4. I tool degli Hacker: Kali Linux

-Host Discovery (oltre il nostro host Kali, sulla rete abbiamo individuato un altro host, che corrisponde a Metasploitable).

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 14:42 CET
Nmap scan report for 192.168.50.100
Host is up (0.000037s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.50.101
Host is up (0.0097s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 256 IP addresses (2 hosts up) scanned in 70.69 seconds
```

7 servizi attivi su Metasploitable

Tabella degli scan effettuati

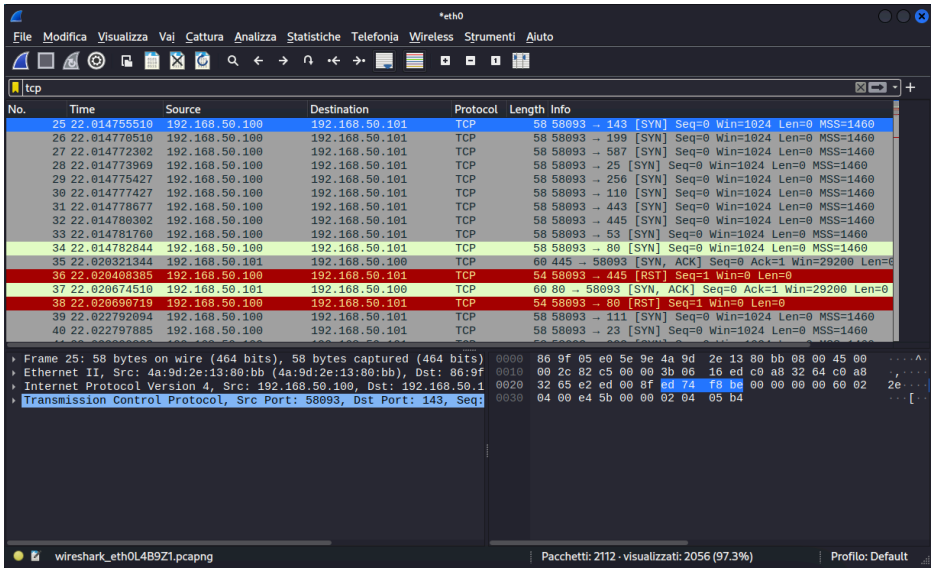
Fonte dello scan	Target dello scan	Tipo di scan	Risultati ottenuti
Kali 192.168.50.100	Meta 192.168.50.101	Scansione SYN sulle porte well-known	Servizi attivi: 5
Kali 192.168.50.100	Meta 192.168.50.101	Scansione TCP sulle porte well-known	Servizi attivi: 5
Kali 192.168.50.100	Meta 192.168.50.101	Scansione con switch -A delle porte well-known	Servizi attivi: 5

-Scansione SYN e relativa cattura con Wireshark.

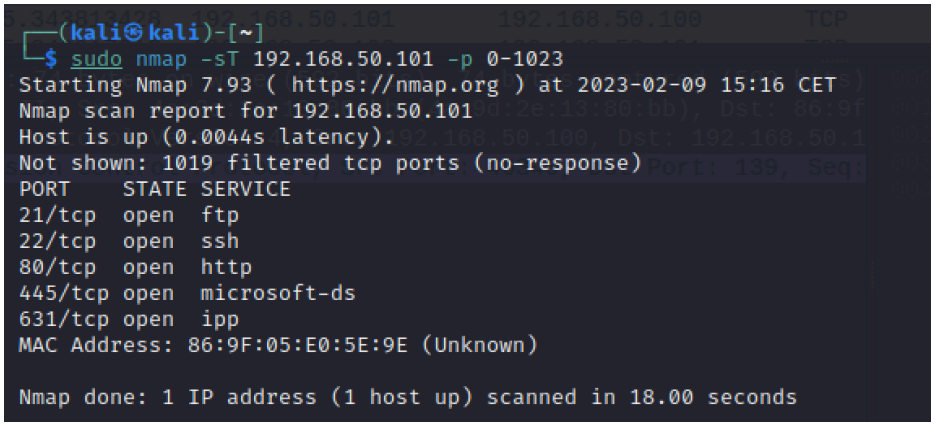
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 0-1023
[sudo] password di kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 15:13 CET
Nmap scan report for 192.168.50.101
Host is up (0.0035s latency).
Not shown: 1019 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
445/tcp open  microsoft-ds
631/tcp open  ipp
MAC Address: 86:9F:05:E0:5E:9E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 18.17 seconds
```

