

MIT WORLD PEACE UNIVERSITY

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

---

---

INFORMATION GATHERING WITH SCANNING  
TOOLS

---

---

ASSIGNMENT 7

Prepared By

Krishnaraj Thadesar  
Cyber Security and Forensics  
Batch A1, PA 10

April 21, 2024

# Contents

<b>1</b>	<b>Aim</b>	<b>1</b>
<b>2</b>	<b>Objectives</b>	<b>1</b>
<b>3</b>	<b>Theory</b>	<b>1</b>
<b>4</b>	<b>whois</b>	<b>1</b>
4.1	Uses . . . . .	1
4.2	Advantages . . . . .	1
4.3	Disadvantages . . . . .	1
<b>5</b>	<b>Angry IP Scanner</b>	<b>2</b>
5.1	Uses . . . . .	2
5.2	Advantages . . . . .	2
5.3	Disadvantages . . . . .	2
<b>6</b>	<b>Metasploit</b>	<b>2</b>
6.1	Uses . . . . .	2
6.2	Mega Ping . . . . .	2
6.3	Disadvantages . . . . .	2
<b>7</b>	<b>Netscan Tools Pro</b>	<b>3</b>
7.1	Uses . . . . .	3
7.2	Advantages . . . . .	3
7.3	Disadvantages . . . . .	3
<b>8</b>	<b>Implementation</b>	<b>3</b>
8.1	whois . . . . .	3
8.2	whois . . . . .	4
8.3	Angry IP Scanner . . . . .	6
8.4	Metasploit . . . . .	6
8.5	Ports in Megaping . . . . .	9
8.6	IP Scanner in Megaping . . . . .	9
8.7	TraceRoute in Megaping . . . . .	10
8.8	IP Scanner in Range in Megaping . . . . .	10
8.9	NetScanTools Pro Demo Ping Scan Results in Browser . . . . .	11
<b>9</b>	<b>Platform</b>	<b>11</b>
<b>10</b>	<b>FAQs</b>	<b>11</b>
<b>11</b>	<b>Conclusion</b>	<b>12</b>

## **1 Aim**

To gather information about a target system using various scanning tools and techniques that include port scanners, network scanners etc.

## **2 Objectives**

1. To understand the concept of information gathering and reconnaissance.
2. To explore various scanning tools and techniques for network reconnaissance.
3. To perform network scanning and enumeration using tools like Nmap, Angry IP Scanner, and Metasploit.
4. To analyze the results of network scanning and identify potential vulnerabilities in target systems.
5. To understand the importance of information gathering in penetration testing and vulnerability assessment.

## **3 Theory**

## **4 whois**

### **4.1 Uses**

- Retrieves registration information for domain names and IP addresses.
- Helps identify the owner, registrar, and contact details associated with a domain or IP.
- Provides valuable information for network troubleshooting and security analysis.

### **4.2 Advantages**

- Provides comprehensive domain and IP registration details.
- Helps in identifying potential security threats and malicious actors.
- Useful for verifying ownership and contact information for legitimate purposes.

### **4.3 Disadvantages**

- Limited effectiveness for domains with privacy protection services.
- Accuracy of information may vary depending on the registrar's data accuracy.
- Requires caution in handling sensitive contact information to avoid misuse or privacy violations.

## 5 Angry IP Scanner

### 5.1 Uses

- Scans IP addresses and ports to discover active hosts and services on a network.
- Provides a quick and simple way to identify network devices and potential vulnerabilities.
- Offers fast scanning capabilities and a user-friendly interface for network reconnaissance.

### 5.2 Advantages

- Cross-platform compatibility, supporting Windows, macOS, and Linux.
- Lightweight and easy to use, suitable for both beginners and experienced users.
- Offers customization options and advanced features for network scanning and analysis.

### 5.3 Disadvantages

- Limited scanning options compared to more advanced tools like Nmap.
- May produce false positives or miss certain vulnerabilities in complex network environments.
- Lacks advanced features for detailed vulnerability assessment and exploitation.

## 6 Metasploit

### 6.1 Uses

- Penetration testing framework for identifying and exploiting vulnerabilities in target systems.
- Provides a wide range of exploit modules, payloads, and post-exploitation tools.
- Used by security professionals and researchers for ethical hacking, red teaming, and vulnerability assessment.

### 6.2 Mega Ping

- *This subsection does not appear to be relevant to Metasploit.*

### 6.3 Disadvantages

- Steep learning curve for beginners due to its complexity and extensive feature set.
- Requires caution and ethical considerations to avoid misuse and potential harm.
- May trigger false positives or lead to unintended consequences if not used carefully.

## 7 Nmap Tools Pro

### 7.1 Uses

- Comprehensive network scanning tool for discovering hosts, open ports, and services.
- Offers a wide range of scanning techniques and customization options.
- Provides detailed reports and analysis for network security assessment and troubleshooting.

### 7.2 Advantages

- User-friendly interface with intuitive features and workflows.
- Supports various scanning methods, including TCP, UDP, and SYN scanning.
- Offers real-time monitoring and reporting capabilities for network administrators.

