

MIT WORLD PEACE UNIVERSITY

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

NETWORK SERVICE SCANNING WITH NMAP IN
XML AND HTML FORMAT

ASSIGNMENT 4

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

April 20, 2024

Contents

1	Aim	1
2	Objectives	1
3	Theory	1
3.1	XML Format	1
3.2	Uses	1
3.3	Advantages	1
3.4	Disadvantages	2
4	Implementation	2
4.1	2
4.2	3
4.3	4
4.4	5
4.5	6
4.6	7
4.7	8
4.8	9
5	Platform	10
6	FAQs	10
7	Conclusion	11

1 Aim

To Discover Network service to Organize and sort through Nmap scan output

2 Objectives

1. To Discover Network service
2. To Organize and sort through Nmap scan output
3. To Generate Nmap scan output in XML and HTML format

3 Theory

3.1 XML Format

XML stands for eXtensible Markup Language. It was designed to store and transport data. It was designed to be both human- and machine-readable. XML plays an important role in many different IT systems. It is used to store data, to configure programs, and to create user interfaces. XML is often used for distributing data over the Internet. It is important to note that XML is not a replacement for HTML. XML and HTML were designed with different goals.

3.2 Uses

- Storing and transporting data in a structured format.
- Configuring programs and defining settings in a readable manner.
- Creating user interfaces and defining document structures.
- Exchanging data between different systems and platforms.
- Representing data hierarchies and relationships in a standardized format.

3.3 Advantages

- Human-readable format, making it easy to understand and modify by developers and users.
- Machine-readable format, allowing for automated processing and interoperability between systems.
- Platform-independent, enabling data exchange between different operating systems and software applications.
- Extensibility, allowing users to define custom tags and structures to meet specific requirements.
- Well-defined syntax and rules, ensuring consistency and reliability in data representation.

3.4 Disadvantages

- Verbosity, as XML documents can become large and complex due to the use of tags and attributes.
- Overhead, as XML parsing and processing may require additional computational resources compared to other data formats.
- Lack of native support for complex data types and structures, leading to the need for custom solutions or additional standards (e.g., XML Schema).
- Limited support for binary data, as XML is primarily designed for text-based data representation.
- Potential security risks, such as XML External Entity (XXE) attacks, if not properly validated and sanitized.

