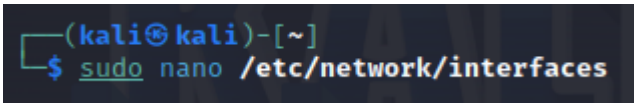
REPORT (18.05.2023) **ESEGUITO DA ANATOLIY PRYSYAZHNYUK**

SCANSIONI CON NMAP

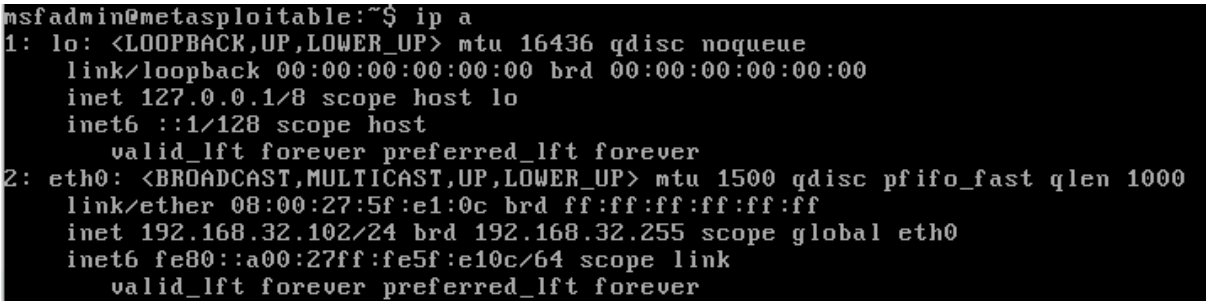
Sulla macchina virtuale (VM) Kali Linux:

Rimetto in rete interna con il comando sottostante, dopodichè nel config cambio l'IP:

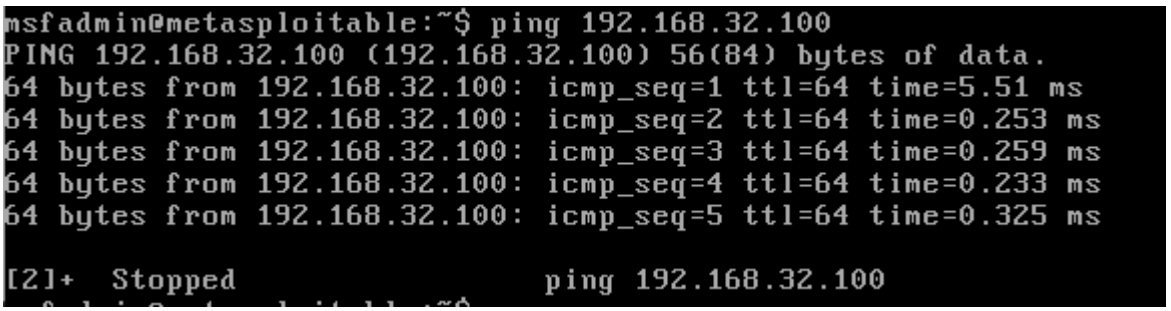


Sulla VM **Metasploitable**:

Ho cambiato l'IP di **Metasploitable** a 192.168.32.102
con: "*sudo nano /etc/network/interfaces*", modificandolo nel config



Ho controllato se le reti sono collegate tra loro, con *ping*:



Su VM **Kali Linux**:

Eseguo l'intercettazione con **Nmap, target: VM Metasploitable, IP: 192.168.32.102**:

Eseguo l'**Host Discovery** con **-Pn** *(che ipotizza tutti gli host attivi)*:

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.32.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:47 EDT
Nmap scan report for 192.168.32.102
Host is up (0.00032s 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

Nmap done: 1 IP address (1 host up) scanned in 14.24 seconds
```

Target: VM Metasploitable, IP: 192.168.32.102:
Eseguo la scansione del **TCP** (*Transmission Control Protocol*) con **-sV** (notiamo la versione):

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1-1024 192.168.32.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:50 EDT
Nmap scan report for 192.168.32.102
Host is up (0.00026s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
53/tcp  open  domain      ISC BIND 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind     2 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.43 seconds
```

Target: VM Metasploitable, IP: 192.168.32.102:
Effettuo la scansione **SYN** con "***sudo*** *nano nmap -sS -p 1-1024 192.168.32.102*"
(recuperiamo anche il MAC Address):