### 7.3 Disadvantages

- Paid software, may require a license for full functionality.
- Limited platform support compared to open-source alternatives.
- May lack some advanced features available in other commercial network scanning tools.

## 8 Implementation

### 8.1 whois

#### Syntax

```
$ whois <domain_name>
```

#### Command

```
$ whois mitwpu.edu.in
```

#### Purpose

This command retrieves registration information for the specified domain name, including the owner, registrar, and contact details associated with the domain.

## Output

```
└─# whois mitwpu.edu.in
Domain Name: mitwpu.edu.in
Registry Domain ID: D414400000004565716-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2022-06-08T06:01:49Z
Creation Date: 2017-06-28T09:03:25Z
Registry Expiry Date: 2024-06-28T09:03:25Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: MIT World Peace University
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
```

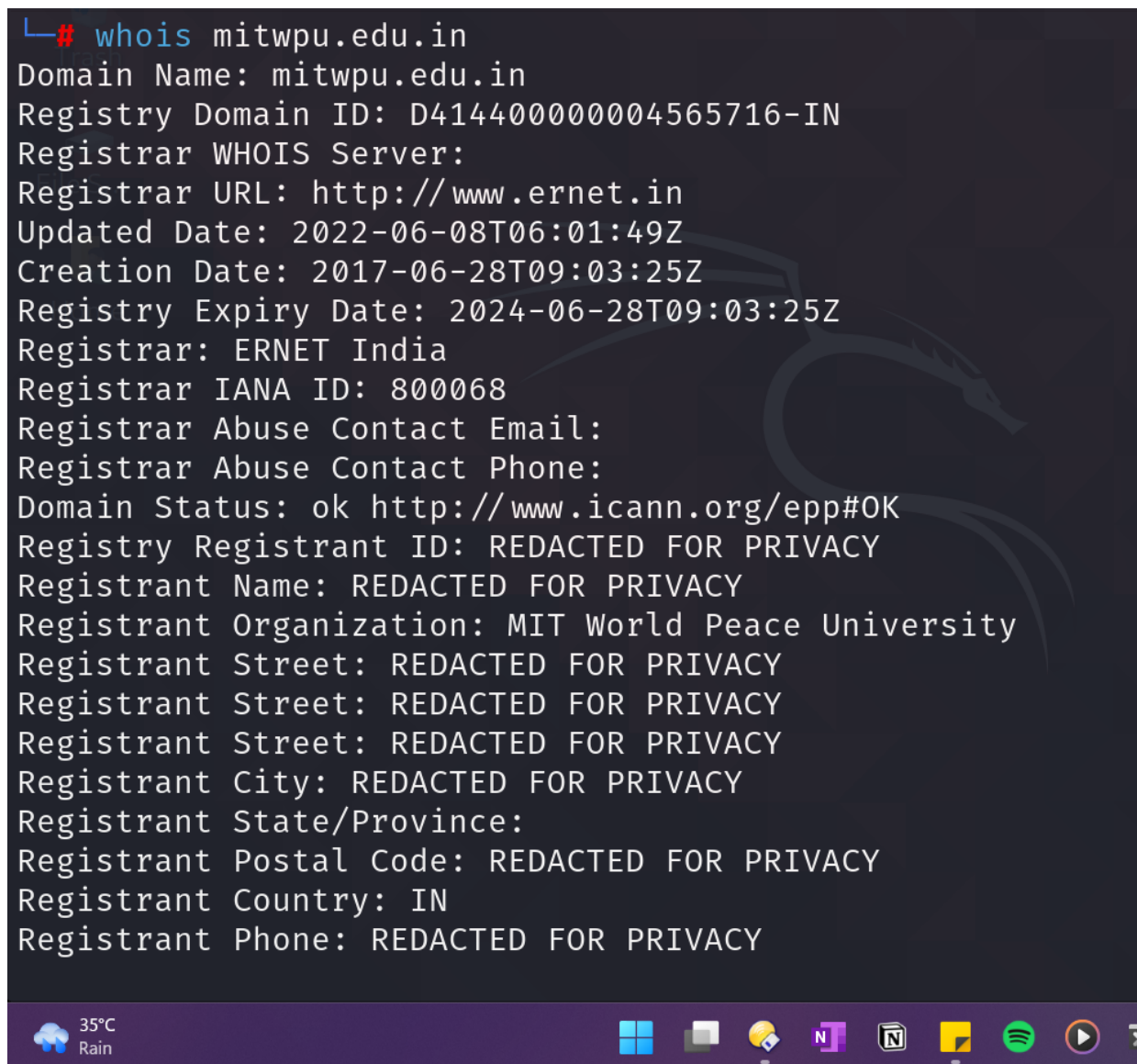


Figure 1: Output of the Command

## 8.2 whois

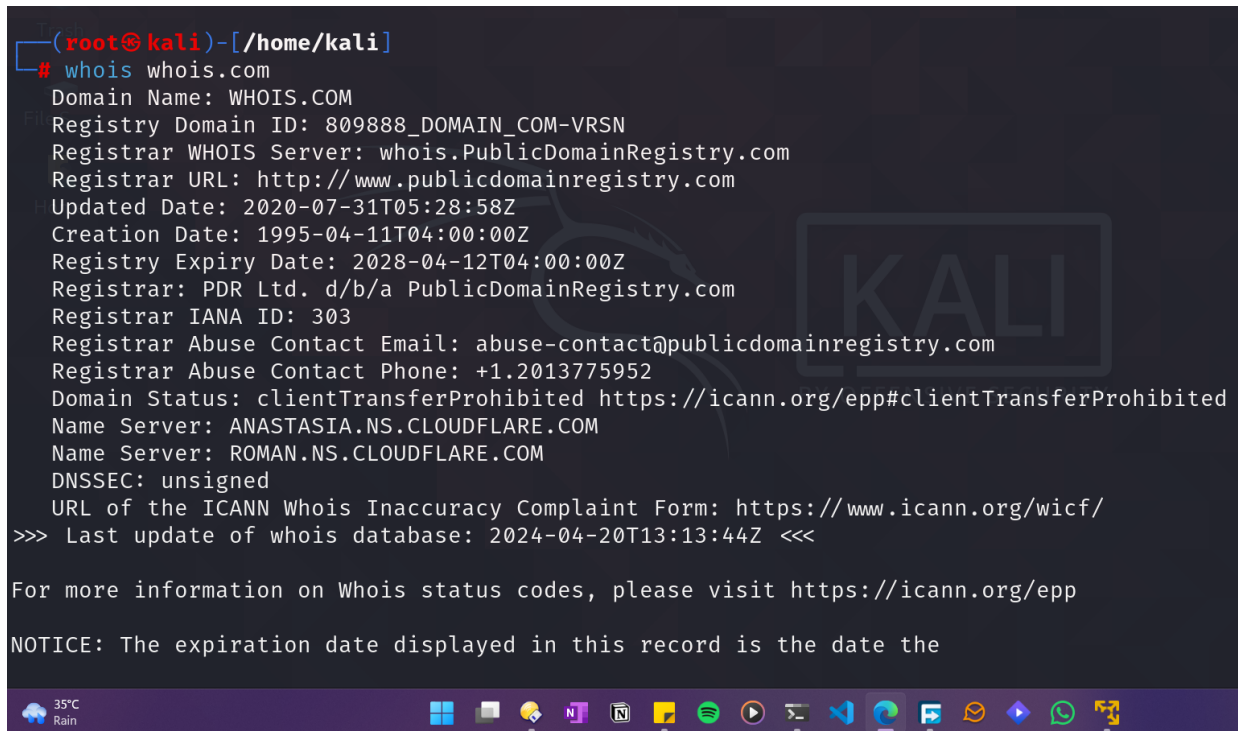
### Syntax

```
$ whois <domain_name>
```

