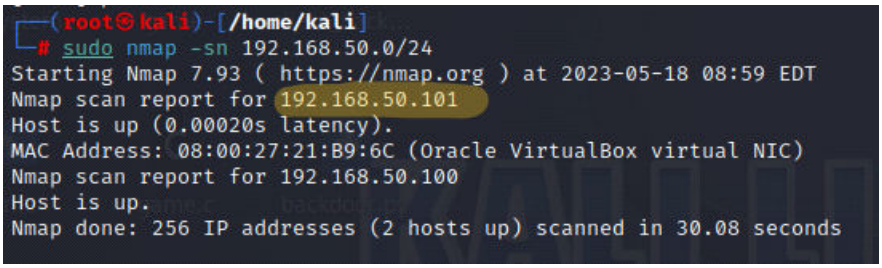
REPORT SCANNING NETWORK

Per prima cosa cambiamo le impostazioni di rete da NAT a rete locale andando sulle impostazioni di "scheda di rete" di kali. Una volta fatto cio reimpostiamo l'ip in modo statico con l'indirizzo IP "192.168.50.100" come gia visto in pregedenza da terminale.

Ora che abbiamo kali in locale utiliziamo nmap per vedere una scan degli indirizzi IP che riusciamo a visualizzare con il comando qui in basso:



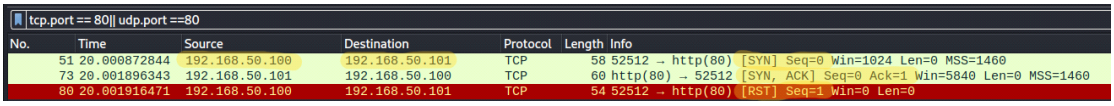
Come possimao vedere ha trovato l'indirizzo IP "192.168.50.101".

Il prossimo passo è andare a vedere sempre con nmap i servizi, e quindi, le porte aperte. Per farlo possiamo usare più di un tipo di switch (o opzione): Partiamo con il vedere il primo: -sS . Anche detto SYN scan, è un metodo meno invasivo, in quanto , una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake, ma una volta capito che la porta è aperta chiude la comunicazione:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:53 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:21:B9:6C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.100
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Come possiamo vedere dall'output ci sono diversi servizi e porte aperte. Per vedere meglio pero cosa effetivamente succede usiamo il progrmma di sniffing Wireshark:



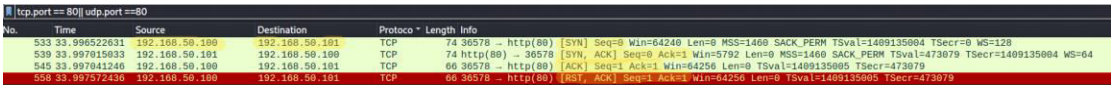
Qui possiamo vedere nel particolare lo scambio di richieste e risposte tra client e host el'invio del pacchetto RST (reset).

Ora vediamo il secondo switch: -sT. Questo è un metodo più invasivo rispetto a quello di prima, che, a differenza di quello precedente completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:01 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00043s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:21:B9:6C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.100
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
```

Vediamo cosa accade su Wireshark:



Come si puo vedere nmap completa il 3-way-handshake ed è dunque una tecnica di scanning più identificabile e che su grosse reti potrebbe creare congestioni di rete.

Un ulteriore scan potrebbe esssere usando lo switch -A:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:08 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35224/udp   mountd
|   100005  1,2,3      41945/tcp   mountd
|   100021  1,3,4      37750/udp   nlockmgr
|   100021  1,3,4      52124/tcp   nlockmgr
|   100024  1          49270/tcp   status
|_  100024  1          49317/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
```

Qui abbiamo più informazioni su i vari servizi.

In oltre possiamo ache avere un piccolo Host script con molte informazioni utili:

```
Host script results:
|_clock-skew: mean: 1h22m30s, deviation: 2h18m38s, median: 2m27s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-18T09:12:19-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.24 ms 192.168.50.101

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 141.51 seconds
```

Infine ecco una tabella riassuntiva su tutti i servizi e porte aperte trovate:

IP fonte scan	IP target scan	tipo di scan	servizi trovati	IP fonte scan	IP target scan	tipo di scan	servizi trovati
192.168.50.100	192.168.50.101	sS (SYN scan)	21/tcp open ftp	192.168.50.100	192.168.50.101	sT	21/tcp open ftp
			22/tcp open ssh				22/tcp open ssh
			23/tcp open telnet				23/tcp open telnet
			25/tcp open smtp				25/tcp open smtp
			53/tcp open domain				53/tcp open domain
			80/tcp open http				80/tcp open http
			111/tcp open rpcbind				111/tcp open rpcbind
			139/tcp open netbios-ssn				139/tcp open netbios-ssn
			445/tcp open microsoft-ds				445/tcp open microsoft-ds
			512/tcp open exec				512/tcp open exec
			513/tcp open login				513/tcp open login
			514/tcp open shell				514/tcp open shell
			1099/tcp open rmiregistry				1099/tcp open rmiregistry
			1524/tcp open ingreslock				1524/tcp open ingreslock
			2049/tcp open nfs				2049/tcp open nfs
			2121/tcp open ccproxy-ftp				2121/tcp open ccproxy-ftp
			3306/tcp open mysql				3306/tcp open mysql
			5432/tcp open postgresql				5432/tcp open postgresql
			5900/tcp open vnc				5900/tcp open vnc
			6000/tcp open X11				6000/tcp open X11
			6667/tcp open irc				6667/tcp open irc
			8009/tcp open ajp13				8009/tcp open ajp13
			8180/tcp open unknown				8180/tcp open unknown