

Final Project Covert Communication

Mario Enriquez

British Columbia Institute of Technology

COMP 8505, 7D

Aman Abdulla

December 12, 2016

Contents

Introduction	3
How to Run	3
Victim	3
Host	4
Design Work	5
Test Cases	6
Test 1	8
Test 2	11
Test 3	13
Test 4	15
Test 5	18
Observations	21
Pseudocode	21
Victim Machine	21
Host Machine	23

Introduction

For this assignment, I created a Covert Communication program. The program has two functions:

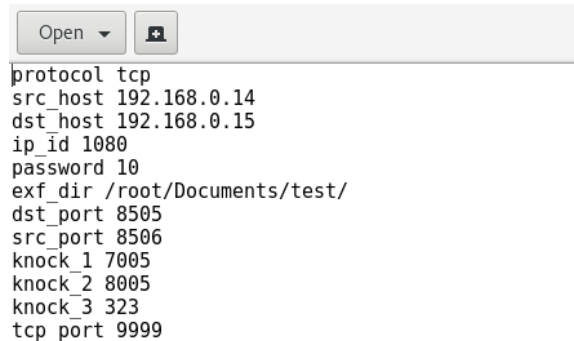
- To send and execute commands from a remote machine on a victim machine, and to get the results of the commands.
- To act as an exfiltration tool which detects the creation or modification of a file in a selected directory of a victim machine, and sends the contents of the created or modified file to a remote machine.

This is with the purpose of using everything we learned during this term in a single program. We have to implement raw sockets, backdoors, port knocking and exfiltration to create one tool which lets us gain control of a remote machine.

How to Run

Victim

-Set configuration file parameters



The image shows a configuration file editor window. At the top, there is a toolbar with an 'Open' button and a file icon. Below the toolbar, the configuration parameters are listed in a text area:

```
protocol tcp
src_host 192.168.0.14
dst_host 192.168.0.15
ip_id 1080
password 10
exf_dir /root/Documents/test/
dst_port 8505
src_port 8506
knock_1 7005
knock_2 8005
knock_3 323
tcp_port 9999
```

```
root@datacomm:~/Document
File Edit View Search Terminal Help
[root@datacomm victim]# make clean
rm -f *.o core covert
[root@datacomm victim]# make covert
g++ -c send_packet.cpp
g++ -c headers.cpp
g++ -c exfilt.cpp
g++ -o covert covert.cpp send_packet.o headers.o exfilt.o -lpcap -lpthread
[root@datacomm victim]# ./covert HELLO config.txt
```

Host

-Set configuration file parameters

```
config.txt
~/Documents/host
protocol tcp
src_host 192.168.0.15
dst_host 192.168.0.14
ip_id 1080
password 10
dst_port 8505
src_port 8506
knock_1 7005
knock_2 8005
knock_3 323
tcp_port 9999
```

-Make clean

-Make covert

- run \$./covert (mask) (configuration file)

```

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# make clean
rm -f *.o core covert
[root@datacomm host]# make covert
g++ -c send_packet.cpp
g++ -c headers.cpp
g++ -c recv_packet.cpp
g++ -o covert covert.cpp recv_packet.o send_packet.o headers.o -lpcap -lpthread
[root@datacomm host]# ./covert MARIO config.txt
Please input your command:

```

Design Work

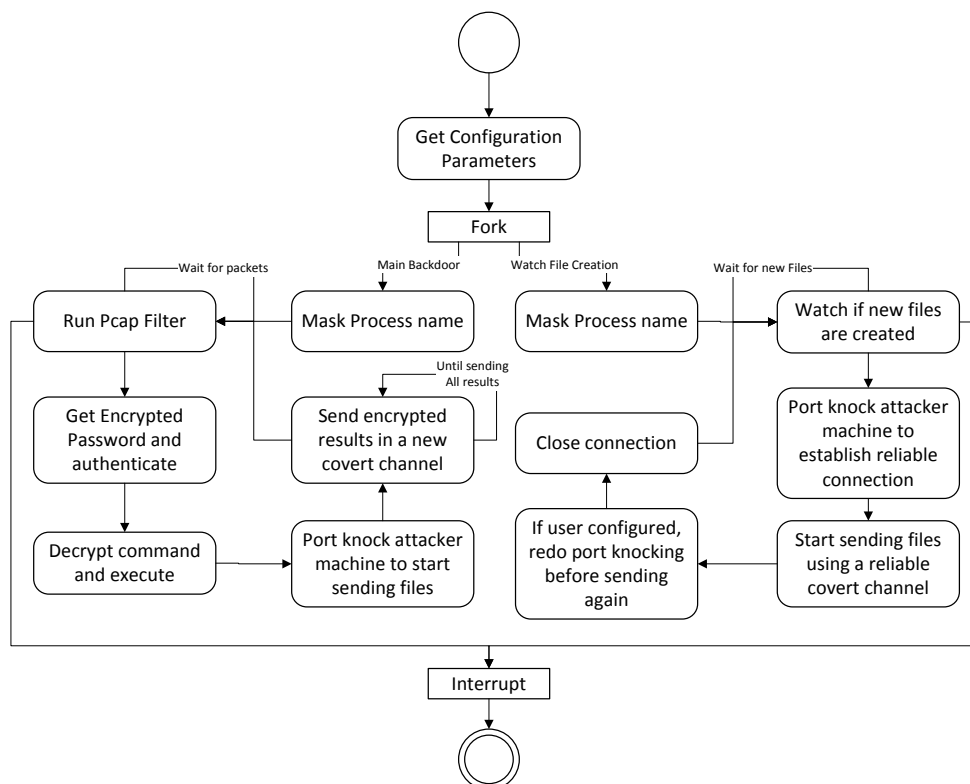


Figure 1 Victim Machine

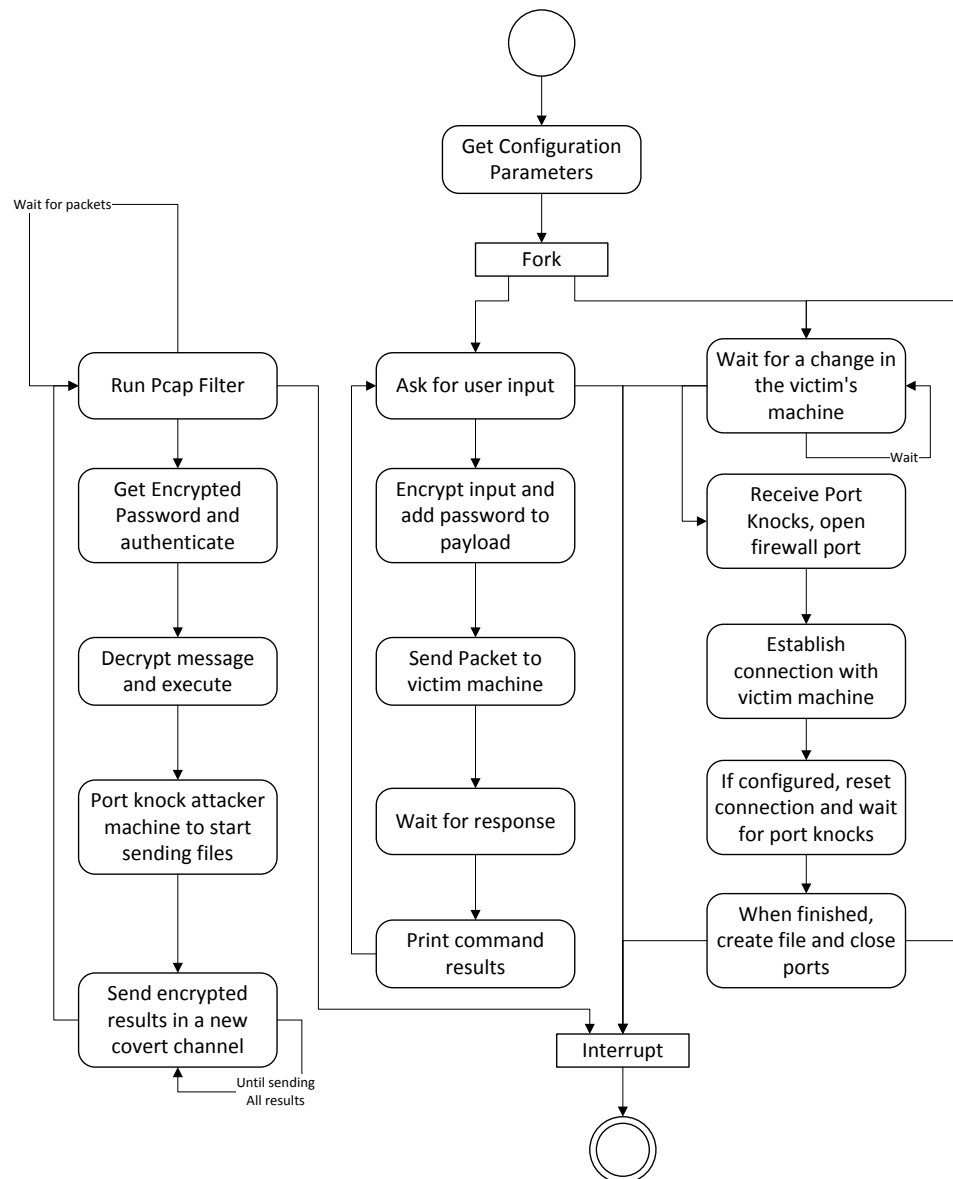


Figure 2 Host Machine

Test Cases

Test	Scenario	Tools	Expected Results	Actual Results
1	Test running a command to get current machine	Fedora	Success	Success, ipconfig returns the victim's IP
2	Test running a	Fedora	Success	Success we get the