4 Implementation

4.1

Syntax

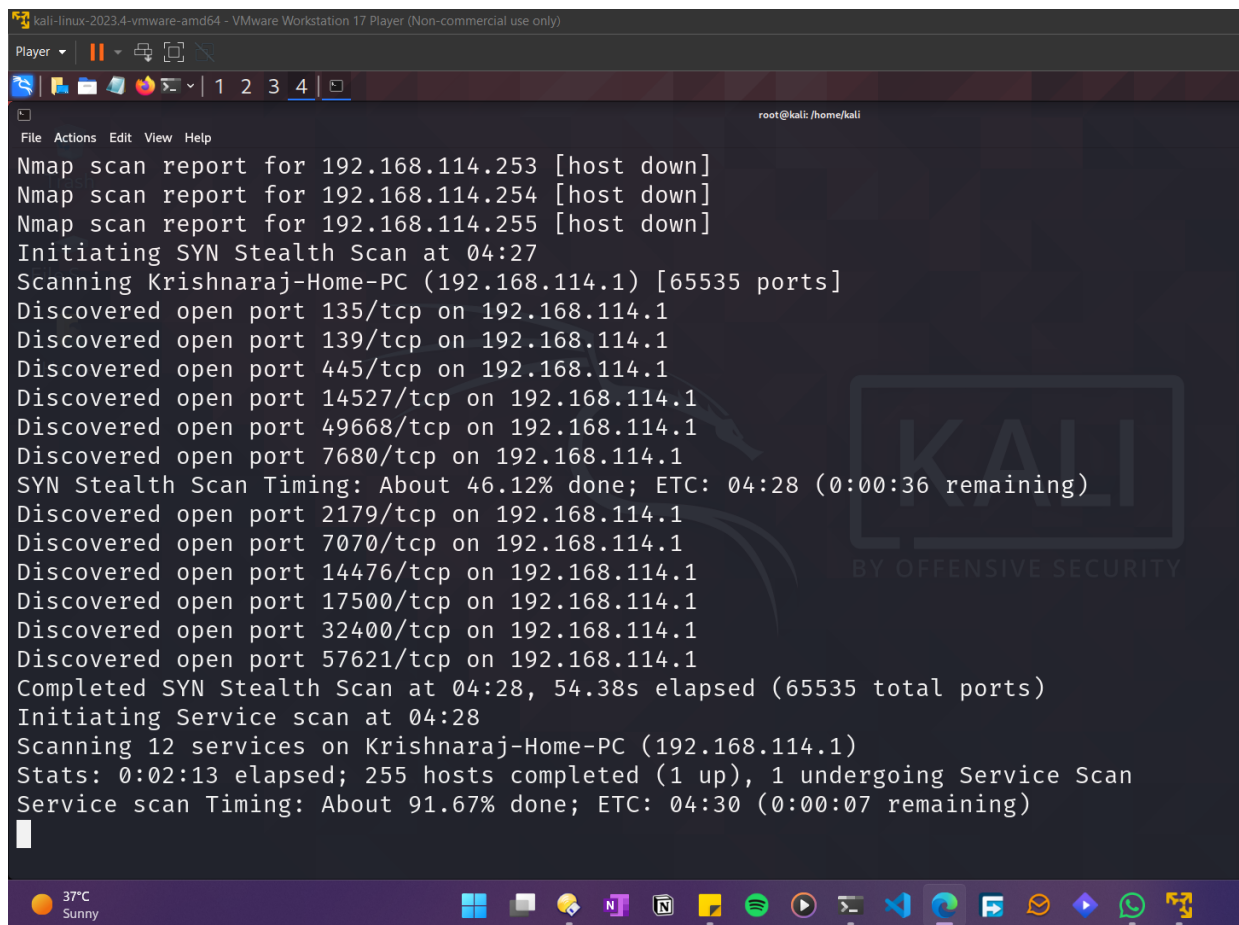
\$

Command

\$

Purpose

Output



```
kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
root@kali: /home/kali
Nmap scan report for 192.168.114.253 [host down]
Nmap scan report for 192.168.114.254 [host down]
Nmap scan report for 192.168.114.255 [host down]
Initiating SYN Stealth Scan at 04:27
Scanning Krishnaraj-Home-PC (192.168.114.1) [65535 ports]
Discovered open port 135/tcp on 192.168.114.1
Discovered open port 139/tcp on 192.168.114.1
Discovered open port 445/tcp on 192.168.114.1
Discovered open port 14527/tcp on 192.168.114.1
Discovered open port 49668/tcp on 192.168.114.1
Discovered open port 7680/tcp on 192.168.114.1
SYN Stealth Scan Timing: About 46.12% done; ETC: 04:28 (0:00:36 remaining)
Discovered open port 2179/tcp on 192.168.114.1
Discovered open port 7070/tcp on 192.168.114.1
Discovered open port 14476/tcp on 192.168.114.1
Discovered open port 17500/tcp on 192.168.114.1
Discovered open port 32400/tcp on 192.168.114.1
Discovered open port 57621/tcp on 192.168.114.1
Completed SYN Stealth Scan at 04:28, 54.38s elapsed (65535 total ports)
Initiating Service scan at 04:28
Scanning 12 services on Krishnaraj-Home-PC (192.168.114.1)
Stats: 0:02:13 elapsed; 255 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 04:30 (0:00:07 remaining)
```

