Scanning and Enumeration

Day2_Scan.md

Recall

LAST TIME TOPICS

Topics

- What is Scanning?
- Why do we scan?
- Network Scanning
- Nmap
- Host detection
- Port Detection
- OS detection
- NSE

What is Scanning?

- Scanning is the 2nd phase of Ethical Hacking.
- It is the step which helps to test a system based on the information we gathered.
- Scanning is another essential step, which is necessary, and it refers to the package of techniques or procedures used to identify hosts, ports, and various services within a system

Why do we do scanning?

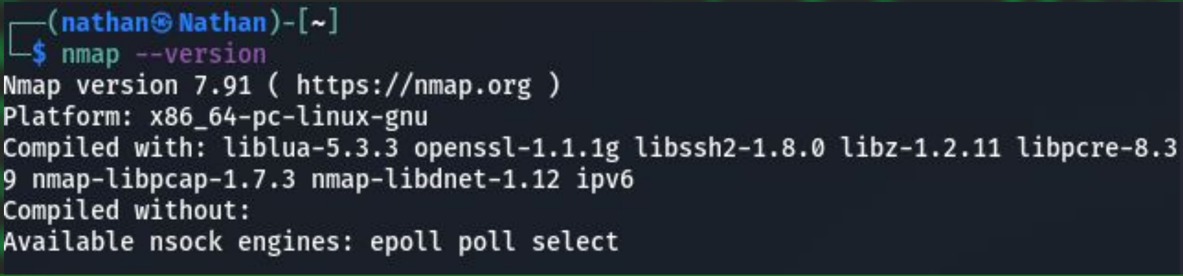
- It helps to Identify HOST’s System detail
  - Operation System
  - Service versions
- To Discover Open Ports
- To Discover Live Systems

Network Scanning

- This is a method of Scanning a network and getting more informations.
- There are Many kinds of scanning methods and tools for different purpose.
  - **For Network mainly**: NMAP,netdiscovery
  - **For Subdomain**: Sublist3r,subfinder,amass
  - **For website:** Nuclei , Nessus, Acunitix..

Nmap - Network Mapper

- Nmap is A network scanning and exploring tool used by network and security experts.
- It is used to scan Network,Ports,OS,...
- It is made for windows and linux
- ON kali linux it is built in.
- To check the existence of nmap on your system
    - `nmap --version`



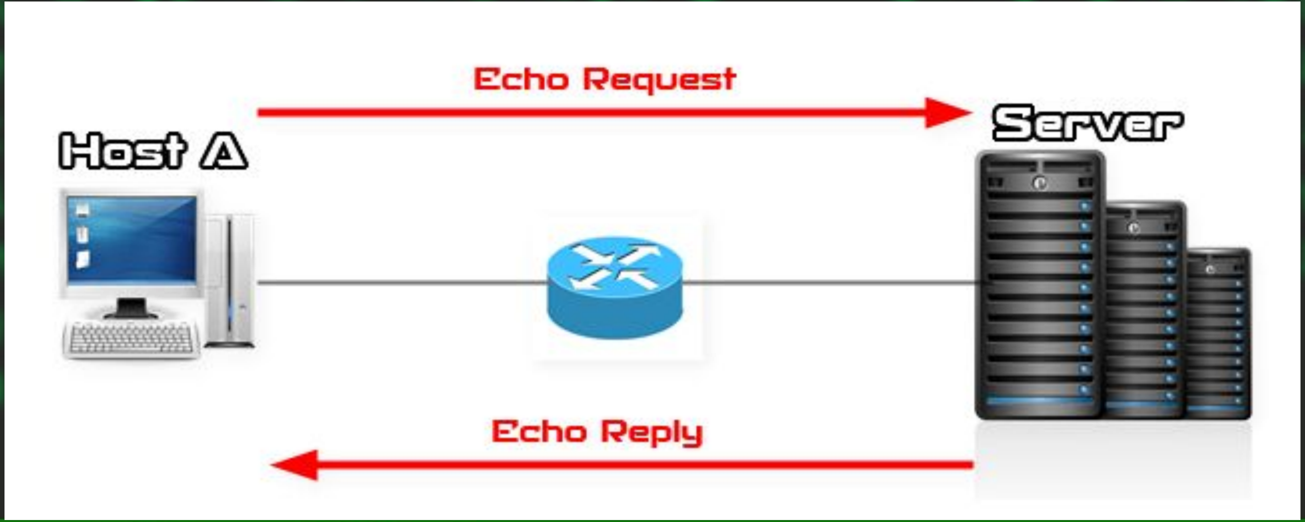
```
┌──(nathan㉿Nathan)-[~]
└─$ nmap --version
Nmap version 7.91 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1g libssh2-1.8.0 libz-1.2.11 libpcre-8.3
9 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Live System Discovery

- Discovering live system means, Checking up and running hosts(clients/servers) on a network.
- We have seen Host checking last time with ping sweep method.(getting ip with link)
- But How does the ping worked?

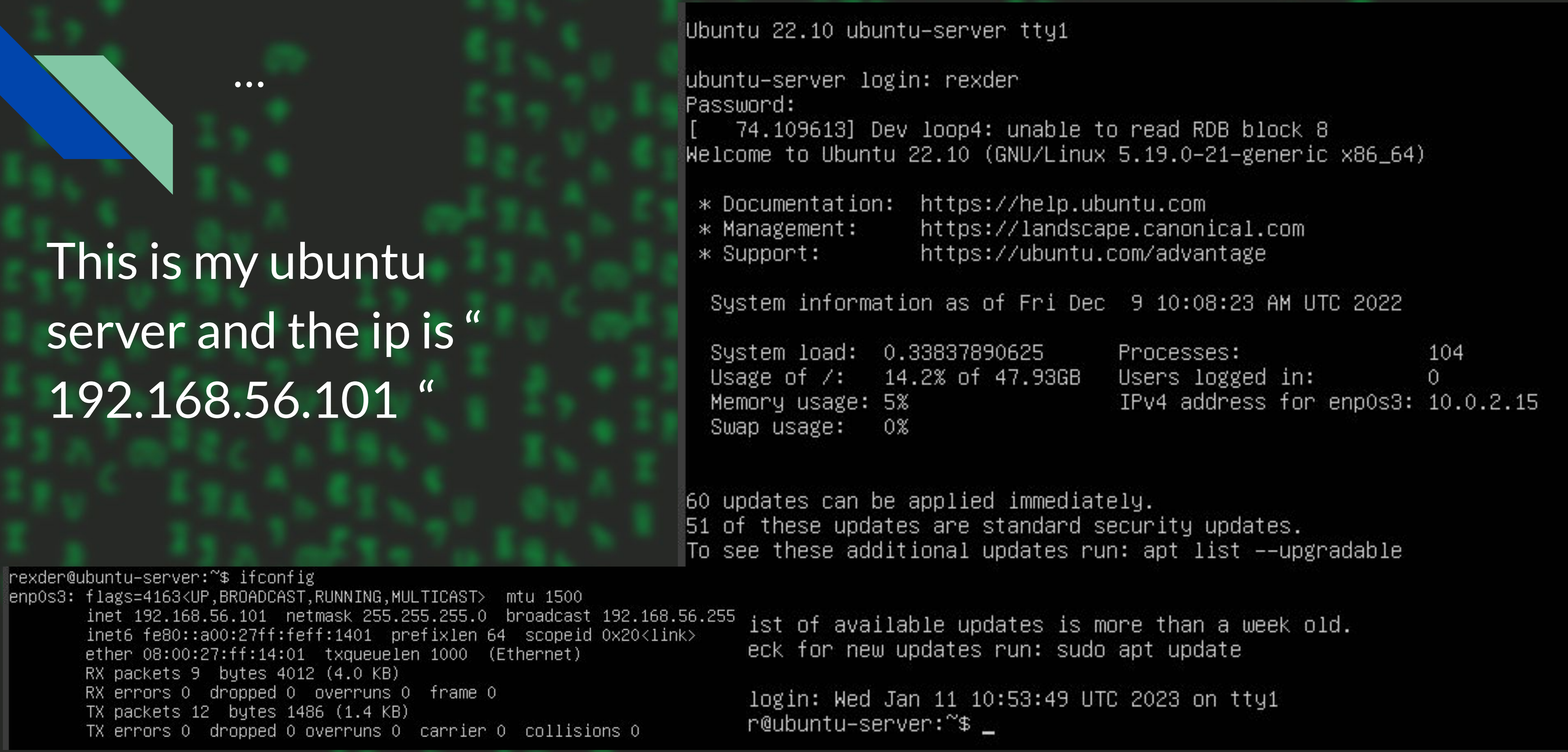
Ping Sweep

- This is a method of checking if host is up or down.
- It uses ICMP(Internet Control Message Protocol) packets for checking purpose
- It sends **Echo request** and waits for response if there is **Echo reply** then that system is up!



…

This is my ubuntu server and the ip is “ 192.168.56.101 “



```
Ubuntu 22.10 ubuntu-server tty1

ubuntu-server login: rexder
Password:
[   74.109613] Dev loop4: unable to read RDB block 8
Welcome to Ubuntu 22.10 (GNU/Linux 5.19.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Dec  9 10:08:23 AM UTC 2022

  System load:  0.33837890625      Processes:               104
  Usage of /:   14.2% of 47.93GB   Users logged in:         0
  Memory usage: 5%                 IPv4 address for enp0s3: 10.0.2.15
  Swap usage:   0%


60 updates can be applied immediately.
51 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

ist of available updates is more than a week old.
eck for new updates run: sudo apt update

login: Wed Jan 11 10:53:49 UTC 2023 on tty1
r@ubuntu-server:~$ _
```

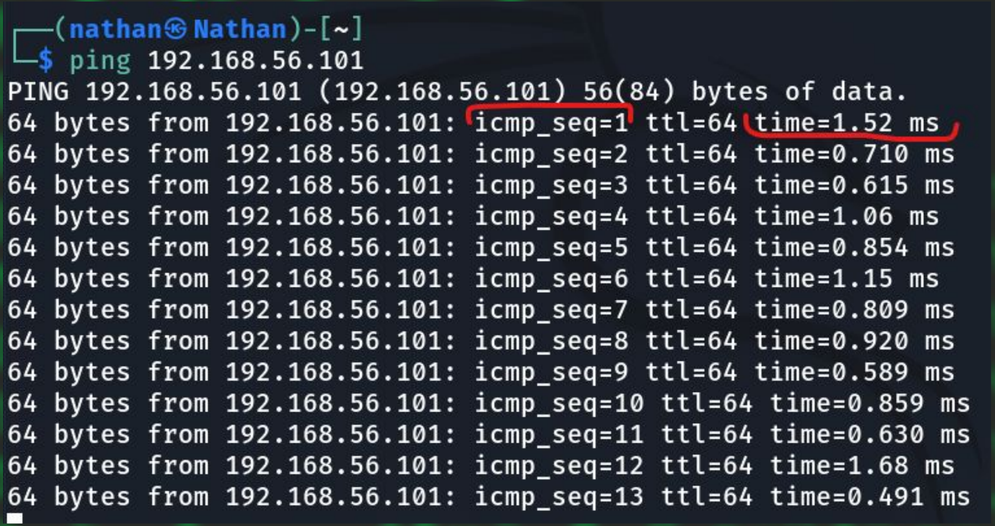
```
rexder@ubuntu-server:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:feff:1401  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ff:14:01  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 4012 (4.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 1486 (1.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

demo

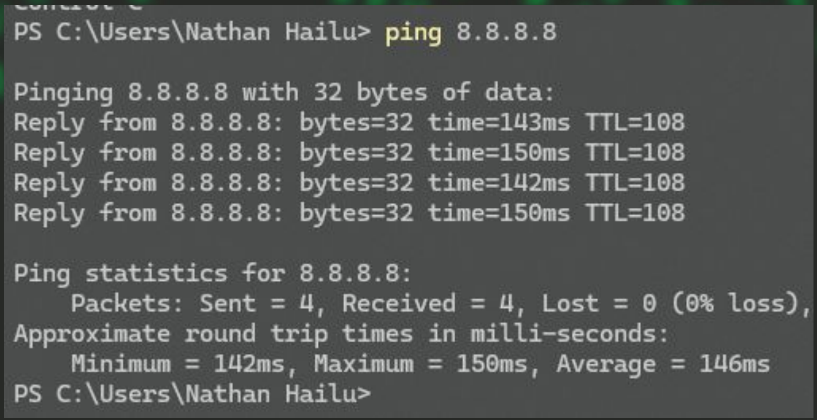
Let's Check if my ubuntu server is UP! With ping sweep

