**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.

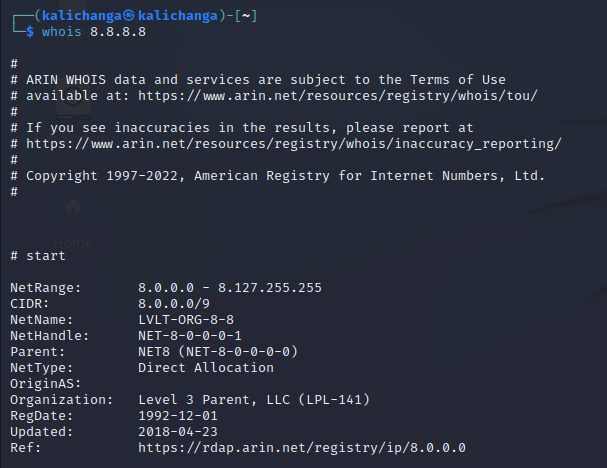
**NetCat**:

* 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**

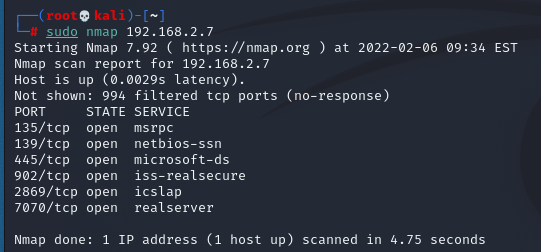
**Using whois command:**

* Syntax: whois ip\_address

****

**Port Scanning using nmap:**

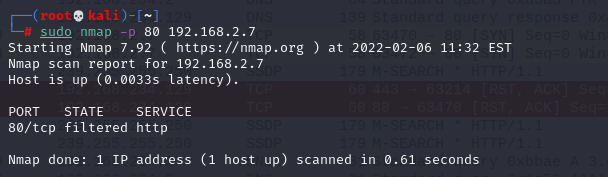
* Write sudo nmap ip address of device
* This is the basic format for **Nmap**, and it will return information about the ports on that system.



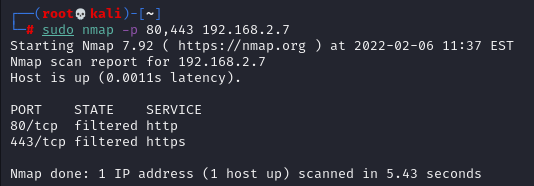
* Write sudo nmap ip address range



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



* For multiple ports, type the following command



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



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



* 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



**CONCLUSION**

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