Figure 1: Get IP Address

4.2

Syntax

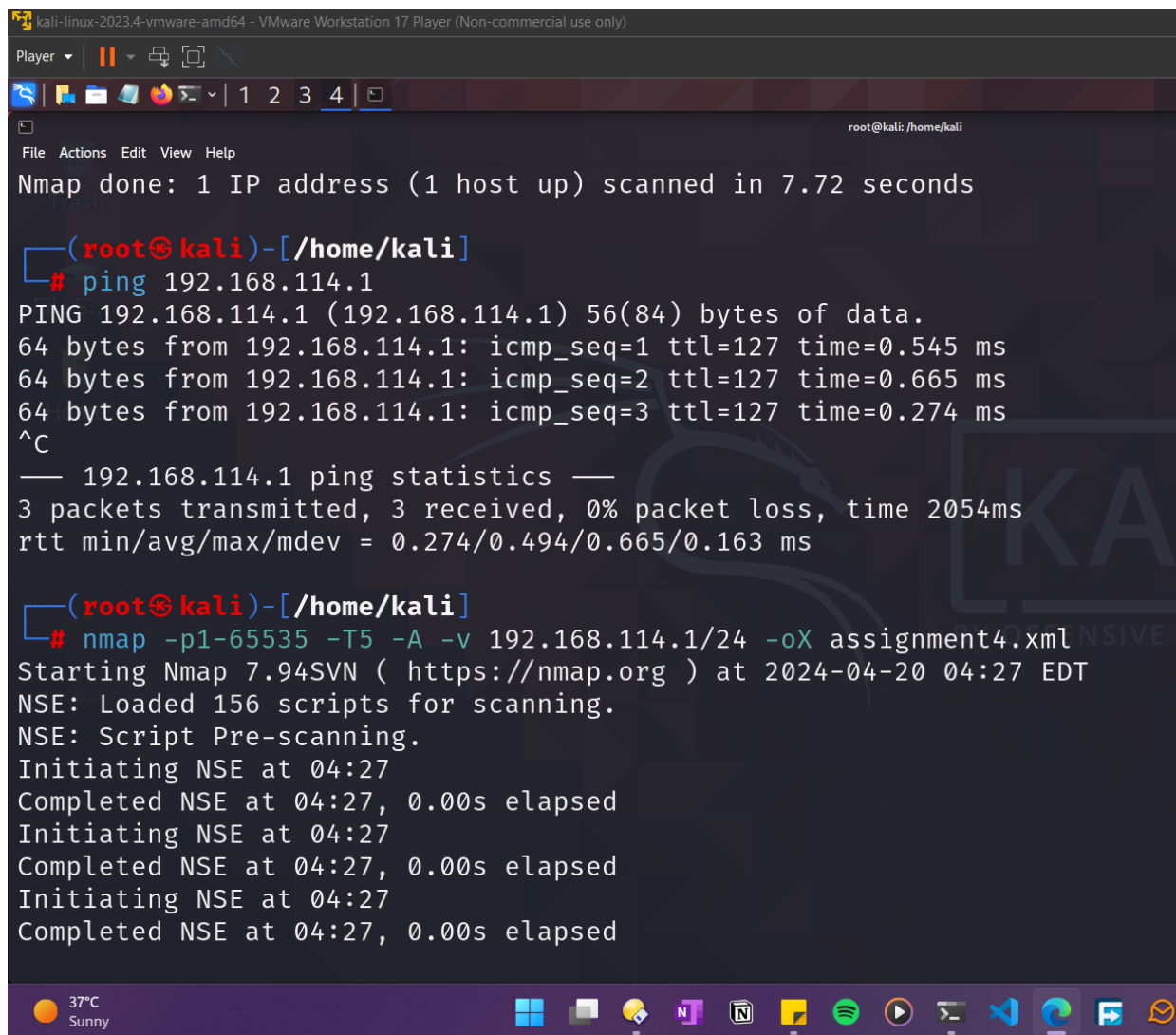
\$

Command

\$

Purpose

Output

A screenshot of a Kali Linux terminal window running inside a VMware Workstation 17 Player. The terminal shows the output of an Nmap scan and a ping command. The Nmap scan was performed on 192.168.114.1/24, and the ping command was used to test connectivity to 192.168.114.1. The terminal output is as follows:

```
kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 7.72 seconds

(root@kali)-[/home/kali]
# ping 192.168.114.1
PING 192.168.114.1 (192.168.114.1) 56(84) bytes of data.
64 bytes from 192.168.114.1: icmp_seq=1 ttl=127 time=0.545 ms
64 bytes from 192.168.114.1: icmp_seq=2 ttl=127 time=0.665 ms
64 bytes from 192.168.114.1: icmp_seq=3 ttl=127 time=0.274 ms
^C
— 192.168.114.1 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.274/0.494/0.665/0.163 ms

(root@kali)-[/home/kali]
# nmap -p1-65535 -T5 -A -v 192.168.114.1/24 -oX assignment4.xml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 04:27 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:27
Completed NSE at 04:27, 0.00s elapsed
Initiating NSE at 04:27
Completed NSE at 04:27, 0.00s elapsed
Initiating NSE at 04:27
Completed NSE at 04:27, 0.00s elapsed
```

