

Host Discovery -

Nella prima scansione viene richiesta un host discovery la quale si può facilmente eseguire con il comando di NMAP '-sn' così andrò a visualizzare tutti gli host presenti inviando una richiesta ICMP.

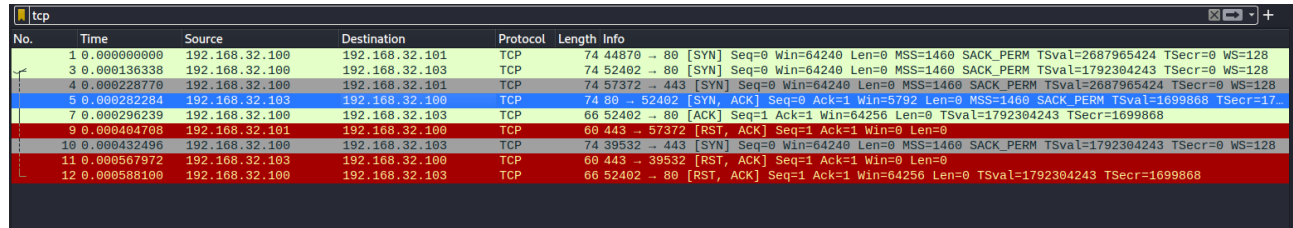
Ho impostato un range delle mie macchine locali con 100-103 per non affaticare lo scanner con un range troppo lungo.

Per non inviare il ping potrei usare '-Pn' ma in questo esempio ho voluto usare ICMP:

```
(kali㉿kali)-[~]
$ nmap -sn 192.168.32.100-103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:23 EDT
Nmap scan report for 192.168.32.100
Host is up (0.00019s latency).
Nmap scan report for 192.168.32.101
Host is up (0.00036s latency).
Nmap scan report for 192.168.32.103
Host is up (0.00023s latency).
Nmap done: 4 IP addresses (3 hosts up) scanned in 14.23 seconds
```

Viene fuori che 3 macchine sono attive, (Windows, Kali , Metasploitable2)

Screen WireShark:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.100	192.168.32.101	TCP	74	44870 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2687965424 TSecr=0 WS=128
3	0.000136338	192.168.32.100	192.168.32.103	TCP	74	52402 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1792304243 TSecr=0 WS=128
4	0.000228770	192.168.32.100	192.168.32.101	TCP	74	57372 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2687965424 TSecr=0 WS=128
5	0.000282284	192.168.32.103	192.168.32.100	TCP	74	80 → 52402 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1699868 TSecr=17...
7	0.000296239	192.168.32.100	192.168.32.103	TCP	66	52402 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1792304243 TSecr=1699868
9	0.000404708	192.168.32.101	192.168.32.100	TCP	60	443 → 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	0.000432496	192.168.32.100	192.168.32.103	TCP	74	39532 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1792304243 TSecr=0 WS=128
11	0.000567972	192.168.32.103	192.168.32.100	TCP	60	443 → 39532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	0.000588100	192.168.32.100	192.168.32.103	TCP	66	52402 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1792304243 TSecr=1699868

Vengono inviate le richieste su wireshark verso il range 100-103 (La macchina .102 non esiste).

Scansione TCP sulle porte well-known:

Nella prima scansione viene richiesta una TCP Connect/Full Open Scan che comprende un three-way handshake cioè viene inviato prima il pacchetto SYN poi successivamente il server risponde con SYN+ACK e infine viene la conversazione continua con ACK fino al RST.

Comando nmap:

```

(kali@kali)-[~]
$ sudo nmap -sT 192.168.32.100-103 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:41 EDT
Nmap scan report for 192.168.32.100
Host is up (0.000095s latency).
All 1000 scanned ports on 192.168.32.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.32.101
Host is up (0.0020s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 00:0C:29:72:81:37 (VMware)

Nmap scan report for 192.168.32.103
Host is up (0.00078s 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

```

Vengono visualizzati i due sistemi operativi (Metasploitable2, Windows) e nmap evita di scansionare Kali la macchina locale(Ecco perché non esce scritta).

Comunque su wireshark viene visualizzato il port scanning con l'handshake completo.

