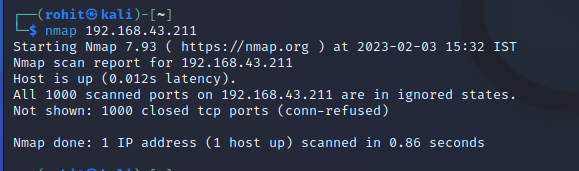
**Assignment - 2**

**Nmap**

**Target Specification**

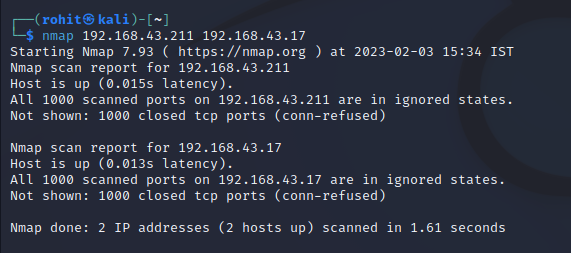
1. **nmap 192.168.43.211**

* Scan a single IP



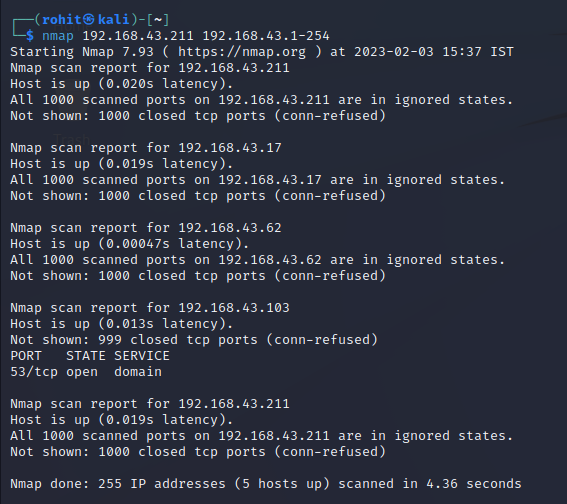
1. **nmap 192.168.43.211 192.168.43.17**

* Scan specific Ips



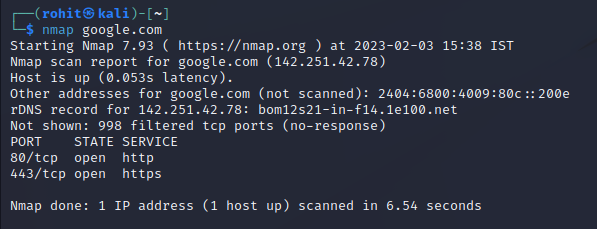
1. **nmap 192.168.43.211 192.168.43.1-254**

