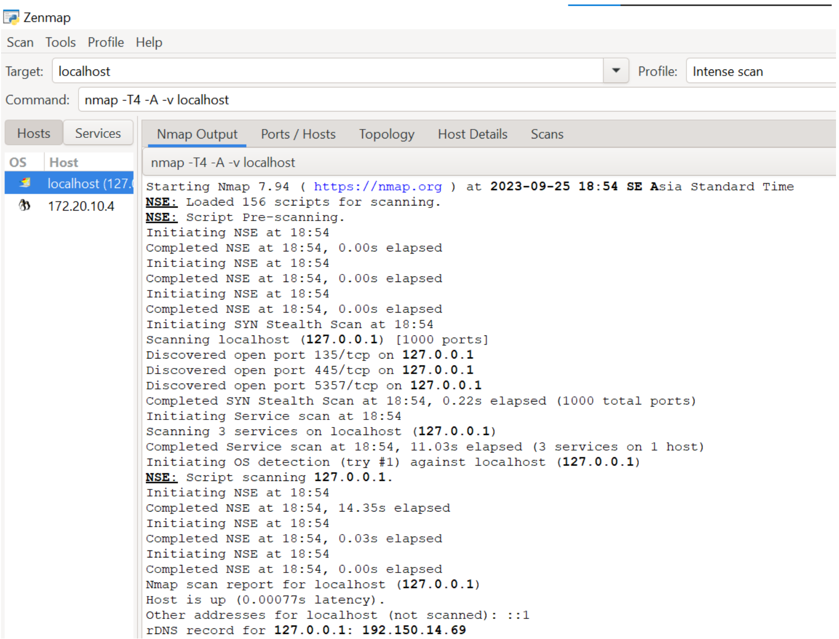
Activity 6

Attacker Window - 172.20.10.3
Victim notebook - 172.20.10.6
Victim VM - 172.20.10.4

1. Notice the open ports on all 3 devices (the attacker notebook, the target notebook, and the target Linux VM).

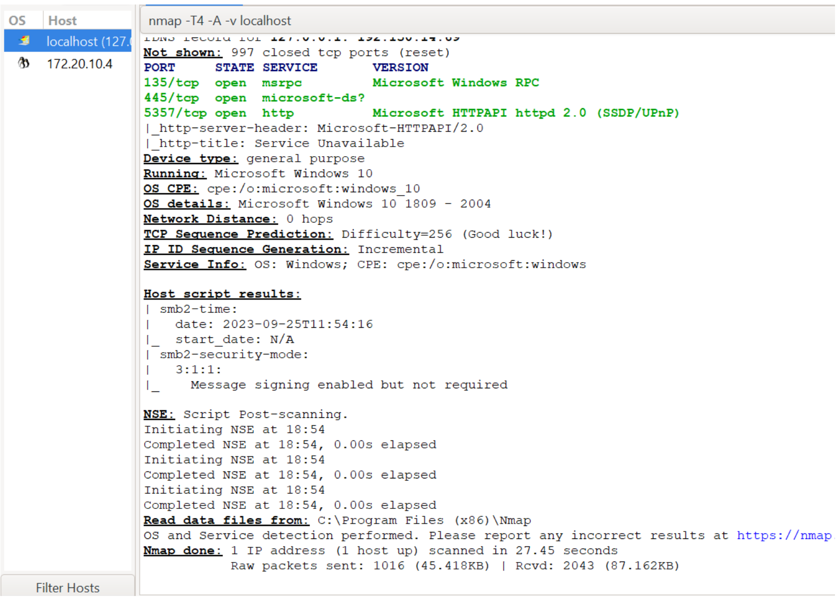
Does anything look suspicious, i.e., some ports that you are not aware of that are open on the VM or on your notebooks? **(Just notice the MySQL in the background)**

Attacker Window - 172.20.10.3



Target: localhost
Profile: Intense scan
Command: nmap -T4 -A -v localhost

```
nmap -T4 -A -v localhost
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 18:54 SE Asia Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Initiating SYN Stealth Scan at 18:54
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Completed SYN Stealth Scan at 18:54, 0.22s elapsed (1000 total ports)
Initiating Service scan at 18:54
Scanning 3 services on localhost (127.0.0.1)
Completed Service scan at 18:54, 11.03s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 18:54
Completed NSE at 18:54, 14.35s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.03s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00077s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: 192.150.14.69
```

