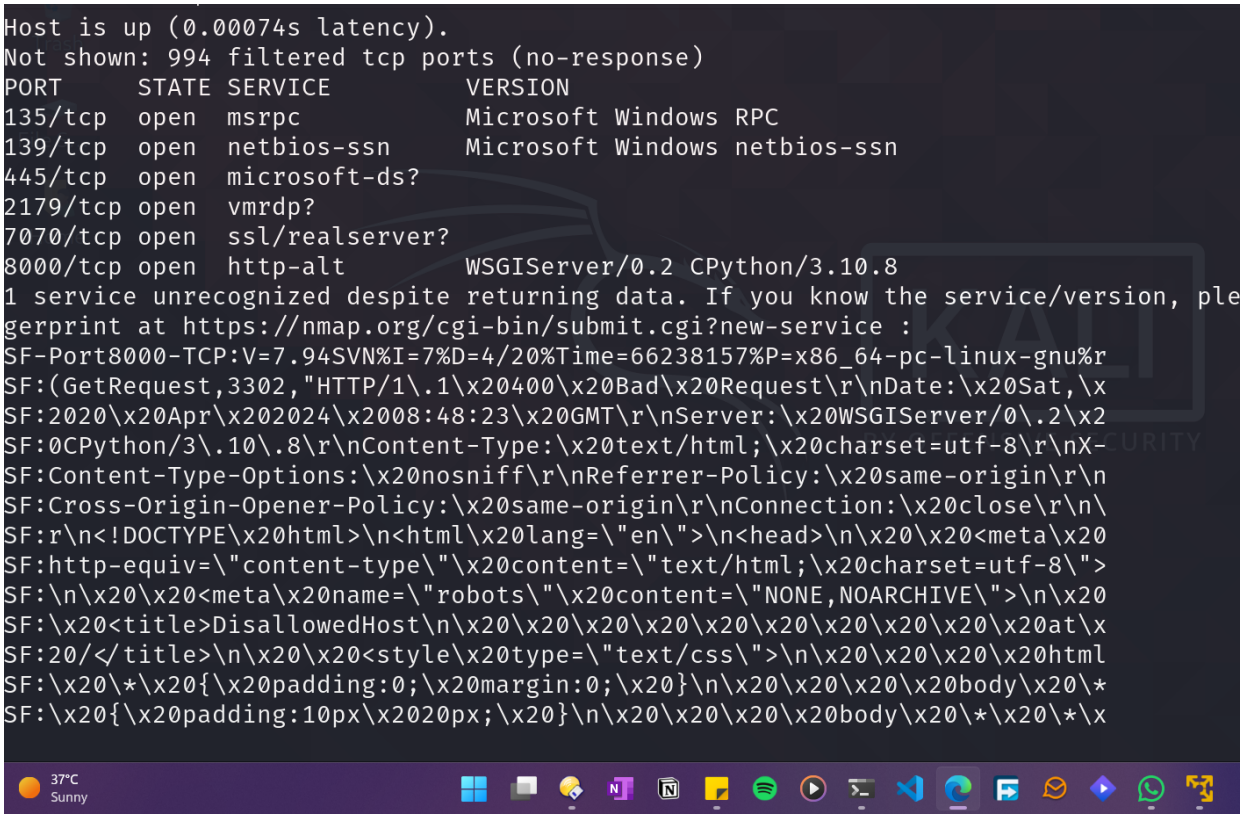

Figure 4: Get IP Address

5.5

Syntax

$

Command

$

Purpose

Output

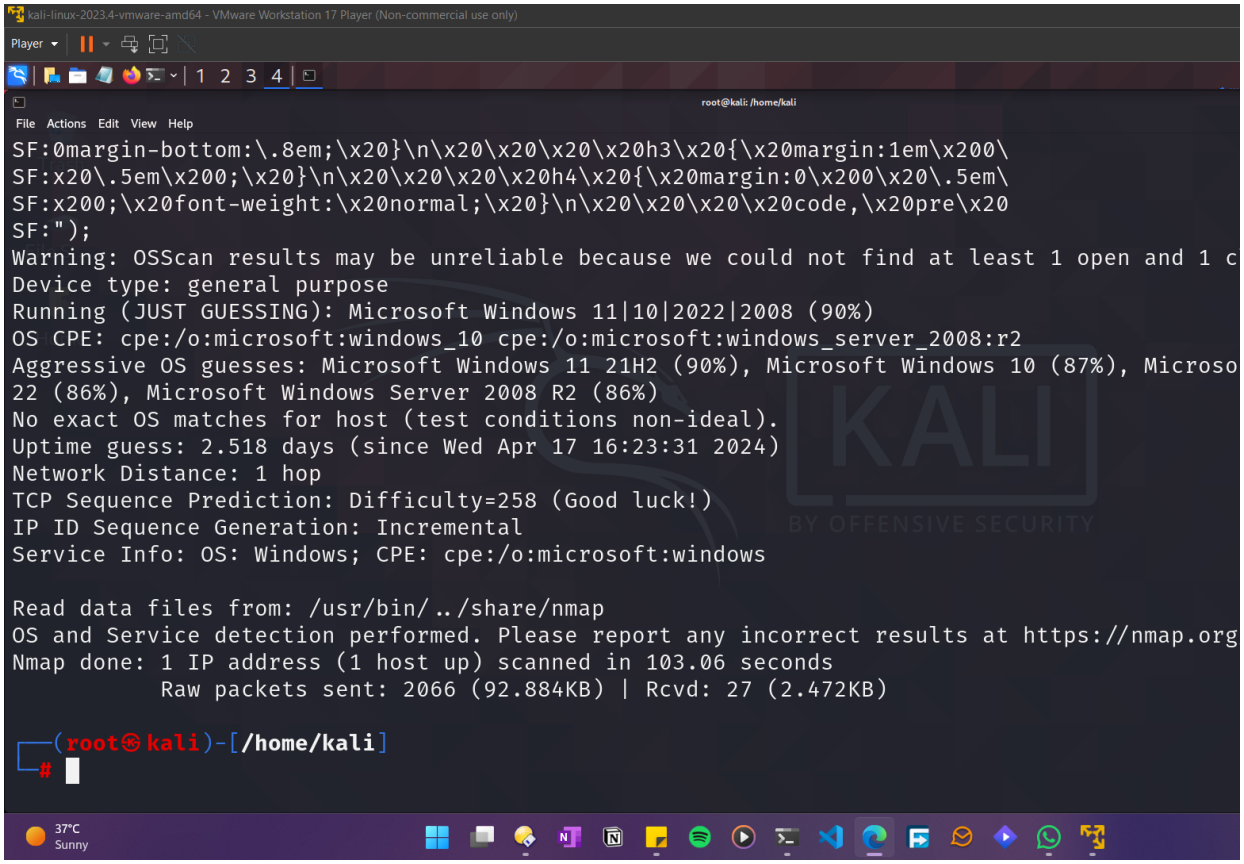

Figure 5: Get IP Address

5.6

Syntax

$

Command

$

Purpose

Output

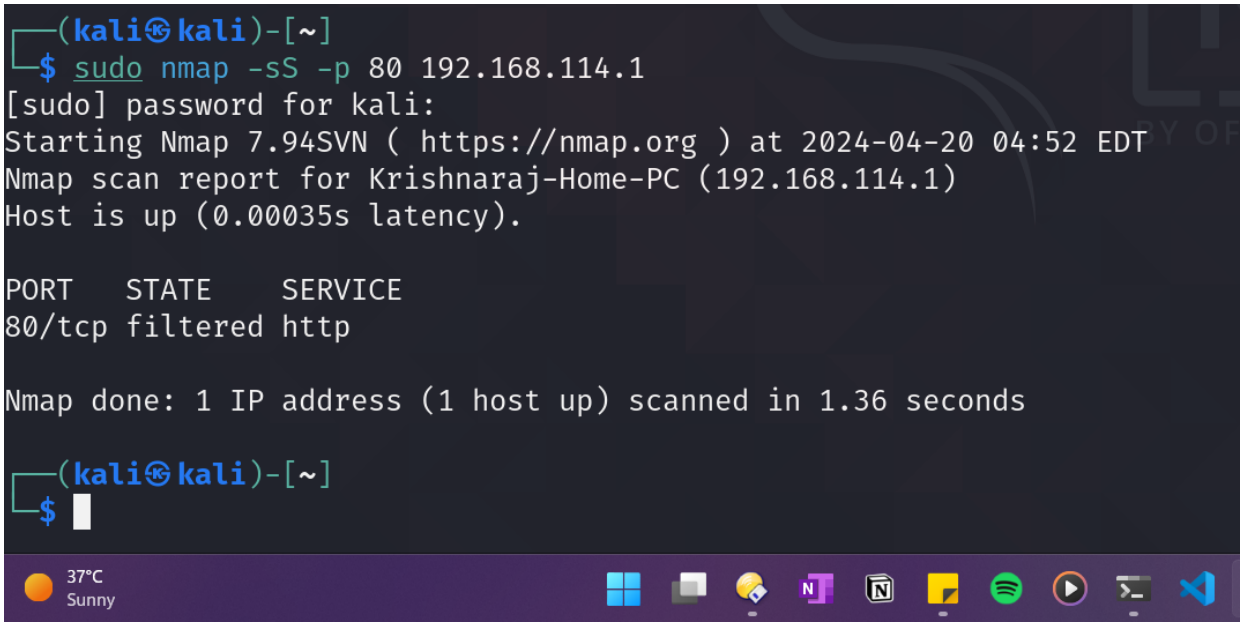

Figure 6: Get IP Address

5.7

Syntax

$

Command

$

Purpose

Output

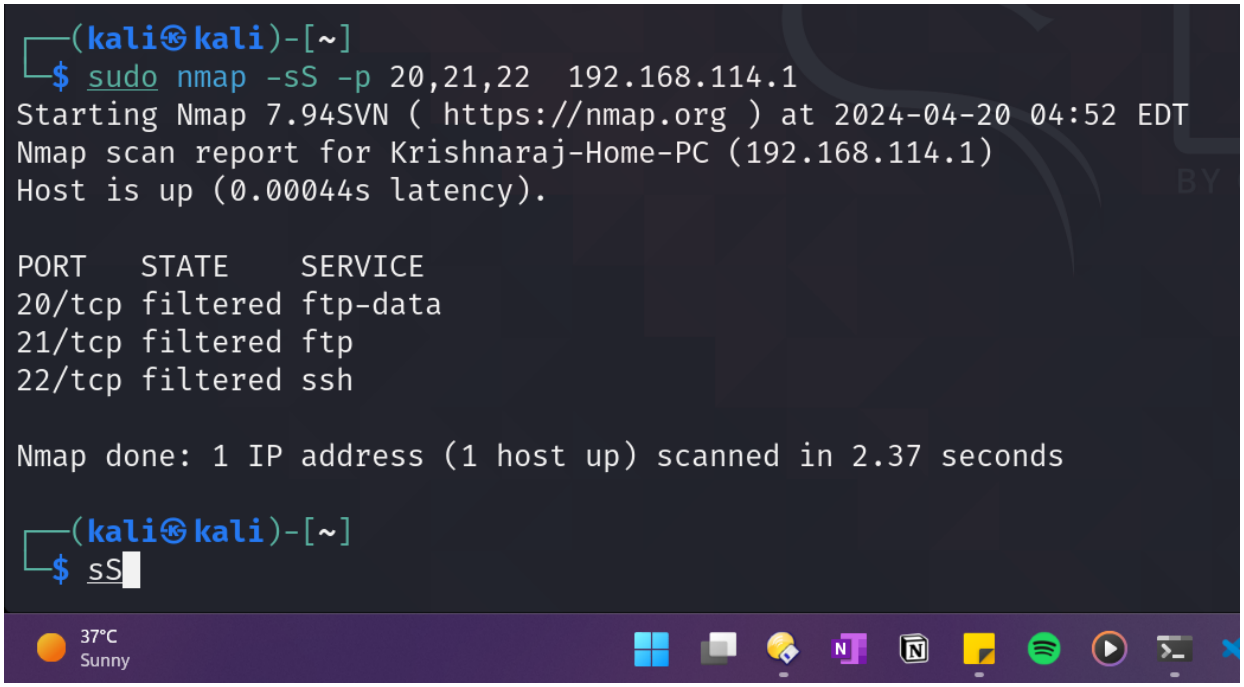

Figure 7: Get IP Address

5.8

Syntax

$

Command

$

Purpose

Output

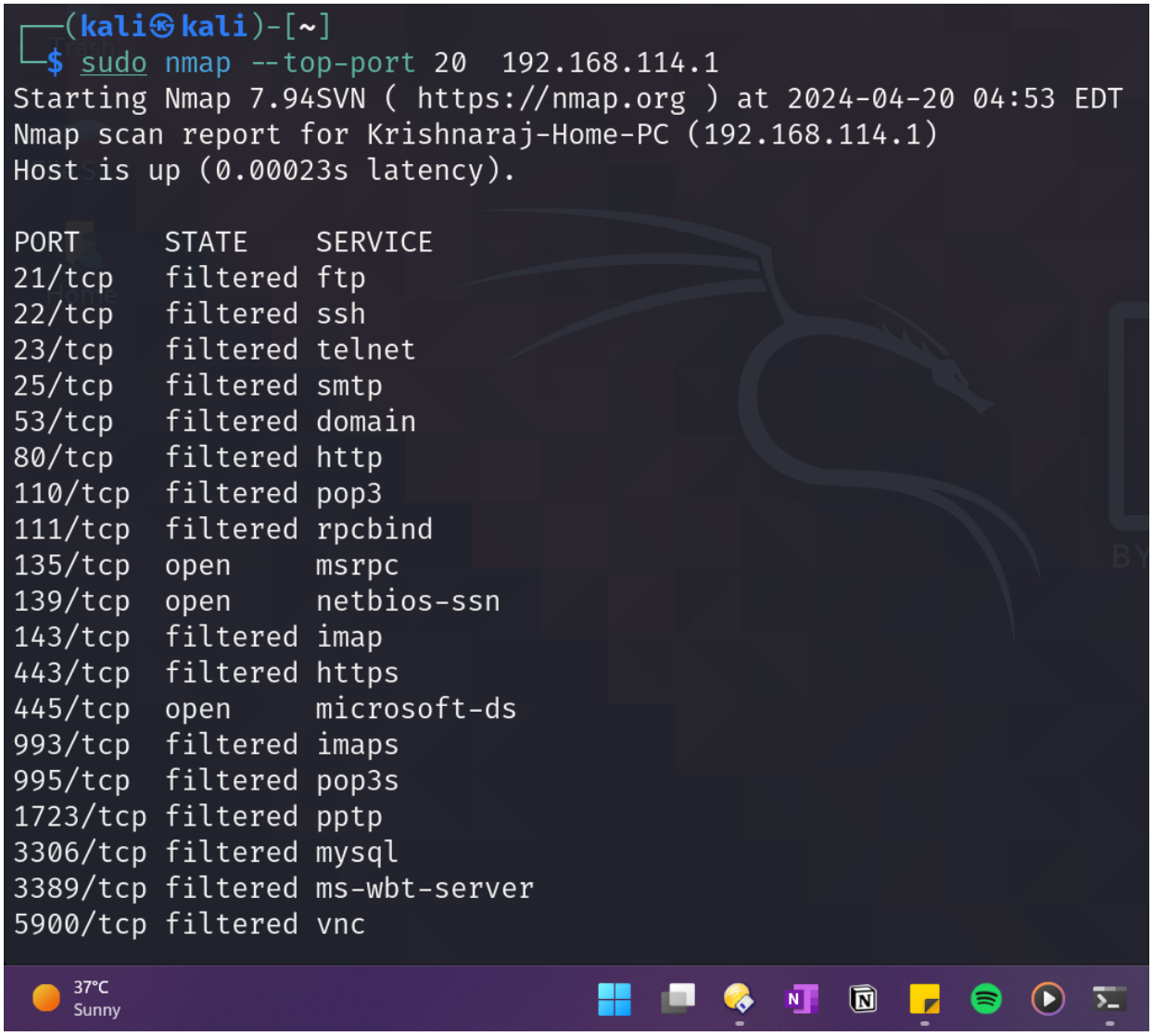

Figure 8: Get IP Address

5.9

Syntax

$

Command

$

Purpose

Output

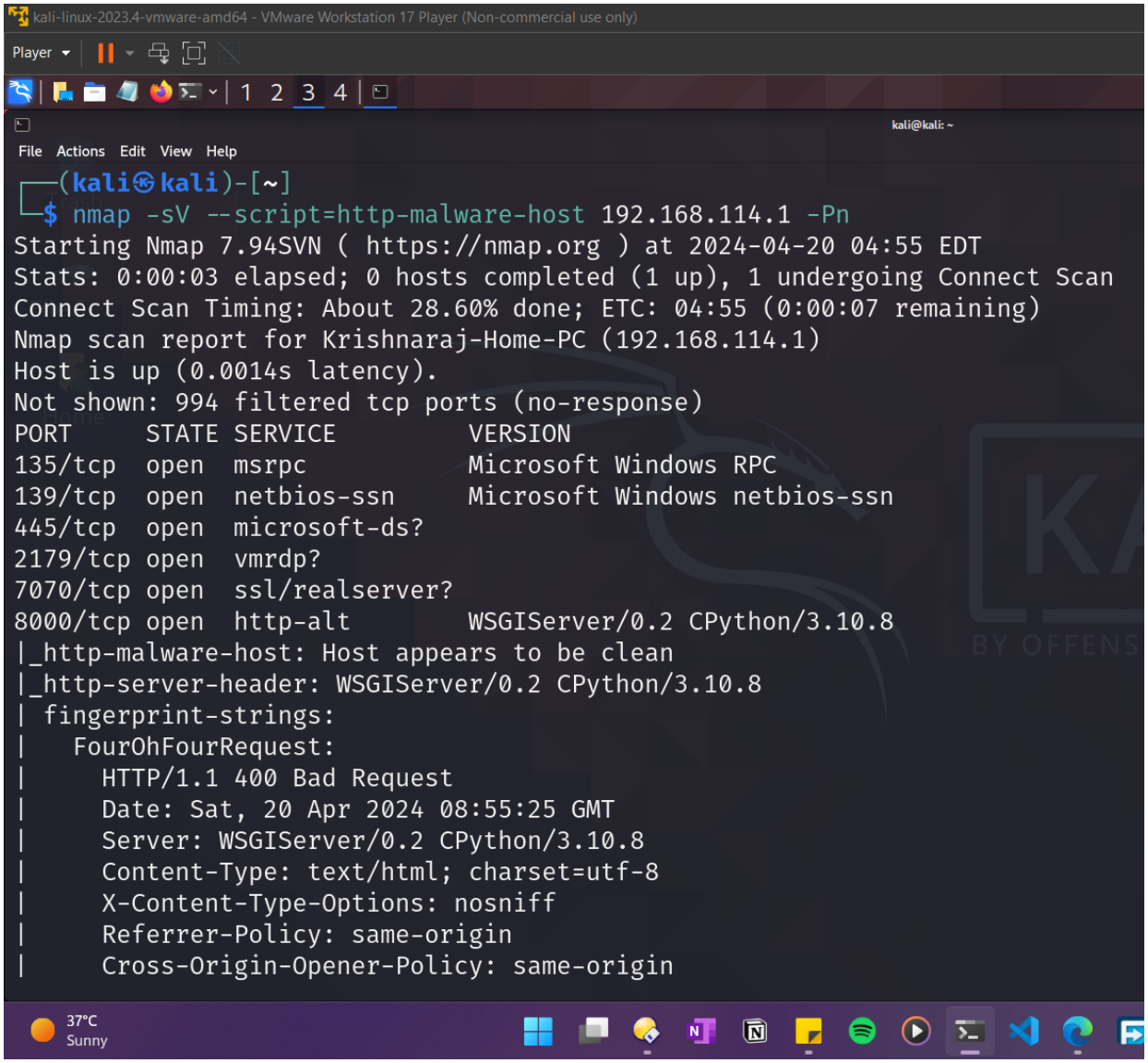