	command to get text			results through the payload
3	Test Exfiltration component by creating and transferring a small file	Fedora	Success	Success, we get the new file in our host machine
4	Test Port knocking by analyzing the iptables rules	Fedora	Success	Success, the iptables allow the victim to establish connection
5	UDP test, run different commands	Fedora	Success	Partial Success, while the command execution runs fine, it makes the exfiltration don't work.

Test 1

Host

```

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
root      24585  0.0  0.0  45644  1928 tty2      S+   07:40   0:00 /usr/sbin/dumpcap -n -
i eno1 -y EN10MB -Z none
root      24613  0.0  0.0  17808  1148 ?            Ss   07:40   0:00 /usr/lib/systemd/syste
md-hostnamed
root      24623  0.0  0.0  151188  3596 pts/0      R+   07:40   0:00 ps auxw
sudo ifconfig
udp
sending datagram
Please input your command:
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.14  netmask 255.255.255.0  broadcast 192.168.0.255
    inet6 fe80::9804:585d:31c2:9bab  prefixlen 64  scopeid 0x20<link>
    ether 98:90:96:dc:ed:2f  txqueuelen 1000  (Ethernet)
    RX packets 104920  bytes 56180488 (53.5 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 34457  bytes 3549395 (3.3 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
    device interrupt 20  memory 0xf7d00000-f7d20000

enp3s2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    ether 00:0e:0c:51:2c:cc  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1  (Local Loopback)
    RX packets 68  bytes 5256 (5.1 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 68  bytes 5256 (5.1 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
    ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

Figure 3 ifconfig victim


```

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
    inet6 fe80::9804:585d:31c2:9bab prefixlen 64 scopeid 0x20<link>
    ether 98:90:96:dc:ed:2f txqueuelen 1000 (Ethernet)
    RX packets 104920 bytes 56180488 (53.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34457 bytes 3549395 (3.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xf7d00000-f7d20000

enp3s2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:0e:0c:51:2c:cc txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 68 bytes 5256 (5.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 5256 (5.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
    ether 00:00:00:00:00:00 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

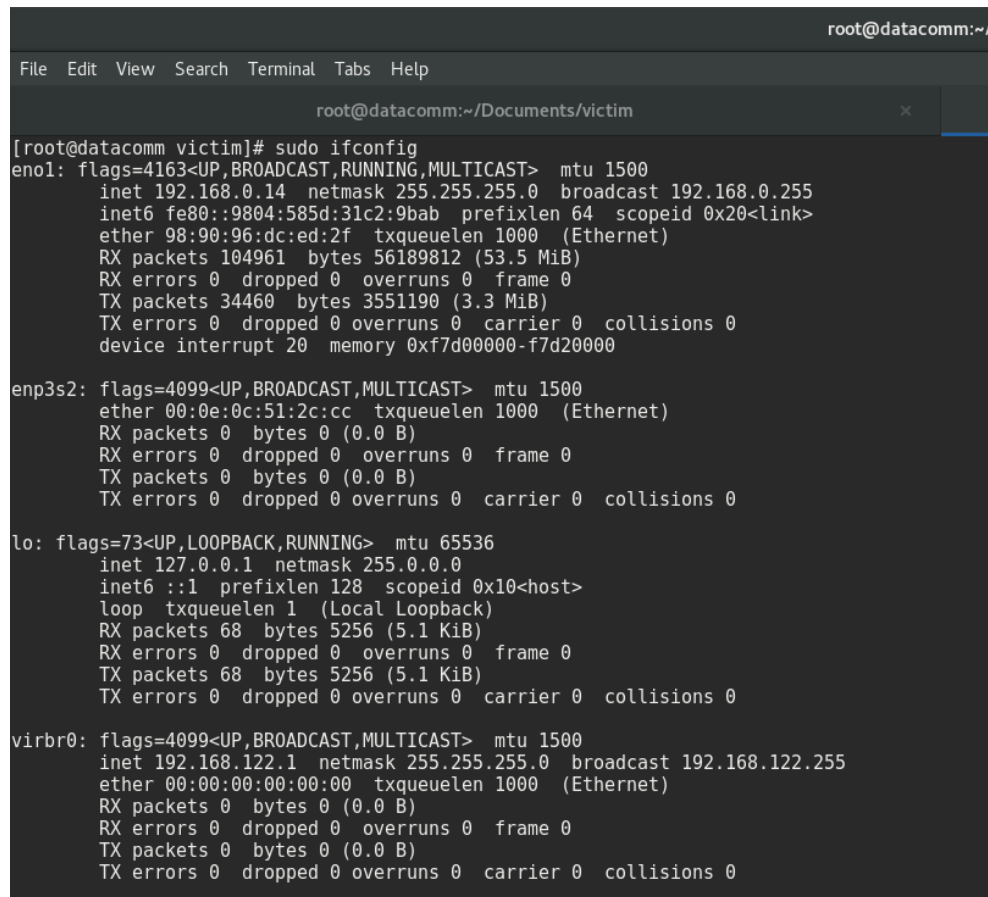
^C
[root@datacomm host]# sudo ifconfig
enol: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.15 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::7ec7:657a:eaf6:64f4 prefixlen 64 scopeid 0x20<link>
    ether 98:90:96:d4:af:4f txqueuelen 1000 (Ethernet)
    RX packets 164805 bytes 116920741 (111.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 66194 bytes 8410954 (8.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xf7d00000-f7d20000