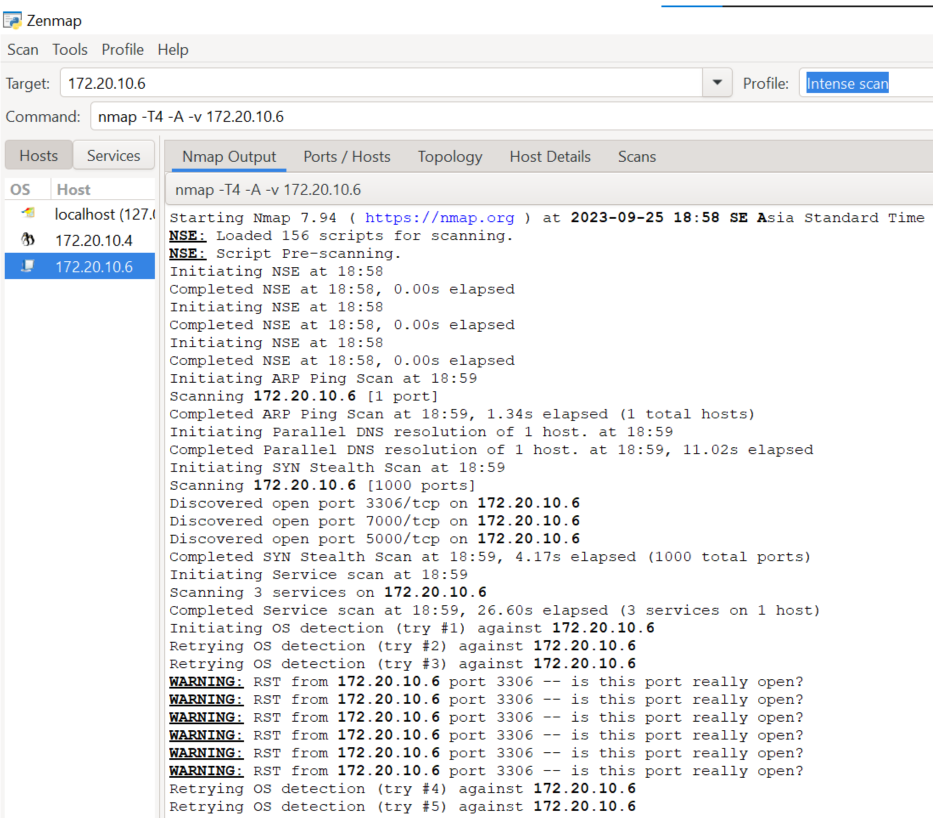


```
nmap -T4 -A -v localhost
rDNS record for 127.0.0.1: 192.150.14.69
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 2004
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-09-25T11:54:16
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap
Nmap done: 1 IP address (1 host up) scanned in 27.45 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2043 (87.162KB)
```

