

## Esercizio 21-12-2023

- Nmap -sS 192.168.50.101 -p 1-1024

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-07 05:54 EST
Nmap scan report for 192.168.50.101
Host is up (0.0033s 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
MAC Address: 08:00:27:05:91:73 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

The image shows a Wireshark packet capture of a SYN flood attack. The packet list table contains 24 entries, all of which are TCP SYN packets from 192.168.50.100 to 192.168.50.101 on port 139. The packet details pane shows the structure of a TCP packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the captured packet.

No.	Time	Source	Destination	Protocol	Length	Info
35	13.079364517	192.168.50.100	192.168.50.101	TCP	60	57600 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	13.079626184	192.168.50.101	192.168.50.100	TCP	62	256 → 57600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	13.079904869	192.168.50.100	192.168.50.101	TCP	60	57600 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
38	13.079817531	192.168.50.100	192.168.50.101	TCP	60	57600 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39	13.079926986	192.168.50.101	192.168.50.100	TCP	62	22 → 57600 [SYN, ACK] Seq=0 Ack=1 Win=5640 Len=0 MSS=1460
40	13.079926731	192.168.50.101	192.168.50.100	TCP	62	445 → 57600 [SYN, ACK] Seq=0 Ack=1 Win=5640 Len=0 MSS=1460
41	13.079923783	192.168.50.100	192.168.50.101	TCP	56	57600 → 22 [RST] Seq=1 Win=0 Len=0
42	13.079947070	192.168.50.100	192.168.50.101	TCP	56	57600 → 445 [RST] Seq=1 Win=0 Len=0
43	13.080127242	192.168.50.100	192.168.50.101	TCP	60	57600 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	13.080248726	192.168.50.101	192.168.50.100	TCP	60	57600 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	13.080351744	192.168.50.101	192.168.50.100	TCP	62	110 → 57600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46	13.080493153	192.168.50.101	192.168.50.100	TCP	62	23 → 57600 [SYN, ACK] Seq=0 Ack=1 Win=5640 Len=0 MSS=1460
47	13.080493813	192.168.50.100	192.168.50.101	TCP	56	57600 → 23 [RST] Seq=1 Win=0 Len=0
48	13.080674019	192.168.50.100	192.168.50.101	TCP	60	57600 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	13.080777050	192.168.50.101	192.168.50.100	TCP	62	80 → 57600 [SYN, ACK] Seq=0 Ack=1 Win=5640 Len=0 MSS=1460
50	13.080778671	192.168.50.100	192.168.50.101	TCP	56	57600 → 80 [RST] Seq=1 Win=0 Len=0
51	13.080950616	192.168.50.100	192.168.50.101	TCP	60	57600 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	13.081079154	192.168.50.100	192.168.50.101	TCP	60	57600 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	13.081100856	192.168.50.101	192.168.50.100	TCP	62	443 → 57600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
54	13.081320264	192.168.50.101	192.168.50.100	TCP	62	993 → 57600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface any, id 0  
Linux cooked capture v1  
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101  
Transmission Control Protocol, Src Port: 57600, Dst Port: 139, Seq: 0, Len: 0

```
- Nmap -sT 192.168.50.101 -p 1-1024
```

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-07 05:49 EST
Nmap scan report for 192.168.50.101
Host is up (0.00083s 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: 08:00:27:05:91:73 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

```
(kali㉿kali)-[~]  
$
```

[illegible]

- Nmap -A 192.168.50.101 -p 1-1024

```
—(kali@kali)-[~]
_-$ nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-07 06:12 EST
Nmap scan report for 192.168.50.101
Host is up (0.0024s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:  UNIX (AKA) Seq=84 Ack=1 Win=64256 Len=0 TSval=2933758368 TSecr=3844588888
|_STAT:      200 OK
|_FTP server status:
|_  Connected to 192.168.50.101
|_  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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA) 2 Error: bad syntax
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA) 1-2033768377 TSecr=
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_ssl2:
|_  SSLv2 supported
|_  ciphers:
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_RC4_128_WITH_MD5
|_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-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 47519/udp  mountd
|_  100005 1,2,3 50391/tcp  mountd
|_  100021 1,3,4 35820/tcp  nlockmgr
|_  100021 1,3,4 46385/udp  nlockmgr
|_  100024 1 45871/udp  status
|_  100024 1 54697/tcp  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  smb         Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell       Netkit rshd
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linu
x:linux_kernel
```

```
SSL2_RC2_128_CBC_WITH_MD5
SSL2_RC4_128_WITH_MD5
|_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-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 47519/udp  mountd
|_  100005 1,2,3 50391/tcp  mountd
|_  100021 1,3,4 35820/tcp  nlockmgr
|_  100021 1,3,4 46385/udp  nlockmgr
|_  100024 1 45871/udp  status
|_  100024 1 54697/tcp  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  smb         Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell       Netkit rshd
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linu
x:linux_kernel
Host script results:
|_clock-skew: mean: 2h30m06s, deviation: 3h32m17s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unkn
own> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|_  account_used: guest
|_  authentication_level: user
|_  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb-os-discovery:
|_  OS: Unix (Samba 3.0.20-Debian)
|_  Computer name: metasploitable
|_  NetBIOS computer name:
|_  Domain name: localdomain
|_  FQDN: metasploitable.localdomain
|_  System time: 2024-01-07T06:13:40-05:00
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 97.80 seconds