- From echo requests we can gather the following informations
  - **OS type**
    - Windows (32 byte)
      - ttl=108
    - Linux (64 byte)
      - ttl=64
  - **Connection stability**
    - Time

Ttl : time to live



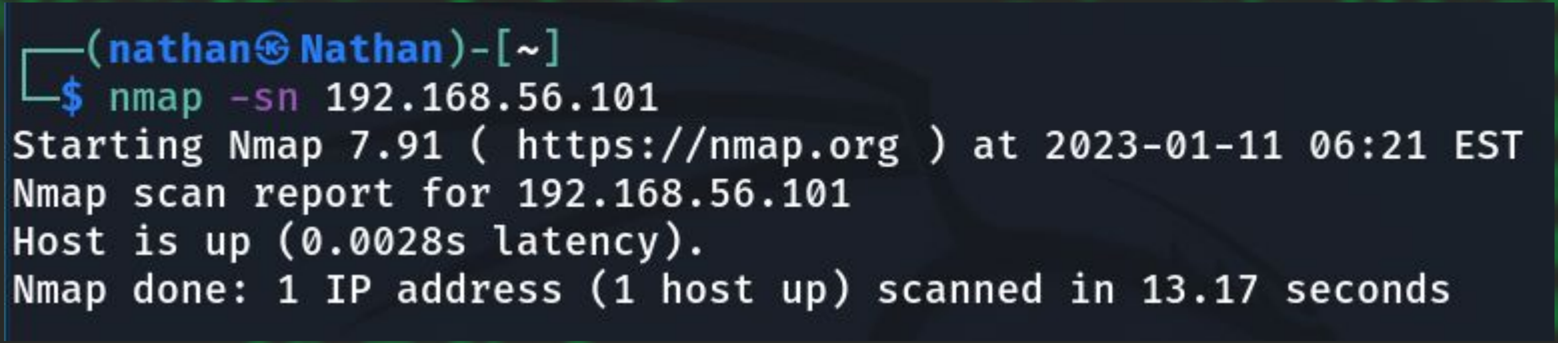
```
┌──(nathan㉿Nathan)-[~]
└─$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.52 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.710 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.615 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.06 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.854 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=1.15 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.809 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.920 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.589 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.859 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=0.630 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=1.68 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.491 ms
```



```
PS C:\Users\Nathan Hailu> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=143ms TTL=108
Reply from 8.8.8.8: bytes=32 time=150ms TTL=108
Reply from 8.8.8.8: bytes=32 time=142ms TTL=108
Reply from 8.8.8.8: bytes=32 time=150ms TTL=108

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 142ms, Maximum = 150ms, Average = 146ms
PS C:\Users\Nathan Hailu>
```

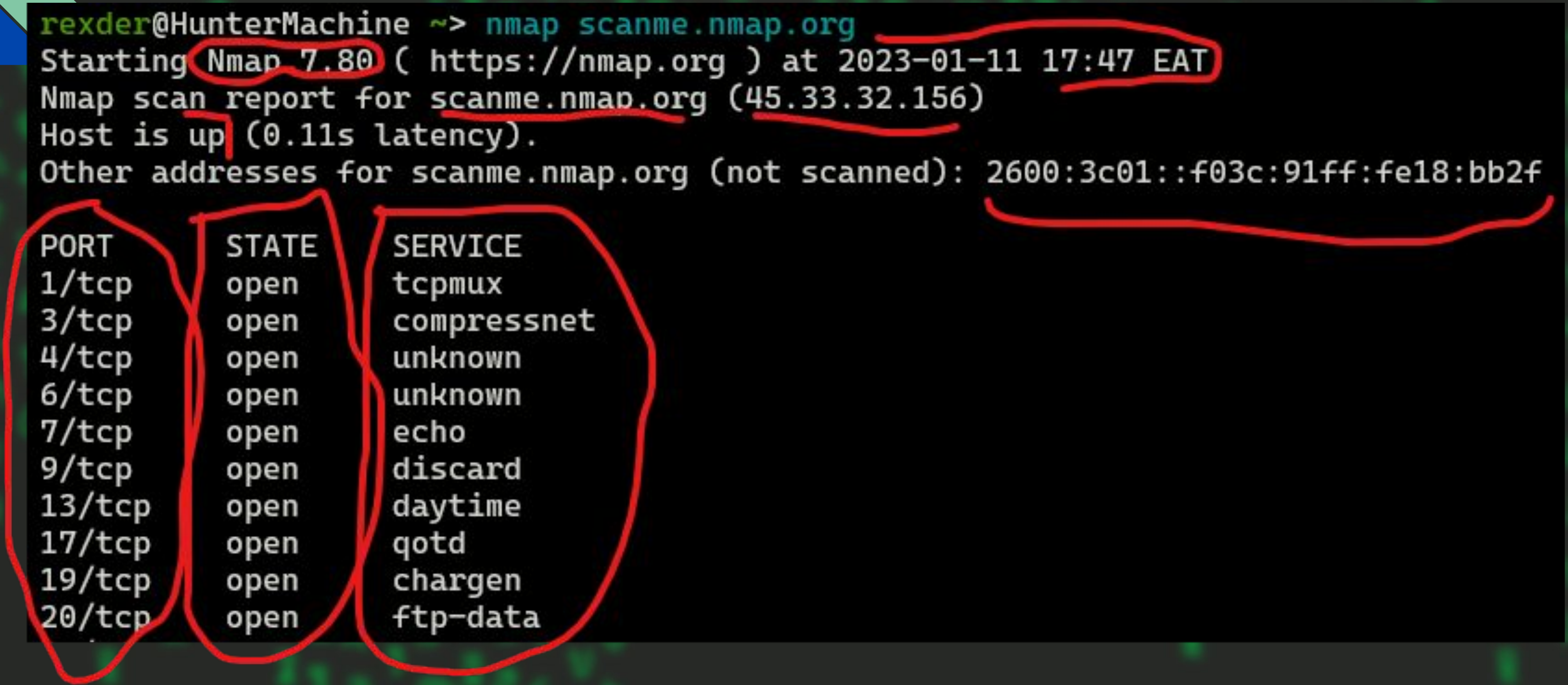
Nmap ping sweep

- Nmap can perform ping sweep too.
- Syntax:
    - `nmap -sn IP` `-sn` = no port scan



```
┌──(nathan㉿Nathan)-[~]
└─$ nmap -sn 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 06:21 EST
Nmap scan report for 192.168.56.101
Host is up (0.0028s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

demo



```
rexder@HunterMachine ~> nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-11 17:47 EAT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT     STATE  SERVICE
1/tcp    open   tcpmux
3/tcp    open   compressnet
4/tcp    open   unknown
6/tcp    open   unknown
7/tcp    open   echo
9/tcp    open   discard
13/tcp   open   daytime
17/tcp   open   qotd
19/tcp   open   chargen
20/tcp   open   ftp-data
```

- Nmap result have lots of things inside of it.

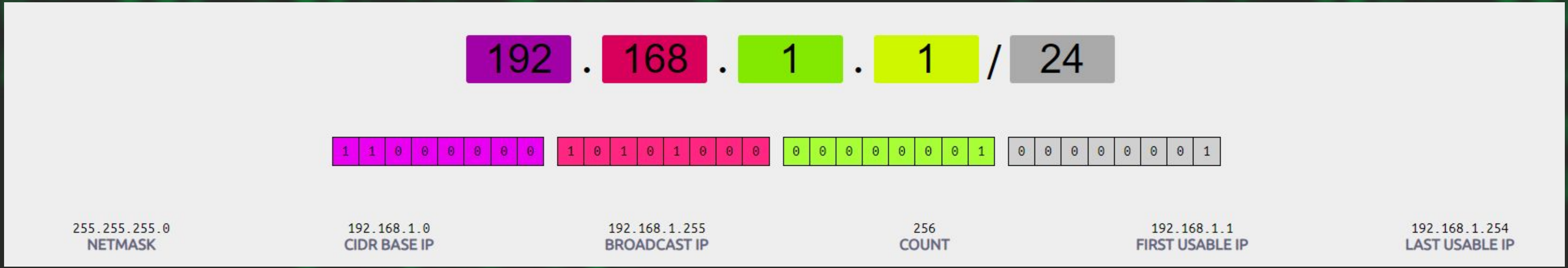
cont...

- -> What do we do ,to know all the hosts on our system?
- ping can take 1 host only??
- Nmap can scan the whole range.
- Guess how?
- You can do the ping sweep with little modification on the IP
- Syntax:
  - nmap -sn GatewayIP-255
  - nmap -sn GatewayIP/networkBits(subnet mask) - CIDR notation
    - Network bits depend on the IP Class.
- This will not work on Virtual machines network.

QUICK QUIZ

- AS we learned about network address and host address

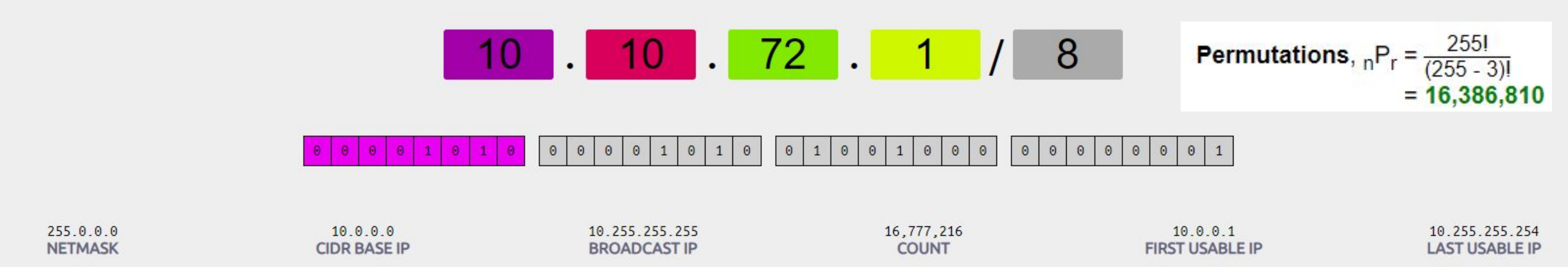
1. What is the class type of this subnet mask - 255.255.255.0
   a. 255 is the place holder for network address
   b. This shows there is only 8 bit of host address that means range between
      i. 0 - 254
   c. This means it is Class C IP type.
2. How many network bits are there on Class C



192 . 168 . 1 . 1 / 24