* Scan a range



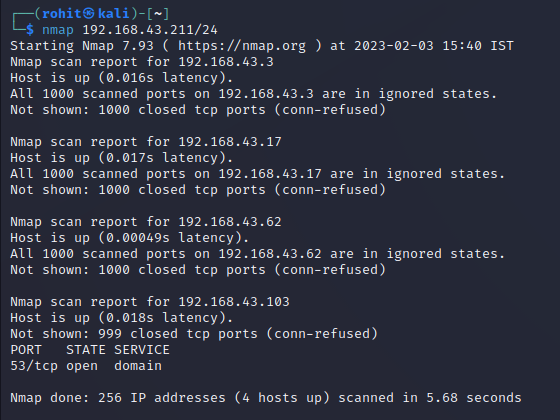
1. **nmap google.com**

* Scan a domain



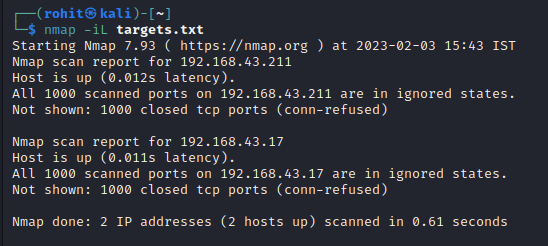
1. **nmap 192.168.43.211/24**

* Scan using CIDR notation



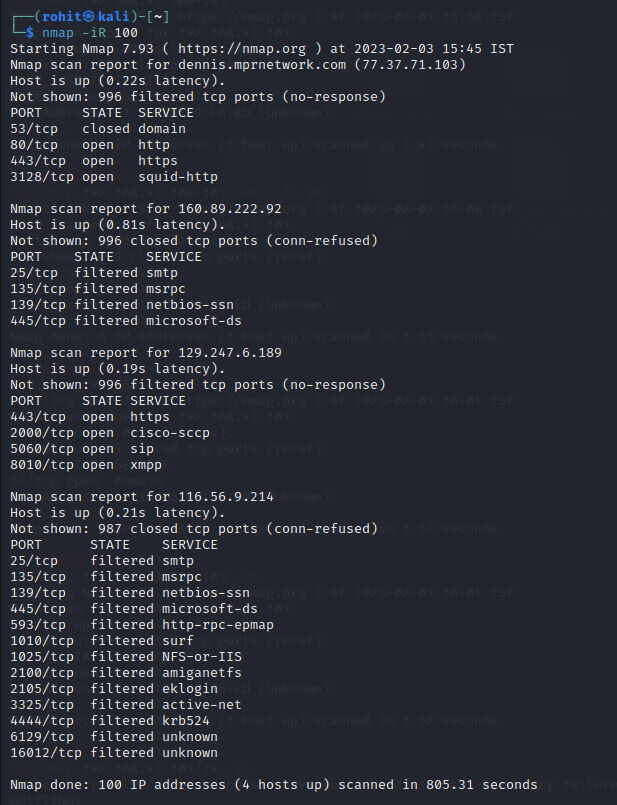
1. **nmap -iL targets.txt**

* Scan targets from a file



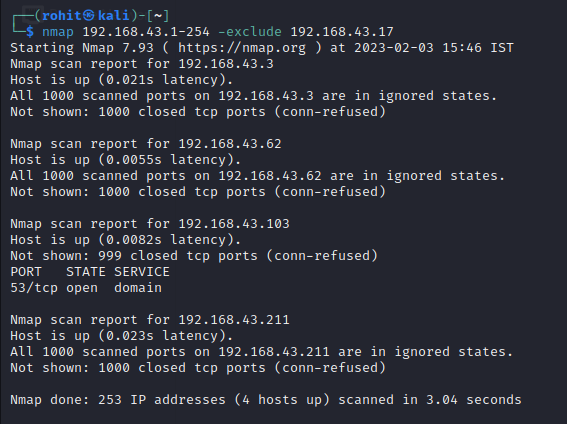
1. **nmap -iR 100**

* Scan 100 random hosts



1. **nmap 192.168.43.1-254 -exclude 192.168.43.17**

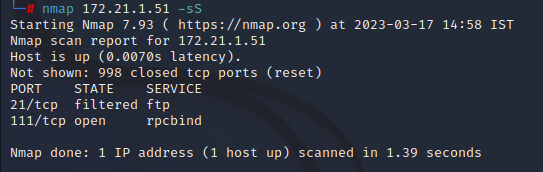
* Exclude listed hosts



**Scan Techniques**

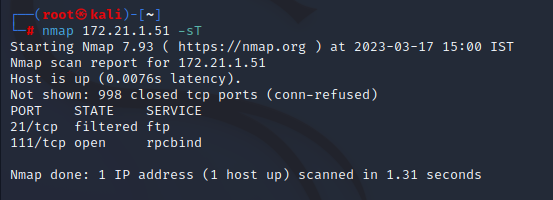
1. **nmap 192.21.1.51 -sS**

* TCP SYN port scan (Default)



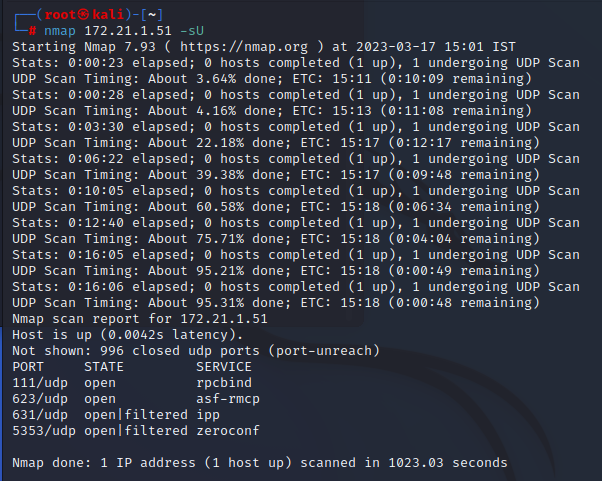
1. **nmap 192.21.1.51 -sT**

* TCP connect port scan (Default without root privilege)



