**Lab Practical 2\_\_Nmap:**

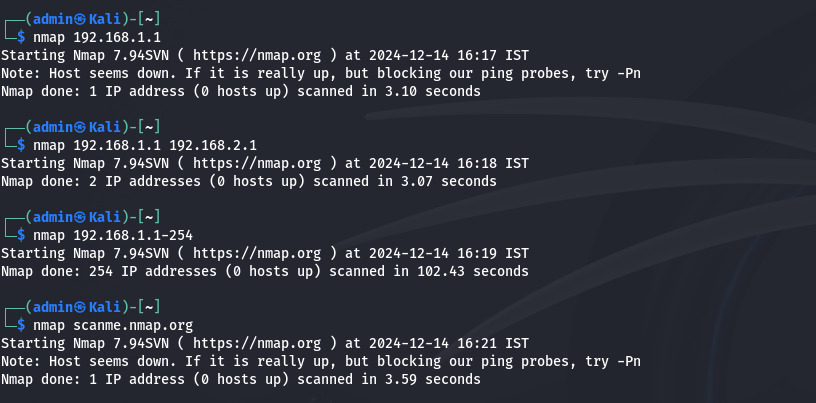
### ****Nmap (Network Mapper):****

Nmap is a powerful open-source network scanning tool widely used for network discovery, security auditing, and penetration testing. It allows you to identify live hosts, services, operating systems, and potential vulnerabilities in a network.

nmap 192.168.1.1: Scan for open TCP ports on a target.

nmap 192.168.1.1 192.168.1.2 : Scan List of Ips.

nmap 192.168.1.1-254 : To scan a specific range of IP.

****

Host /192.168.1.1 Discovery :

-sL (nmap 192.168.1.1-3 -sL):

No Scan. List targets only

-sn(nmap 192.168.1.1/24 -sn) :

Disable port scanning

-Pn (nmap 192.168.1.1-5 -Pn) :

Disable host discovery. Port scan only

-PS (nmap 192.168.1.1-5 -PS22-25,80) :

TCP SYN discovery on port x. Port 80 by default

-PA (nmap 192.168.1.1-5 -PA22-25,80):

TCP ACK discovery on port x. Port 80 by default

-PU (nmap 192.168.1.1-5 -PU53):

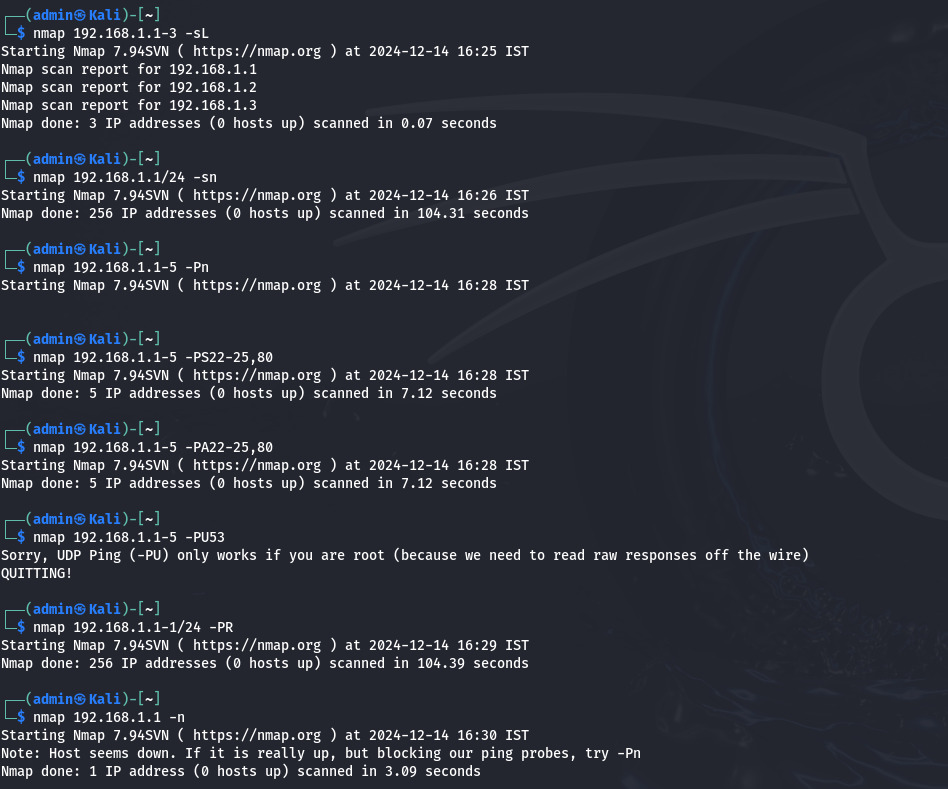
UDP discovery on port x. Port 40125 by default

-PR (nmap 192.168.1.1-1/24 -PR):

ARP discovery on local network

-n (nmap 192.168.1.1 -n):

Never do DNS resolution



Port Specification :

-p (nmap 192.168.1.1 -p U:53,T:21-25,80):

Port scan multiple TCP and UDP ports

-p (nmap 192.168.1.1 -p 21-100) :

Port range.

-p (nmap 192.168.1.1 -p http,https) :

Port scan from service name

-F (nmap 192.168.1.1 –F) :

Fast port scan (100 ports)



Service and Version Detection :

-sV (nmap 192.168.1.1 –sV) :

Attempts to determine the version of the service running on port.

-sV (nmap 192.168.1.1 –sV –v):

Shows the process of the command