Figure 2: Get IP Address

4.3

Syntax

\$

Command

\$

Purpose

Output

```

kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
root@kali:~/homekali
SF:173,"HTTP/1.1\x20401\x20Unauthorized\r\nX-Plex-Protocol:\x201.0\r\nC
SF:ontent-Length:\x20193\r\nContent-Type:\x20text/html\r\nConnection:\x20c
SF:lose\r\nCache-Control:\x20no-cache\r\nDate:\x20Sat,\x2020\x20Apr\x20202
SF:4\x2008:29:09\x20GMT\r\n\r\n<html><head><script>>window.location\x20=\x
SF:20window.location.href.match(/^(^\.|+\/|\/)[^\/\]*$/)[1]\x2
SF:0+\'web/index.html\';</script><title>Unauthorized</title></head><bo
SF:dy><h1>401\x20Unauthorized</h1></body></html>")%r(RPCCheck,109,"HTTP/1\
SF:.1\x20400\x20Bad\x20Request\r\nX-Plex-Protocol:\x201.0\r\nContent-Leng
SF:th:\x2089\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nCach
SF:e-Control:\x20no-cache\r\nDate:\x20Sat,\x2020\x20Apr\x202024\x2008:29:1
SF:2\x2008:29:09\x20GMT\r\n\r\n<html><head><title>Bad\x20Request</title></head><body><
SF:h1>400\x20Bad\x20Request</h1></body></html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2022|2008 (90%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows 11 21H2 (90%), Microsoft Windows 10 (87%), Microsoft Windows Server 20
22 (86%), Microsoft Windows Server 2008 R2 (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 2.505 days (since Wed Apr 17 16:23:31 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
37°C Sunny 1402 20-04-2024

```

Figure 3: Get IP Address

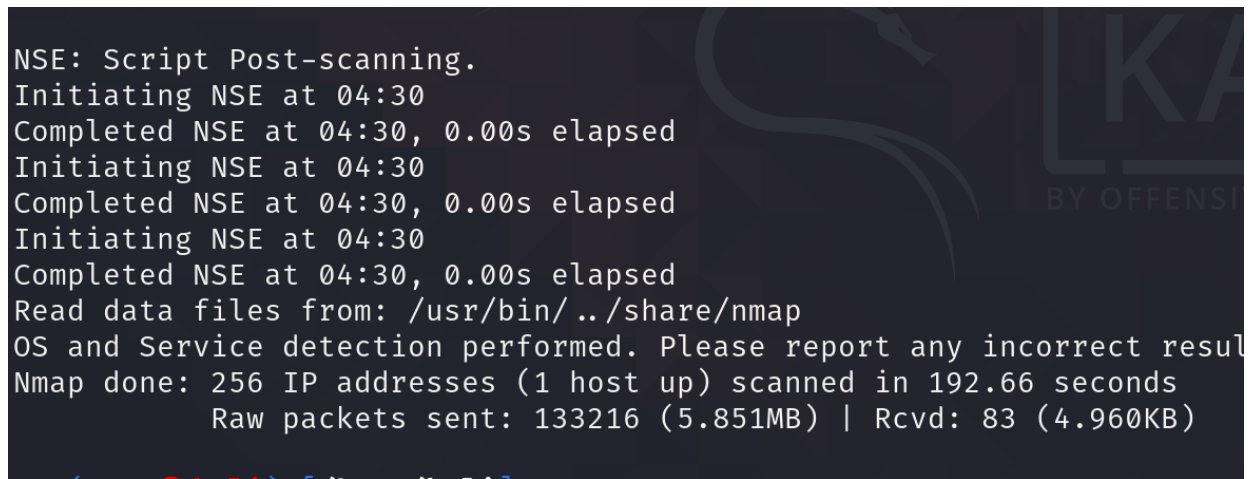
4.4

Syntax

\$

Command

\$

Purpose**Output**A terminal window with a dark background and light-colored text. The text shows the output of an NSE script post-scanning process. It includes three iterations of 'Initiating NSE' and 'Completed NSE' at 04:30 with 0.00s elapsed. It then shows the path for nmap data files, a message about OS and service detection, and finally the completion of the scan for 256 IP addresses in 192.66 seconds, with raw packet statistics.

```
NSE: Script Post-scanning.  
Initiating NSE at 04:30  
Completed NSE at 04:30, 0.00s elapsed  
Initiating NSE at 04:30  
Completed NSE at 04:30, 0.00s elapsed  
Initiating NSE at 04:30  
Completed NSE at 04:30, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
OS and Service detection performed. Please report any incorrect results  
Nmap done: 256 IP addresses (1 host up) scanned in 192.66 seconds  
Raw packets sent: 133216 (5.851MB) | Rcvd: 83 (4.960KB)
```