enp3s2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

```

Figure 4 ifconfig host vs victim

Victim



```
root@datacomm:~/Documents/victim
[root@datacomm victim]# sudo ifconfig
enol: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.14  netmask 255.255.255.0  broadcast 192.168.0.255
    inet6 fe80::9804:585d:31c2:9bab  prefixlen 64  scopeid 0x20<link>
    ether 98:90:96:dc:ed:2f  txqueuelen 1000  (Ethernet)
    RX packets 104961  bytes 56189812 (53.5 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 34460  bytes 3551190 (3.3 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
    device interrupt 20  memory 0xf7d00000-f7d20000

enp3s2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    ether 00:0e:0c:51:2c:cc  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

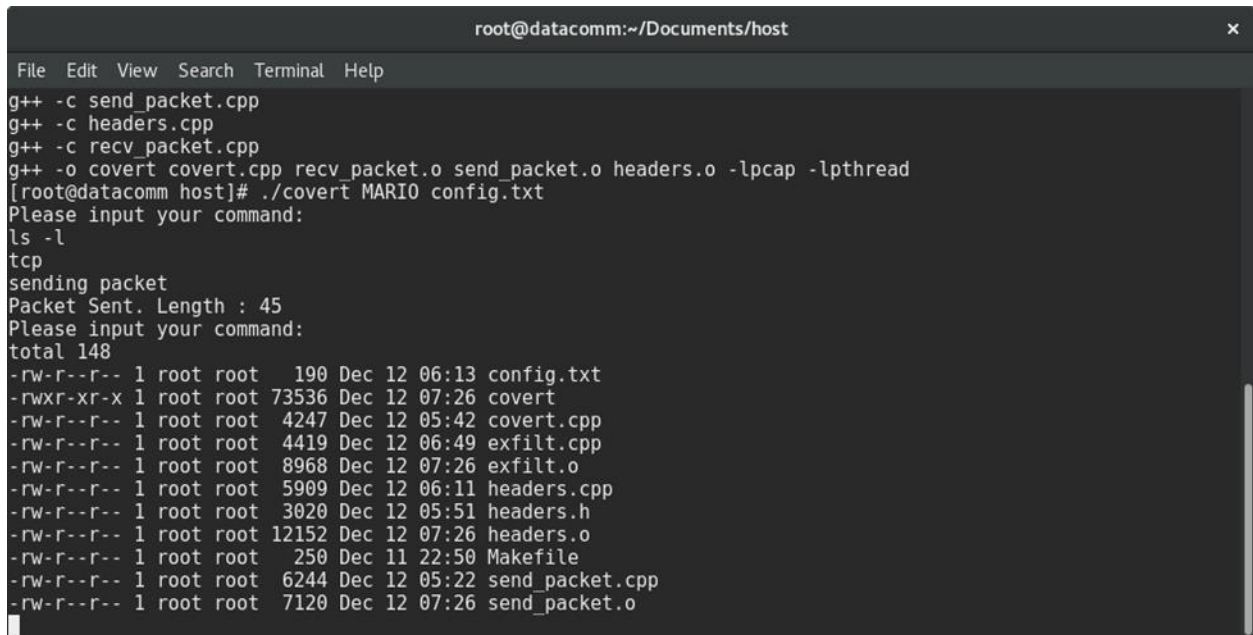
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1  (Local Loopback)
    RX packets 68  bytes 5256 (5.1 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 68  bytes 5256 (5.1 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
    ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Figure 5 Ifconfig of Victim