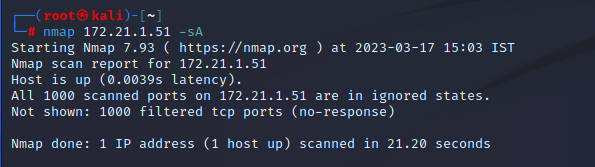
1. **nmap 192.21.1.51 -sU**

* UDP port scan



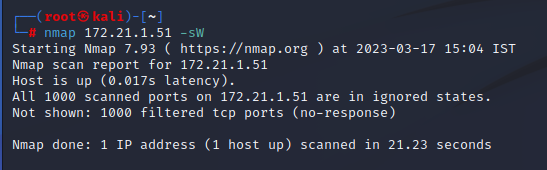
1. **nmap 192.21.1.51 -sA**

* TCP ACK port scan



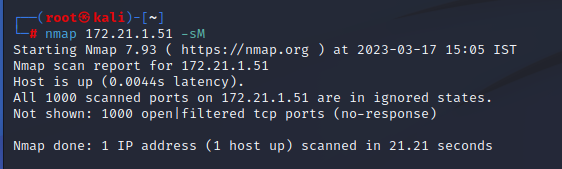
1. **nmap 192.21.1.51 -sW**

* TCP Window port scan



1. **nmap 192.21.1.51 -sM**

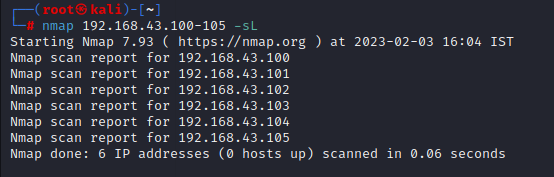
* TCP Maimon port scan

****

**Host Discovery**

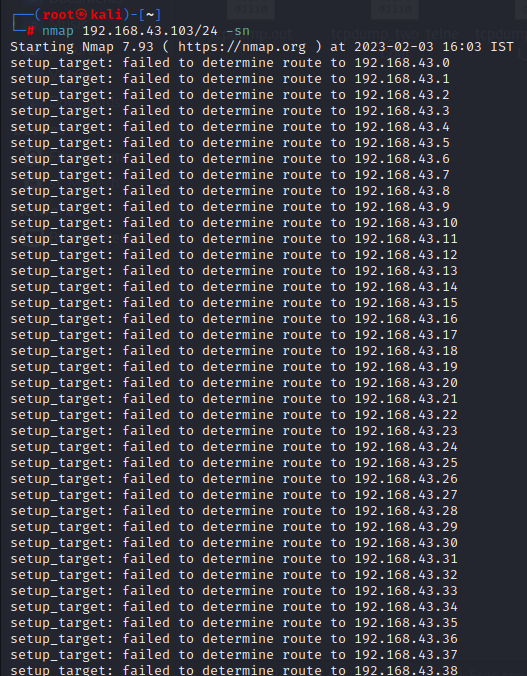
1. **nmap 192.168.43.100-105 -sL**

* No Scan. List targets only



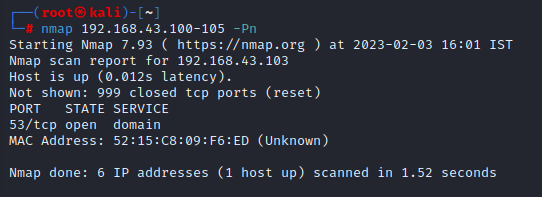
1. **nmap 192.168.43.103/24 -sn**

* Disable port scanning



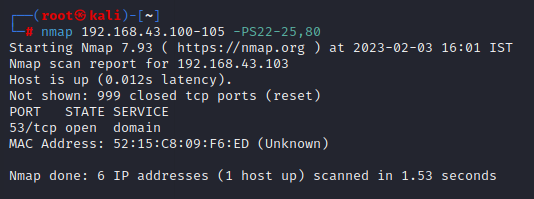
1. **nmap 192.168.43.100-105 -Pn**

* Disable host discovery. Port scan only



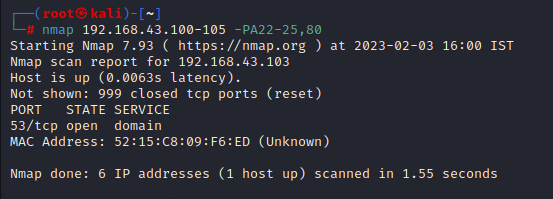
1. **nmap 192.168.43.100-105 -PS22-25,80**

* TCP SYN discovery on port x. Port 80 by default



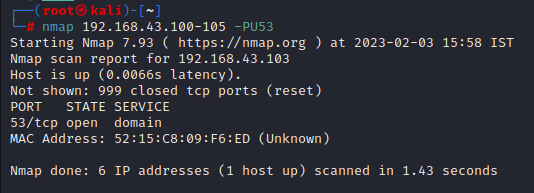
1. **nmap 192.168.43.100-105 -PA22-25,80**

