

```

(kali@kali)-[~]
$ nmap -f 23 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:22 CET
Nmap scan report for Metasploitable2 (192.168.1.100)
Host is up (0.000092s 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: 2 IP addresses (1 host up) scanned in 3.27 seconds

```

Utilizzo dello switch -f

Frammentazione dei pacchetti d'origine per bypassare firewall

In wireshark sono riconoscibili dalla voce Offset > 0

No.	Time	Source	Destination	Protocol	Length	Info
2748	6.0871937...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2749	6.0871979...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID
2750	6.0872146...	192.168.1.50	192.168.1.100	TCP	42	43792 → 843 [SYN] Seq=0 Win=1024 Len=0 MSS=146
2751	6.0872197...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2752	6.0872234...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID
2753	6.0872267...	192.168.1.50	192.168.1.100	TCP	42	43792 → 1164 [SYN] Seq=0 Win=1024 Len=0 MSS=14
2758	6.0873843...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2759	6.0873899...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID
2760	6.0873931...	192.168.1.50	192.168.1.100	TCP	42	43792 → 2998 [SYN] Seq=0 Win=1024 Len=0 MSS=14
2761	6.0873974...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2762	6.0874145...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID
2763	6.0874193...	192.168.1.50	192.168.1.100	TCP	42	43792 → 7938 [SYN] Seq=0 Win=1024 Len=0 MSS=14
2764	6.0874228...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2765	6.0874268...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID
2766	6.0874455...	192.168.1.50	192.168.1.100	TCP	42	43792 → 464 [SYN] Seq=0 Win=1024 Len=0 MSS=146
2767	6.0874504...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2768	6.0874549...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID
2769	6.0874581...	192.168.1.50	192.168.1.100	TCP	42	43792 → 9929 [SYN] Seq=0 Win=1024 Len=0 MSS=14
2773	6.0874910...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2774	6.0874958...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID
2775	6.0874994...	192.168.1.50	192.168.1.100	TCP	42	43792 → 50003 [SYN] Seq=0 Win=1024 Len=0 MSS=1
2776	6.0875034...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID
2776	6.0875034...	192.168.1.50	192.168.1.100	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID

```

> Frame 2470: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_10:ec:ae (08:00:27:10:ec:ae), Dst: Tablet-Bimbi (08:00:27:db:64:29)
> Internet Protocol Version 4, Src: 192.168.1.50, Dst: 192.168.1.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 28
    Identification: 0x51bc (20924)
  > 0000 .... = Flags: 0x0
    ...0 0000 0000 0010 = Fragment Offset: 16
    Time to Live: 51
    Protocol: TCP (6)
    Header Checksum: 0xb237 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.50
    Destination Address: 192.168.1.100
  > [3 IPv4 Fragments (24 bytes): #2466(8), #2467(8), #2470(8)]
    [Stream index: 5]
> Transmission Control Protocol, Src Port: 43792, Dst Port: 5200, Seq: 0, Len: 0

```

```

(kali@kali)-[~]
$ nmap -g 21 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:15 CET
Nmap scan report for Metasploitable2 (192.168.1.100)
Host is up (0.00015s 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 0.25 seconds

```

Utilizzo dello switch -g

Specifica la porta di origine (21) dei pacchetti inviati per tentare di bypassare firewall.

In wireshark è possibile visualizzare la porta 21 dei pacchetti inviati.

4425	87.796970...	192.168.1.50	192.168.1.100	TCP	58	21	→	61900	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4426	87.796977...	192.168.1.50	192.168.1.100	TCP	58	21	→	5431	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4427	87.796983...	192.168.1.50	192.168.1.100	TCP	58	21	→	4125	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4428	87.796989...	192.168.1.50	192.168.1.100	TCP	58	21	→	2869	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4429	87.796993...	192.168.1.50	192.168.1.100	TCP	58	21	→	666	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4430	87.796996...	192.168.1.50	192.168.1.100	TCP	58	21	→	6689	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4431	87.797001...	192.168.1.50	192.168.1.100	TCP	58	21	→	9485	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4432	87.797006...	192.168.1.50	192.168.1.100	TCP	58	21	→	10180	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4433	87.797010...	192.168.1.50	192.168.1.100	TCP	58	21	→	1169	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4434	87.797014...	192.168.1.50	192.168.1.100	TCP	58	21	→	9594	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460
4435	87.797019...	192.168.1.50	192.168.1.100	TCP	58	21	→	3404	[SYN]	Seq=0	Win=1024	Len=0	MSS=1460