PRACTICAL-6

AIM

Implementation to gather information from any PC's connected to the LAN using whois, port scanners, network scanning, IP Scanners.

THEORY

Nmap:

- Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.
- These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features.
- Nmap can adapt to network conditions including latency and congestion during a scan.
- Nmap started as a Linux utility and was ported to other systems including Windows, macOS, and BSD. It is most popular on Linux, followed by Windows.

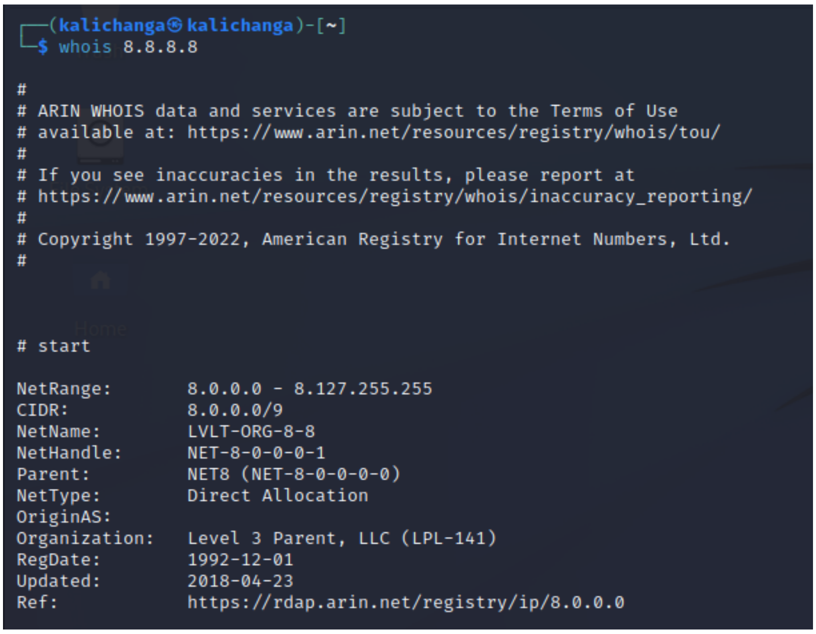
NetCat:

- netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP.
- The command is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.
- At the same time, it is a feature-rich network debugging and investigation tool, since it can produce almost any kind of connection its user could need and has a number of built-in capabilities.
- Its list of features includes port scanning, transferring files, and port listening, and it can be used as a backdoor.

IMPLEMENTATION

Using whois command:

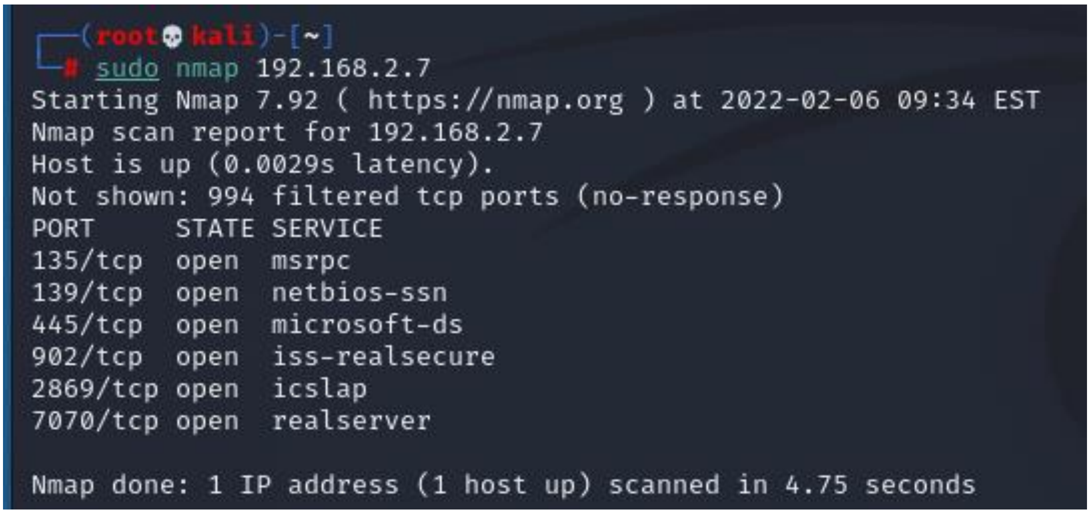
- Syntax: whois ip_address



```
┌──(kalichanga㉿kalichanga)-[~]
└─$ whois 8.8.8.8

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#


# start

NetRange:       8.0.0.0 - 8.127.255.255
CIDR:           8.0.0.0/9
NetName:        LVLT-ORG-8-8
NetHandle:      NET-8-0-0-0-1
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Level 3 Parent, LLC (LPL-141)
RegDate:        1992-12-01
Updated:        2018-04-23
Ref:            https://rdap.arin.net/registry/ip/8.0.0.0
```