### Command

```
$ whois whois.com
```

## Output



```
(root@kali)-[/home/kali]
# whois whois.com
Domain Name: WHOIS.COM
Registry Domain ID: 809888_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2020-07-31T05:28:58Z
Creation Date: 1995-04-11T04:00:00Z
Registry Expiry Date: 2028-04-12T04:00:00Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ANASTASIA.NS.CLOUDFLARE.COM
Name Server: ROMAN.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-20T13:13:44Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

Figure 2: Output of the Command

### 8.3 Angry IP Scanner

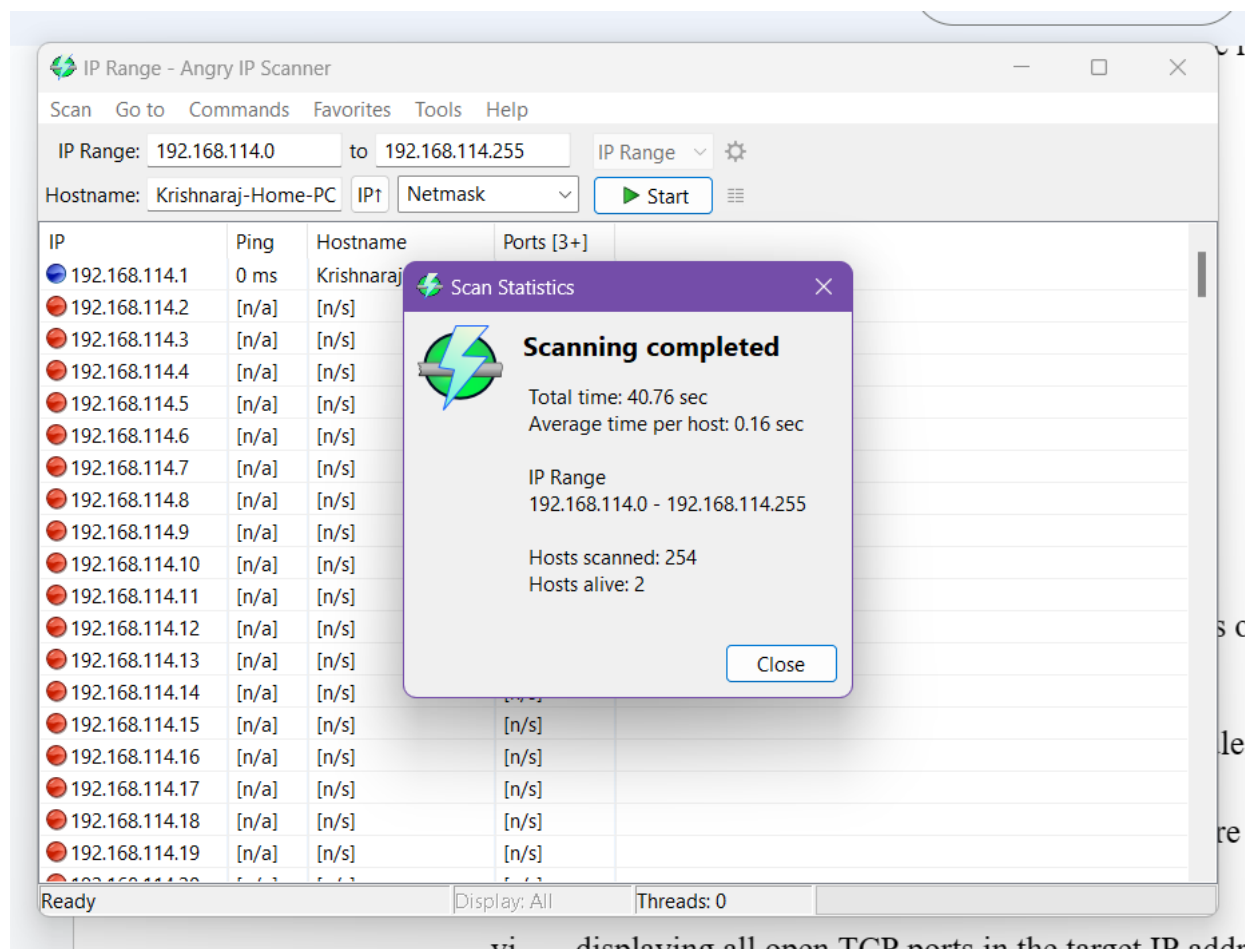


Figure 3: Output of the Command

### 8.4 Metasploit

#### Command

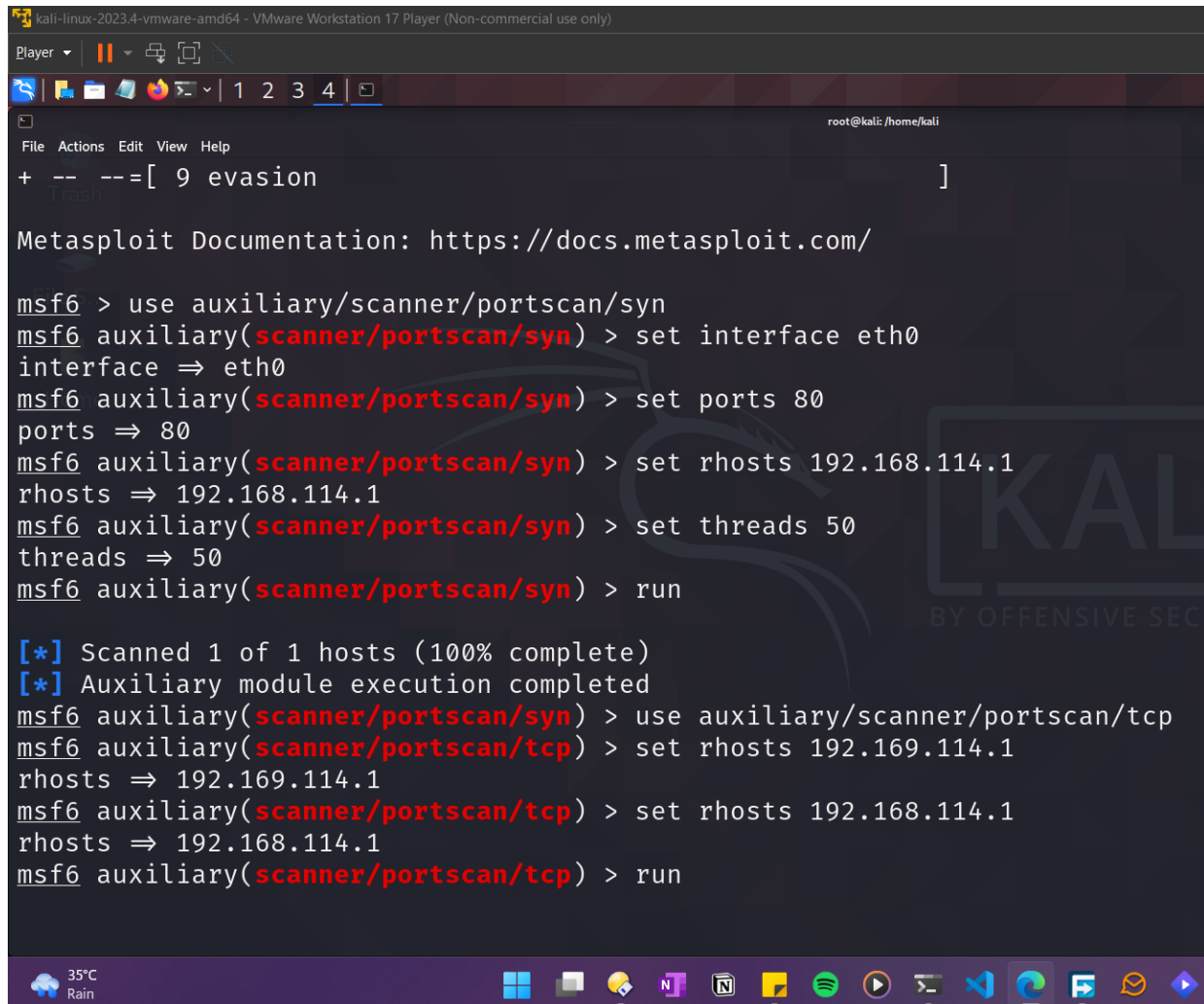
```
$ use auxiliary/scanner/portscan/syn
$ set interface eth0
$ set ports 80
$ set rhosts 192.168.114.1
$ set threads 50
```

#### Purpose

These commands configure Metasploit to perform a SYN port scan on the specified target IP address ( 192.168.114.1 ) using port 80 and 50 threads for parallel scanning.



## Output

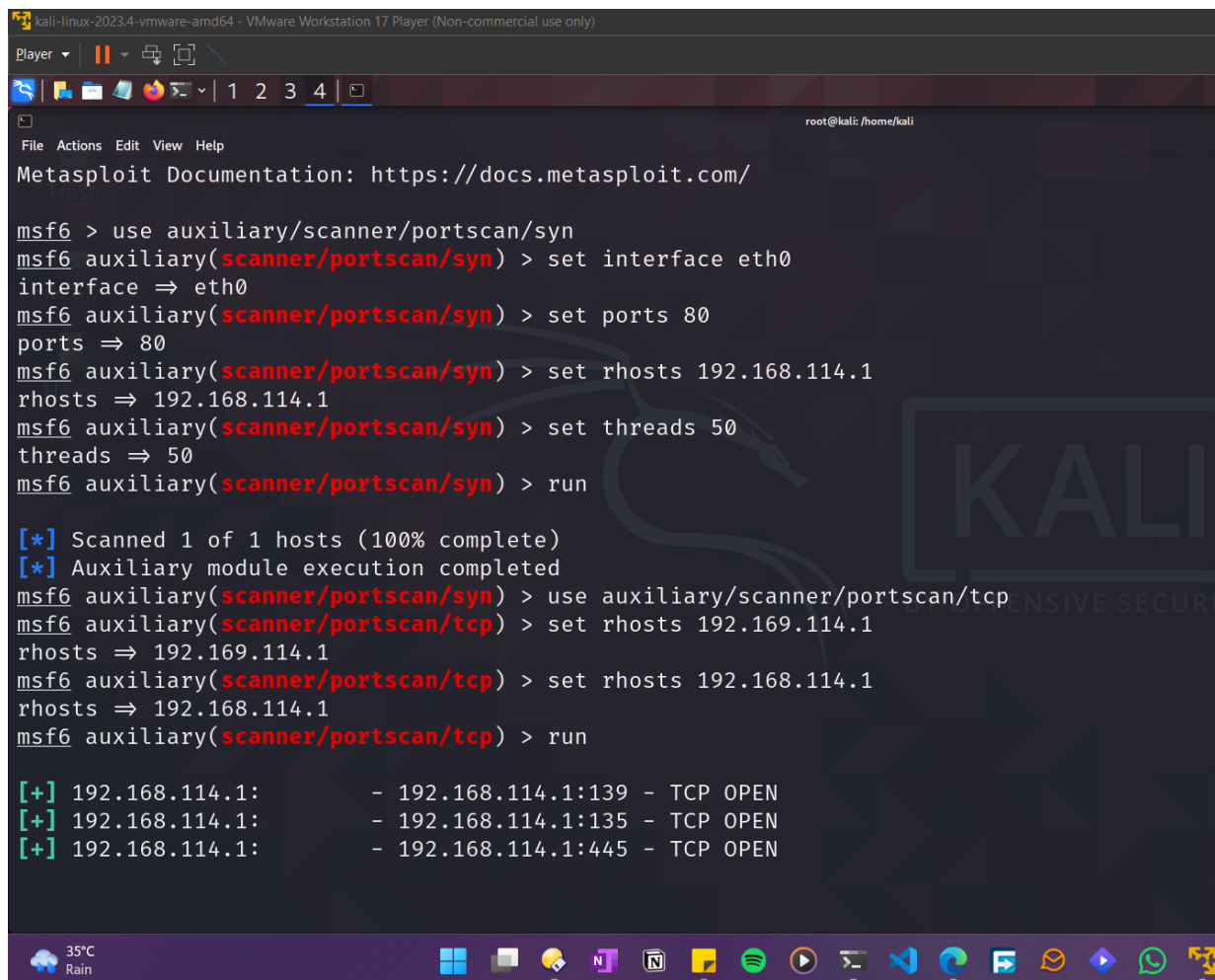