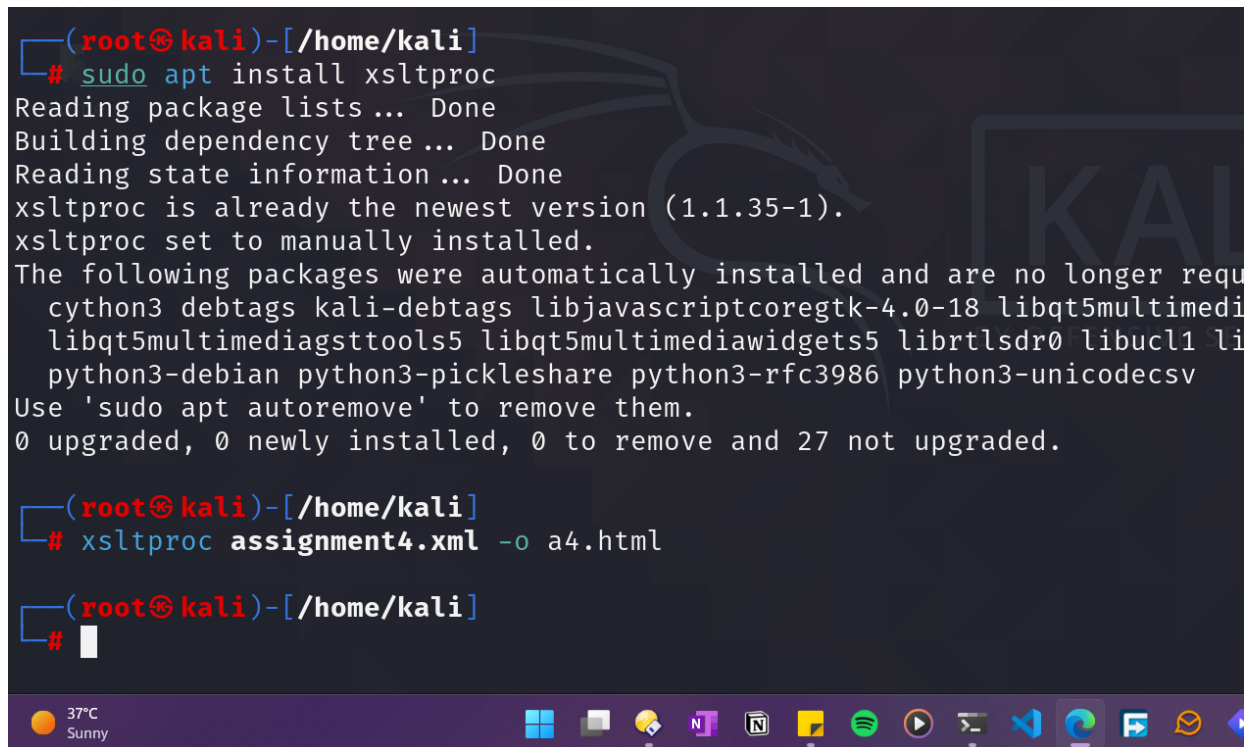
Figure 4: Get IP Address

4.5**Syntax**

\$

Command

\$

Purpose**Output**

```
(root@kali)-[/home/kali]
# sudo apt install xsltproc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xsltproc is already the newest version (1.1.35-1).
xsltproc set to manually installed.
The following packages were automatically installed and are no longer required:
  cython3 debtags kali-debtags libjavascriptcoregtk-4.0-18 libqt5multimedia5
  libqt5multimedia5gsttools5 libqt5multimediawidgets5 librtlsdr0 libucl1 libucl1-dev
  python3-debian python3-pickleshare python3-rfc3986 python3-unicodedsv
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 27 not upgraded.

(root@kali)-[/home/kali]
# xsltproc assignment4.xml -o a4.html

(root@kali)-[/home/kali]
#
```