```
1 1 0 0 0 0 0 0   1 0 1 0 1 0 0 0   0 0 0 0 0 0 0 1   0 0 0 0 0 0 0 1
```

255.255.255.0	192.168.1.0	192.168.1.255	256	192.168.1.1	192.168.1.254
NETMASK	CIDR BASE IP	BROADCAST IP	COUNT	FIRST USABLE IP	LAST USABLE IP

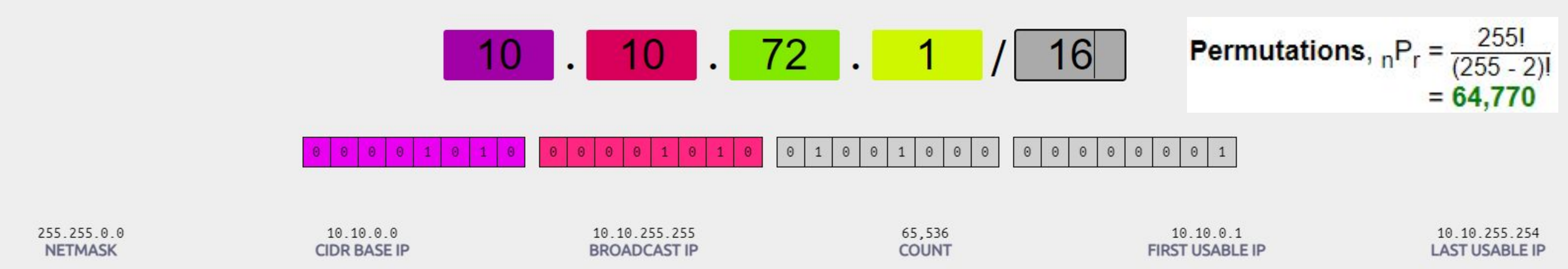


10 . 10 . 72 . 1 / 8

Permutations, $_nP_r = \frac{255!}{(255 - 3)!} = \mathbf{16,386,810}$

0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0
0	1	0	0	1	0	0	0
0	0	0	0	0	0	0	1

NETMASK	CIDR BASE IP	BROADCAST IP	COUNT	FIRST USABLE IP	LAST USABLE IP
255.0.0.0	10.0.0.0	10.255.255.255	16,777,216	10.0.0.1	10.255.255.254

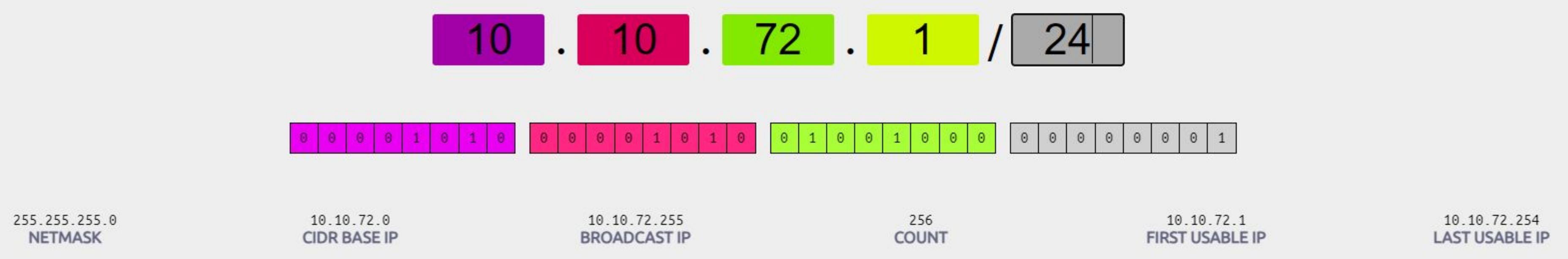


10 . 10 . 72 . 1 / 16

Permutations, $_nP_r = \frac{255!}{(255 - 2)!} = \mathbf{64,770}$

0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0
0	1	0	0	1	0	0	0
0	0	0	0	0	0	0	1

NETMASK	CIDR BASE IP	BROADCAST IP	COUNT	FIRST USABLE IP	LAST USABLE IP
255.255.0.0	10.10.0.0	10.10.255.255	65,536	10.10.0.1	10.10.255.254



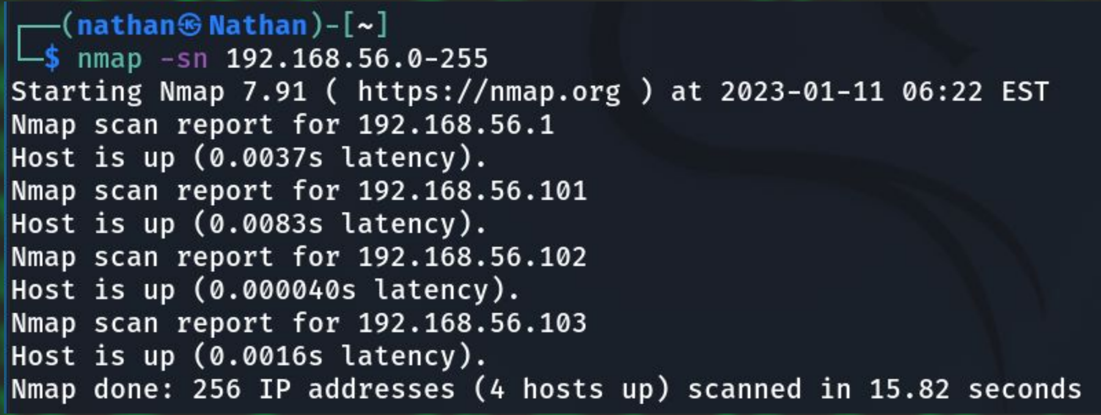
10 . 10 . 72 . 1 / 24

0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0
0	1	0	0	1	0	0	0
0	0	0	0	0	0	0	1

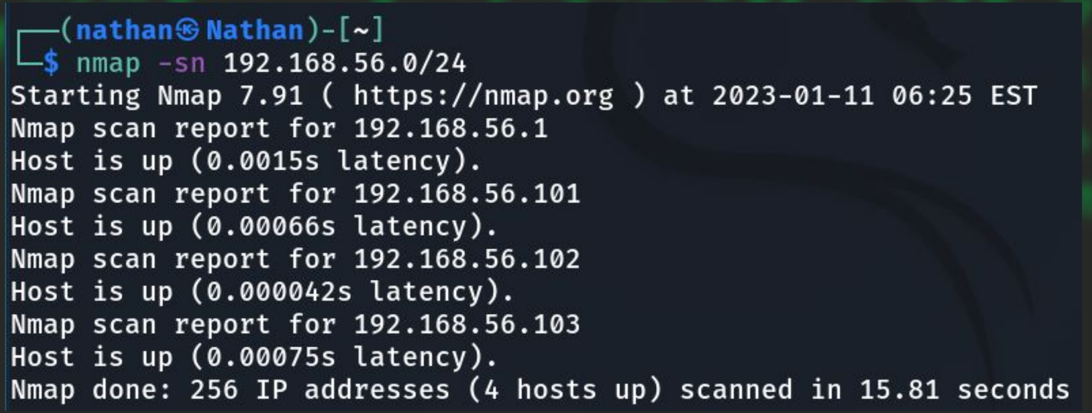
NETMASK	CIDR BASE IP	BROADCAST IP	COUNT	FIRST USABLE IP	LAST USABLE IP
255.255.255.0	10.10.72.0	10.10.72.255	256	10.10.72.1	10.10.72.254

demo

Look scanned all the network range and found 4 hosts up.



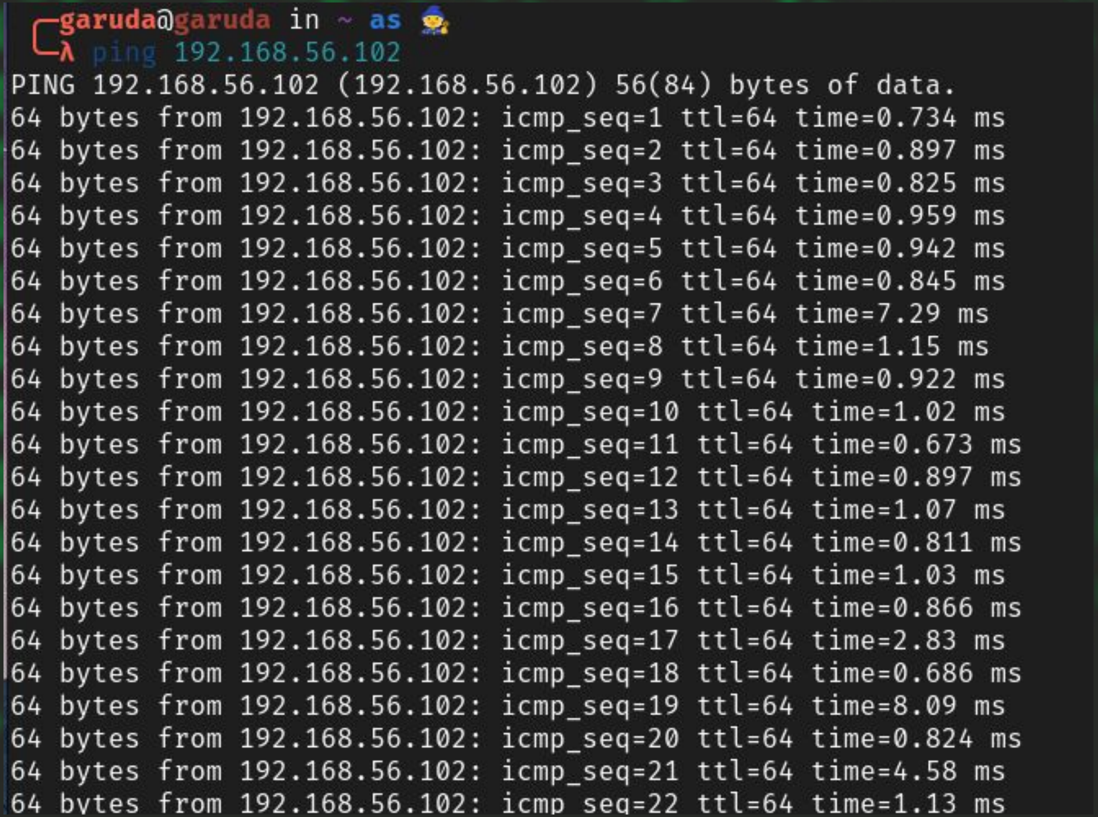
```
┌──(nathan㉿Nathan)-[~]
└─$ nmap -sn 192.168.56.0-255
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 06:22 EST
Nmap scan report for 192.168.56.1
Host is up (0.0037s latency).
Nmap scan report for 192.168.56.101
Host is up (0.0083s latency).
Nmap scan report for 192.168.56.102
Host is up (0.000040s latency).
Nmap scan report for 192.168.56.103
Host is up (0.0016s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.82 seconds
```



