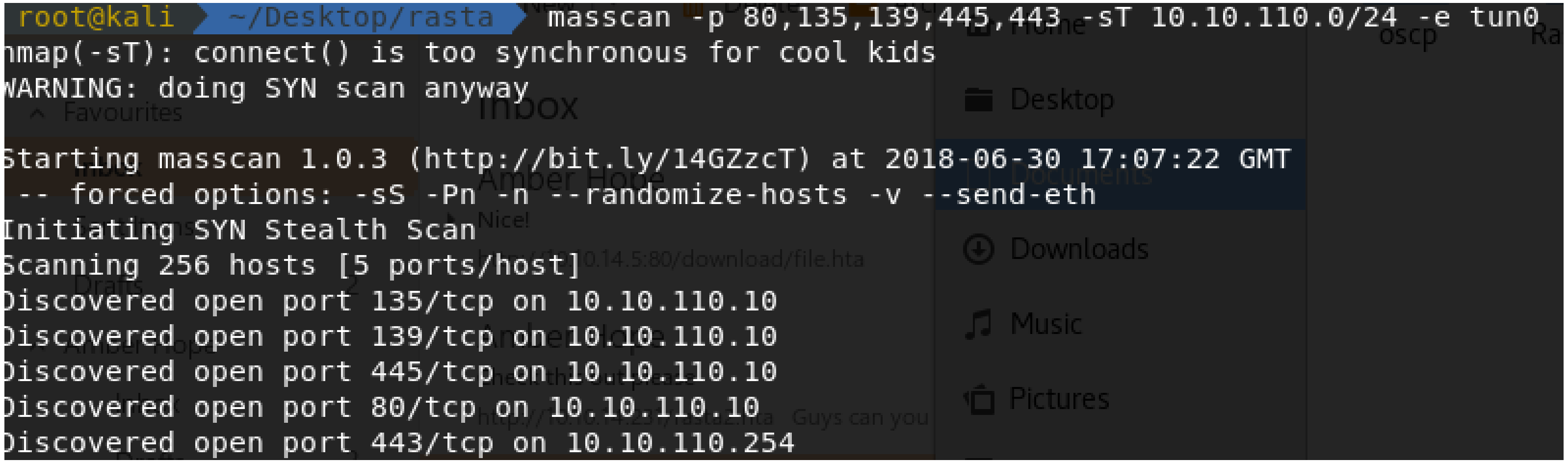
Given access to labs, my tun0 ip is 10.10.14.83