Figure 5: Get IP Address

4.6**Syntax**

\$

Command

\$

Purpose

Output

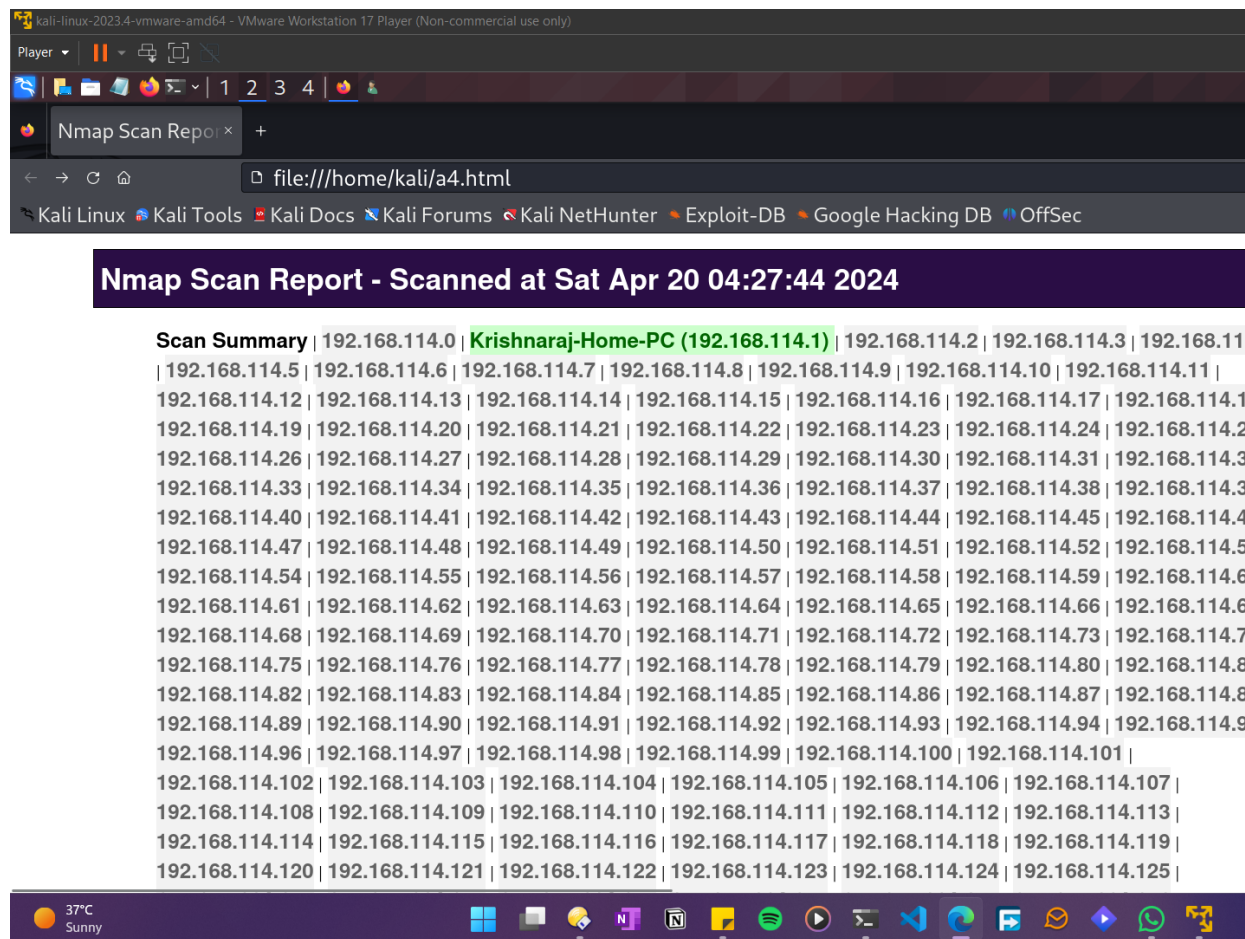


Figure 6: Get IP Address

4.7

Syntax

\$

Command

\$

Purpose

Output

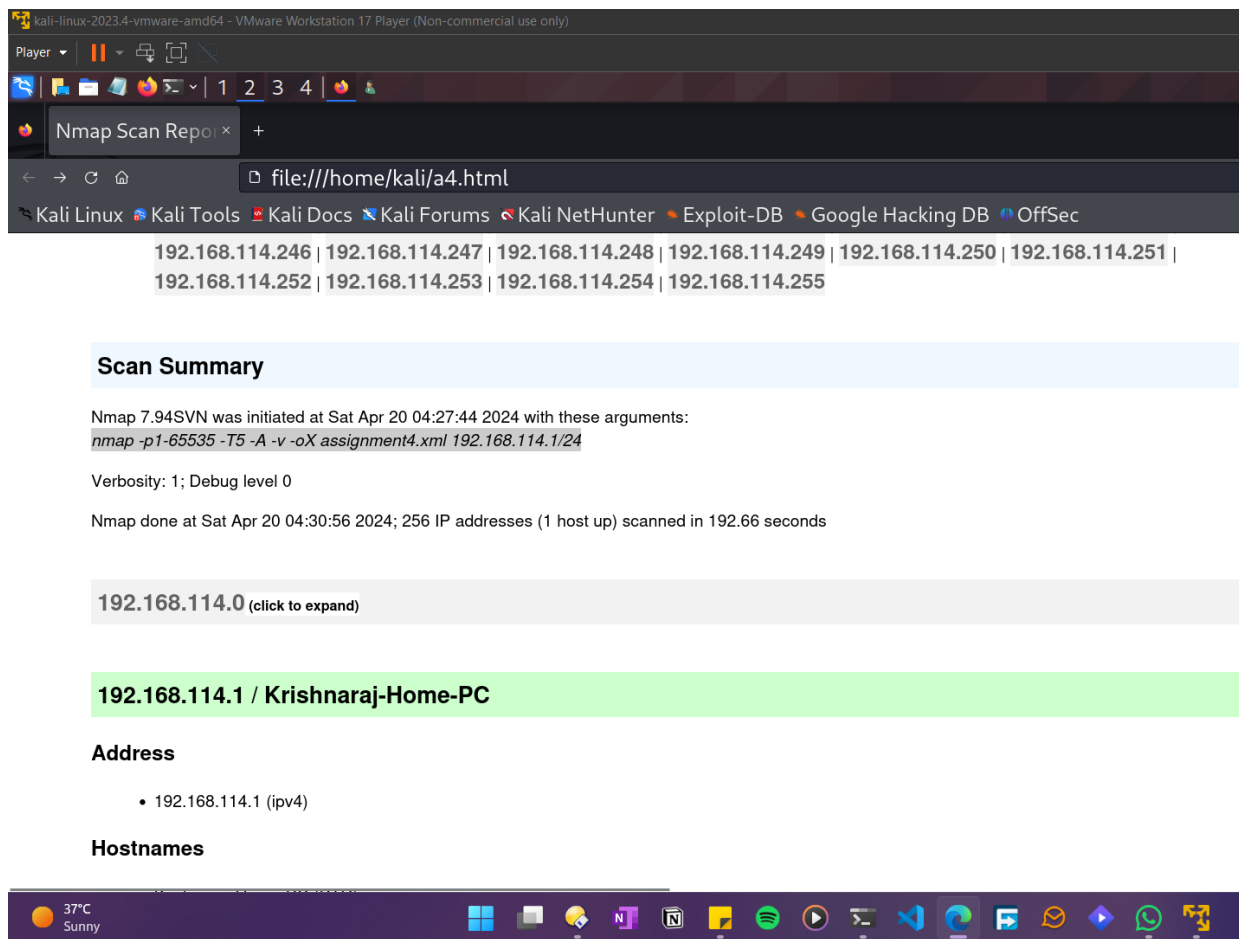


Figure 7: Get IP Address

4.8

Syntax

\$

Command

\$

Purpose

Output

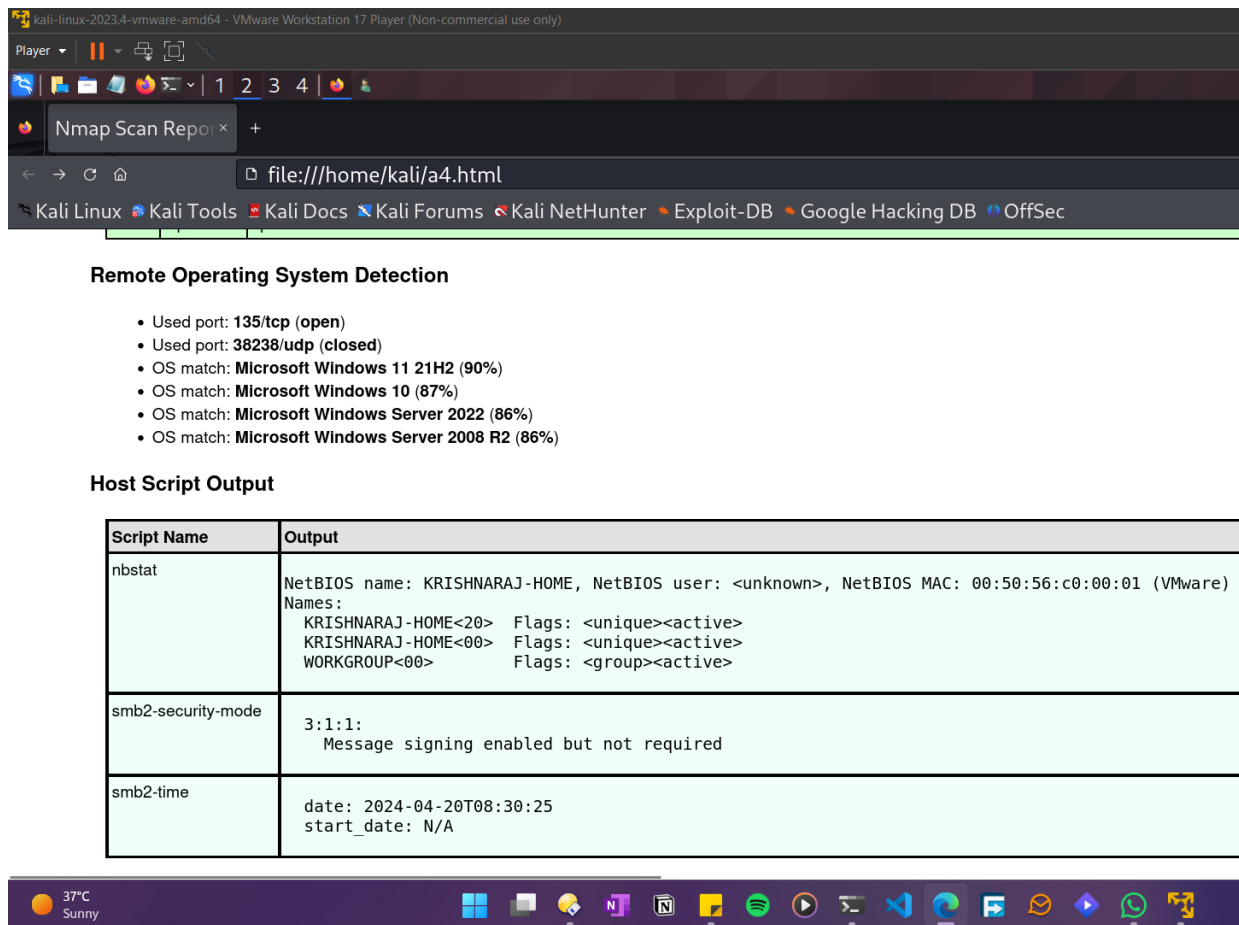


Figure 8: Get IP Address

5 Platform

Operating System: Arch Linux X8664

IDEs or Text Editors Used: Visual Studio Code

6 FAQs

1. What is the meaning of subnet?

- Subnet: Division of an IP network for efficient resource management.
- Facilitates organization and management of network devices and addresses.

2. Explain subnet mask? Meaning of /8, /16, /24, /32?

- Subnet Mask: Binary pattern dividing IP address into network and host portions.