```
kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
+ -- --=[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set interface eth0
interface => eth0
msf6 auxiliary(scanner/portscan/syn) > set ports 80
ports => 80
msf6 auxiliary(scanner/portscan/syn) > set rhosts 192.168.114.1
rhosts => 192.168.114.1
msf6 auxiliary(scanner/portscan/syn) > set threads 50
threads => 50
msf6 auxiliary(scanner/portscan/syn) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 192.169.114.1
rhosts => 192.169.114.1
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 192.168.114.1
rhosts => 192.168.114.1
msf6 auxiliary(scanner/portscan/tcp) > run
```

Figure 4: Output of the Command



The screenshot shows a Kali Linux terminal window with the Metasploit framework running. The user sets the interface to eth0, ports to 80, and rhosts to 192.168.114.1. They then run the auxiliary/scanner/portscan/syn module. The output shows that the scan is 100% complete and lists three open TCP ports: 139, 135, and 445. The user then switches to the auxiliary/scanner/portscan/tcp module and sets rhosts to 192.168.114.1, but the output for this command is not visible in the screenshot.

```
kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set interface eth0
interface => eth0
msf6 auxiliary(scanner/portscan/syn) > set ports 80
ports => 80
msf6 auxiliary(scanner/portscan/syn) > set rhosts 192.168.114.1
rhosts => 192.168.114.1
msf6 auxiliary(scanner/portscan/syn) > set threads 50
threads => 50