Scansione Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
25	33.055117967	192.168.32.100	192.168.32.103	TCP	74	38196 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1790866297 TSecr=0 WS=128
26	33.055245892	192.168.32.100	192.168.32.103	TCP	74	33172 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1790866297 TSecr=0 WS=128
27	33.055274433	192.168.32.103	192.168.32.100	TCP	74	21 → 38196 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1556008 TSecr=1790866297
28	33.055336027	192.168.32.100	192.168.32.103	TCP	66	38196 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1790866297 TSecr=1556008
29	33.055372412	192.168.32.103	192.168.32.100	TCP	60	135 → 33172 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	33.055410478	192.168.32.100	192.168.32.103	TCP	74	32794 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1790866297 TSecr=0 WS=128
31	33.055490340	192.168.32.103	192.168.32.100	TCP	60	8888 → 32794 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	33.055499158	192.168.32.100	192.168.32.103	TCP	74	50408 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1790866297 TSecr=0 WS=128
33	33.055534041	192.168.32.100	192.168.32.103	TCP	74	50408 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1790866297 TSecr=0 WS=128
34	33.055582377	192.168.32.103	192.168.32.100	TCP	74	53 → 50408 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1556008 TSecr=1790866297
35	33.055582430	192.168.32.103	192.168.32.100	TCP	74	80 → 50408 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1556008 TSecr=1790866297
36	33.055589182	192.168.32.100	192.168.32.103	TCP	66	50408 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1790866297 TSecr=1556008
37	33.055618213	192.168.32.100	192.168.32.103	TCP	66	56426 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1790866297 TSecr=1556008
38	33.055655715	192.168.32.100	192.168.32.103	TCP	74	32796 → 50408 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1790866297 TSecr=0 WS=128
39	33.055724867	192.168.32.103	192.168.32.100	TCP	74	3306 → 32796 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1556008 TSecr=1790866297
40	33.055739673	192.168.32.100	192.168.32.103	TCP	66	32796 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1790866297 TSecr=1556008
41	33.055761319	192.168.32.100	192.168.32.103	TCP	74	39796 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1790866297 TSecr=0 WS=128
42	33.055840445	192.168.32.103	192.168.32.100	TCP	60	3389 → 39796 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 34: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
 Ethernet II, Src: VMware_08:0c:29:68:3c:3a, Dst: VMware_a6:27:24 (00:0c:29:a6:27:24)
 Internet Protocol Version 4, Src: 192.168.32.103, Dst: 192.168.32.100
 Transmission Control Protocol, Src Port: 53, Dst Port: 50408, Seq: 0, Ack: 1, Len: 0
 Source Port: 53
 Destination Port: 50408
 [Stream index: 3]
 Conversation completeness: Complete, NO_DATA (39)
 [TCP Segment Len: 0]
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 576208973
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment Number (raw): 4198340669
 1010 ... = Header Length: 40 bytes (10)
 Flags: 0x012 (SYN, ACK)
 Window: 5792

Scansione SYN sulle porte well-known-> Questo tipo di scansione non completa l'handshake, ma invia semplicemente il pacchetto 'SYN' e successivamente lo chiude con RST. Questa è anche detta scansione Stealth Scan poiché tenta di evitare di stabilire una connessione completa con il server.

Comando Nmap :

```

(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.100-103 with msfadmin/msfadmin to get st
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:52 EDT
Nmap scan report for 192.168.32.100
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.32.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 192.168.32.101
Host is up (0.00020s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:72:81:37 (VMware)

Nmap scan report for 192.168.32.103
Host is up (0.0017s 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
  
```

Screen Wireshark:

```

o. Time Source Destination Protocol Length Info
46 22.452790614 192.168.32.103 192.168.32.100 TCP 60 143 → 59385 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47 22.452861225 192.168.32.103 192.168.32.100 TCP 60 256 → 59385 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 22.452925987 192.168.32.100 192.168.32.103 TCP 58 59385 → 80 [RST, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
49 22.452964700 192.168.32.100 192.168.32.103 TCP 58 59385 → 500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50 22.452986099 192.168.32.100 192.168.32.103 TCP 58 59385 → 95 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51 22.453007969 192.168.32.100 192.168.32.103 TCP 58 59385 → 35 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52 22.453024660 192.168.32.103 192.168.32.100 TCP 60 80 → 59385 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
53 22.453030137 192.168.32.100 192.168.32.103 TCP 58 59385 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54 22.453067817 192.168.32.100 192.168.32.103 TCP 54 59385 → 0 [RST] Seq=1 Win=0 Len=0
55 22.453090491 192.168.32.100 192.168.32.103 TCP 58 59385 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56 22.453104537 192.168.32.103 192.168.32.100 TCP 60 5900 → 59385 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
57 22.453104592 192.168.32.103 192.168.32.100 TCP 60 995 → 59385 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58 22.453104618 192.168.32.103 192.168.32.100 TCP 60 135 → 59385 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 22.453104638 192.168.32.103 192.168.32.100 TCP 60 139 → 59385 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
60 22.453110937 192.168.32.100 192.168.32.103 TCP 58 59385 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
61 22.453125529 192.168.32.100 192.168.32.103 TCP 54 59385 → 590 [RST] Seq=1 Win=0 Len=0
62 22.453127098 192.168.32.100 192.168.32.103 TCP 54 59385 → 139 [RST] Seq=1 Win=0 Len=0
63 22.453148639 192.168.32.100 192.168.32.103 TCP 58 59385 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 27: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
Ethernet II, Src: VMware_a6:27:24 (00:0c:29:a6:27:24), Dst: VMware_68:3c:3a (00:0c:29:68:3c:3a)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.103
Transmission Control Protocol, Src Port: 59385, Dst Port: 1025, Seq: 0, Len: 0
Source Port: 59385
Destination Port: 1025
[Stream index: 4]
[Conversation completeness: Incomplete (37)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1125920813
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0110 .... = Header Length: 24 bytes (6)
Flags: 0x002 (SYN)