```
┌──(nathan㉿Nathan)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 06:25 EST
Nmap scan report for 192.168.56.1
Host is up (0.0015s latency).
Nmap scan report for 192.168.56.101
Host is up (0.00066s latency).
Nmap scan report for 192.168.56.102
Host is up (0.000042s latency).
Nmap scan report for 192.168.56.103
Host is up (0.00075s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.81 seconds
```

Warning+=1

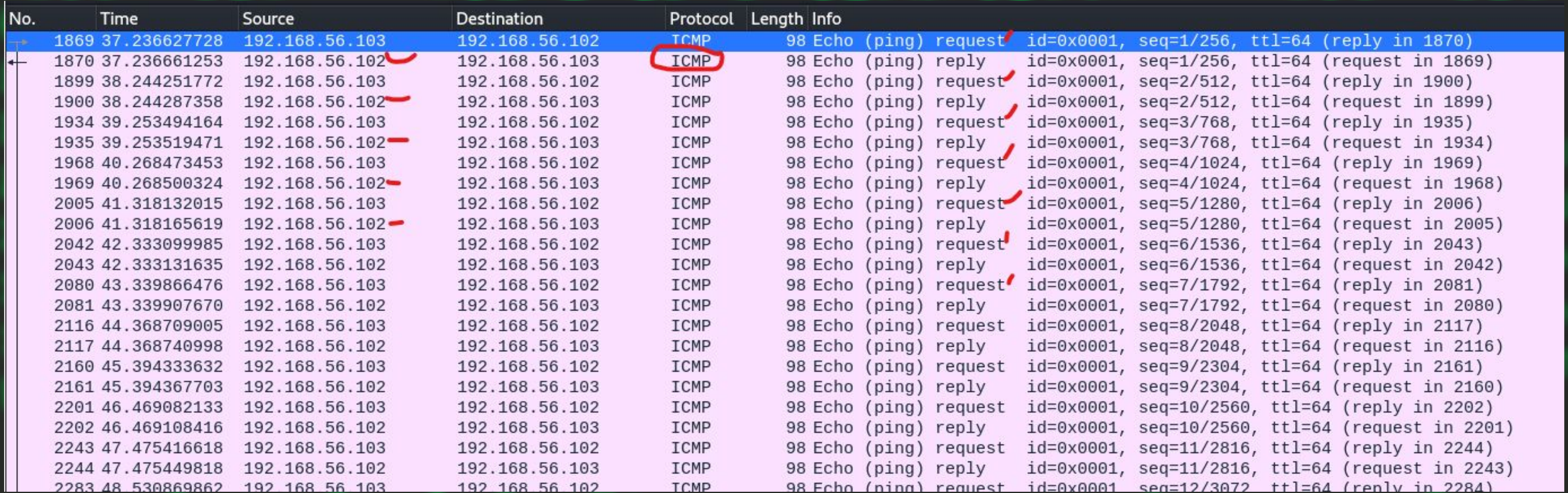
- Doing ping sweep is not undetectable thing check this.
- You are trying to ping the ip 192.168.56.102
- And you are trying to do security pentest on my system. And you are script kiddie
- But am a security Guy.so…



```
╭─garuda@garuda in ~ as 🧙
╰─λ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.734 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.897 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.825 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.959 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.942 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.845 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=7.29 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=1.15 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=0.922 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=1.02 ms
64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=0.673 ms
64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=0.897 ms
64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=1.07 ms
64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=0.811 ms
64 bytes from 192.168.56.102: icmp_seq=15 ttl=64 time=1.03 ms
64 bytes from 192.168.56.102: icmp_seq=16 ttl=64 time=0.866 ms
64 bytes from 192.168.56.102: icmp_seq=17 ttl=64 time=2.83 ms
64 bytes from 192.168.56.102: icmp_seq=18 ttl=64 time=0.686 ms
64 bytes from 192.168.56.102: icmp_seq=19 ttl=64 time=8.09 ms
64 bytes from 192.168.56.102: icmp_seq=20 ttl=64 time=0.824 ms
64 bytes from 192.168.56.102: icmp_seq=21 ttl=64 time=4.58 ms
64 bytes from 192.168.56.102: icmp_seq=22 ttl=64 time=1.13 ms
```

BOOM!!

- I can see you on my system when you try to do pings on my system. BE SAFE!

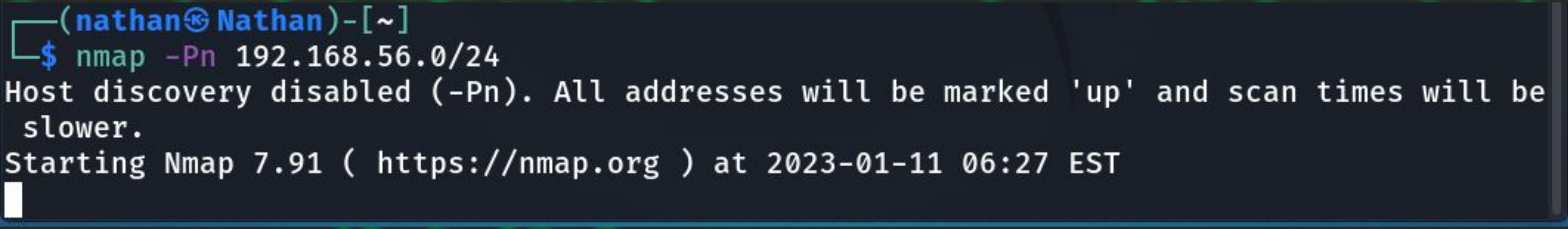


No.	Time	Source	Destination	Protocol	Length	Info
1869	37.236627728	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1870)
1870	37.236661253	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1869)
1899	38.244251772	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 1900)
1900	38.244287358	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 1899)
1934	39.253494164	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 1935)
1935	39.253519471	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 1934)
1968	40.268473453	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 1969)
1969	40.268500324	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 1968)
2005	41.318132015	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 2006)
2006	41.318165619	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in 2005)
2042	42.333099985	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 2043)
2043	42.333131635	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request in 2042)
2080	43.339866476	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in 2081)
2081	43.339907670	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=7/1792, ttl=64 (request in 2080)
2116	44.368709005	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=8/2048, ttl=64 (reply in 2117)
2117	44.368740998	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=8/2048, ttl=64 (request in 2116)
2160	45.394333632	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (reply in 2161)
2161	45.394367703	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 2160)
2201	46.469082133	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (reply in 2202)
2202	46.469108416	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 2201)
2243	47.475416618	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=11/2816, ttl=64 (reply in 2244)
2244	47.475449818	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 2243)
2283	48.530869862	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=12/3072, ttl=64 (reply in 2284)

- Blue Team Hackers Do this. Like { log analysis, SOC analysis, Intrusion Detection, Incident Response }

warning++

- Some Organizations or system admins, will block any ICMP requests
- Here the ping sweep wont work, and when you try this it says “host is down” but it is not
- To make it work we just escape the some option
- Syntax:
    - nmap -Pn IP
- This method will Jump host discovery because it will take the ip as Up and try to do port discoveries.



```
┌──(nathan㉿Nathan)-[~]
└─$ nmap -Pn 192.168.56.0/24
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be
 slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 06:27 EST
█
```

What is PORT?

- Port is process-specific or an application-specific construct serving as a **communication endpoint**, which is used by the Transport Layer protocols of Internet Protocol suite, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP)
- It is like a door for some purpose/service
- Example: if you want to get in to your house by which method do u get it?
  - BY DOOR
- Here there are different objects to get in, if wind is wanted in the house we might use windows.
- So here in there scenario
  - Windows are for winds
  - Doors are for human
- These are ports those can help u to get it.

…

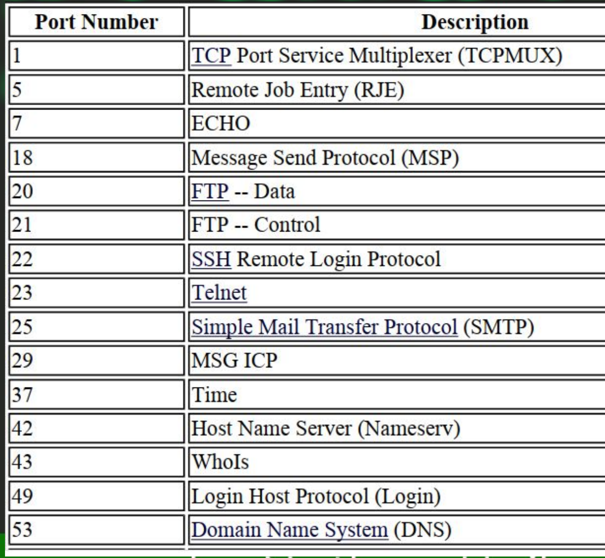
Also you home can have different doors and the main gate in your bedroom can be number 1 ,the salon door is number 2….

On computer there are different 65,536 ports with different job(like the window and door)

- 1-1024 = reserved(well known) ports

Example:

- HTTP(80) - unsecured Web port
- HTTPS(443) - secured web port
- FTP(21) - File transfering port
- SSH(22) - Secured shell port



Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name System (DNS)

Port status

Ports can be on different status

- Open ports
  - THESE are ports open for accepting any requests.
  - Having an open window can lead to any kind of gas(ጭስ) or air getting to our house.
- Closed ports
  - THESE are ports which are not accepting any request but there is some service running on it.
  - Ex: Having your home door close.
    - still the door helps sometime, but not for now
- Filtered ports
  - These are ports which nmap is not sure of being open or closed.

Open port discovery

On some system ports can be open for some purpose

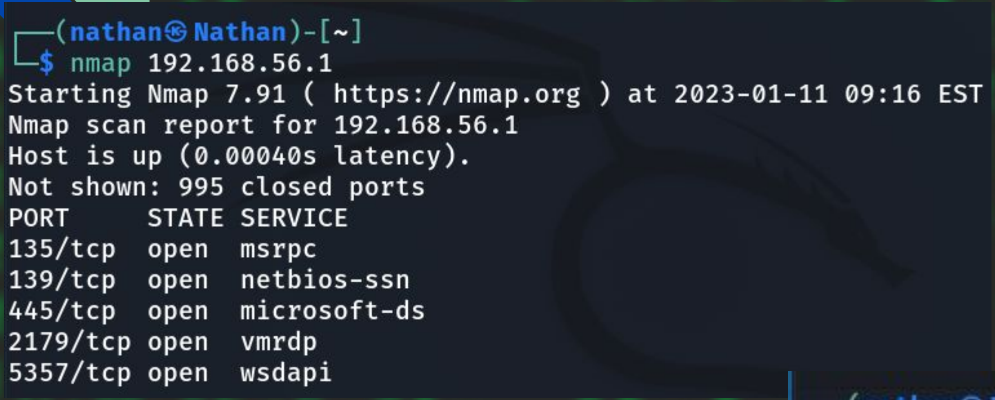
Example: anywhere when you access websites there is web port open(80,443),

If you are getting some shell activity there is port 22 open

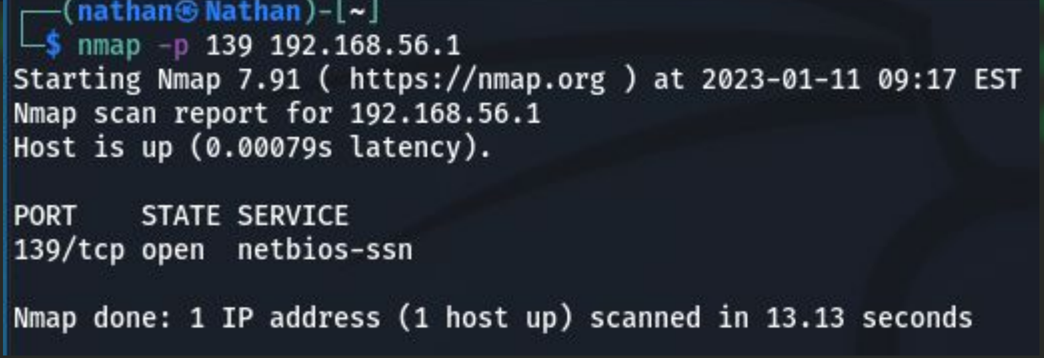
- there problem, is there are some ports open without intention, this leads to attack

- We can use nmap to check which port is open/closed
- And this is called port discovery
- Syntax:
  - nmap IP => only the 1000 ports
  - nmap -p port 1,port2,port3 IP => only port 1,2,3
  - nmap -p- IP => All the 65K port

Demo

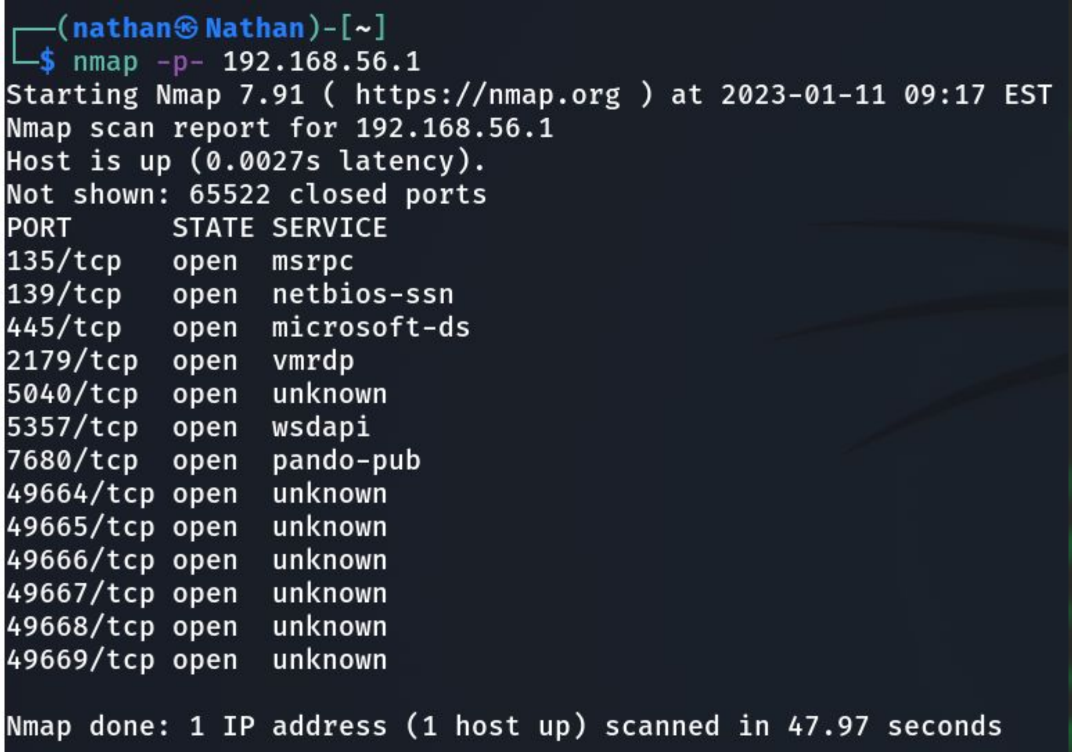