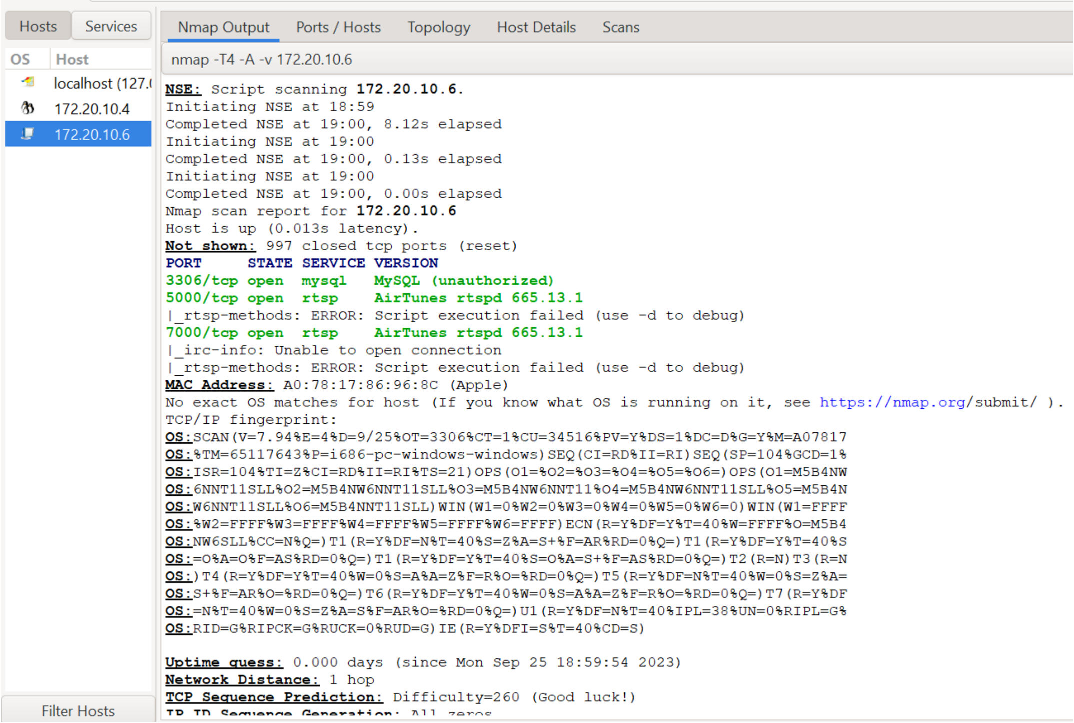
Victim notebook - 172.20.10.6



Target: 172.20.10.6 Profile: Intense scan

Command: nmap -T4 -A -v 172.20.10.6

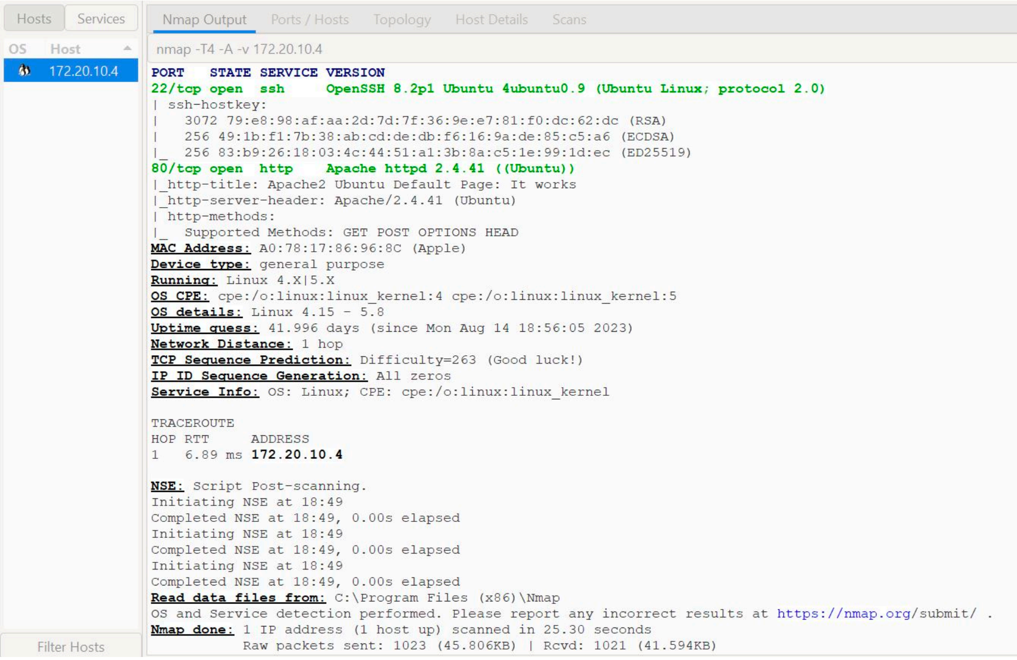
```
nmap -T4 -A -v 172.20.10.6
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 18:58 SE Asia Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:58
Completed NSE at 18:58, 0.00s elapsed
Initiating NSE at 18:58
Completed NSE at 18:58, 0.00s elapsed
Initiating NSE at 18:58
Completed NSE at 18:58, 0.00s elapsed
Initiating ARP Ping Scan at 18:59
Scanning 172.20.10.6 [1 port]
Completed ARP Ping Scan at 18:59, 1.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:59
Completed Parallel DNS resolution of 1 host. at 18:59, 11.02s elapsed
Initiating SYN Stealth Scan at 18:59
Scanning 172.20.10.6 [1000 ports]
Discovered open port 3306/tcp on 172.20.10.6
Discovered open port 7000/tcp on 172.20.10.6
Discovered open port 5000/tcp on 172.20.10.6
Completed SYN Stealth Scan at 18:59, 4.17s elapsed (1000 total ports)
Initiating Service scan at 18:59
Scanning 3 services on 172.20.10.6
Completed Service scan at 18:59, 26.60s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 172.20.10.6
Retrying OS detection (try #2) against 172.20.10.6
Retrying OS detection (try #3) against 172.20.10.6
WARNING: RST from 172.20.10.6 port 3306 -- is this port really open?
WARNING: RST from 172.20.10.6 port 3306 -- is this port really open?
WARNING: RST from 172.20.10.6 port 3306 -- is this port really open?
WARNING: RST from 172.20.10.6 port 3306 -- is this port really open?
WARNING: RST from 172.20.10.6 port 3306 -- is this port really open?
WARNING: RST from 172.20.10.6 port 3306 -- is this port really open?
