Utilizzo dello switch -D per mascherare il mio IP (ME) tra altri IP indicati nel comando (.55, .85, .89)

```
┌──(kali㉿kali)-[~]
└─$ nmap -D 192.168.1.55,192.168.1.85,192.168.1.89,ME 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:48 CET
Nmap scan report for Metasploitable2 (192.168.1.100)
Host is up (0.000086s 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
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
MAC Address: 08:00:27:DB:64:29 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

In Wireshark possiamo vedere gli IP « fasulli » nella colonna « Source ».

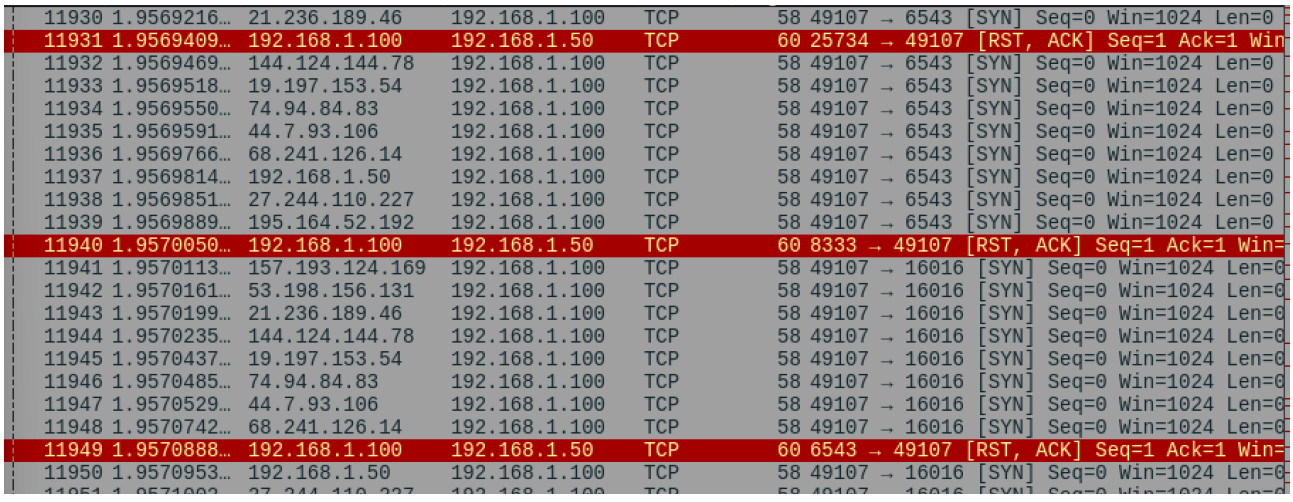
4994	3.4324073…	192.168.1.100	192.168.1.50	TCP	60	787 → 33910 [RST, ACK] Seq=1 Ack=1 Win=0
4995	3.4324073…	192.168.1.100	192.168.1.50	TCP	60	1218 → 33910 [RST, ACK] Seq=1 Ack=1 Win=
4996	3.4324113…	192.168.1.89	192.168.1.100	TCP	58	33910 → 49161 [SYN] Seq=0 Win=1024 Len=0
4997	3.4324198…	192.168.1.50	192.168.1.100	TCP	58	33910 → 49161 [SYN] Seq=0 Win=1024 Len=0
4998	3.4324296…	192.168.1.55	192.168.1.100	TCP	58	33910 → 9415 [SYN] Seq=0 Win=1024 Len=0
4999	3.4324399…	192.168.1.85	192.168.1.100	TCP	58	33910 → 9415 [SYN] Seq=0 Win=1024 Len=0
5000	3.4324489…	192.168.1.89	192.168.1.100	TCP	58	33910 → 9415 [SYN] Seq=0 Win=1024 Len=0
5001	3.4324575…	192.168.1.50	192.168.1.100	TCP	58	33910 → 9415 [SYN] Seq=0 Win=1024 Len=0
5002	3.4324616…	192.168.1.55	192.168.1.100	TCP	58	33910 → 1149 [SYN] Seq=0 Win=1024 Len=0
5003	3.4324671…	192.168.1.100	192.168.1.50	TCP	60	1999 → 33910 [RST, ACK] Seq=1 Ack=1 Win=
5004	3.4324700…	192.168.1.85	192.168.1.100	TCP	58	33910 → 1149 [SYN] Seq=0 Win=1024 Len=0
5005	3.4324861…	192.168.1.89	192.168.1.100	TCP	58	33910 → 1149 [SYN] Seq=0 Win=1024 Len=0
5006	3.4324901…	192.168.1.50	192.168.1.100	TCP	58	33910 → 1149 [SYN] Seq=0 Win=1024 Len=0
5007	3.4324957…	192.168.1.55	192.168.1.100	TCP	58	33910 → 50006 [SYN] Seq=0 Win=1024 Len=0
5008	3.4324977…	192.168.1.100	192.168.1.50	TCP	60	49161 → 33910 [RST, ACK] Seq=1 Ack=1 Win
5009	3.4324978…	192.168.1.100	192.168.1.50	TCP	60	9415 → 33910 [RST, ACK] Seq=1 Ack=1 Win=
5010	3.4325006…	192.168.1.85	192.168.1.100	TCP	58	33910 → 50006 [SYN] Seq=0 Win=1024 Len=0
5011	3.4325064…	192.168.1.89	192.168.1.100	TCP	58	33910 → 50006 [SYN] Seq=0 Win=1024 Len=0
5012	3.4325142…	192.168.1.50	192.168.1.100	TCP	58	33910 → 50006 [SYN] Seq=0 Win=1024 Len=0
5013	3.4325196…	192.168.1.55	192.168.1.100	TCP	58	33910 → 50800 [SYN] Seq=0 Win=1024 Len=0
5014	3.4325307…	192.168.1.85	192.168.1.100	TCP	58	33910 → 50800 [SYN] Seq=0 Win=1024 Len=0
5015	3.4325400…	192.168.1.89	192.168.1.100	TCP	58	33910 → 50800 [SYN] Seq=0 Win=1024 Len=0

Utilizzo dello switch -D RND:10 per mascherare il mio IP tra 10 IP generati casualmente