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 1-1024 192.168.32.102
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:56 EDT
Nmap scan report for 192.168.32.102
Host is up (0.000067s latency).
Not shown: 1012 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
MAC Address: 08:00:27:5F:E1:0C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```

Target: VM Metasploitable, IP: 192.168.32.102:

Eseguo la scansione con lo switch (*opzione*) **-A**, con:

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p 1-1024 192.168.32.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:58 EDT
Nmap scan report for 192.168.32.102
Host is up (0.00030s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.32.100
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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, ENHANC
EDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

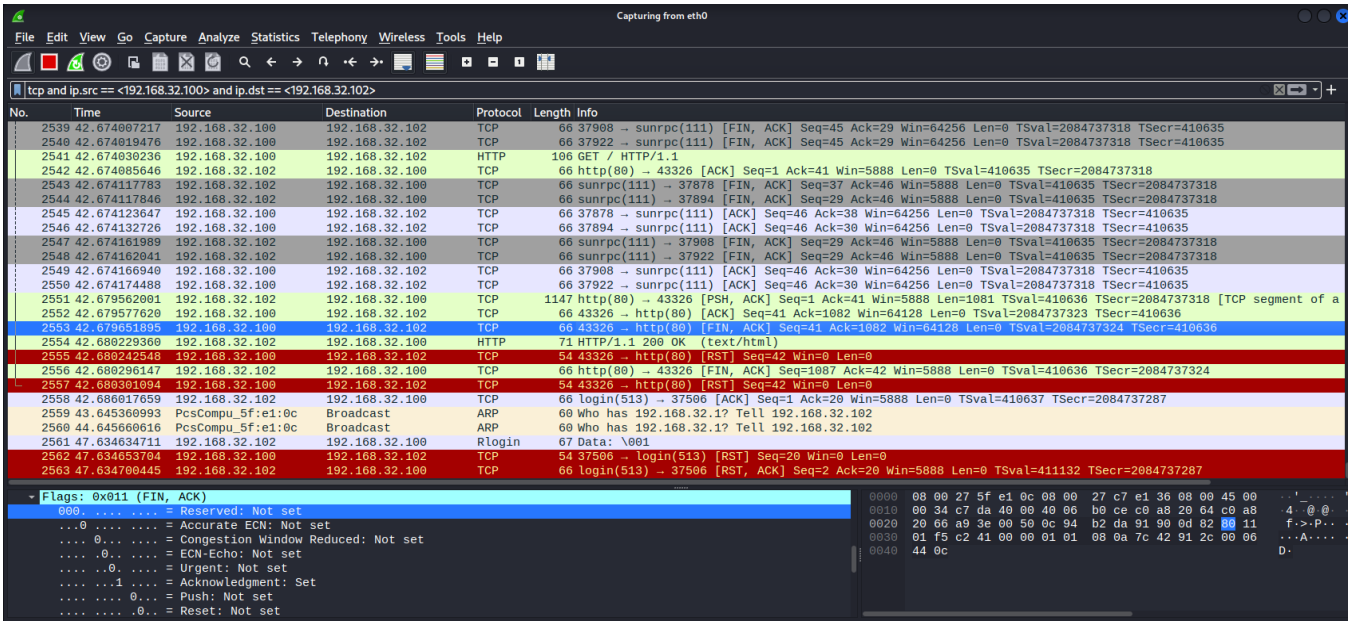
```
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    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      33586/udp   mountd
|   100005  1,2,3      50743/tcp   mountd
|   100021  1,3,4      51917/udp   nlockmgr
|   100021  1,3,4      60536/tcp   nlockmgr
|   100024  1          46383/tcp   status
|_  100024  1          47757/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?
514/tcp open  shell       Netkit rshd
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h59m58s, deviation: 2h50m17s, median: -26s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-18T08:59:34-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 112.46 seconds
```

Scansioni TCP/SYN intercettate con Wireshark:

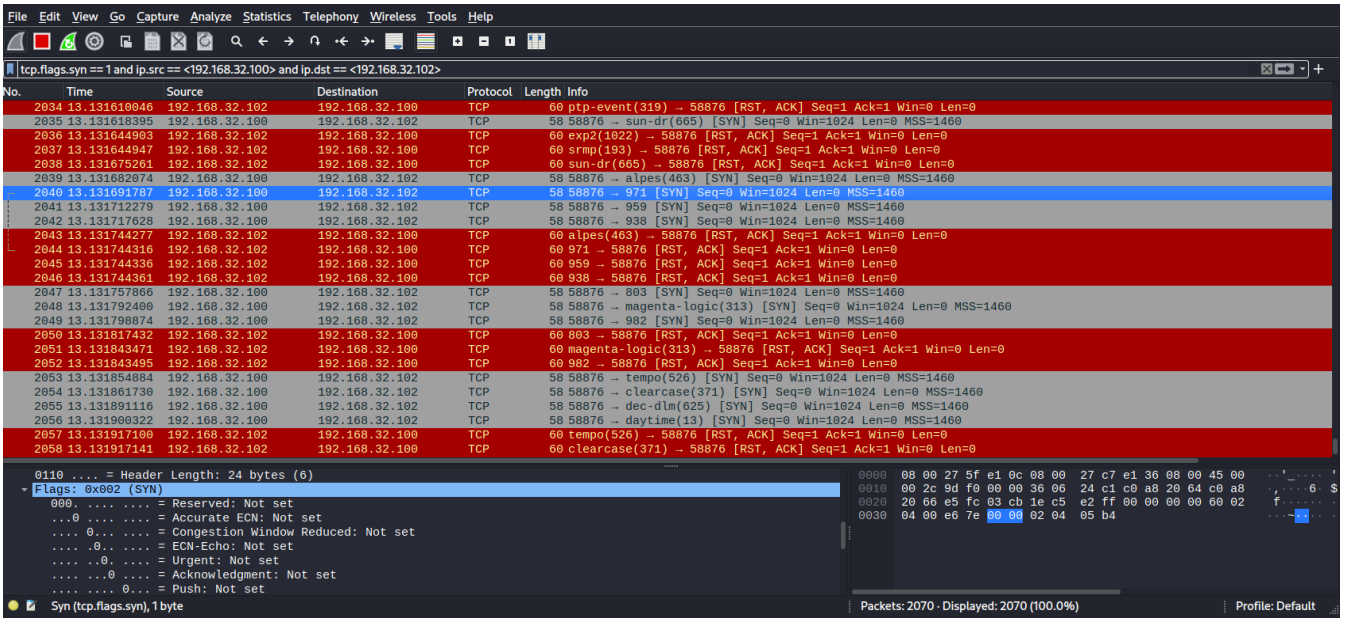
Per farlo mi collego su **Wireshark** su **eth0**,
metto il **filtro (per TCP)**:
tcp and ip.src == <indirizzo_IP_Kali> and ip.dst == <indirizzo_IP_Metasploitable>

Il filtro per SYN:
tcp.flags.syn == 1 and ip.src == <indirizzo_IP_Kali> and ip.dst == <indirizzo_IP_Metasploitable>

Intercettazione **TCP** con Wireshark:



Intercettazione **SYN** con Wireshark:



Che differenze notiamo con le intercettazioni TCP/SYN:

- **Tipi di pacchetti:** Durante una scansione TCP, possiamo vedere pacchetti con flags TCP come SYN, ACK, e FIN. La scansione SYN, invece, si concentra principalmente su pacchetti con flag SYN.
- **Stato della connessione:** Durante una scansione TCP, osserviamo la sequenza di pacchetti che costituiscono una connessione TCP completa, ad esempio la sequenza SYN-ACK-SYN-ACK. Durante la scansione SYN, vediamo principalmente pacchetti SYN inviati ai sistemi di destinazione.
- **Risposte dei pacchetti:** Durante una scansione TCP, osserviamo pacchetti di risposta come SYN-ACK e ACK per stabilire la connessione. Durante la scansione SYN, vediamo principalmente risposte SYN-ACK dai sistemi di destinazione.
- **Porte di destinazione:** Durante una scansione TCP, vediamo i pacchetti TCP inviati a porte specifiche per determinare se sono aperte o chiuse. Durante la scansione SYN, saremo principalmente interessati a identificare le porte che rispondono con pacchetti SYN-ACK.
- **Numero di sequenza**: Durante una scansione TCP, osserviamo i numeri di sequenza che vengono scambiati tra i sistemi durante la connessione. Durante la scansione SYN, vediamo principalmente i numeri di sequenza nei pacchetti SYN e SYN-ACK.