Retrying OS detection (try #4) against 172.20.10.6
Retrying OS detection (try #5) against 172.20.10.6
```



```
nmap -T4 -A -v 172.20.10.6
NSE: Script scanning 172.20.10.6.
Initiating NSE at 18:59
Completed NSE at 19:00, 8.12s elapsed
Initiating NSE at 19:00
Completed NSE at 19:00, 0.13s elapsed
Initiating NSE at 19:00
Completed NSE at 19:00, 0.00s elapsed
Nmap scan report for 172.20.10.6
Host is up (0.013s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
5000/tcp open  rtsp    AirTunes rtspd 665.13.1
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
7000/tcp open  rtsp    AirTunes rtspd 665.13.1
|_irc-info: Unable to open connection
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
MAC Address: A0:78:17:86:96:8C (Apple)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=9/25%OT=3306%CT=1%CU=34516%PV=Y%DS=1%DC=D%G=Y%M=A07817
OS:%TM=65117643%P=i686-pc-windows-windows)SEQ(CI=RD%II=RI)SEQ(SP=104%GCD=1%
OS:ISR=104%TI=Z%CI=RD%II=RI%TS=21)OPS(O1=%O2=%O3=%O4=%O5=%O6=)OPS(O1=M5B4NW
OS:6NNT11SLL%O2=M5B4NW6NNT11SLL%O3=M5B4NW6NNT11%O4=M5B4NW6NNT11SLL%O5=M5B4N
OS:W6NNT11SLL%O6=M5B4NNT11SLL)WIN(W1=0%W2=0%W3=0%W4=0%W5=0%W6=0)WIN(W1=FFFF
OS:%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4
OS:NW6SLL%CC=N%Q=)T1(R=Y%DF=N%T=40%S=Z%A=S+%F=AR%RD=0%Q=)T1(R=Y%DF=Y%T=40%S
OS:=O%A=O%F=AS%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N
OS:)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF
OS:=N%T=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%
OS:RID=G%RIPCK=G%RUCK=0%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Uptime guess: 0.000 days (since Mon Sep 25 18:59:54 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

Victim VM - 172.20.10.4

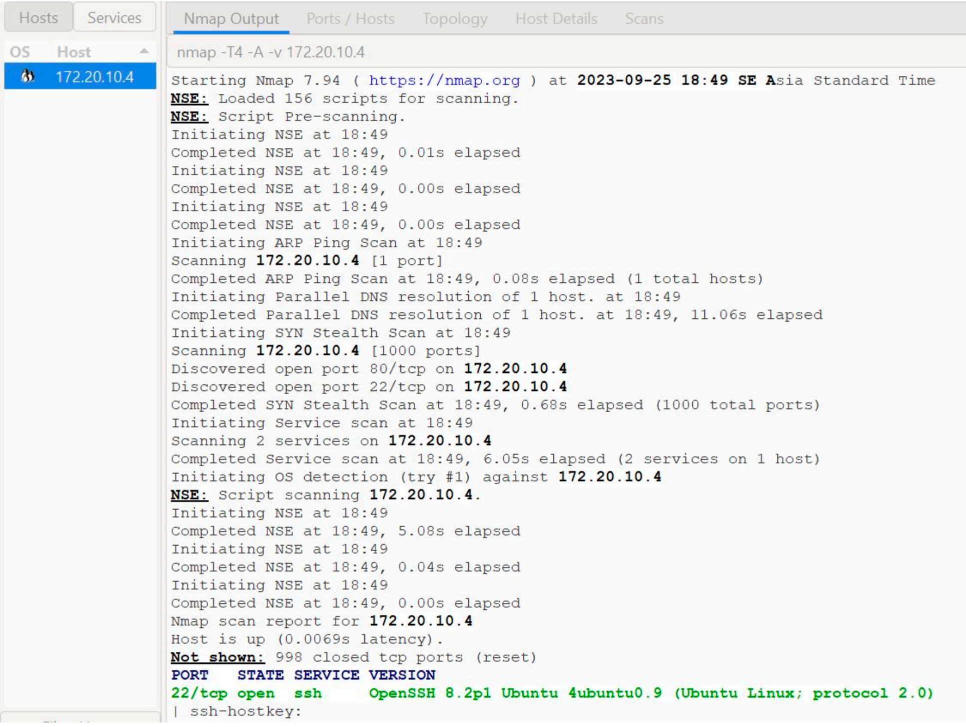