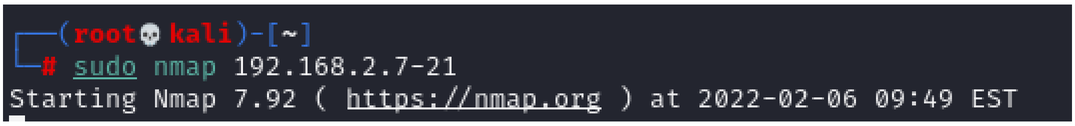
Port Scanning using nmap:

- Write sudo nmap ip address of device
- This is the basic format for **Nmap**, and it will return information about the ports on that system.



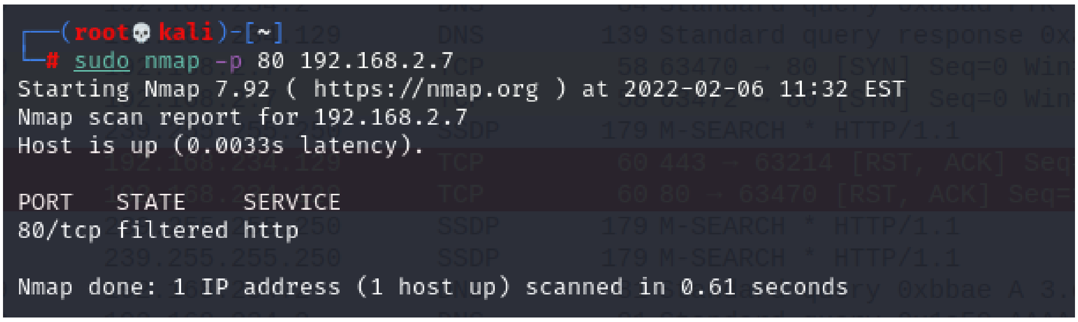
```
┌──(root💀kali)-[~]
└─# sudo nmap 192.168.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-06 09:34 EST
Nmap scan report for 192.168.2.7
Host is up (0.0029s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
2869/tcp open  icslap
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds
```

- Write sudo nmap ip address range



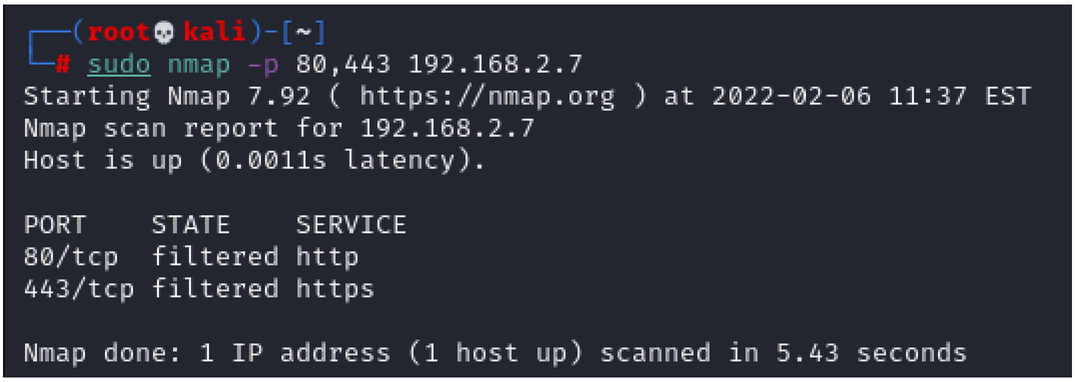
```
┌──(root💀kali)-[~]
└─# sudo nmap 192.168.2.7-21
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-06 09:49 EST
```

