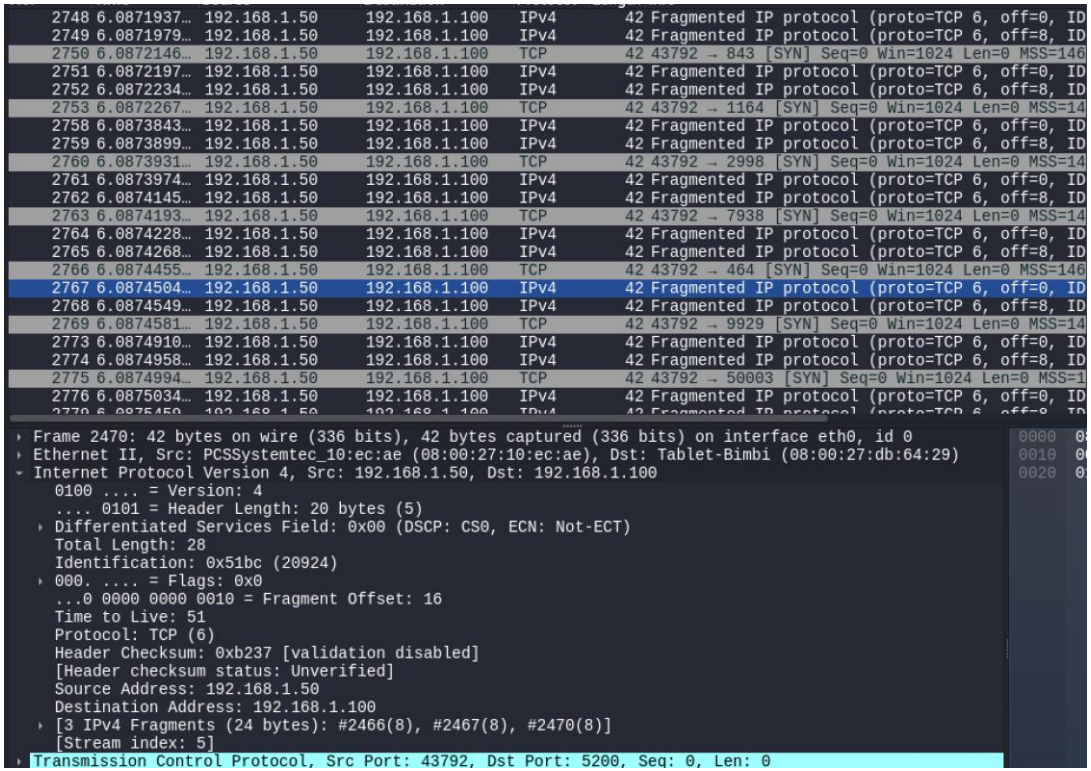
Utilizzo dello switch -f

Frammentazione dei pacchetti d'origine per bypassare firewall

In wireshark sono riconoscibili dalla voce Offset > 0

```
┌──(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
```



```
┌──(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 orgine (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
```