```
nmap -T4 -A -v 172.20.10.4
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 79:e8:98:af:aa:2d:7d:7f:36:9e:e7:81:f0:dc:62:dc (RSA)
|   256 49:1b:f1:7b:38:ab:cd:de:db:f6:16:9a:de:85:c5:a6 (ECDSA)
|_  256 83:b9:26:18:03:4c:44:51:a1:3b:8a:c5:1e:99:1d:ec (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: A0:78:17:86:96:8C (Apple)
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 - 5.8
Uptime guess: 41.996 days (since Mon Aug 14 18:56:05 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   6.89 ms 172.20.10.4

NSE: Script Post-scanning.
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.30 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1021 (41.594KB)
```



```
nmap -T4 -A -v 172.20.10.4
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 18:49 SE Asia Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:49
Completed NSE at 18:49, 0.01s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Initiating ARP Ping Scan at 18:49
Scanning 172.20.10.4 [1 port]
Completed ARP Ping Scan at 18:49, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:49
Completed Parallel DNS resolution of 1 host. at 18:49, 11.06s elapsed
Initiating SYN Stealth Scan at 18:49
Scanning 172.20.10.4 [1000 ports]
Discovered open port 80/tcp on 172.20.10.4
Discovered open port 22/tcp on 172.20.10.4
Completed SYN Stealth Scan at 18:49, 0.68s elapsed (1000 total ports)
Initiating Service scan at 18:49
Scanning 2 services on 172.20.10.4
Completed Service scan at 18:49, 6.05s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 172.20.10.4
NSE: Script scanning 172.20.10.4.
Initiating NSE at 18:49
Completed NSE at 18:49, 5.08s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.04s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Nmap scan report for 172.20.10.4
Host is up (0.0069s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

2. Look at the information provided by nmap about your OS's on all 3 devices. Is the information correct? Why is it or why is it not correct?

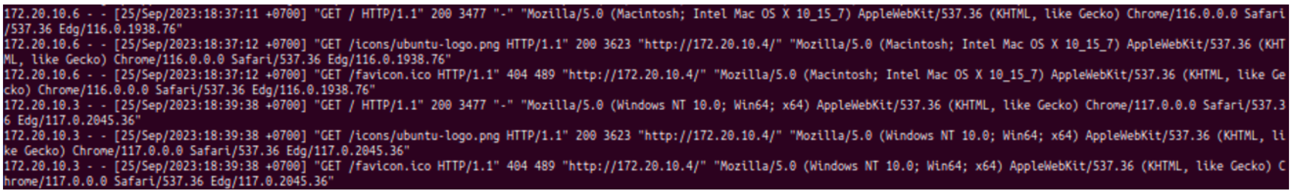
For Victim Laptop - Correct -> there is mysql sever run in the background (But The OS is still undetected)
For Victim VM - Correct -> Since I just started Apache2
For Attacker - Correct -> There is the network protocol from Microsoft run in the background (Microsoft Directory Services)

3. What do you think about the information you can get using nmap? Scary?

This information can be highly valuable to hackers because it allows them to determine what services are currently running on the victim's machine and, furthermore, it provides insight into the versions of these services in use. Knowing the service versions is particularly important because different versions may have distinct vulnerabilities, giving hackers the ability to choose the most effective method for exploiting the system.