msf6 auxiliary(scanner/portscan/syn) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 192.169.114.1
rhosts => 192.169.114.1
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 192.168.114.1
rhosts => 192.168.114.1
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.114.1: - 192.168.114.1:139 - TCP OPEN
[+] 192.168.114.1: - 192.168.114.1:135 - TCP OPEN
[+] 192.168.114.1: - 192.168.114.1:445 - TCP OPEN
```

Figure 5: Output of the Command

## 8.5 Ports in Megaping

### Output

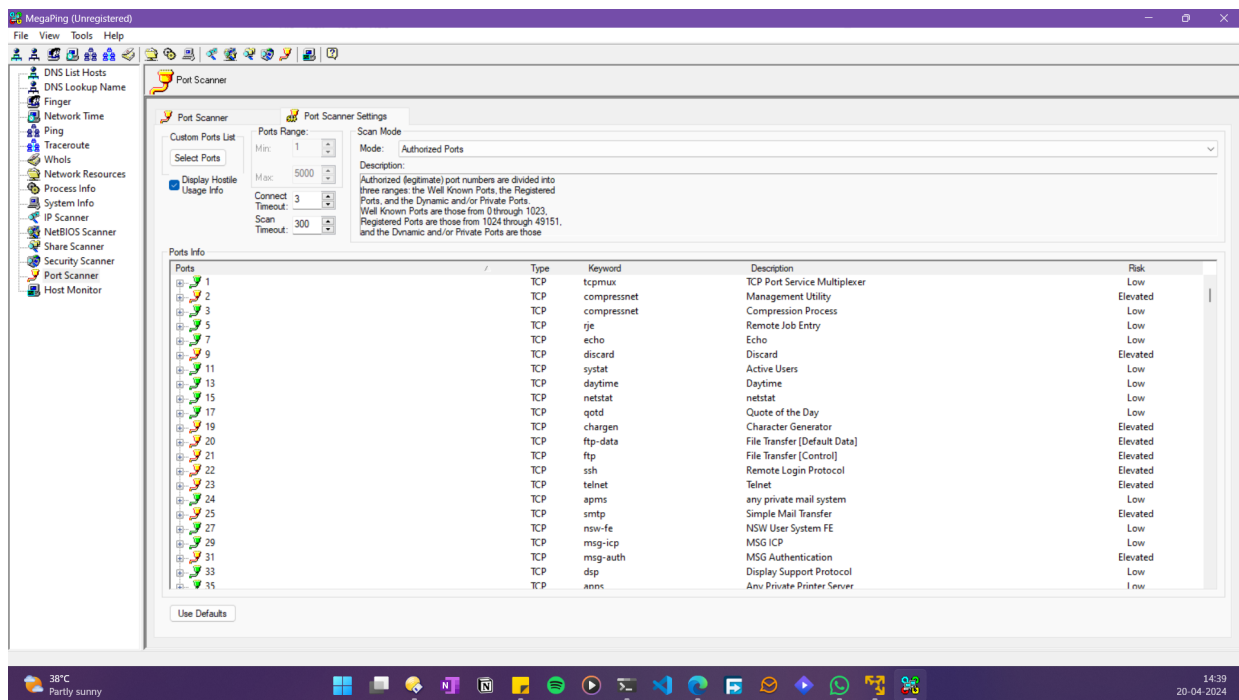


Figure 6: Output of the Command

## 8.6 IP Scanner in Megaping

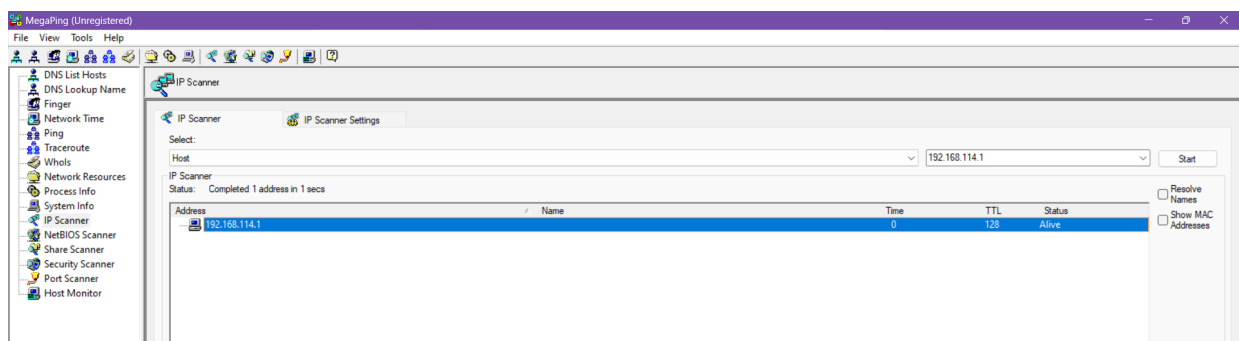


Figure 7: Output of the Command

## 8.7 TraceRoute in Megaping

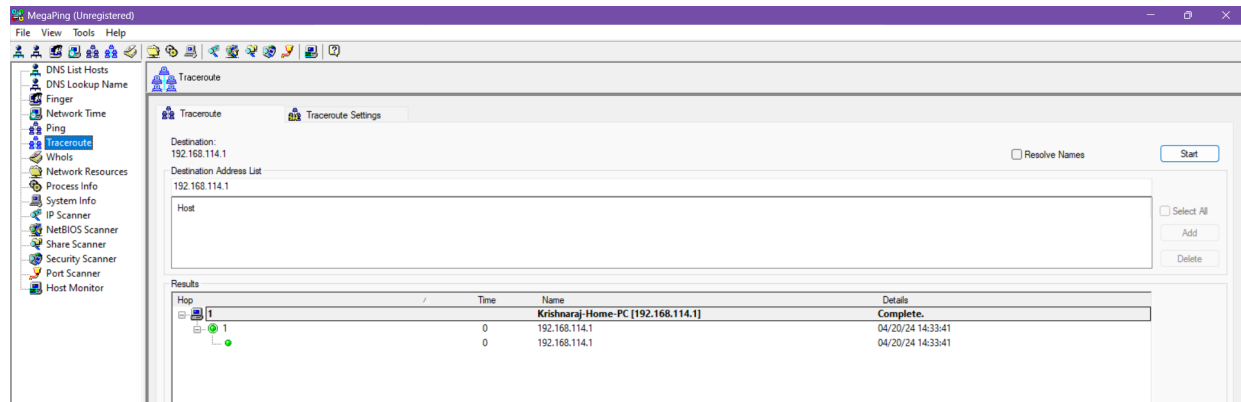


Figure 8: Output of the Command

## 8.8 IP Scanner in Range in Megaping

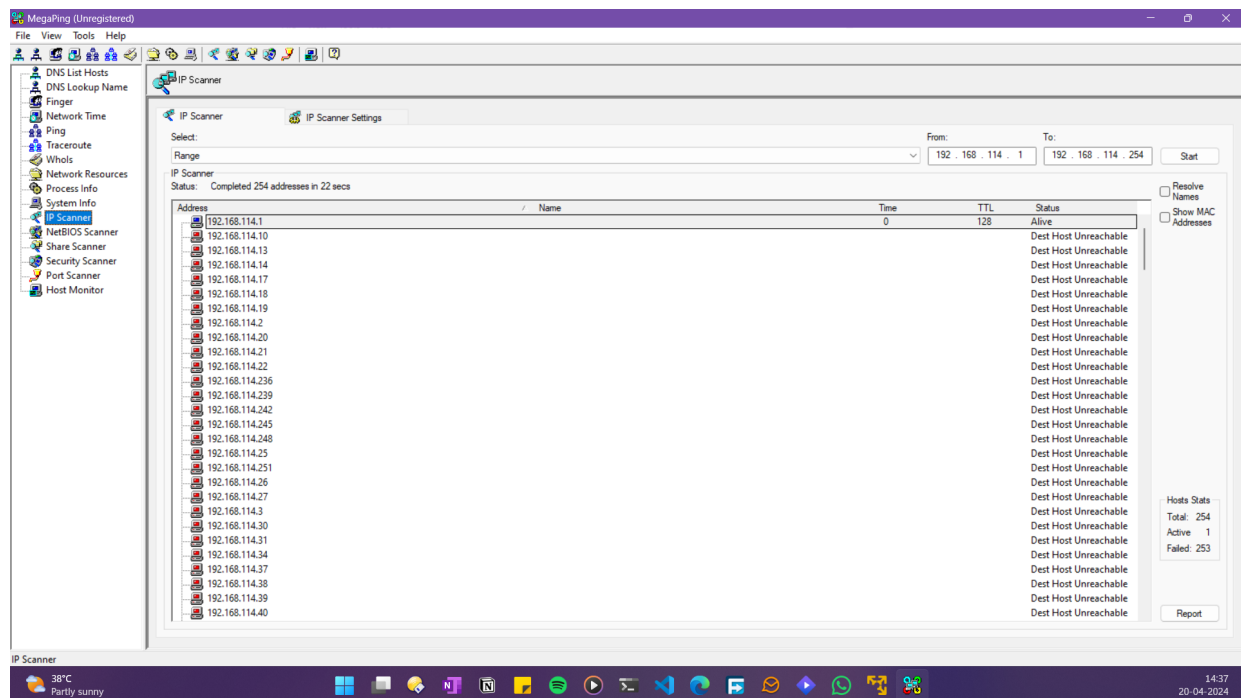


Figure 9: Output of the Command

## 8.9 NetScanTools Pro Demo Ping Scan Results in Browser

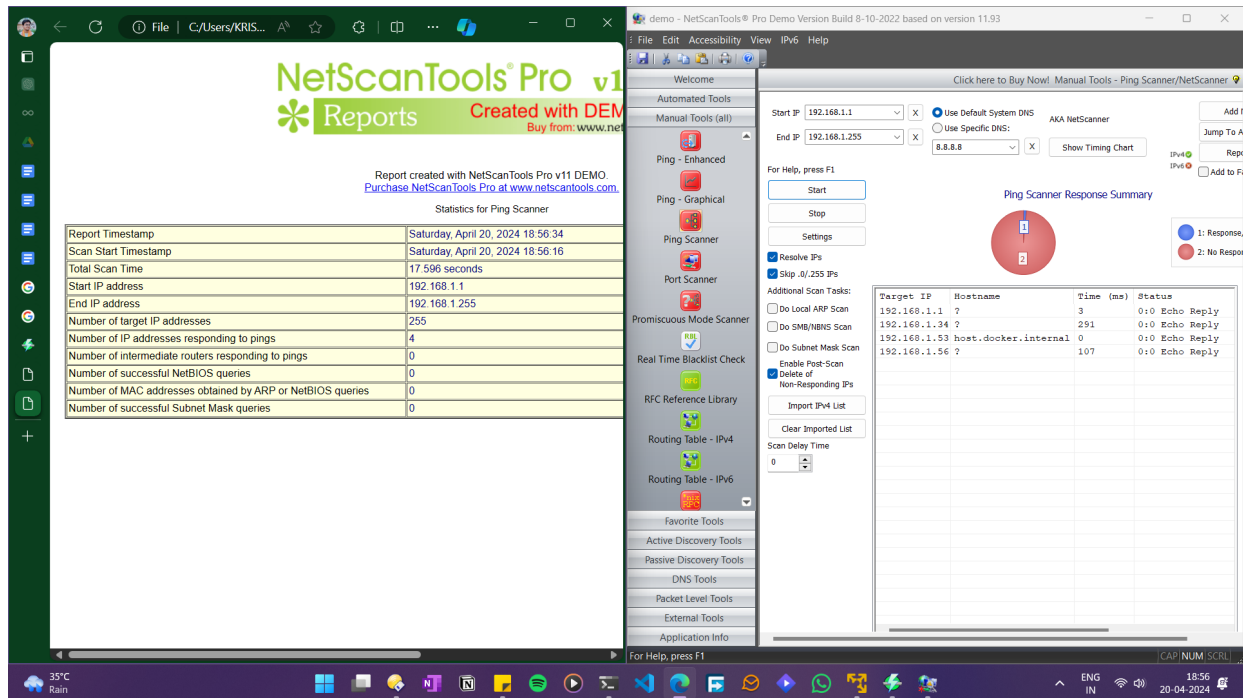


Figure 10: Output of the Command

## 9 Platform

**Operating System:** Arch Linux X8664

**IDEs or Text Editors Used:** Visual Studio Code

## 10 FAQs

### 1. What is an Angry IP Scanner?

- **Angry IP Scanner:** A cross-platform network scanner used to scan IP addresses and ports, providing information about active hosts and services.
- Offers fast scanning capabilities and a user-friendly interface for network reconnaissance.

### 2. What is dpkg? Explain the purpose of it.

- **dpkg:** Debian Package Manager, used for installing, removing, and managing software packages on Debian-based Linux distributions.