```
┌──(nathan㉿Nathan)-[~]
└─$ nmap 192.168.56.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 09:16 EST
Nmap scan report for 192.168.56.1
Host is up (0.00040s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
5357/tcp open  wsdapi
```

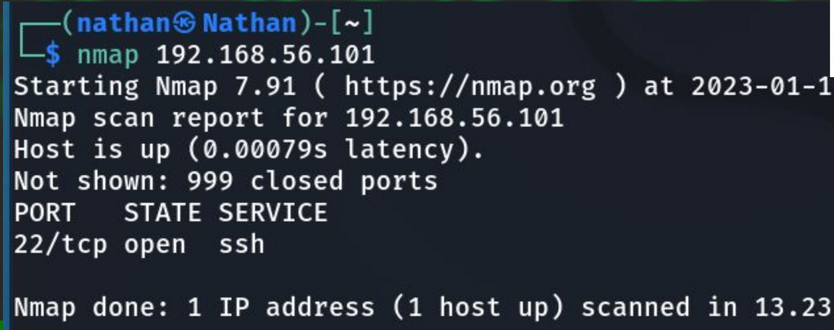


```
┌──(nathan㉿Nathan)-[~]
└─$ nmap -p 139 192.168.56.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 09:17 EST
Nmap scan report for 192.168.56.1
Host is up (0.00079s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
```

Demo

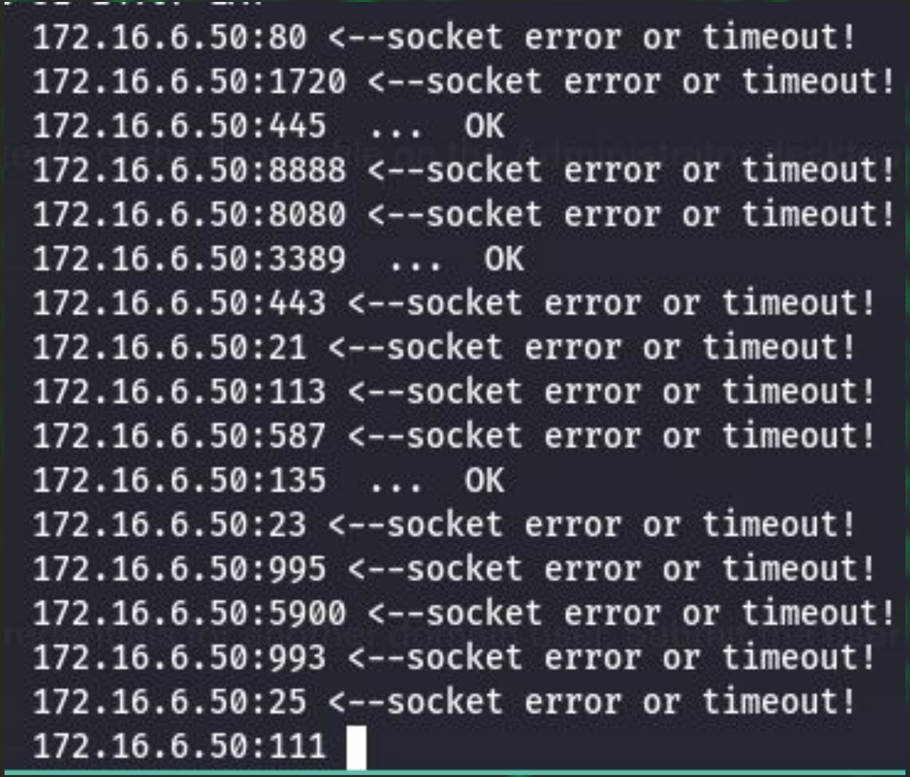


```
┌──(nathan㉿Nathan)-[~]
└─$ nmap -p- 192.168.56.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 09:17 EST
Nmap scan report for 192.168.56.1
Host is up (0.0027s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2179/tcp  open  vmrdp
5040/tcp  open  unknown
5357/tcp  open  wsdapi
7680/tcp  open  pando-pub
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 47.97 seconds
```



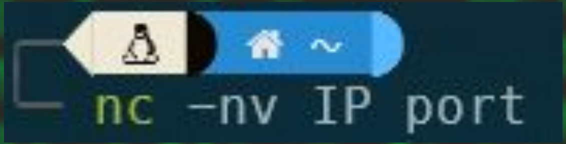
```
┌──(nathan㉿Nathan)-[~]
└─$ nmap 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 09:16 EST
Nmap scan report for 192.168.56.101
Host is up (0.00079s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

It will send request with the top 1000 ports by default

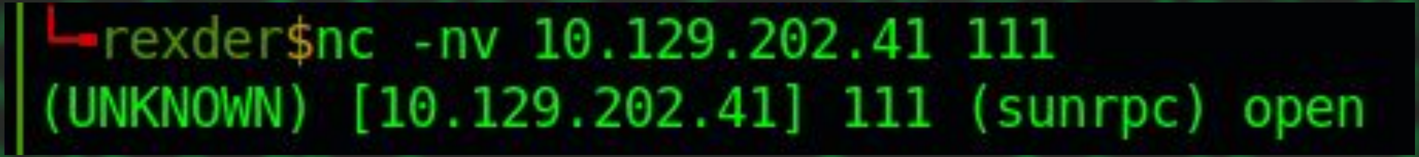


```
172.16.6.50:80 <--socket error or timeout!
172.16.6.50:1720 <--socket error or timeout!
172.16.6.50:445  ...  OK
172.16.6.50:8888 <--socket error or timeout!
172.16.6.50:8080 <--socket error or timeout!
172.16.6.50:3389  ...  OK
172.16.6.50:443 <--socket error or timeout!
172.16.6.50:21 <--socket error or timeout!
172.16.6.50:113 <--socket error or timeout!
172.16.6.50:587 <--socket error or timeout!
172.16.6.50:135  ...  OK
172.16.6.50:23 <--socket error or timeout!
172.16.6.50:995 <--socket error or timeout!
172.16.6.50:5900 <--socket error or timeout!
172.16.6.50:993 <--socket error or timeout!
172.16.6.50:25 <--socket error or timeout!
172.16.6.50:111
```

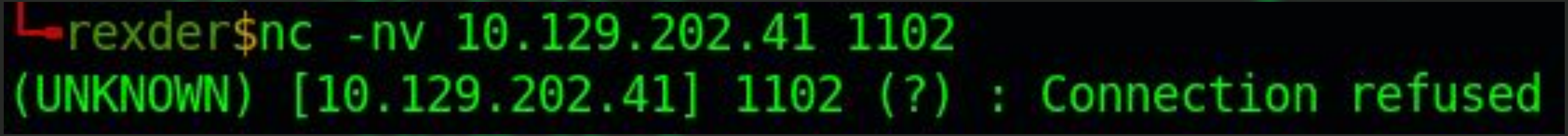
We can use Another Trick with netcat



```
nc -nv IP port
```



```
└─rexder$nc -nv 10.129.202.41 111
(UNKNOWN) [10.129.202.41] 111 (sunrpc) open
```



```
└─rexder$nc -nv 10.129.202.41 1102
(UNKNOWN) [10.129.202.41] 1102 (?) : Connection refused
```

Scanning methods

Nmap scans network in different modes

1. TCP connect (TCP scan)
2. TCP SYN (Stealth scan)
3. UDP scan
4. Xmas scan

TCP Scan

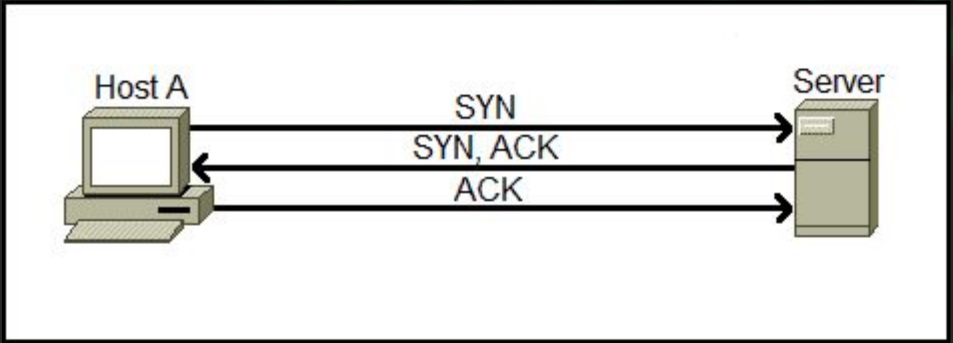
- As we saw last time TCP is the best on doing connection oriented Things.
- it is reliable But how?
- This is Because it uses 3-way HANDSHAKE!!!
- What is 3-way handshake?