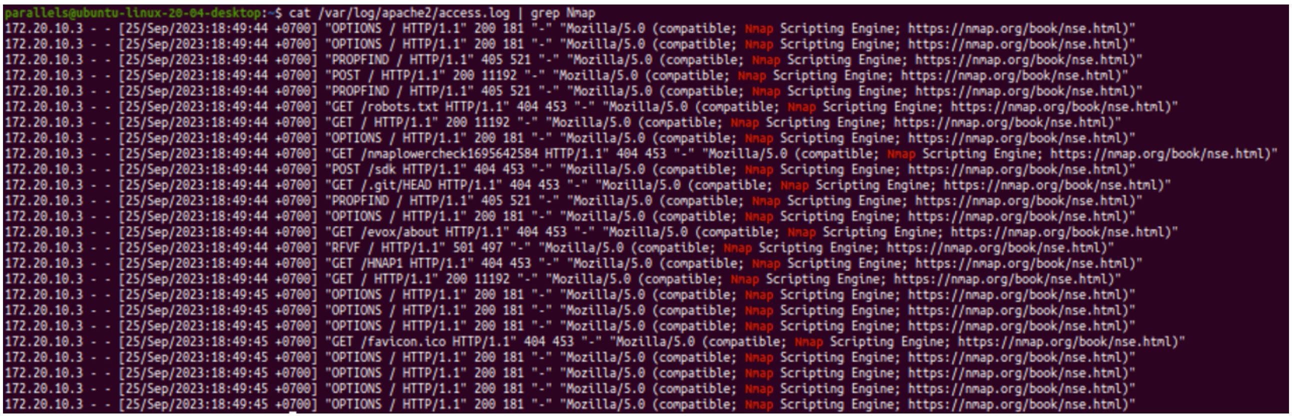
4. Look at the access.log file for the web server in your Linux VM. What IP addresses do you see accessing the web server? Which devices do these IP addresses belong to?

2 IP Address from 172.20.10.3 (From attacker) and 172.20.10.3 (From Victim laptop)



```
172.20.10.6 - - [25/Sep/2023:18:37:11 +0700] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari
/537.36 Edg/116.0.1938.76"
172.20.10.6 - - [25/Sep/2023:18:37:12 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://172.20.10.4/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHT
ML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Edg/116.0.1938.76"
172.20.10.6 - - [25/Sep/2023:18:37:12 +0700] "GET /favicon.ico HTTP/1.1" 404 489 "http://172.20.10.4/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Ge
cko) Chrome/116.0.0.0 Safari/537.36 Edg/116.0.1938.76"
172.20.10.3 - - [25/Sep/2023:18:39:38 +0700] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.3
6 Edg/117.0.2045.36"
172.20.10.3 - - [25/Sep/2023:18:39:38 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://172.20.10.4/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
ke Gecko) Chrome/117.0.0.0 Safari/537.36 Edg/117.0.2045.36"
172.20.10.3 - - [25/Sep/2023:18:39:38 +0700] "GET /favicon.ico HTTP/1.1" 404 489 "http://172.20.10.4/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C
hrome/117.0.0.0 Safari/537.36 Edg/117.0.2045.36"
```

5. Find the nmap scan in the web server log. Copy the lines from the log file that were created because of the nmap scan.