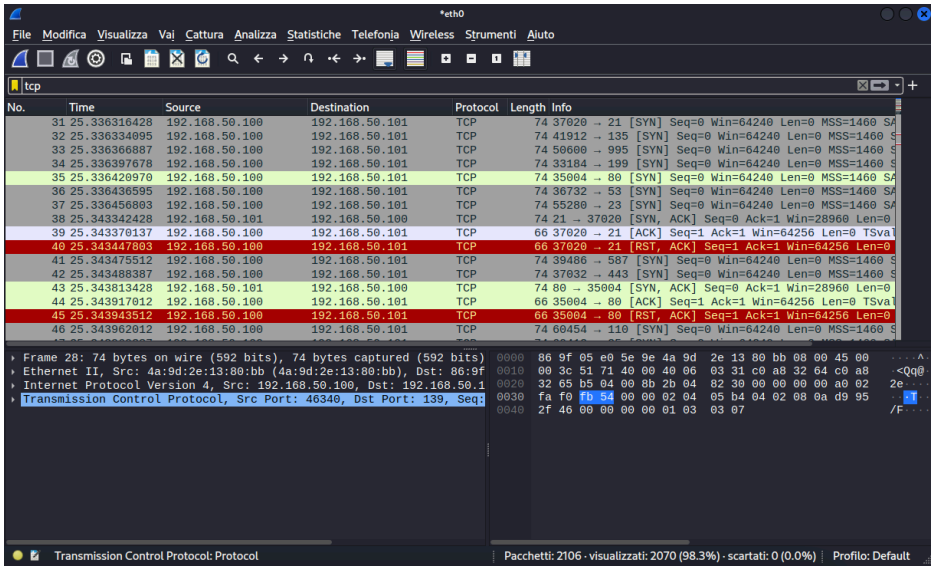
Utilizzando il comando -sS non si conclude lo scambio 3-way-handshake dove si invia un pacchetto RST (reset) per chiudere la comunicazione con Meta.



-Scansione TCP e relativa cattura con Wireshark.



Utilizzando il comando -sT (più invasivo) si conclude il 3-way-handshake dove la comunicazione invia e riceve risposta con il SYN -SYN ACK- ACK



-Scansione con switch < -A > sulle porte well-known.
Entriamo più dettagliatamente nelle informazioni dei servizi sulle relative porte.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 21,22,80,445,631 -A 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 15:23 CET
Nmap scan report for 192.168.50.101
Host is up (0.0042s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.5
22/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b2e1fa4542687761226595800dda3b04 (DSA)
|   2048 c9ac70eff8de8ba3a344ab3d320a5c6a (RSA)
|   256 c049cc187b27a4070d2a0dbb424c3617 (ECDSA)
|_  256 a076f376f8f0704d09cae110fda9cc0a (ED25519)
80/tcp  open  http        Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp open  ipp         CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: Home - CUPS 1.7.2
| http-robots.txt: 1 disallowed entry
| /
```

```
MAC Address: 86:9F:05:E0:5E:9E (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
 port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 0s, deviation: 1s, median: -1s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-02-09T14:24:09
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: ubuntu
|   NetBIOS computer name: UBUNTU\x00
|   Domain name: \x00
|   FQDN: ubuntu
|_  System time: 2023-02-09T14:24:08+00:00

TRACEROUTE
HOP RTT     ADDRESS
1   4.22 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 61.90 seconds
```