3 way handshake

- When you establish a TCP connections there is something going behind the scenes
- What was the packet sent while the Ping sweep, it was the ICMP.
  - Here When we start connection we will send a Synchronization flag.
  - When the server got and accepted our request it will reply with Synchronization and Acknowledgment.
  - Finally, we will send Acknowledgement or Reset(RST) and continue because we have connection/network now.

It is like meeting someone.

1. You: hi.
2. They: hello
3. You: Nice to meet you..

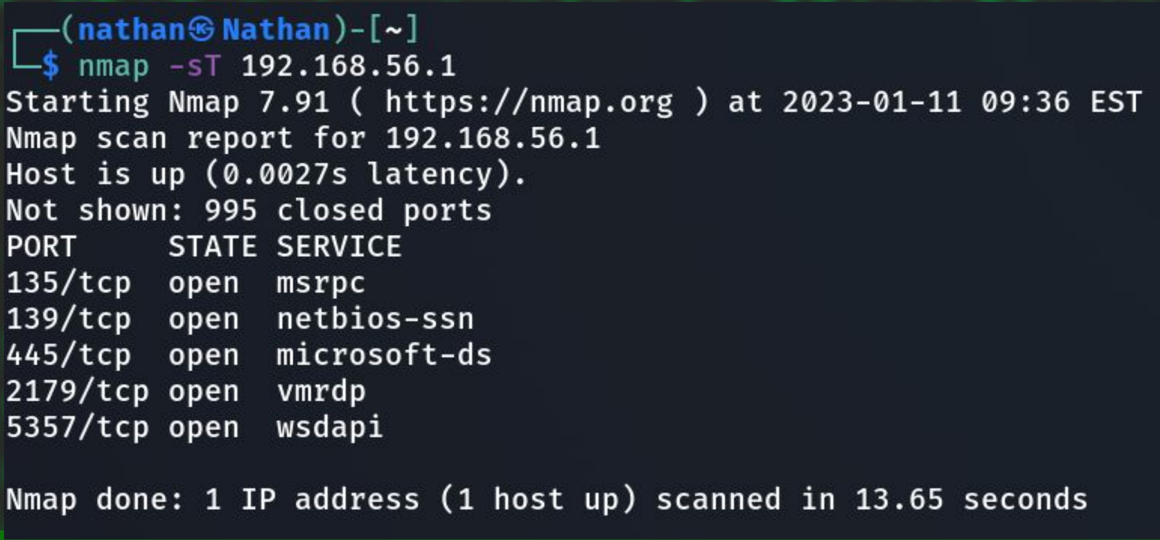


…

TCP scan works like this, so nmap will send the SYN request to the ports and if they reply with SYN/ACK nmap will reply with ACK BOOM!!! That port is open!! Else the port is closed/filtered.

Syntax:

```
nmap -sT IP
```



```
┌──(nathan㉿Nathan)-[~]
└─$ nmap -sT 192.168.56.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 09:36 EST
Nmap scan report for 192.168.56.1
Host is up (0.0027s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
```

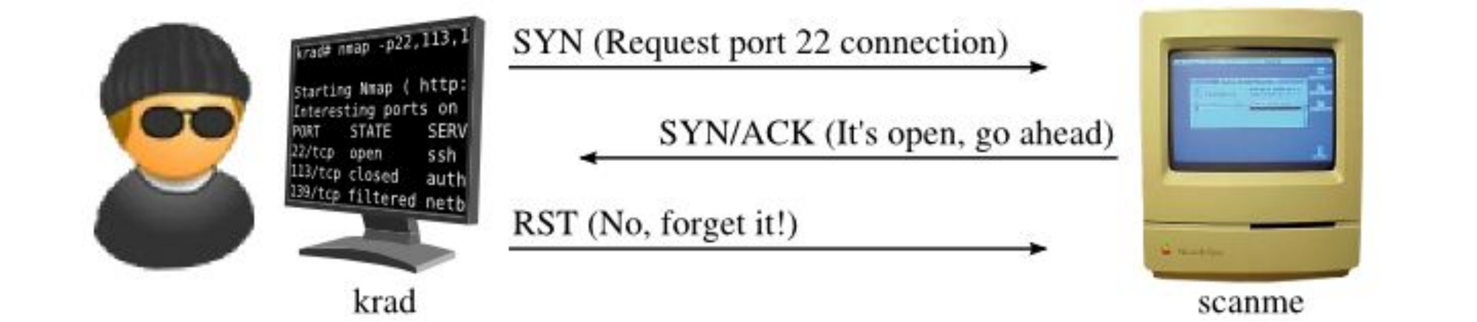
Exercise 1

some scans might take time so show me the command on the group

1. How many ports are open on google
2. What is the largest known(named) service on scanme.nmap.org
3. What is the IP address of google?
4. What the service name of port 1000 on google.com?
5. What is the largest filtered port on youtube.com?
6. How much seconds took your youtube.com scan?
7. What is the port number for service telnet on youtube.com
8. How many ports are filtered(not shown) on your youtube scan.

Stealth Scan.

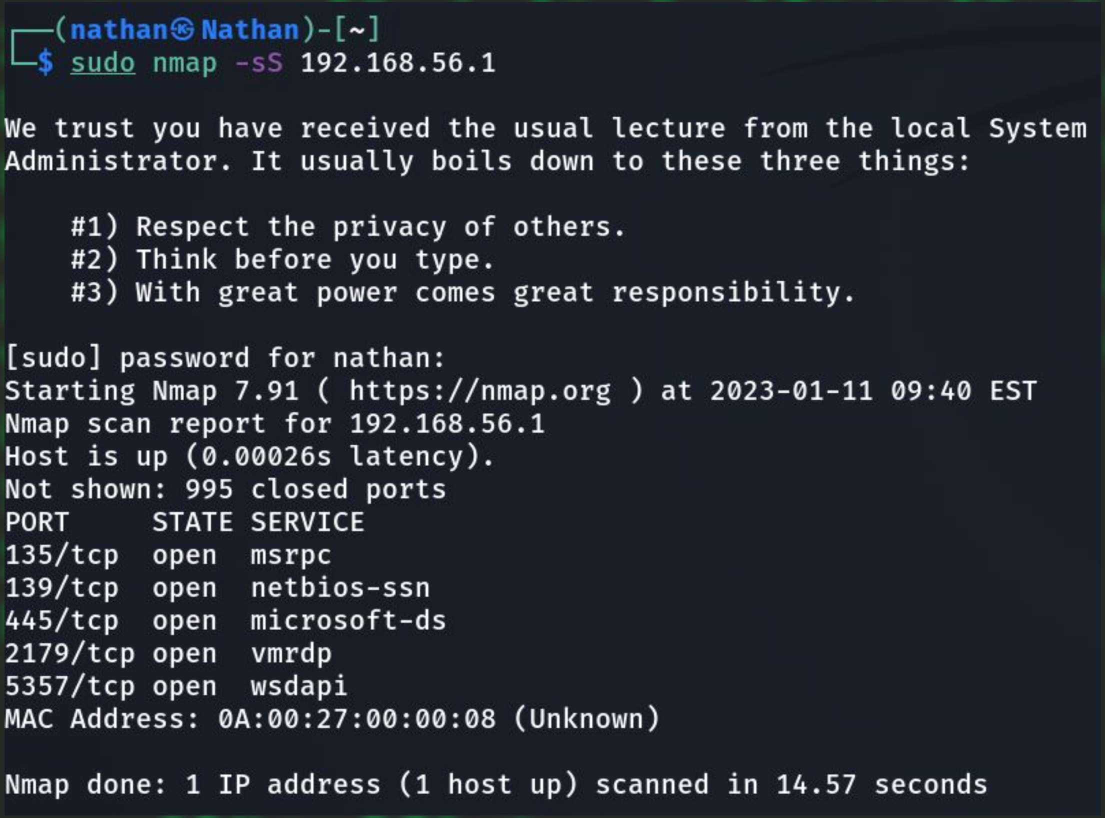
- This is TCP scan but here we dont send the last ACK flag.
- But we send the RESET flag.
- Syntax:
  - sudo nmap -sS IP



```
krad# nmap -p22,113,1

Starting Nmap ( http:
Interesting ports on
PORT    STATE    SERV
22/tcp  open     ssh
113/tcp closed   auth
139/tcp filtered netb
```

SYN (Request port 22 connection)
SYN/ACK (It's open, go ahead)
RST (No, forget it!)
krad
scanme