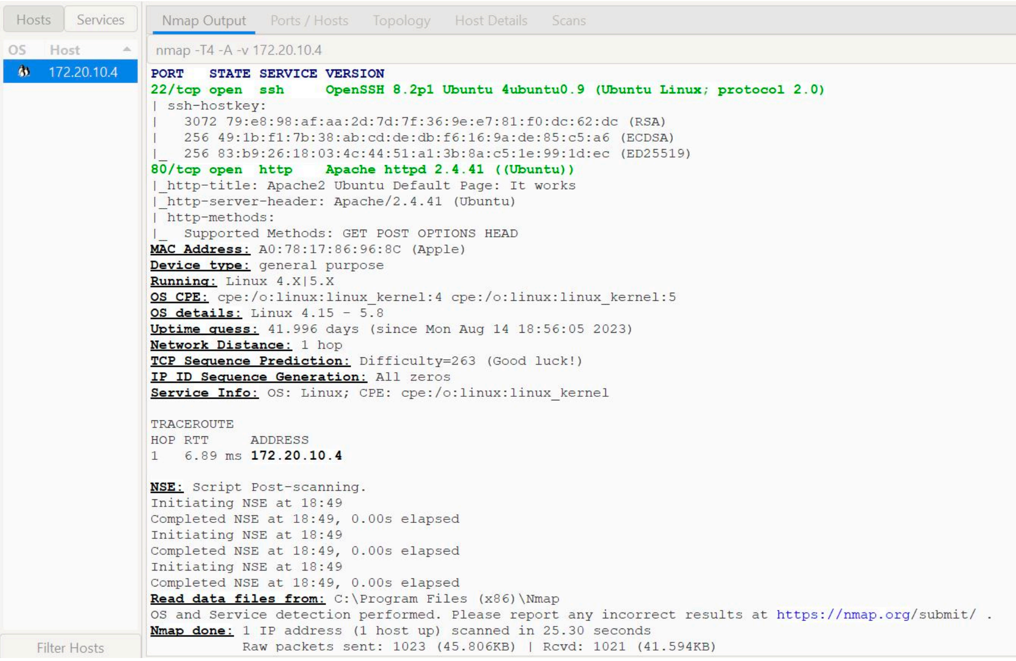
```
parallels@ubuntu-linux-20-04-desktop:~$ cat /var/log/apache2/access.log | grep Nmap
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "PROPFIND / HTTP/1.1" 405 521 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "POST / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "PROPFIND / HTTP/1.1" 405 521 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "GET /robots.txt HTTP/1.1" 404 453 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "GET / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "GET /nmaplowercheck1695642584 HTTP/1.1" 404 453 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "POST /sdk HTTP/1.1" 404 453 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "GET /.git/HEAD HTTP/1.1" 404 453 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "PROPFIND / HTTP/1.1" 405 521 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "GET /evox/about HTTP/1.1" 404 453 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "RFVF / HTTP/1.1" 501 497 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "GET /HNAP1 HTTP/1.1" 404 453 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:44 +0700] "GET / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "GET /favicon.ico HTTP/1.1" 404 453 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.10.3 - - [25/Sep/2023:18:49:45 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

6. After you successfully install your iptable rule(s), how do the reported results from your new nmap scan compare to your previous scan before using iptables? Look to see if OS detection, port open results, etc. have changed. Something(s) have definitely changed.

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
sudo iptables -A INPUT -s 172.20.10.6 -p tcp --sport 22 -j ACCEPT
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

After I added the rules the scan found only 80/tcp in the second result.

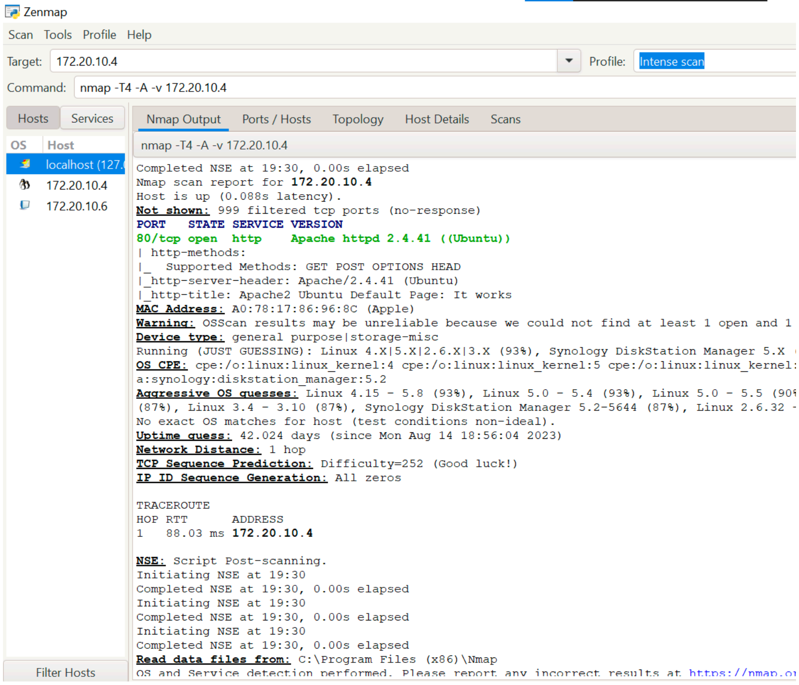
And the OS is Linux