- You will get the result of scan for the whole range
- To know the status of a particular port, enter the following command



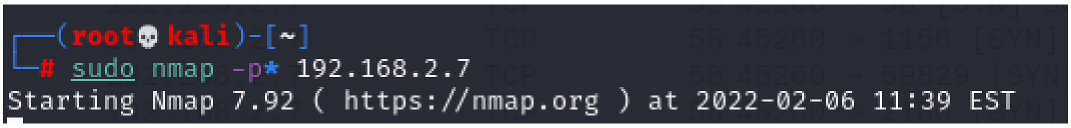
```
┌──(root💀kali)-[~]
└─# sudo nmap -p 80 192.168.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-06 11:32 EST
Nmap scan report for 192.168.2.7
Host is up (0.0033s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

- For multiple ports, type the following command



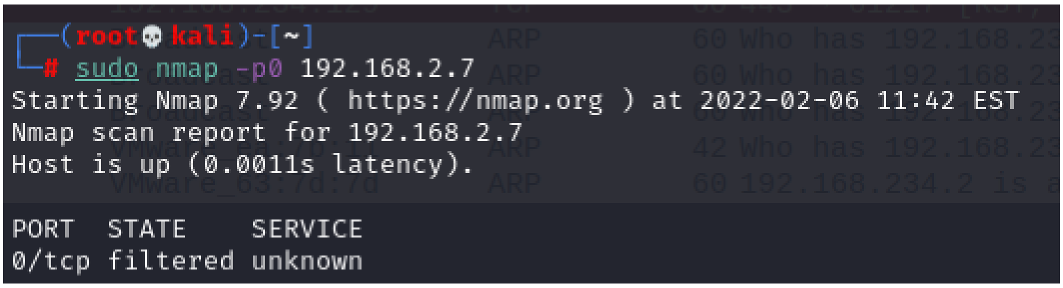
```
┌──(root💀kali)-[~]
└─# sudo nmap -p 80,443 192.168.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-06 11:37 EST
Nmap scan report for 192.168.2.7
Host is up (0.0011s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds
```

- To scan all the possible ports, write the following command



```
┌──(root💀kali)-[~]
└─# sudo nmap -p* 192.168.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-06 11:39 EST
```

- To scan for all available TCP ports, enter the following command

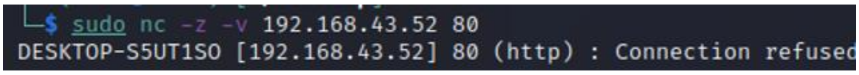


```
┌──(root💀kali)-[~]
└─# sudo nmap -p0 192.168.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-06 11:42 EST
Nmap scan report for 192.168.2.7
Host is up (0.0011s latency).

PORT  STATE    SERVICE
0/tcp filtered unknown
```

- This may useful to know which ports are open and running services on a target machine.
- Try the nc / netcat command as follow.
- The -z flag can be used to tell nc to report open ports, rather than initiate a connection.
- You need to specify hostname / ip along with the port range to limit and speedup operation

Using netcat:

- Command: nc -z -v hostname port-range



```
└─$ sudo nc -z -v 192.168.43.52 80
DESKTOP-S5UT1SO [192.168.43.52] 80 (http) : Connection refused
```

CONCLUSION

In this practical, we implemented different commands and tools to gather information about the ports.