- Provides a command-line interface for package management, ensuring system stability and dependency resolution.

### 3. Enlist the various Port scanning tools.

- **Nmap:** A versatile network scanner with various scanning techniques.

- Masscan: High-speed TCP port scanner.
- Zmap: Fast Internet-scale network scanner.
- Unicornscan: Asynchronous TCP and UDP port scanner.
- Hping: Command-line packet crafter, sender, and analyzer.

#### **4. What are the various modules provided by Metasploit?**

- Exploits: Code to exploit vulnerabilities in target systems.
- Payloads: Code to deliver malicious payloads to compromised systems.
- Auxiliary: Modules for various tasks like information gathering, brute-forcing, and scanning.
- Post: Modules for post-exploitation activities like privilege escalation and data exfiltration.
- Encoders: Modules for encoding payloads to evade detection.

## **11 Conclusion**

In this assignment, we explored various scanning tools and techniques for network reconnaissance, including whois, Angry IP Scanner, Metasploit, MegaPing, and NetScanTools Pro. These tools provide valuable information for identifying active hosts, open ports, and services on a network, helping security professionals and researchers in penetration testing, vulnerability assessment, and network troubleshooting. By analyzing the results of network scanning, we can identify potential vulnerabilities in target systems and take appropriate measures to secure them.