Figure 9: Get IP Address

5.10

Syntax

$

Command

$

Purpose

Output

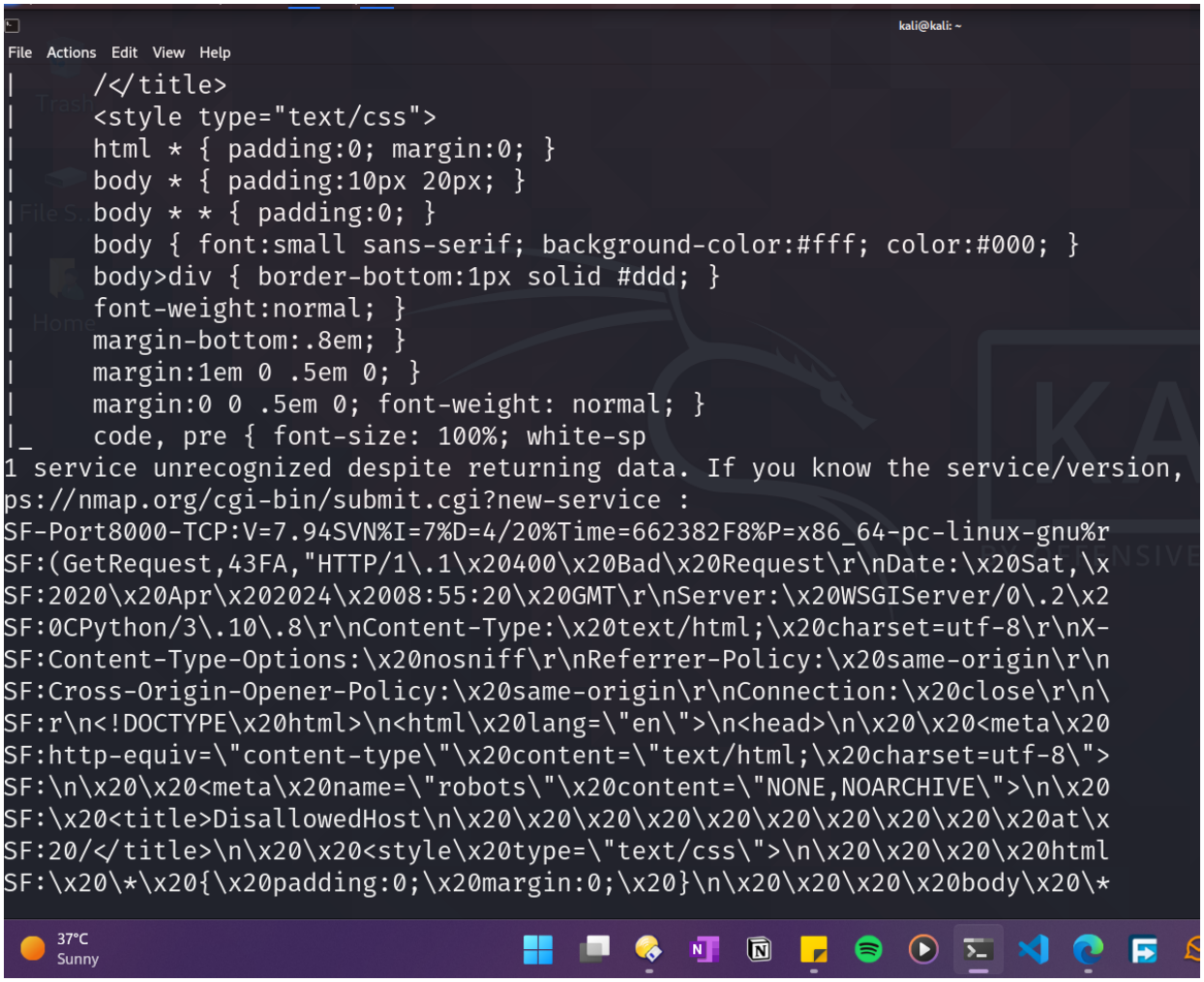

Figure 10: Get IP Address

5.11

Syntax

$

Command

$

Purpose

Output

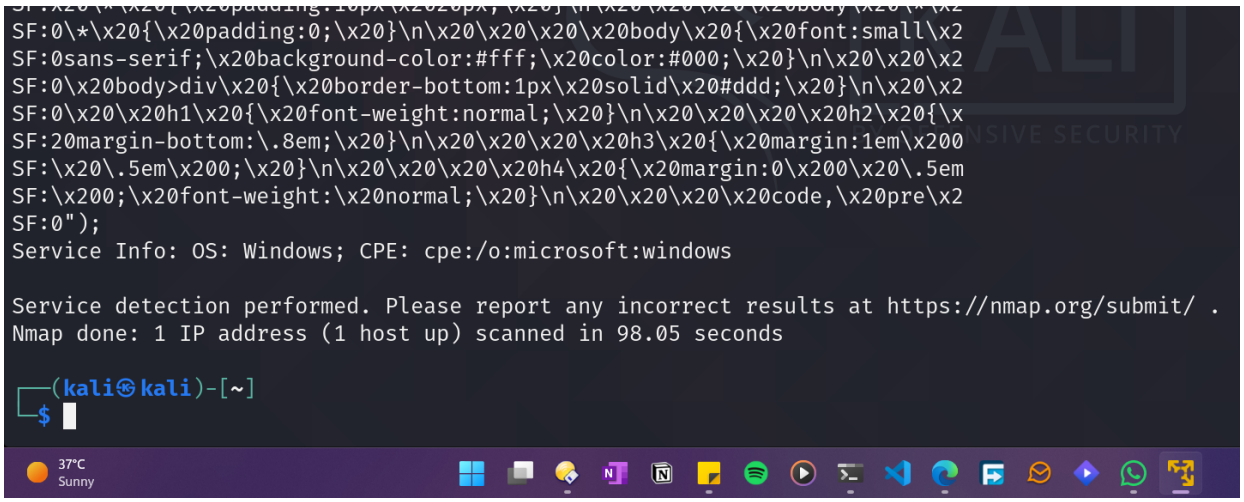

Figure 11: Get IP Address

5.12

Syntax

$

Command

$

Purpose

Output

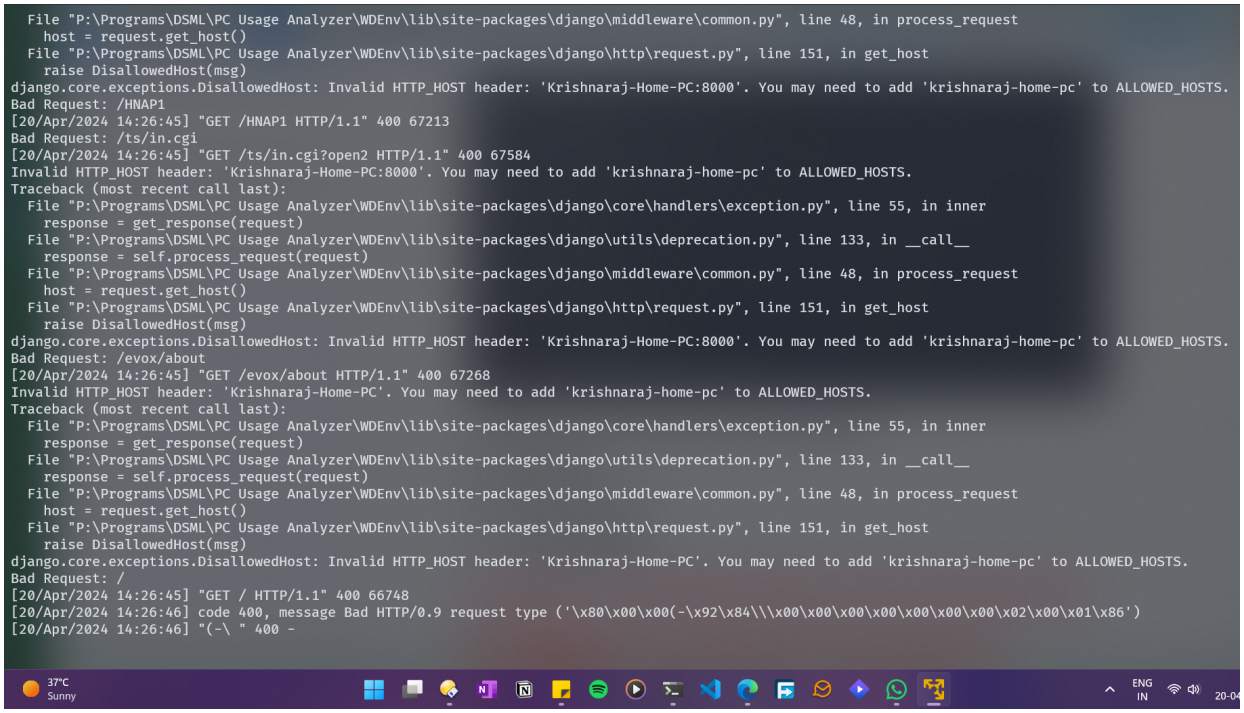

Figure 12: Get IP Address

5.13

Syntax

$

Command

$

Purpose

Output

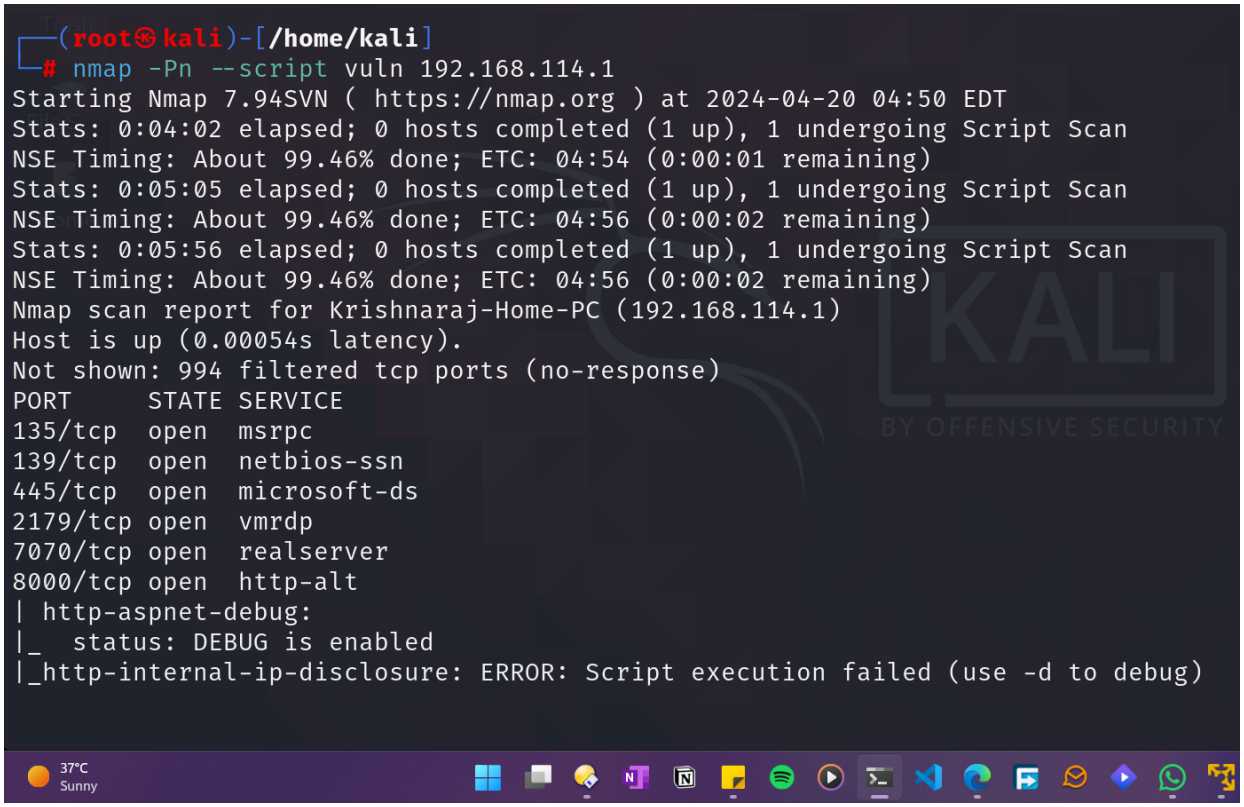

Figure 13: Get IP Address

5.14

Syntax

$

Command

$

Purpose

Output

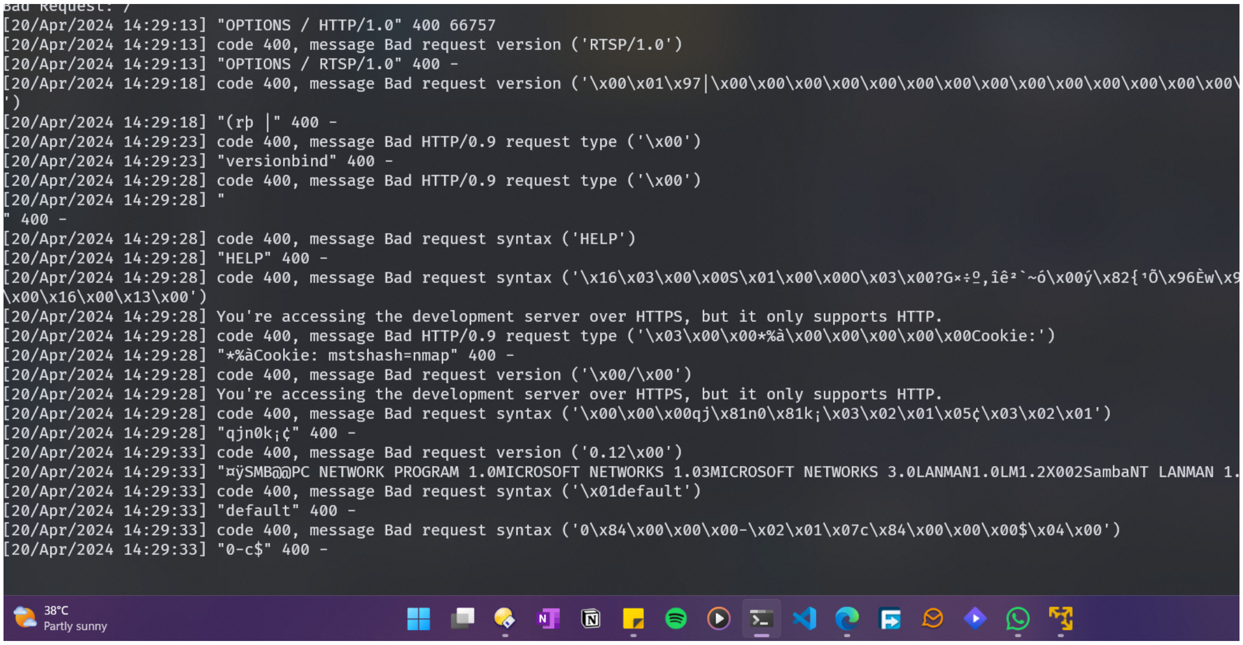

Figure 14: Get IP Address

5.15