```
nmap -T4 -A -v 172.20.10.4
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 79:e8:98:af:aa:2d:7d:7f:36:9e:e7:81:f0:dc:62:dc (RSA)
|   256 49:1b:f1:7b:38:ab:cd:de:db:f6:16:9a:de:85:c5:a6 (ECDSA)
|_  256 83:b9:26:18:03:4c:44:51:a1:3b:8a:c5:1e:99:1d:ec (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: A0:78:17:86:96:8C (Apple)
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 - 5.8
Uptime guess: 41.996 days (since Mon Aug 14 18:56:05 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   6.89 ms 172.20.10.4

NSE: Script Post-scanning.
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.30 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1021 (41.594KB)
```



Target: 172.20.10.4

Profile: Intense scan

Command: nmap -T4 -A -v 172.20.10.4

```
nmap -T4 -A -v 172.20.10.4
Completed NSE at 19:30, 0.00s elapsed
Nmap scan report for 172.20.10.4
Host is up (0.088s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: A0:78:17:86:96:8C (Apple)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (93%), Synology DiskStation Manager 5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:
a:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 4.15 - 5.8 (93%), Linux 5.0 - 5.4 (93%), Linux 5.0 - 5.5 (90
(87%), Linux 3.4 - 3.10 (87%), Synology DiskStation Manager 5.2-5644 (87%), Linux 2.6.32 -
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 42.024 days (since Mon Aug 14 18:56:04 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1   88.03 ms 172.20.10.4

NSE: Script Post-scanning.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.o
```

7. Notice that nmap can still figure out you have Apache httpd running. Look at the access.log file for the web server in your Linux VM. Are the logs the same as in Part II?

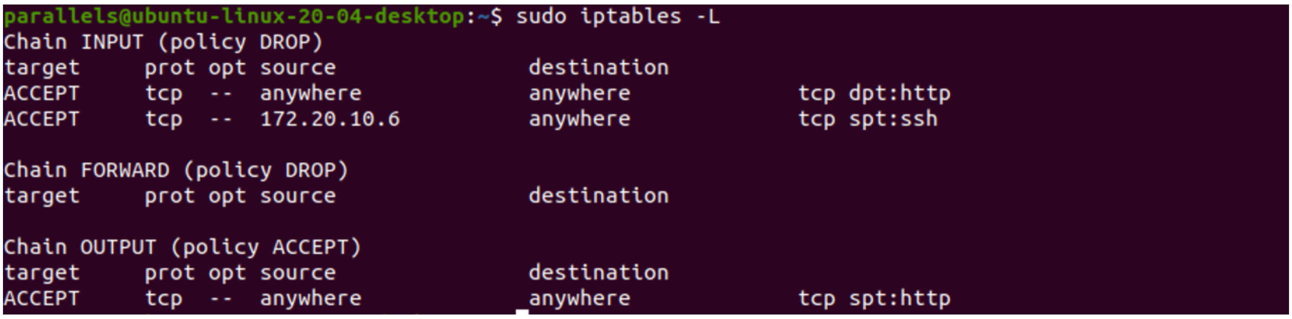
No, many logs are added.

8. Explain whether or not you could prevent nmap from reaching the web server while still allowing legitimate clients to get service. Will a firewall be sufficient for this? Or do you need some other device? Please think critically about this.

Normally, blocking nmap scans while permitting legitimate client access to a web server is a difficult task. If a server owner wants to restrict access from a specific country, they can configure iptables to drop traffic from IP addresses originating in that country. However, people within that country may still access the website using VPNs or other means.

Additionally, nmap can employ standard HTTP methods, similar to regular users, making it complex for a firewall to differentiate between nmap scans and valid requests.

9. What are your firewall rules? Run iptables -L on your VM and enter the output here.



```
parallels@ubuntu-linux-20-04-desktop:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  172.20.10.6          anywhere             tcp spt:ssh

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:http
```