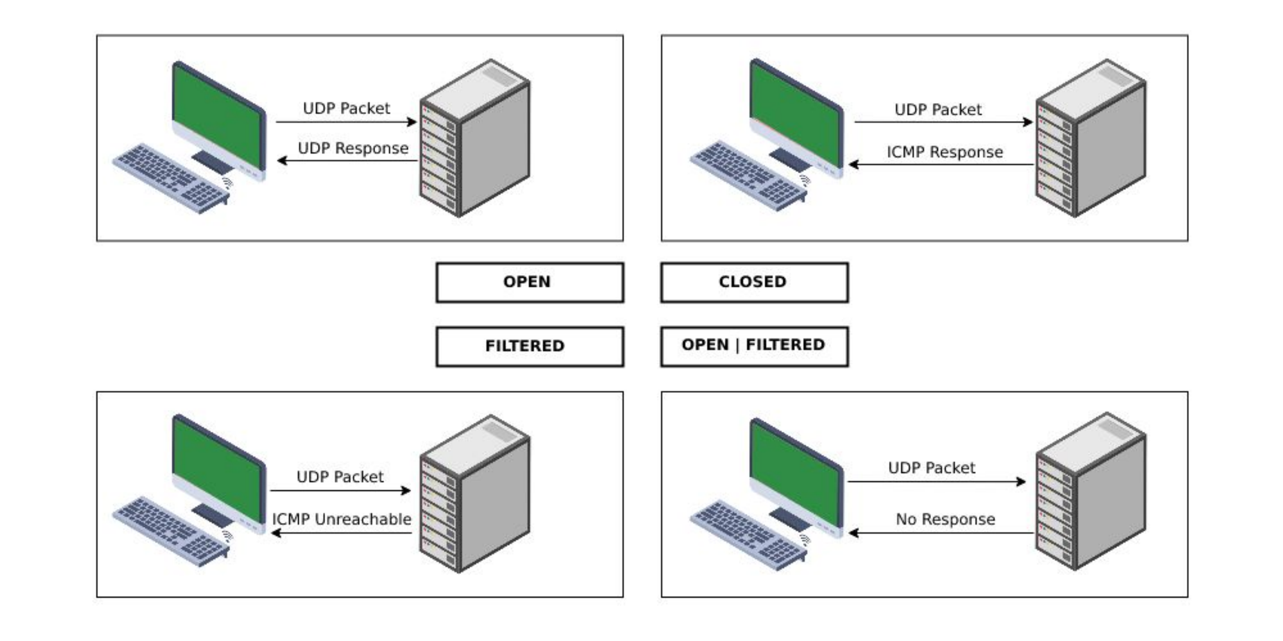
demo



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo nmap -sS 192.168.56.1

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for nathan:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 09:40 EST
Nmap scan report for 192.168.56.1
Host is up (0.00026s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
5357/tcp open  wsdapi
MAC Address: 0A:00:27:00:00:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
```

UDP scan

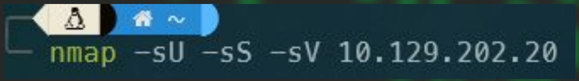
- This is a method to scan if any service/ port is using UDP



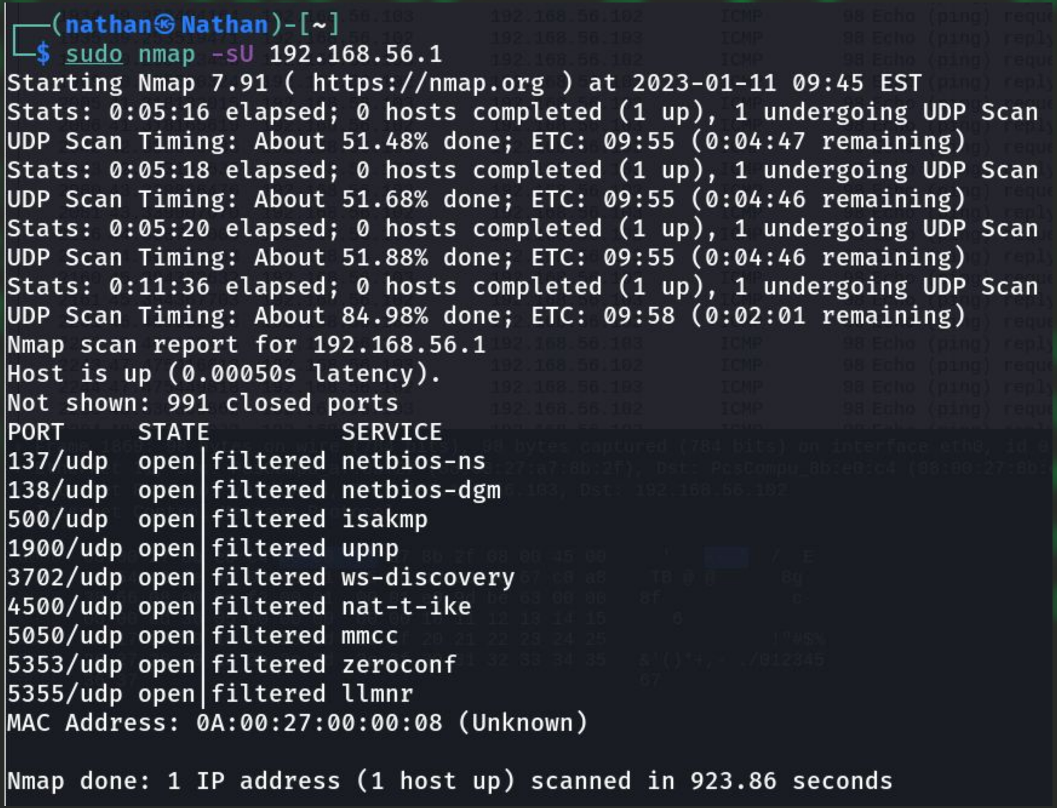
cont...

- It is slow process
- Syntax:
  - sudo nmap -sU IP
- There are some ports work on UDP, SO we need UDP scan

SO when you do Pentest do UDP and TCP scans together



```
nmap -sU -sS -sV 10.129.202.20
```



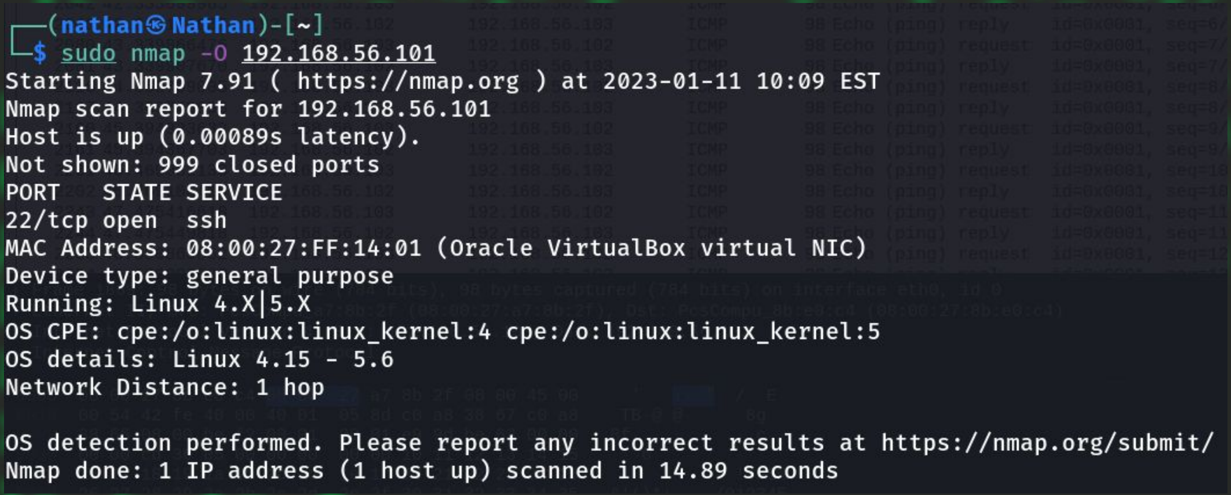
```
┌──(nathan㉿Nathan)-[~]
└─$ sudo nmap -sU 192.168.56.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 09:45 EST
Stats: 0:05:16 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 51.48% done; ETC: 09:55 (0:04:47 remaining)
Stats: 0:05:18 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 51.68% done; ETC: 09:55 (0:04:46 remaining)
Stats: 0:05:20 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 51.88% done; ETC: 09:55 (0:04:46 remaining)
Stats: 0:11:36 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 84.98% done; ETC: 09:58 (0:02:01 remaining)
Nmap scan report for 192.168.56.1
Host is up (0.00050s latency).
Not shown: 991 closed ports
PORT      STATE         SERVICE
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
500/udp   open|filtered isakmp
1900/udp  open|filtered upnp
3702/udp  open|filtered ws-discovery
4500/udp  open|filtered nat-t-ike
5050/udp  open|filtered mmcc
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr
MAC Address: 0A:00:27:00:00:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 923.86 seconds
```

Xmas Scan

- Here, The 1st thing to send is FIN/PSH/URG instead of SYN.
- If there is response like RST flag Then the system is close
- If there is no response the system is open.
- Syntax:
  - sudo nmap -sX IP

Operating System Detection

- Nmap have a feature to detect the operating system of the host.
- Syntax:
  - sudo nmap -O IP => OS detection only
  - sudo nmap -A IP => OS detection including version



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo nmap -O 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 10:09 EST
Nmap scan report for 192.168.56.101
Host is up (0.00089s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:FF:14:01 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds
```

Scan Speeds

- When nmap do its scan, it have a time waiting, after sending 1 packets to a host.
- There are 5 time waitings.
- The nmap time template is -T<0-5>
  - Insane -T5
  - Aggressive -T4
  - Normal -T3
  - Polite -T2
  - Sneaky -T1

Nmap Insane

- sending packets insanely fast and **waits only 0.3 seconds** for the response.
- scan superfast but accuracy is sacrificed sometimes.
- Nmap gives-up on a host if it couldn’t complete the scan within 15 minutes.
- Other than that, -T5 should be used only on a fast network and high-end systems as sending packets this fast can affect the working of the network or system and can result in system failure.
- Syntax:
  - `nmap -T5 IP`

Nmap Aggressive

This template is used for sending packets very fast and **waits only 1.25 seconds** for the response.

Nmap official documentation recommends using –T4 for “reasonably modern and reliable networks”.

Syntax:

```
nmap -T4 IP
```

Nmap Normal

- This is a default nmap timing
- Syntax:
  - nmap -T3 IP

Nmap Polite and Sneaky

These are the slowest timing.

Being slow, helps to not be detected on some risky projects.

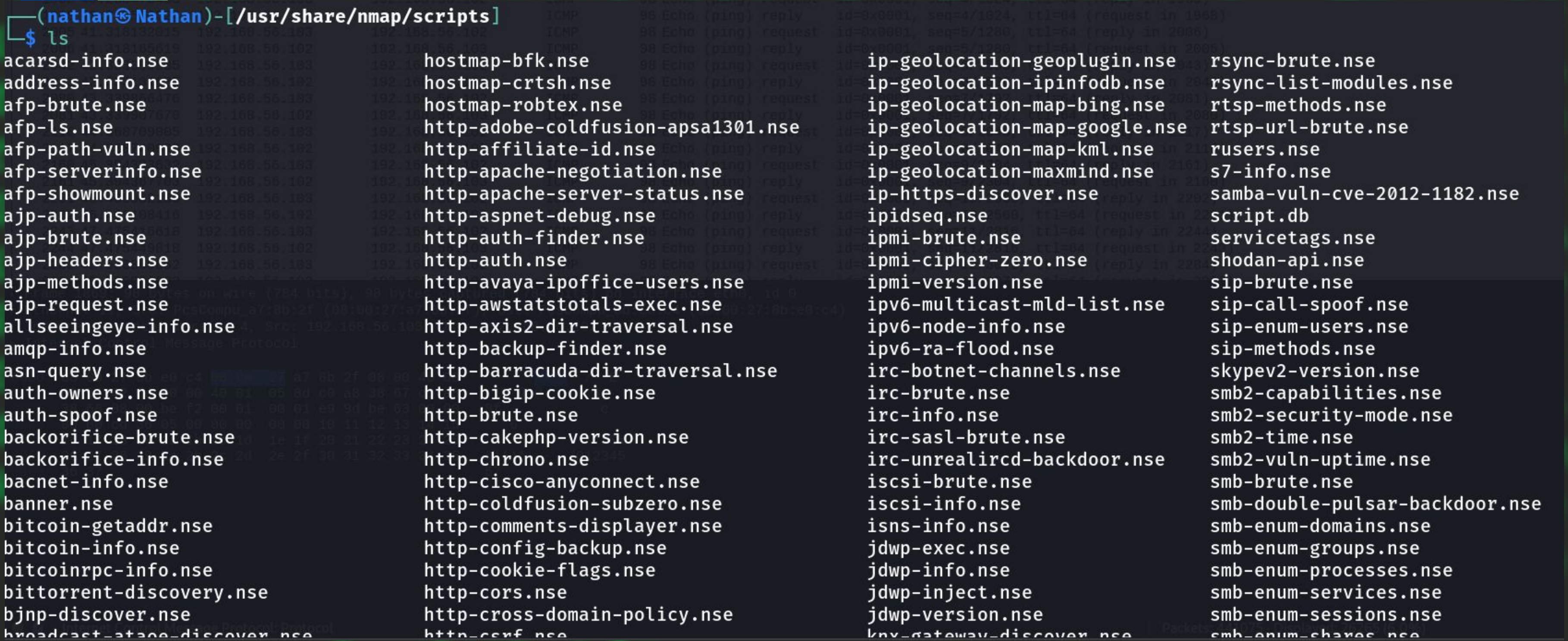
Syntax:

```
nmap -T2 IP

nmap -T1 IP
```

Nmap Script Engine(NSE)