```

Infine l'ultima scansione con l'opzione '-A' va ad eseguire una scansione aggressiva (io l'ho resa più aggressiva aggiungendogli il comando '-T5' che va a impostare il programma alla velocità massima.

Ovviamente va più veloce a costo di un maggiore rilevamento da parte di IDS e Firewall.

Screen Nmap :

```

$ sudo nmap -A 192.168.32.100-103 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:58 EDT
Nmap scan report for 192.168.32.100
Host is up (0.000375 latency).
All 1000 scanned ports on 192.168.32.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Nmap scan report for 192.168.32.101
Host is up (0.000285 latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:72:81:37 (VMware)
Device type: general purpose
Running: Microsoft Windows 7/2008/8.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 ~ SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-LAJMLK1CK00; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: -39m58s, deviation: 1h09m05s, median: -11s
|_ nbstat: NetBIOS name: WIN-LAJMLK1CK00, NetBIOS user: <unknown>, NetBIOS MAC: 000c29728137 (VMware)
|_ smb2-security-mode:
|   210:
|     Message signing enabled but not required
|_ smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-LAJMLK1CK00
|   NetBIOS computer name: WIN-LAJMLK1CK00\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2023-05-18T14:59:59+02:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

```

```
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time:
|   date: 2023-05-18T12:59:47
|   start_date: 2023-05-18T12:21:13
|_
Time      Source      Destination      Protocol Length Info
-----
TRACEROUTE
HOP RTT      ADDRESS
1 0.28 ms 192.168.32.101

Nmap scan report for 192.168.32.103
Host is up (0.00057s 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 192.168.32.100
|     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
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|   1024 600f6fe1c05f6a74d69024fac4d56ccd (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-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 56476/udp mountd
|   100005 1,2,3 60531/tcp mountd
Packets: 7841 - Display
```

La scansione ‘-A’ rileva molte cose in più rispetto alle altre scansioni come vediamo nello screen, effettua anche il banner grabbing del sistema operativo e altri tipi di bruteforce includendoli in modo automatico.

Screen Wireshark :

No.	Time	Source	Destination	Protocol	Length	Info
2955	30.807371147	192.168.32.100	192.168.32.101	TCP	58	57459 → 3030 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2956	30.807400407	192.168.32.100	192.168.32.101	TCP	58	57459 → 340 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2957	30.807404255	192.168.32.100	192.168.32.101	TCP	58	57459 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2958	30.807420790	192.168.32.100	192.168.32.101	TCP	58	57459 → 15002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2959	30.807424645	192.168.32.100	192.168.32.101	TCP	58	57459 → 765 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2960	30.807447667	192.168.32.100	192.168.32.101	TCP	58	57459 → 5120 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2961	30.807451703	192.168.32.100	192.168.32.101	TCP	58	57459 → 3527 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2962	30.807470174	192.168.32.100	192.168.32.101	TCP	58	57459 → 49400 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2963	30.807475797	192.168.32.100	192.168.32.101	TCP	58	57459 → 27353 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2964	30.807510292	192.168.32.100	192.168.32.101	TCP	58	57459 → 7921 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2965	30.807510043	192.168.32.100	192.168.32.101	TCP	58	57459 → 5061 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2966	30.807532090	192.168.32.101	192.168.32.100	TCP	60	1084 → 57459 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2967	30.807533193	192.168.32.101	192.168.32.100	TCP	60	555 → 57459 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2968	30.807533230	192.168.32.101	192.168.32.100	TCP	60	2126 → 57459 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2969	30.807533247	192.168.32.101	192.168.32.100	TCP	60	2009 → 57459 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2970	30.807539622	192.168.32.100	192.168.32.101	TCP	58	57459 → 32782 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2971	30.807544598	192.168.32.100	192.168.32.101	TCP	58	57459 → 7000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2972	30.807565872	192.168.32.100	192.168.32.101	TCP	58	57459 → 27356 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

In questa scansione si vede come il comando ‘-A’ scansioni proprio in modo feroce i tre server in questione. Facendo ciò però viene rilevato più facilmente da IDS o Firewall, perché invia molti pacchetti.

Mendolia Valerio.