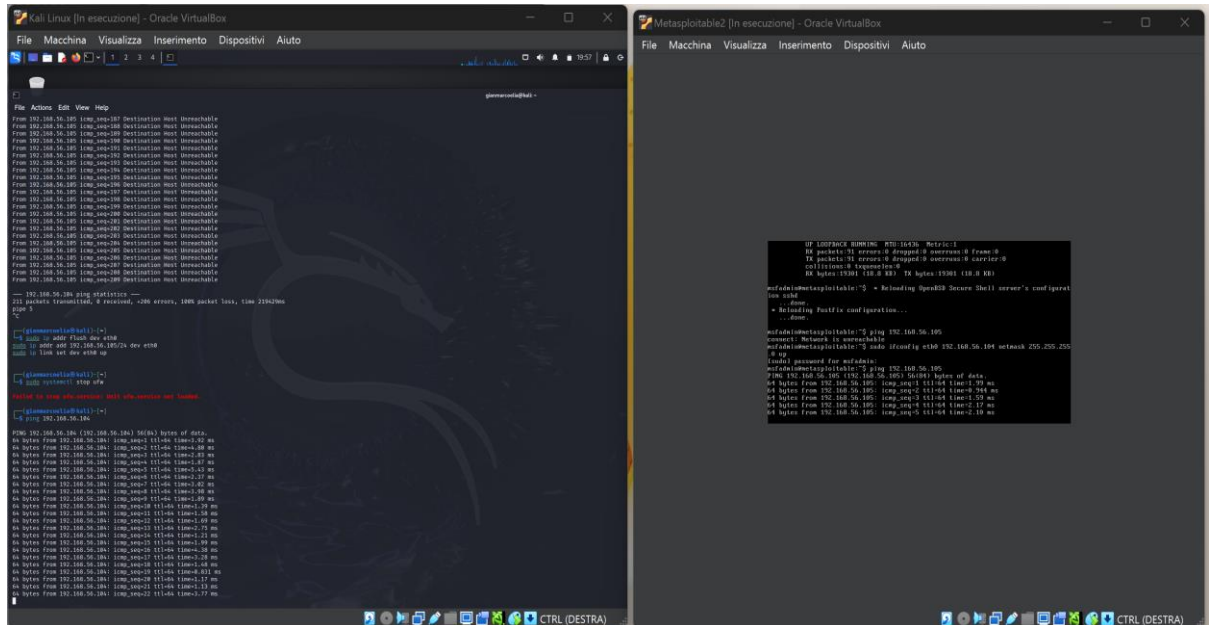
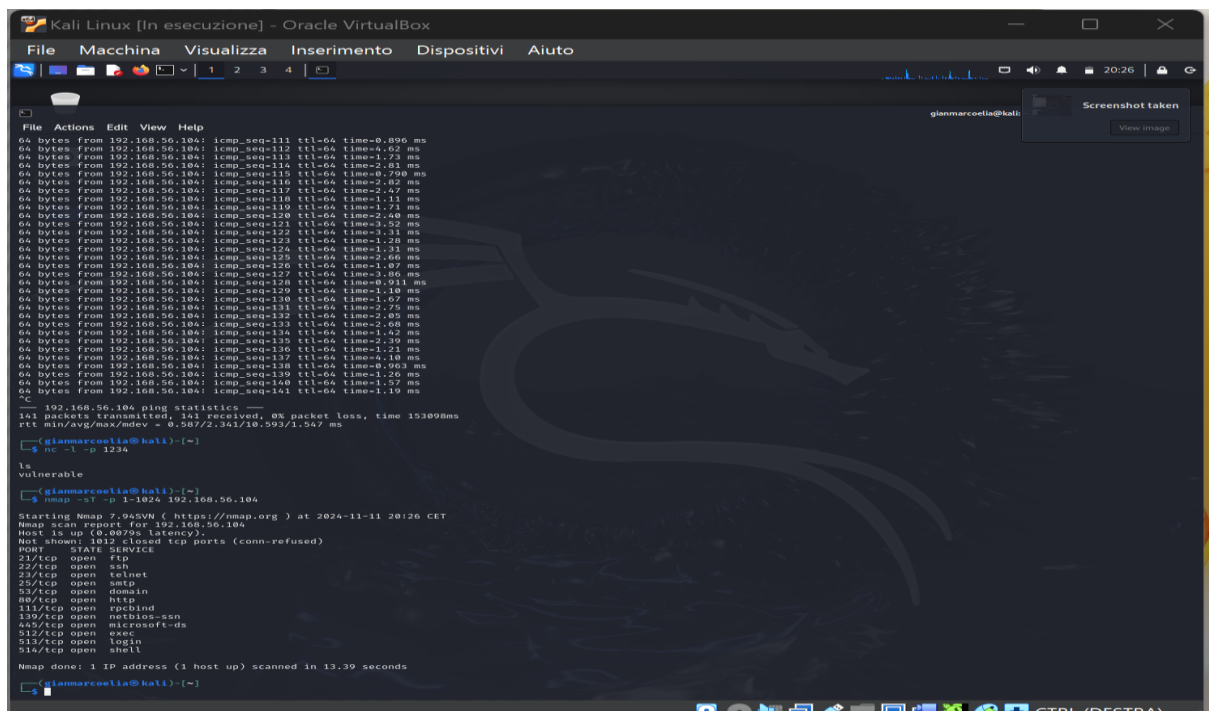