* TCP ACK discovery on port x. Port 80 by default



1. **nmap 192.168.43.100-105 -PU53**

* UDP discovery on port x. Port 40125 by default



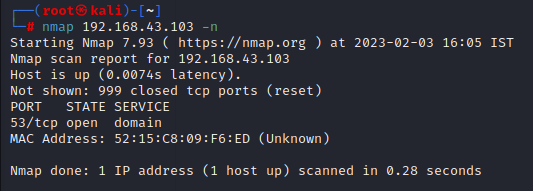
1. **nmap 192.168.43.103/24 -PR**

* ARP discovery on local network



1. **nmap 192.168.43.103 -n**

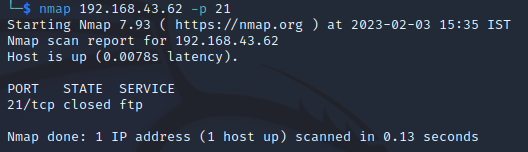
* Never do DNS resolution



**Port Specification:**

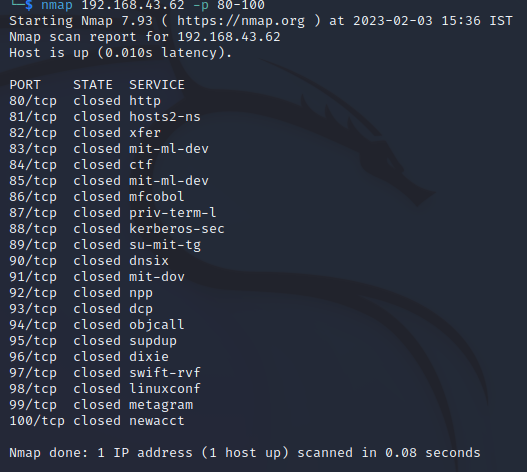
1. **nmap 192.168.43.62 -p 21**

* Port scan for port 21

****

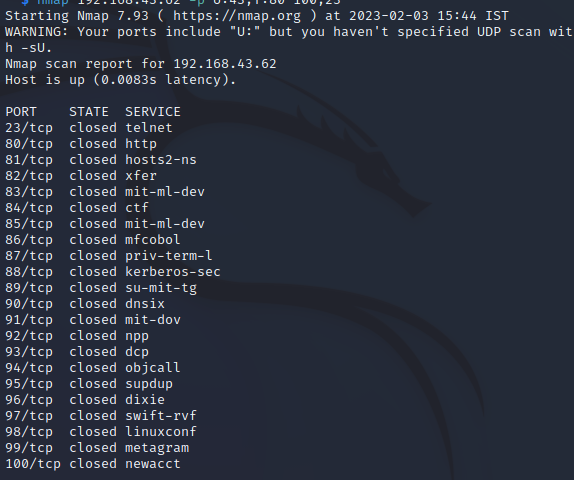
1. **nmap 192.168.43.62 -p 80-100**

* Port range scan



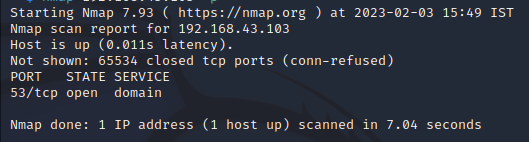
1. **nmap 192.168.43.62 -p U:45,T:80-100,25**

* Port scan multiple TCP and UDP ports



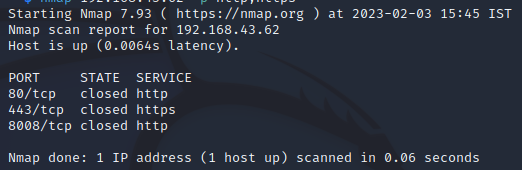
1. **nmap 192.168.43.62 -p-**

* Port scan all ports



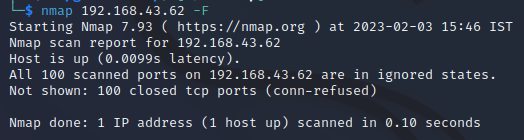
1. **nmap 192.168.43.62 -p http,https**

* Port scan from service name



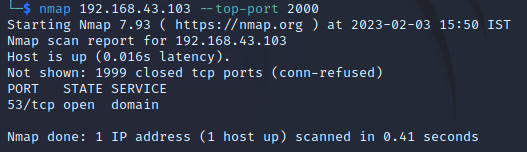
1. **nmap 192.168.43.62 -F**

* Fast port scan (100 ports)



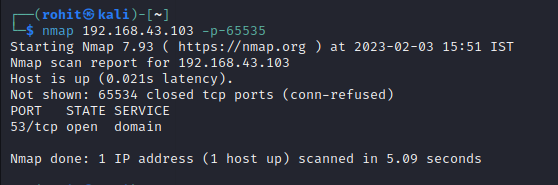
1. **nmap 192.168.1.1 --top-ports 2000**

* Port scan the top 2000 ports



1. **nmap 192.168.43.103 -p-65535**

* Leaving off initial port in range makes the scan start at port 1



1. **nmap 192.168.43.103 -p0-**

* Leaving off end port in range makes the scan go through to port 65535