Syntax

$

Command

$

Purpose

Output

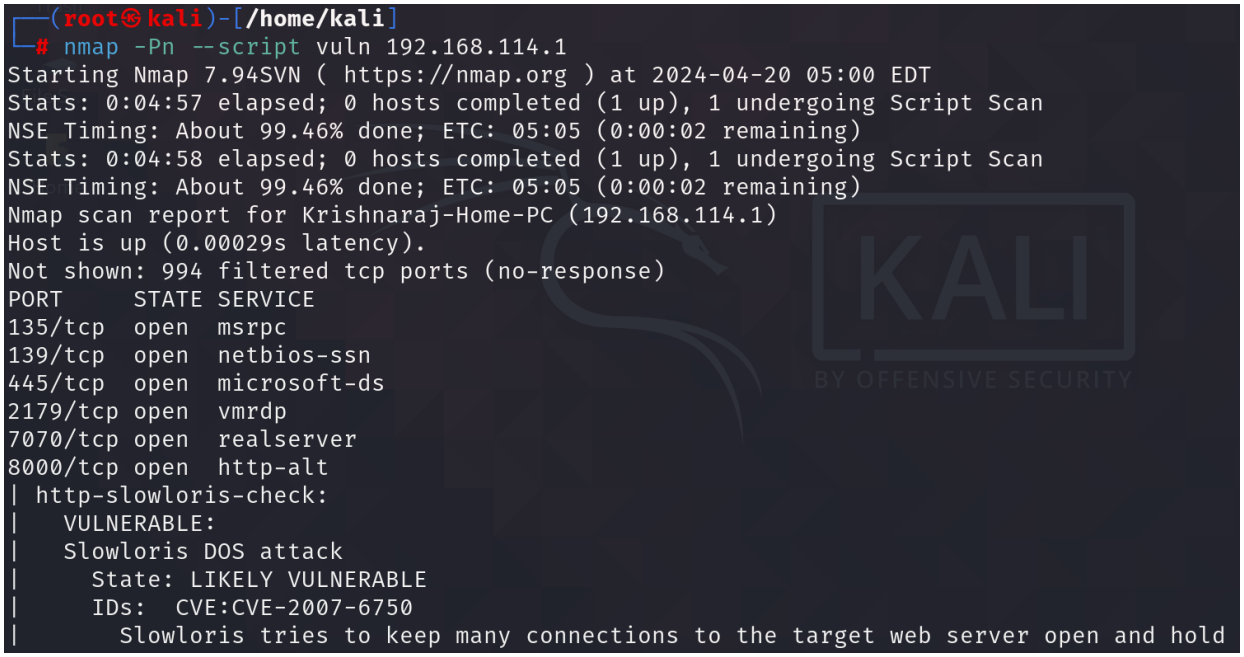

Figure 15: Get IP Address

5.16

Syntax

$

Command

$

Purpose

Output

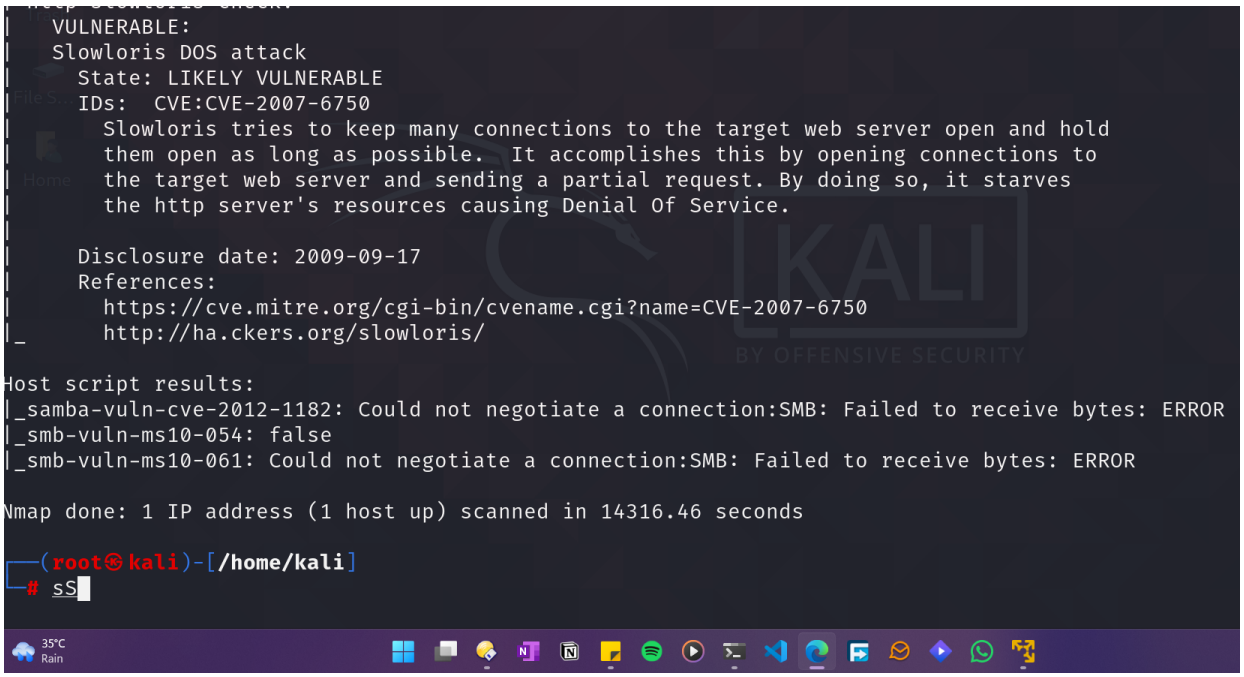

Figure 16: Get IP Address

5.17

Syntax

$

Command

$

Purpose

Output

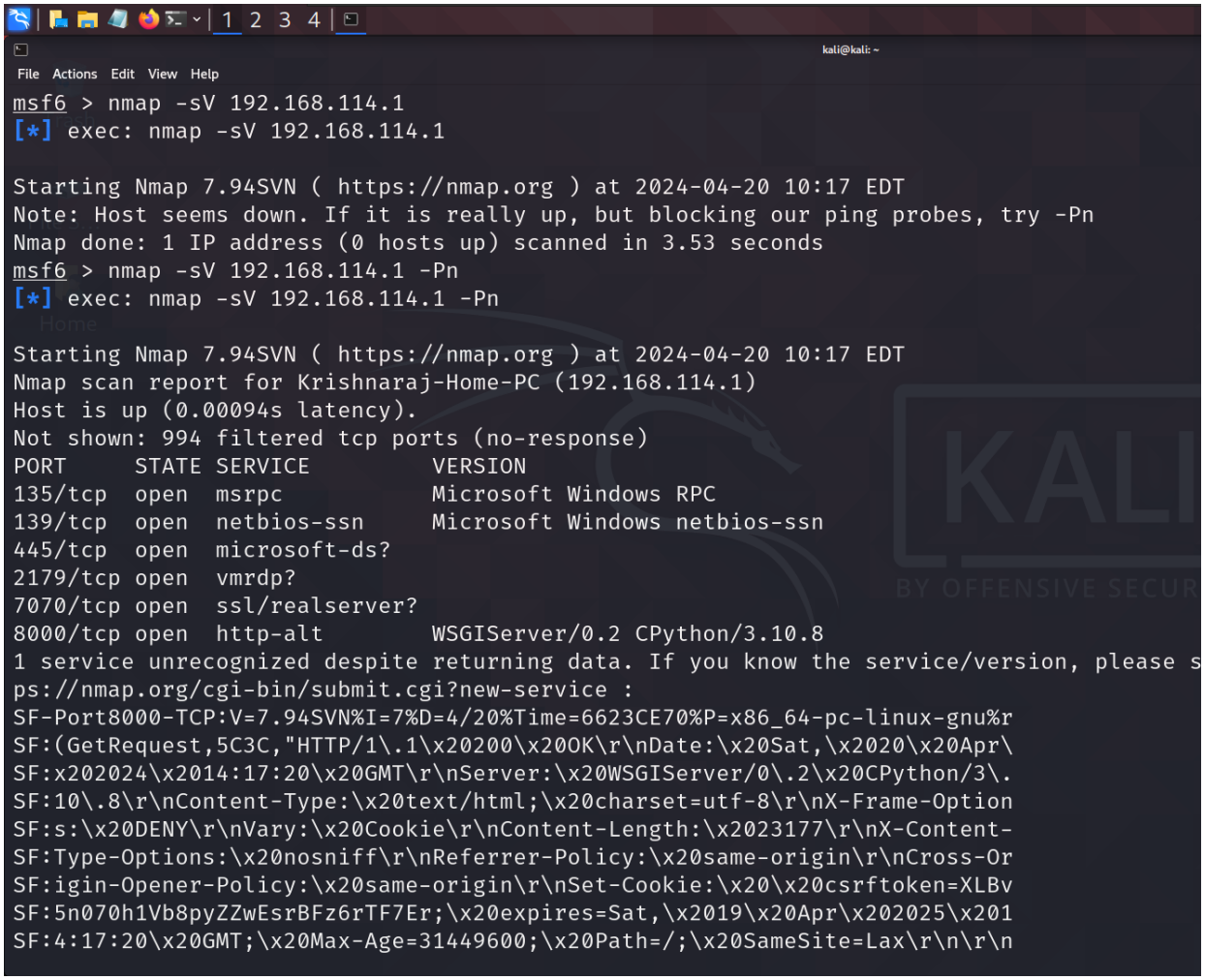

Figure 17: Get IP Address

5.18

Syntax

$

Command

$

Purpose

Output

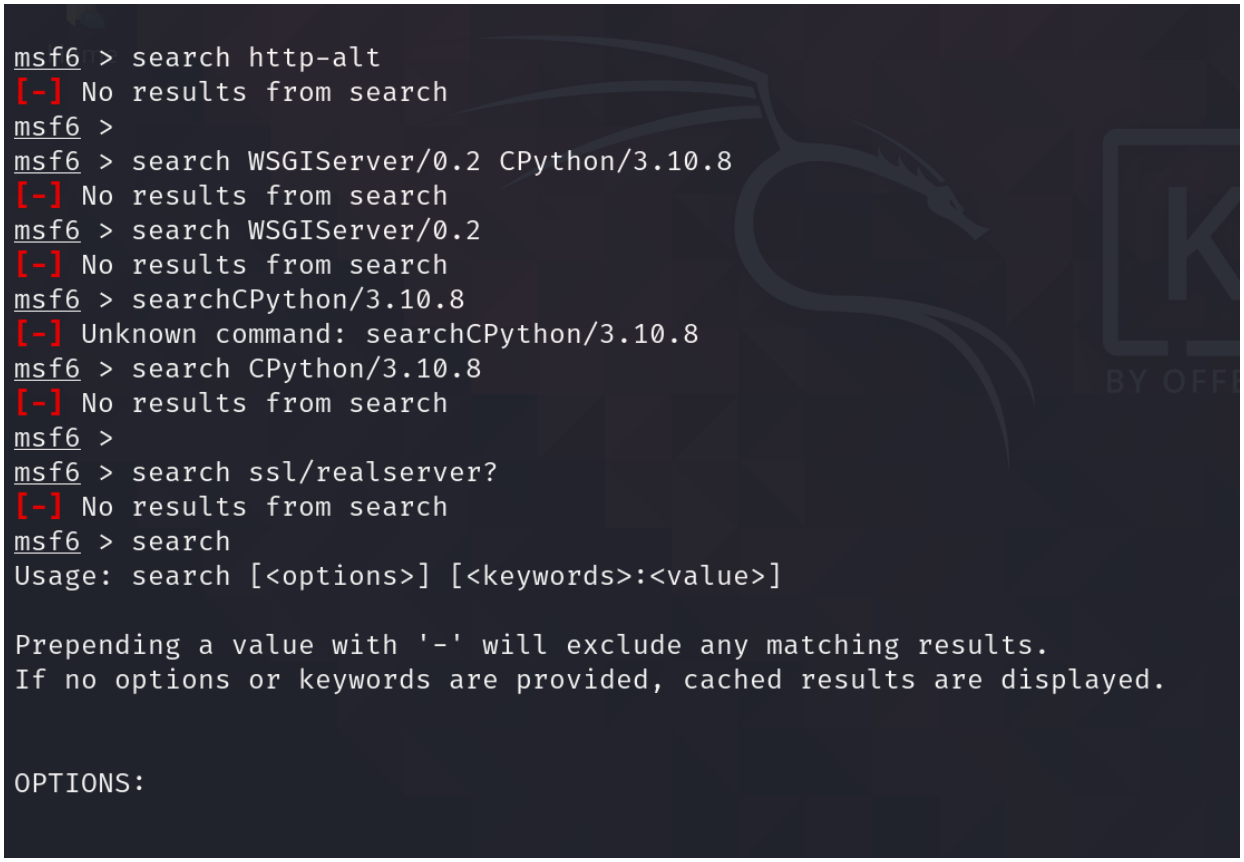

Figure 18: Get IP Address

5.19

Syntax

$

Command

$

Purpose

Output

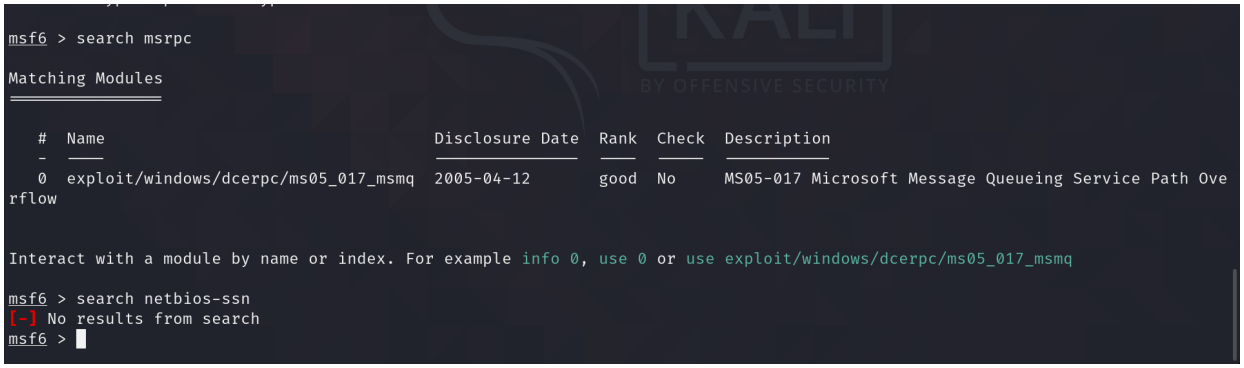

Figure 19: Get IP Address

5.20

Syntax

$

Command

$

Purpose