Gianmarco Elia – W9D1

Innanzitutto si mette in comunicazione Kali Linux con Metasploitable2:



Scansione TCP sulle porte well-known:



Scansione SYN sulle porte well-known:

```
Kali Linux [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

gianmarcoelia@kali: ~
File  Actions  Edit  View  Help
^C
--- 192.168.56.104 ping statistics ---
141 packets transmitted, 141 received, 0% packet loss, time 153098ms
rtt min/avg/max/mdev = 0.587/2.341/10.593/1.547 ms
(gianmarcoelia@kali)~]
$ nc -l -p 1234

ls
vulnerable
(gianmarcoelia@kali)~]
$ nmap -sT -p 1-1024 192.168.56.104

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 20:26 CET
Nmap scan report for 192.168.56.104
Host is up (0.0079s latency).
Not shown: 1012 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

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
(gianmarcoelia@kali)~]
$ nmap -sS -p 1-1024 192.168.56.104

You requested a scan type which requires root privileges.
QUITTING!
(gianmarcoelia@kali)~]
$ sudo nmap -sS -p 1-1024 192.168.56.104

[sudo] password for gianmarcoelia:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 20:28 CET
Nmap scan report for 192.168.56.104
Host is up (0.00064s 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: 08:00:27:19:B6:E2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.96 seconds
(gianmarcoelia@kali)~]
$
```

Scansione con switch -A sulle porte well-known:

```
Kali Linux [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
Screenshot taken
View image
gianmarcoelia@kali:
File Actions Edit View Help
$ sudo nmap -A -p 1-1024 192.168.56.104

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 20:30 CET
Nmap scan report for 192.168.56.104
Host is up (0.0016s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.56.105
|_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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:ca:d5:6:c1cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2018-03-17T14:07:45
|_Not valid after: 2018-04-10T14:07:45
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-11-11T19:30:36+00:00; -1s from scanner time.
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 51766/udp mountd
|_100005 1,2,3 56133/tcp mountd
|_100021 1,2,4 50009/udp nlockmgr
|_100021 1,3,4 55747/tcp nlockmgr
|_100024 1 34318/tcp status
|_100024 1 52781/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 rshcd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  shell       Netkit rshd
MAC Address: 08:00:27:19:B6:E2 (Oracle VirtualBox virtual NIC)

111/tcp   open  rpcbind    2 (RPC #100000)
MAC Address: 08:00:27:19:B6:E2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: metasploitable.localdomain; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-security-mode:
|_account_used: guest
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h9m59s, deviation: 2h5m12s; median: -1s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|_OS: Unix (Samba 3.0.20-Debian)
|_Computer name: metasploitable
|_NetBIOS computer name:
|_Domain name: localdomain
|_FQDN: metasploitable.localdomain
|_System time: 2024-11-11T14:30:27-05:00
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 1.60 ms 192.168.56.104

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 35.91 seconds

gianmarcoelia@kali:~$
```

Ho configurato una rete interna tra Kali Linux e Metasploitable2 su VirtualBox e verificato la connessione tramite ping. Successivamente, ho eseguito varie scansioni con nmap per rilevare le porte aperte su Metasploitable2. Ho iniziato con una scansione TCP completa (nmap -sT), identificando i servizi attivi sulle porte well-known. Poi, ho eseguito una scansione SYN (nmap -sS) per visualizzare le porte aperte senza stabilire una connessione completa. Infine, ho utilizzato Wireshark per confrontare i pacchetti catturati: nella scansione TCP completa si osserva il three-way handshake (SYN, SYN-ACK, ACK), mentre nella scansione SYN il processo si interrompe dopo il SYN-ACK. Tutte le scansioni sono andate a buon fine.