

```
# nmap -PN -sX 10.10.10.45 -p 79-81
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-12-25 15:27 EDT
Nmap scan report for 10.10.10.45
Host is up (0.0018s latency).
PORT      STATE      SERVICE
79/tcp    closed    finger
80/tcp    open|filtered http
81/tcp    closed    hosts2-ns
MAC Address: 00:50:56:17:CF:45 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.28 seconds
```

```
# hping --fin --push --urg --count 3 10.10.10.45 -p ++79
HPING 10.10.10.45 (eth0 10.10.10.45): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.10.45 ttl=64 DF id=0 sport=79 flags=RA seq=0 win=0
rtt=0.8 ms
len=46 ip=10.10.10.45 ttl=64 DF id=0 sport=81 flags=RA seq=2 win=0
rtt=2.9 ms

--- 10.10.10.45 hping statistic ---
3 packets transmitted, 2 packets received, 34% packet loss
round-trip min/avg/max = 0.8/1.8/2.9 ms
```

```
# scapy
Welcome to Scapy (2.1.1)
>>> srl(IP(dst="10.10.10.45")/TCP(dport=(79,81),flags="FPU"),timeout=1)
Begin emission:
.*Finished to send 3 packets.
*..
Received 5 packets, got 2 answers, remaining 1 packets
<IP version=4L ihl=5L tos=0x0 len=40 id=0 flags=DF frag=0L ttl=64
proto=tcp chksum=0xd18e src=10.10.10.45 dst=10.10.75.1 options=[] |<TCP
sport=finger dport=ftp_data seq=0 ack=1 dataofs=5L reserved=0L flags=RA
window=0 chksum=0x462b urgptr=0 |<Padding
load='\x00\x00\x00\x00\x00\x00' |>>>
```

```
# tcpdump -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
15:27:22.491499 IP 10.10.75.1.39731 > 10.10.10.45.80: FP
3431967323:3431967323(0) win 2048 urg 0
15:27:22.491537 IP 10.10.75.1.39731 > 10.10.10.45.81: FP
3431967323:3431967323(0) win 2048 urg 0
15:27:22.491565 IP 10.10.75.1.39731 > 10.10.10.45.79: FP
3431967323:3431967323(0) win 2048 urg 0
15:27:22.491958 IP 10.10.10.45.81 > 10.10.75.1.39731: R 0:0(0) ack
3431967324 win 0
15:27:22.492205 IP 10.10.10.45.79 > 10.10.75.1.39731: R 0:0(0) ack
3431967324 win 0
15:27:23.591965 IP 10.10.75.1.39732 > 10.10.10.45.80: FP
3431901786:3431901786(0) win 3072 urg 0
15:27:42.183352 IP 10.10.75.1.2595 > 10.10.10.45.79: FP
865145577:865145577(0) win 512 urg 0
15:27:42.183996 IP 10.10.10.45.79 > 10.10.75.1.2595: R 0:0(0) ack
865145578 win 0
15:27:43.183654 IP 10.10.75.1.2596 > 10.10.10.45.80: FP
1947954619:1947954619(0) win 512 urg 0
15:27:44.184011 IP 10.10.75.1.2597 > 10.10.10.45.81: FP
625880305:625880305(0) win 512 urg 0
15:27:44.186762 IP 10.10.10.45.81 > 10.10.75.1.2597: R 0:0(0) ack
625880306 win 0
15:27:53.506242 IP 10.10.10.45.81 > 10.10.75.1.20: R 0:0(0) ack 1 win 0
urg 0
15:27:53.509146 IP 10.10.10.45.81 > 10.10.75.1.20: R 0:0(0) ack 1 win 0
urg 0
15:27:53.511633 IP 10.10.10.45.81 > 10.10.75.1.20: R 0:0(0) ack 1 win 0
urg 0
15:27:53.513172 IP 10.10.10.45.81 > 10.10.75.1.20: R 0:0(0) ack 1 win 0
urg 0
15:27:53.514674 IP 10.10.10.45.81 > 10.10.75.1.20: R 0:0(0) ack 1 win 0
```

Oh, Christmas Tree (scan),
 Oh, Christmas Tree (scan),
 Your beauty green will teach me
 That hope and love will ever be
 The way to joy and peace for me.



Oh, Christmas Tree (scan),
 Oh, Christmas Tree (scan),
 How lovely are your packets!

MERRY CHRISTMAS!
 FROM THE SKOUDIS FAMILY