Output

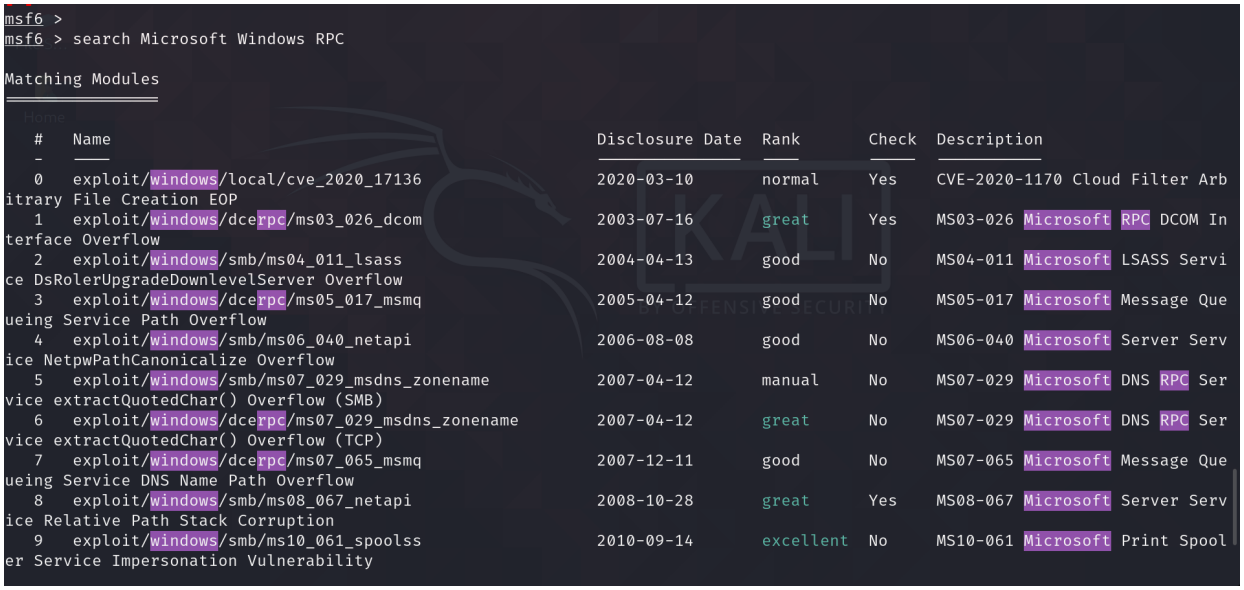

Figure 20: Get IP Address

5.21

Syntax

$

Command

$

Purpose

Output

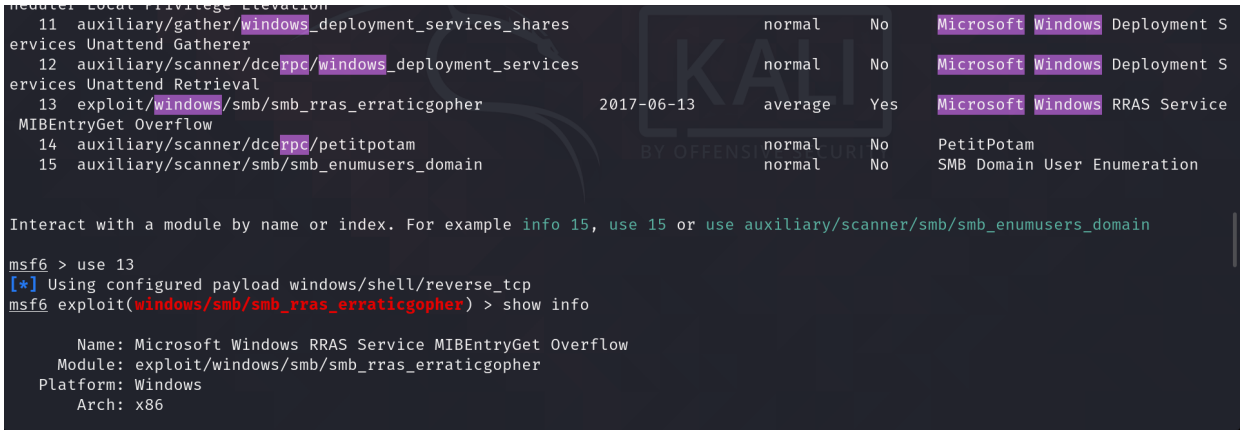

Figure 21: Get IP Address

5.22

Syntax

$

Command

$

Purpose

Output

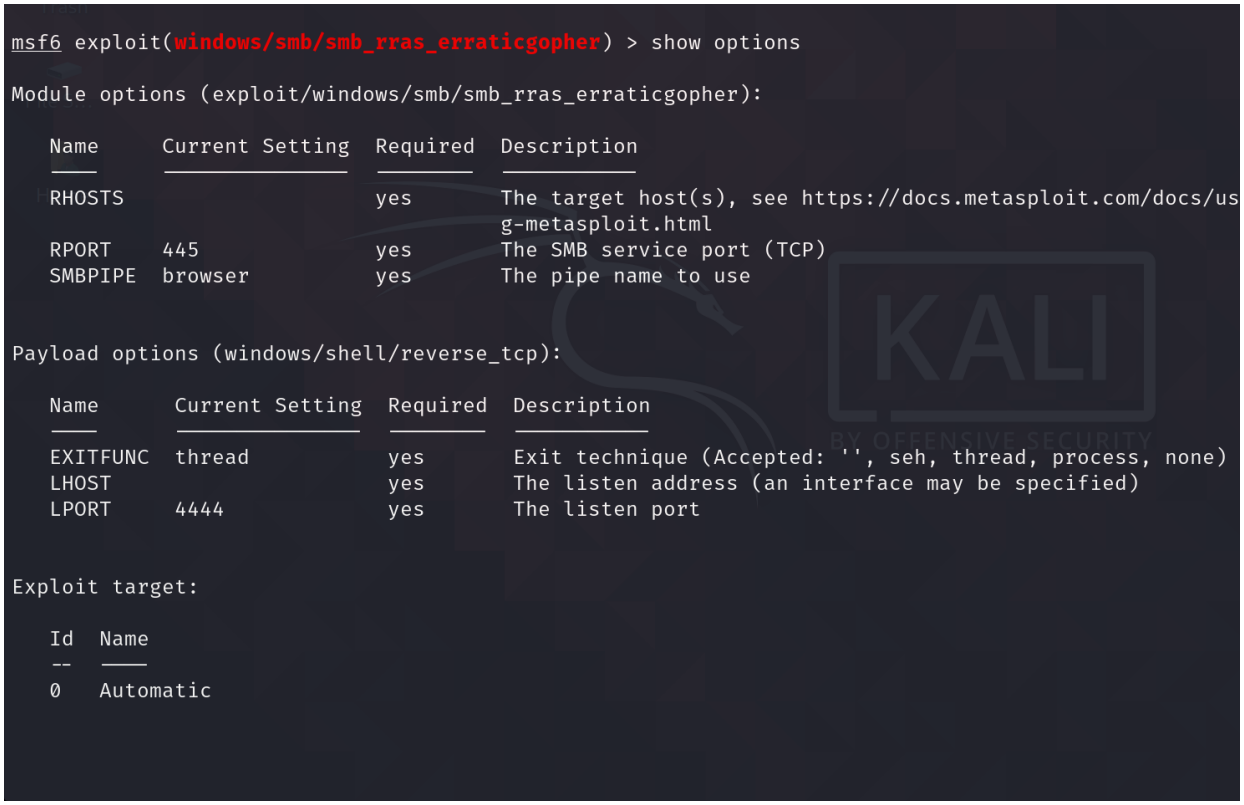

Figure 22: Get IP Address

5.23

Syntax

$

Command

$

Purpose

Output

```
msf6 exploit(windows/smb/smb_rras_erraticgopher) > set rhosts 192.168.114.1
rhosts ⇒ 192.168.114.1
msf6 exploit(windows/smb/smb_rras_erraticgopher) > show options

Module options (exploit/windows/smb/smb_rras_erraticgopher):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.114.1    yes       The target host(s), see https://docs.met
                                       g-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  browser          yes       The pipe name to use
```

Figure 23: Get IP Address

5.24

Syntax

$

Command

$

Purpose

Output

```
msf6 exploit(windows/smb/smb_rras_erraticgopher) > use 12
msf6 auxiliary(scanner/dcerpc/windows_deployment_services) > show options

Module options (auxiliary/scanner/dcerpc/windows_deployment_services):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                       g-metasploit.html
   RPORT    5040             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/dcerpc/windows_deployment_services) > set rhosts 192.168.114.1
rhosts ⇒ 192.168.114.1
msf6 auxiliary(scanner/dcerpc/windows_deployment_services) > exploit

[*] 192.168.114.1:5040    - Binding to 1A927394-352E-4553-AE3F-7CF4AAFCA620:1.0@ncacn_ip_tcp:192.168.114.1[5040] ...
[-] 192.168.114.1:5040    - 192.168.114.1:5040 Connection Error: The connection with (192.168.114.1:5040) timed out.
[*] 192.168.114.1:5040    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/dcerpc/windows_deployment_services) >
```