- /8, /16, /24, /32 denote network size, representing the number of bits in the subnet mask.

3. What is NSE? Explain it.

- NSE (Nmap Scripting Engine): Automates Nmap's functionality for network reconnaissance and exploitation.
- Provides a framework for writing and executing scripts to enhance scanning capabilities.

4. Different flags for output supported by nmap.

- Nmap Output Flags: Include -oN (normal), -oG (grepable), -oX (XML), and -oA (all formats).
- Allow users to customize the format and content of Nmap scan results for analysis and reporting.

5. What is xsltproc? Explain it.

- xsltproc: Command-line tool for transforming XML documents using XSLT stylesheets.
- Facilitates conversion of XML data into different formats such as HTML, text, or other XML formats.

6. Why to see the output in HTML format than XML?

- HTML Output: Provides visually appealing presentation of Nmap scan results compared to XML.
- Allows for easier interpretation and analysis of scan data through structured formatting and styling.

7 Conclusion

In this assignment, we learned about the importance of network service scanning and organizing Nmap scan output. We explored the generation of Nmap scan results in XML and HTML formats to facilitate data analysis and reporting. By leveraging the capabilities of Nmap and related tools, we can enhance our understanding of network vulnerabilities and security risks. This assignment provided valuable insights into the practical aspects of vulnerability identification and penetration testing, which are essential skills for cybersecurity professionals.