searched online for lab range found, 10.10.110.0/24 is the start range

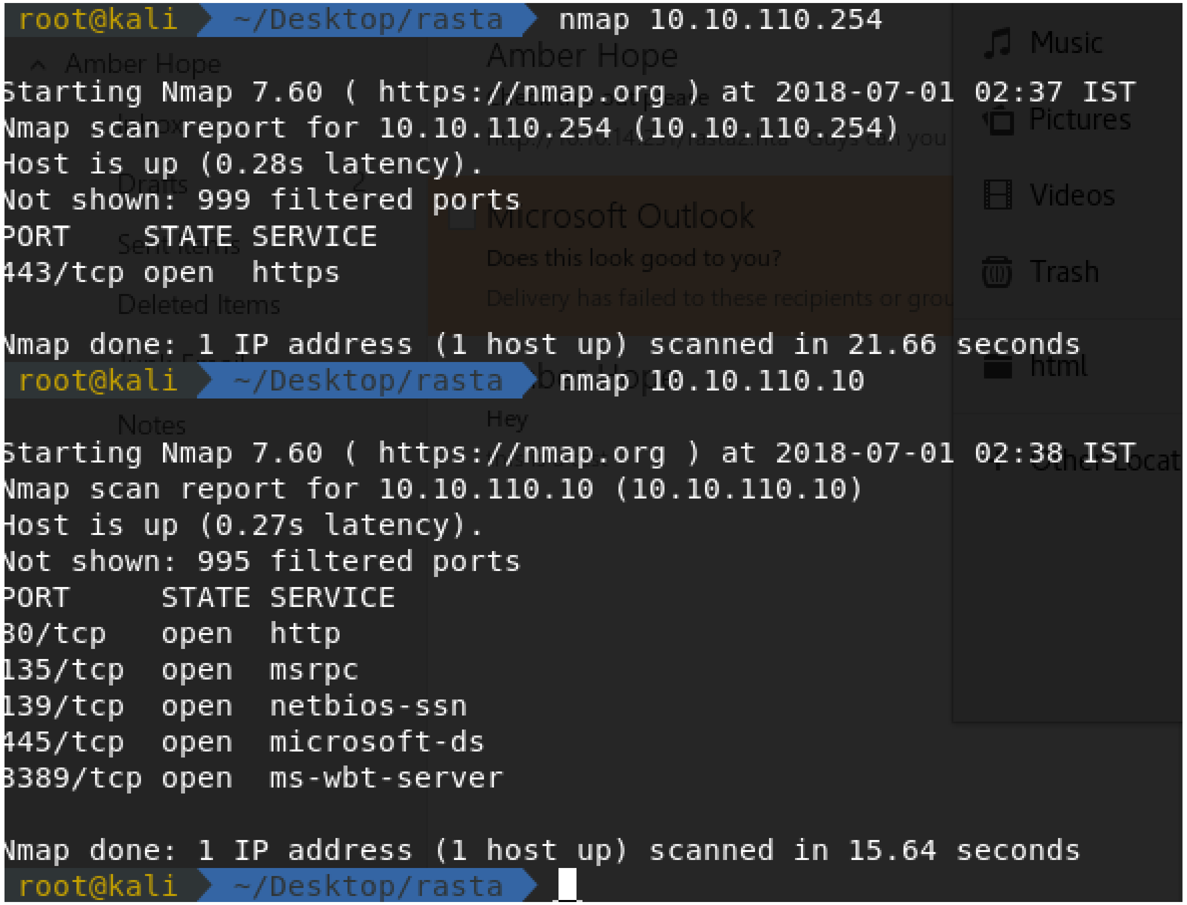
masscan -p 80,135,139,445,443 -sT 10.10.110.0/24 -e tun0



```
root@kali  ~/Desktop/rasta  masscan -p 80,135,139,445,443 -sT 10.10.110.0/24 -e tun0
nmap(-sT): connect() is too synchronous for cool kids
WARNING: doing SYN scan anyway

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-06-30 17:07:22 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [5 ports/host]
Discovered open port 135/tcp on 10.10.110.10
Discovered open port 139/tcp on 10.10.110.10
Discovered open port 445/tcp on 10.10.110.10
Discovered open port 80/tcp on 10.10.110.10
Discovered open port 443/tcp on 10.10.110.254
```

found 2 hosts,
10.10.110.10
10.10.110.254

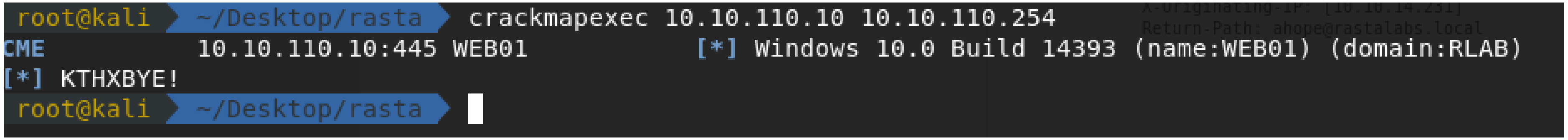
nmap scan on 2 hosts,



```
root@kali  ~/Desktop/rasta  nmap 10.10.110.254

Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-01 02:37 IST
Nmap scan report for 10.10.110.254 (10.10.110.254)
Host is up (0.28s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 21.66 seconds
root@kali  ~/Desktop/rasta  nmap 10.10.110.10

Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-01 02:38 IST
Nmap scan report for 10.10.110.10 (10.10.110.10)
Host is up (0.27s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds
root@kali  ~/Desktop/rasta  
```

i

crackmapexec on 2 hosts, found domain name "Rlab"



```
root@kali  ~/Desktop/rasta  crackmapexec 10.10.110.10 10.10.110.254
CME          10.10.110.10:445 WEB01          [*] Windows 10.0 Build 14393 (name:WEB01) (domain:RLAB)
[*] KTHXBYE!
root@kali  ~/Desktop/rasta  
```

hostname - ip

DC01 - 10.10.120.1

FS01	-	10.10.120.5
MX01	-	10.10.120.10
NIX01	-	10.10.122.20
SQL01	-	10.10.122.15
WEB01	-	10.10.110.10
WS01	-	10.10.121.100
WS02	-	10.10.121.101
WS03	-	10.10.123.100
WS04	-	10.10.123.101
WS05	-	10.10.123.102