Figure 24: Get IP Address

5.25

Syntax

$

Command

$

Purpose

Output

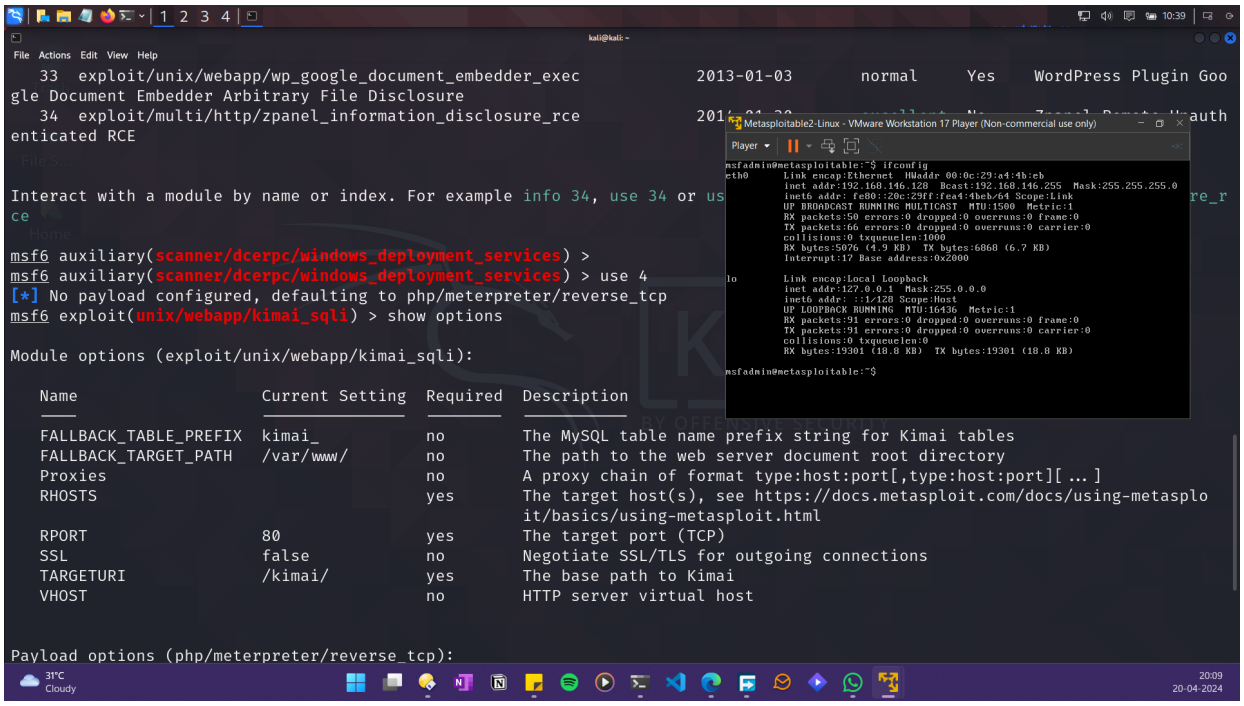

Figure 25: Get IP Address

5.26

Syntax

$

Command

$

Purpose

Output

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/kimai_sqli) > set rhosts 192.168.146.128
rhosts ⇒ 192.168.146.128
msf6 exploit(unix/webapp/kimai_sqli) > set rport 3306
rport ⇒ 3306
msf6 exploit(unix/webapp/kimai_sqli) >
```

Figure 26: Get IP Address

5.27

Syntax

$

Command

$

Purpose

Output

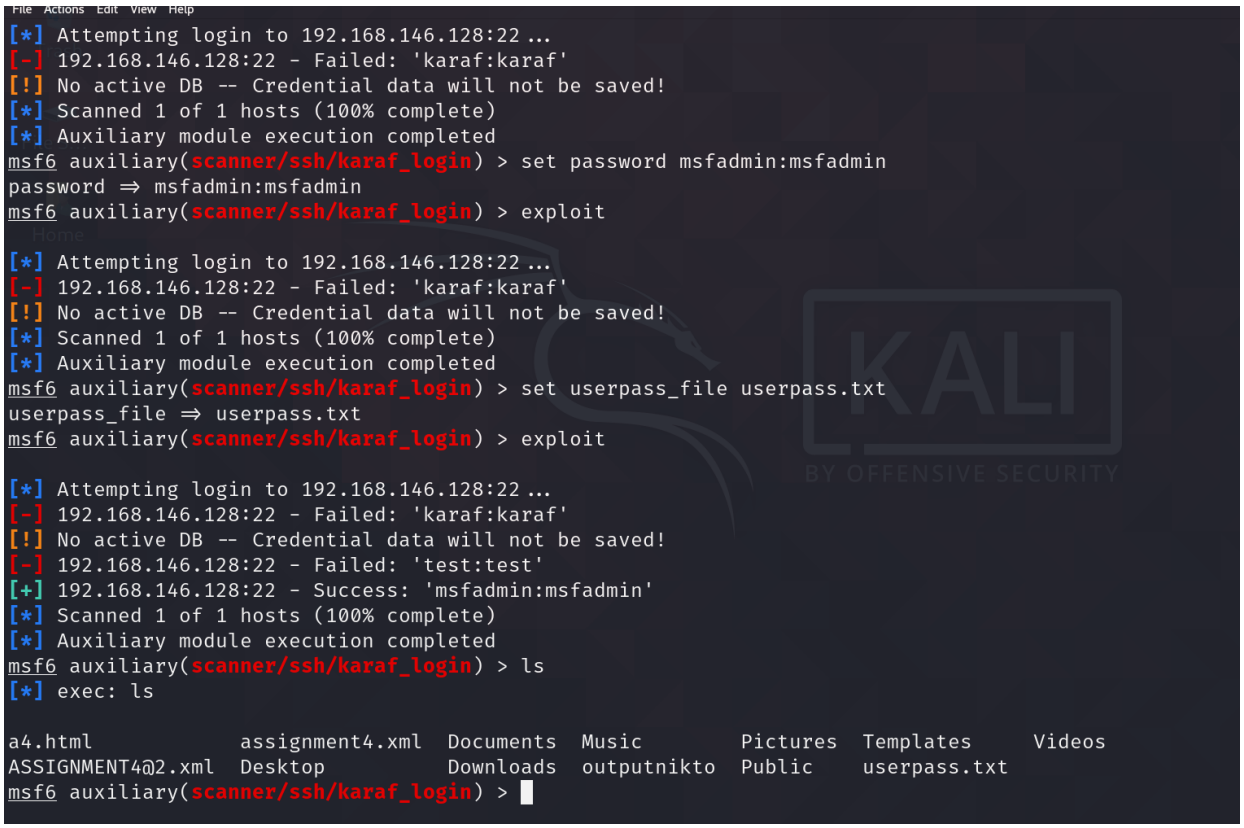

Figure 27: Get IP Address

5.28

Syntax

$

Command

$

Purpose

Output

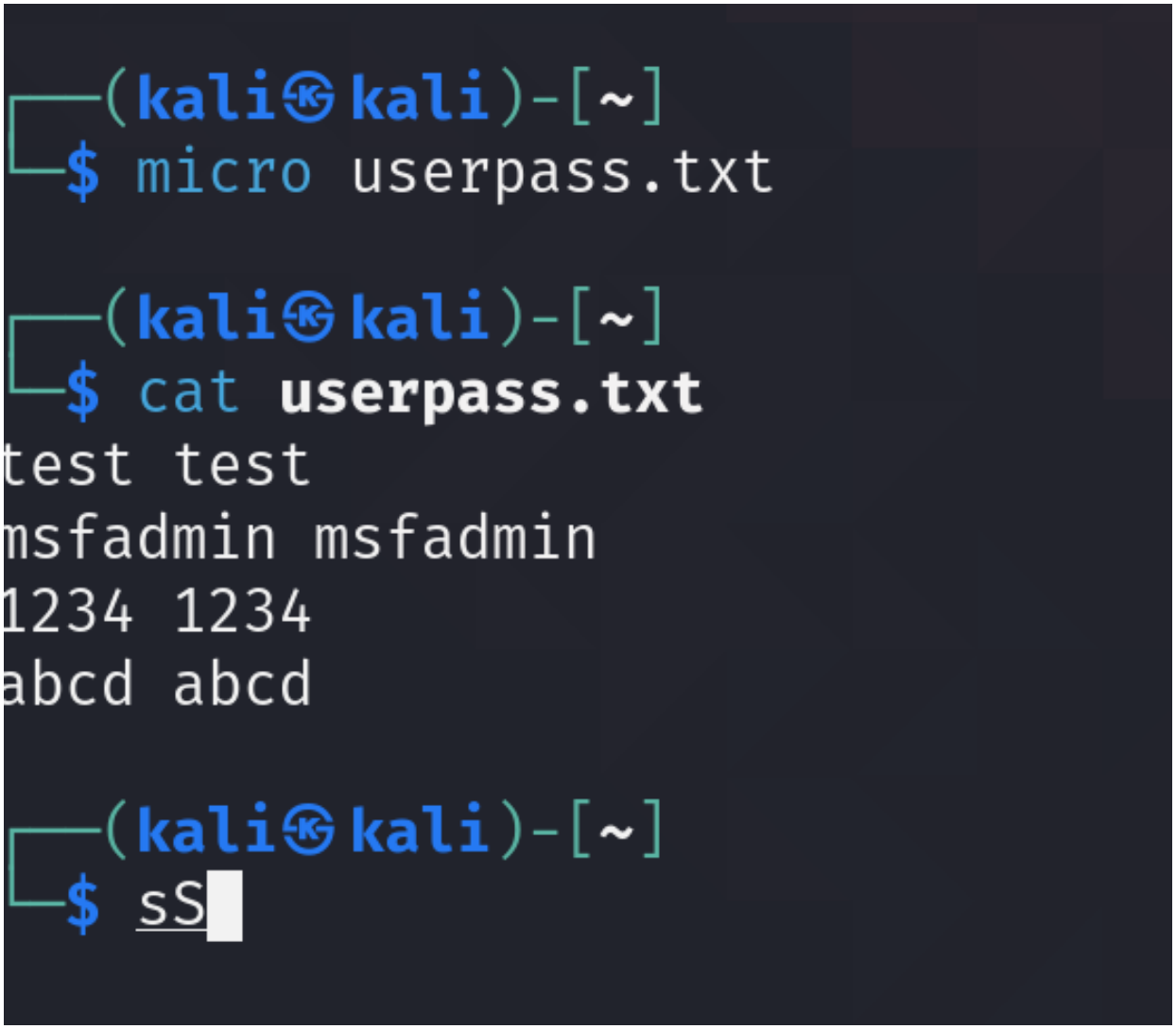

Figure 28: Get IP Address

5.29

Syntax

$

Command

$

Purpose

Output

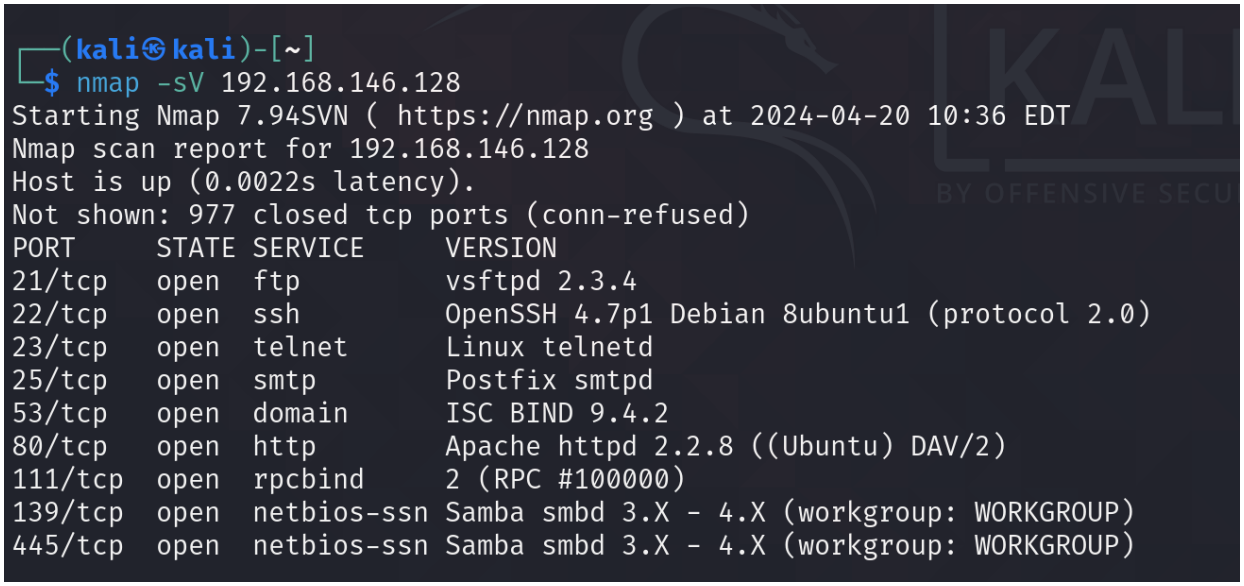

Figure 29: Get IP Address

5.30

Syntax

$

Command

$

Purpose

Output

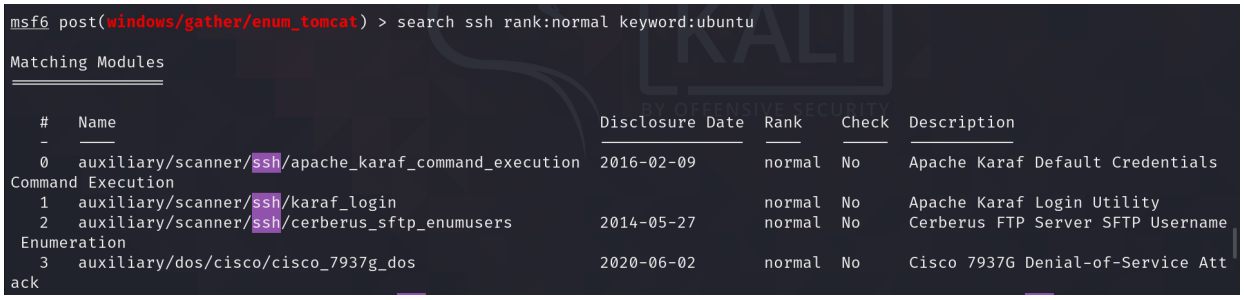

Figure 30: Get IP Address

6 Platform

Operating System: Arch Linux X8664
IDEs or Text Editors Used: Visual Studio Code

7 FAQs

1. Explanation of vulnerabilities:
    - CSRF (Cross-Site Request Forgery) - Exploits a user's authenticated session to perform unauthorized actions.
    - SSRF (Server-Side Request Forgery) - Allows attackers to send crafted requests from the server, potentially accessing internal resources.
    - XSS (Cross-Site Scripting) - Injects malicious scripts into web pages viewed by other users, leading to data theft or manipulation.
    - DOM-based XSS - Occurs when client-side scripts manipulate the DOM in an unsafe way, leading to XSS vulnerabilities.
    - Slowloris Attack - Exploits server-side vulnerabilities by keeping many connections open simultaneously, exhausting resources.
    - SQL Injection - Exploits vulnerabilities in database query interfaces to execute arbitrary SQL code.
    - Remote Code Execution (RCE) - Allows attackers to execute arbitrary code on a target system remotely.
    - Directory Traversal - Exploits insecure file path handling to access files outside of the intended directory.
2. Usage of Metasploit Framework:
    - Metasploit Framework is used for penetration testing and exploit development, allowing testers to identify and exploit vulnerabilities in target systems.
3. Modules supported by Metasploit Framework:
    - Metasploit Framework supports various modules for exploit development, post-exploitation, payload generation, auxiliary scanning, and evasion techniques.

8 Conclusion

In this Assignment, we explored the importance of gathering network information from an attacker's perspective using tools like nmap and Metasploit. We discussed the uses, advantages, and disadvantages of these tools and demonstrated their implementation through practical examples. By understanding the capabilities and limitations of these tools, security professionals can enhance their network reconnaissance and penetration testing activities to identify vulnerabilities and improve defense strategies.