- Nmap is capable of running some script on ports and services.
- These scripts are written in lua-programming language.
- These scripts are located in `/usr/share/nmap/scripts`
- Nmap contains a total number of 589 scripts (Version 7.70), there are a lot of scripts that are useful but not all of them works perfectly, it's like other tools a better for that particular task, so we'll look at how we can use the powerful NSE and what scripts to use.
- You can Write your own script too if you can do lua
- Syntax:
  - `nmap -sC IP`
  - `nmap --script scriptname.nse IP`
  - `Nmap -p 22 --script ssh* IP`

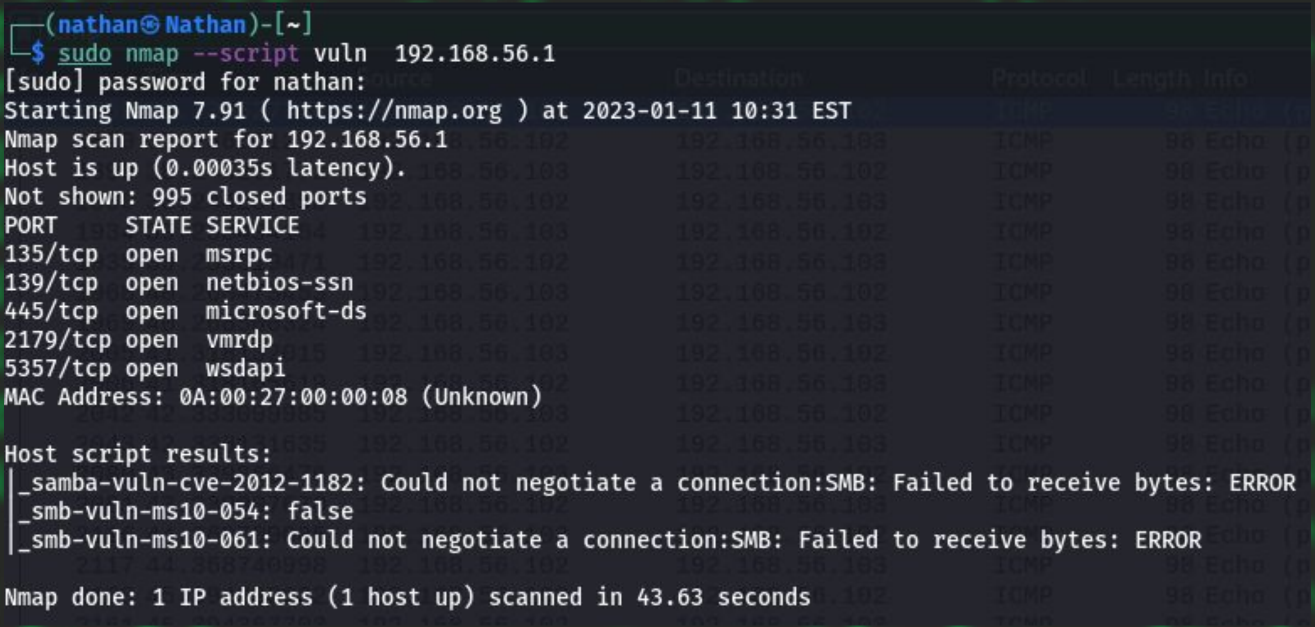
Scripts



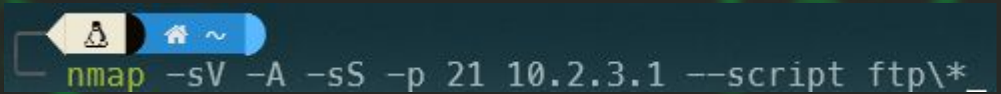
```
┌──(nathan㉿Nathan)-[/usr/share/nmap/scripts]
└─$ ls
acarsd-info.nse                       hostmap-bfk.nse                         ip-geolocation-geoplugin.nse   rsync-brute.nse
address-info.nse                      hostmap-crtsh.nse                       ip-geolocation-ipinfodb.nse    rsync-list-modules.nse
afp-brute.nse                         hostmap-robtex.nse                      ip-geolocation-map-bing.nse    rtsp-methods.nse
afp-ls.nse                            http-adobe-coldfusion-apsa1301.nse      ip-geolocation-map-google.nse  rtsp-url-brute.nse
afp-path-vuln.nse                     http-affiliate-id.nse                   ip-geolocation-map-kml.nse     rusers.nse
afp-serverinfo.nse                    http-apache-negotiation.nse             ip-geolocation-maxmind.nse     s7-info.nse
afp-showmount.nse                     http-apache-server-status.nse           ip-https-discover.nse          samba-vuln-cve-2012-1182.nse
ajp-auth.nse                          http-aspnet-debug.nse                   ipidseq.nse                    script.db
ajp-brute.nse                         http-auth-finder.nse                    ipmi-brute.nse                 servicetags.nse
ajp-headers.nse                       http-auth.nse                           ipmi-cipher-zero.nse           shodan-api.nse
ajp-methods.nse                       http-avaya-ipoffice-users.nse           ipmi-version.nse               sip-brute.nse
ajp-request.nse                       http-awstatstotals-exec.nse             ipv6-multicast-mld-list.nse    sip-call-spoof.nse
allseeingeye-info.nse                 http-axis2-dir-traversal.nse            ipv6-node-info.nse             sip-enum-users.nse
amqp-info.nse                         http-backup-finder.nse                  ipv6-ra-flood.nse              sip-methods.nse
asn-query.nse                         http-barracuda-dir-traversal.nse        irc-botnet-channels.nse        skypev2-version.nse
auth-owners.nse                       http-bigip-cookie.nse                   irc-brute.nse                  smb2-capabilities.nse
auth-spoof.nse                        http-brute.nse                          irc-info.nse                   smb2-security-mode.nse
backorifice-brute.nse                 http-cakephp-version.nse                irc-sasl-brute.nse             smb2-time.nse
backorifice-info.nse                  http-chrono.nse                         irc-unrealircd-backdoor.nse    smb2-vuln-uptime.nse
bacnet-info.nse                       http-cisco-anyconnect.nse               iscsi-brute.nse                smb-brute.nse
banner.nse                            http-coldfusion-subzero.nse             iscsi-info.nse                 smb-double-pulsar-backdoor.nse
bitcoin-getaddr.nse                   http-comments-displayer.nse             isns-info.nse                  smb-enum-domains.nse
bitcoin-info.nse                      http-config-backup.nse                  jdwp-exec.nse                  smb-enum-groups.nse
bitcoinrpc-info.nse                   http-cookie-flags.nse                   jdwp-info.nse                  smb-enum-processes.nse
bittorrent-discovery.nse              http-cors.nse                           jdwp-inject.nse                smb-enum-services.nse
bjnp-discover.nse                     http-cross-domain-policy.nse            jdwp-version.nse               smb-enum-sessions.nse
broadcast-ataoe-discover.nse          http-csrf.nse                           knx-gateway-discover.nse       smb-enum-shares.nse
```

...

- Some known scripts.
  - --script banner
    - => grabbing some details
  - --script broadcast
    - reveals broadcast information
  - --script vuln
    - test if the ports are vulnerable.



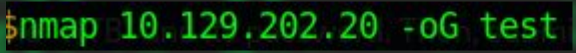
```
┌──(nathan㉿Nathan)-[~]
└─$ sudo nmap --script vuln  192.168.56.1
[sudo] password for nathan:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 10:31 EST
Nmap scan report for 192.168.56.1
Host is up (0.00035s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
5357/tcp open  wsdapi
MAC Address: 0A:00:27:00:00:08 (Unknown)

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 43.63 seconds
```



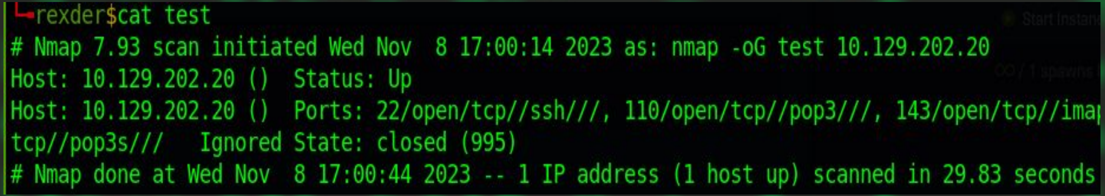
```
nmap -sV -A -sS -p 21 10.2.3.1 --script ftp\*_
```

Nmap Outputs

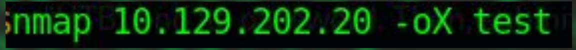
- Nmap Can Save your output using the “-oG|-oX|-oN”
    - -oG -> For Greppable formats
    - -oX -> for xml formats
    - -oN -> for Normal Saving Formats
- You can also add -v to show you results in detail it is called verbose
    - -v - little detail
    - -vv - more detail
    - -vvv - much more details



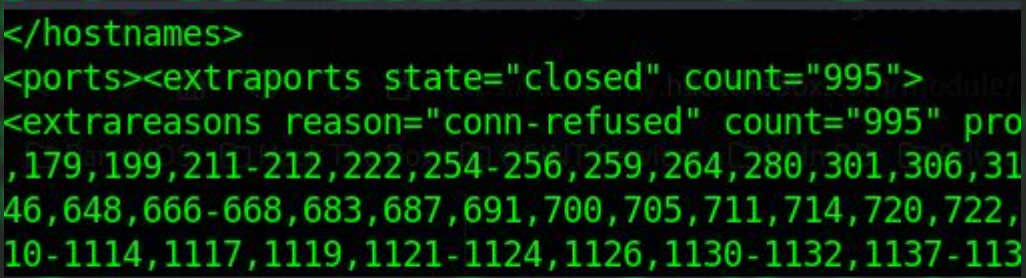
```
$nmap 10.129.202.20 -oG test
```



```
└─rexder$cat test
# Nmap 7.93 scan initiated Wed Nov  8 17:00:14 2023 as: nmap -oG test 10.129.202.20
Host: 10.129.202.20 ()  Status: Up
Host: 10.129.202.20 ()  Ports: 22/open/tcp//ssh///, 110/open/tcp//pop3///, 143/open/tcp//imap
tcp//pop3s///   Ignored State: closed (995)
# Nmap done at Wed Nov  8 17:00:44 2023 -- 1 IP address (1 host up) scanned in 29.83 seconds
```



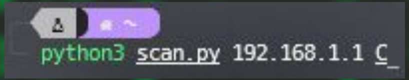
```
$nmap 10.129.202.20 -oX test
```



```
</hostnames>
<ports><extraports state="closed" count="995">
<extrareasons reason="conn-refused" count="995" pro
,179,199,211-212,222,254-256,259,264,280,301,306,31
46,648,666-668,683,687,691,700,705,711,714,720,722,
10-1114,1117,1119,1121-1124,1126,1130-1132,1137-113
```

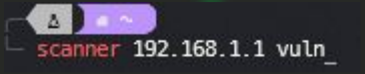
Assignment - 5% point

1. Write a port scanner without using nmap python module
2. Write a port scanner tool using nmap module. Py
    a. Read about nmap module (there will be question)
3. Write a host discovery tool in python you will determine the gateway ip and the IP class



```
python3 scan.py 192.168.1.1 C_
```

4. Write a tool in bash that accepts IP, and NSE script name then it will run nmap scan.



```
scanner 192.168.1.1 vuln_
```

CLass is Over

1) DO the notes
2) Practice well
3) Be safe. There is risky of getting imprisoned

To Advance on Nmap Read about “Firewall and IDS/IPS Evasion with Nmap”