```
┌──(kali㉿kali)-[~]
└─$ nmap -D RND:10 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:53 CET
Nmap scan report for Metasploitable2 (192.168.1.100)
Host is up (0.00021s 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   filtered 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 filtered ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp filtered vnc
6000/tcp open     X11
6667/tcp filtered irc
8009/tcp filtered ajp13
8180/tcp open     unknown
MAC Address: 08:00:27:DB:64:29 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

In Wireshark possiamo vedere i 10 IP « casuali » nella colonna « Source ».



11930	1.9569216…	21.236.189.46	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11931	1.9569409…	192.168.1.100	192.168.1.50	TCP	60 25734 → 49107 [RST, ACK] Seq=1 Ack=1 Win
11932	1.9569469…	144.124.144.78	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11933	1.9569518…	19.197.153.54	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11934	1.9569550…	74.94.84.83	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11935	1.9569591…	44.7.93.106	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11936	1.9569766…	68.241.126.14	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11937	1.9569814…	192.168.1.50	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11938	1.9569851…	27.244.110.227	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11939	1.9569889…	195.164.52.192	192.168.1.100	TCP	58 49107 → 6543 [SYN] Seq=0 Win=1024 Len=0
11940	1.9570050…	192.168.1.100	192.168.1.50	TCP	60 8333 → 49107 [RST, ACK] Seq=1 Ack=1 Win=
11941	1.9570113…	157.193.124.169	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11942	1.9570161…	53.198.156.131	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11943	1.9570199…	21.236.189.46	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11944	1.9570235…	144.124.144.78	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11945	1.9570437…	19.197.153.54	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11946	1.9570485…	74.94.84.83	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11947	1.9570529…	44.7.93.106	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11948	1.9570742…	68.241.126.14	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0
11949	1.9570888…	192.168.1.100	192.168.1.50	TCP	60 6543 → 49107 [RST, ACK] Seq=1 Ack=1 Win=
11950	1.9570953…	192.168.1.50	192.168.1.100	TCP	58 49107 → 16016 [SYN] Seq=0 Win=1024 Len=0