Test 2

Host

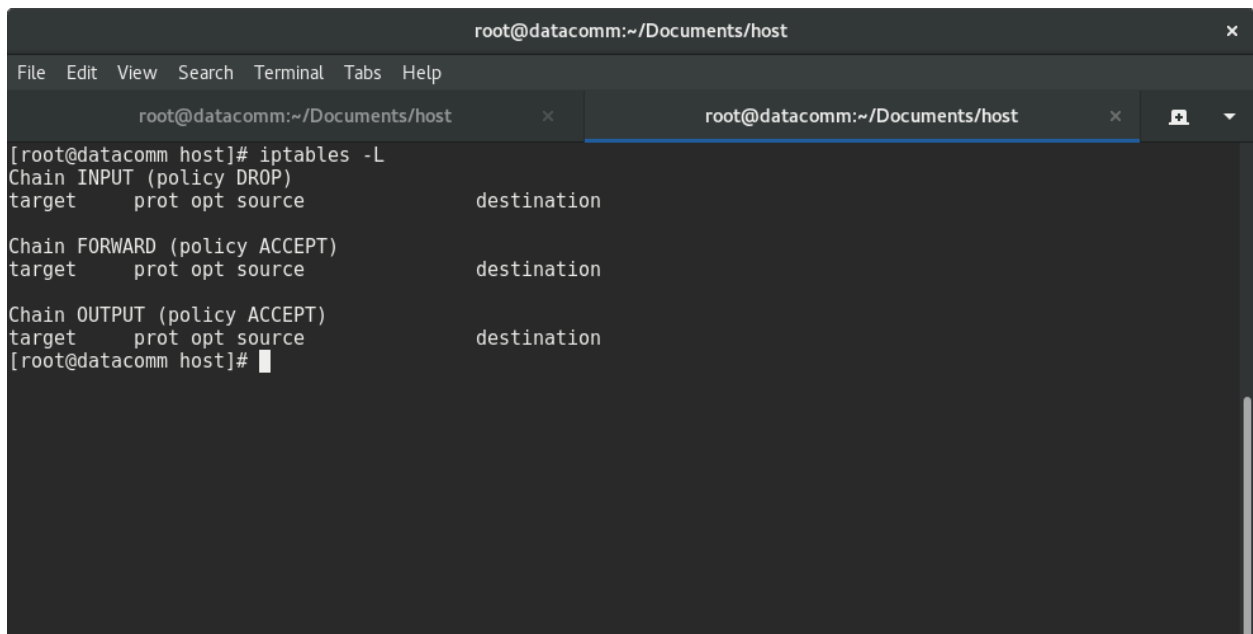


```

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
g++ -c send_packet.cpp
g++ -c headers.cpp
g++ -c recv_packet.cpp
g++ -o covert covert.cpp recv_packet.o send_packet.o headers.o -lpcap -lpthread
[root@datacomm host]# ./covert MARIO config.txt
Please input your command:
ls -l
tcp
sending packet
Packet Sent. Length : 45
Please input your command:
total 148
-rw-r--r-- 1 root root 190 Dec 12 06:13 config.txt
-rwxr-xr-x 1 root root 73536 Dec 12 07:26 covert
-rw-r--r-- 1 root root 4247 Dec 12 05:42 covert.cpp
-rw-r--r-- 1 root root 4419 Dec 12 06:49 exfilt.cpp
-rw-r--r-- 1 root root 8968 Dec 12 07:26 exfilt.o
-rw-r--r-- 1 root root 5909 Dec 12 06:11 headers.cpp
-rw-r--r-- 1 root root 3020 Dec 12 05:51 headers.h
-rw-r--r-- 1 root root 12152 Dec 12 07:26 headers.o
-rw-r--r-- 1 root root 250 Dec 11 22:50 Makefile
-rw-r--r-- 1 root root 6244 Dec 12 05:22 send_packet.cpp
-rw-r--r-- 1 root root 7120 Dec 12 07:26 send_packet.o

```

Figure 6 Successful command



```

root@datacomm:~/Documents/host
File Edit View Search Terminal Tabs Help
root@datacomm:~/Documents/host x root@datacomm:~/Documents/host x
[root@datacomm host]# iptables -L
Chain INPUT (policy DROP)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
[root@datacomm host]#

```

Figure 7 Ip tables

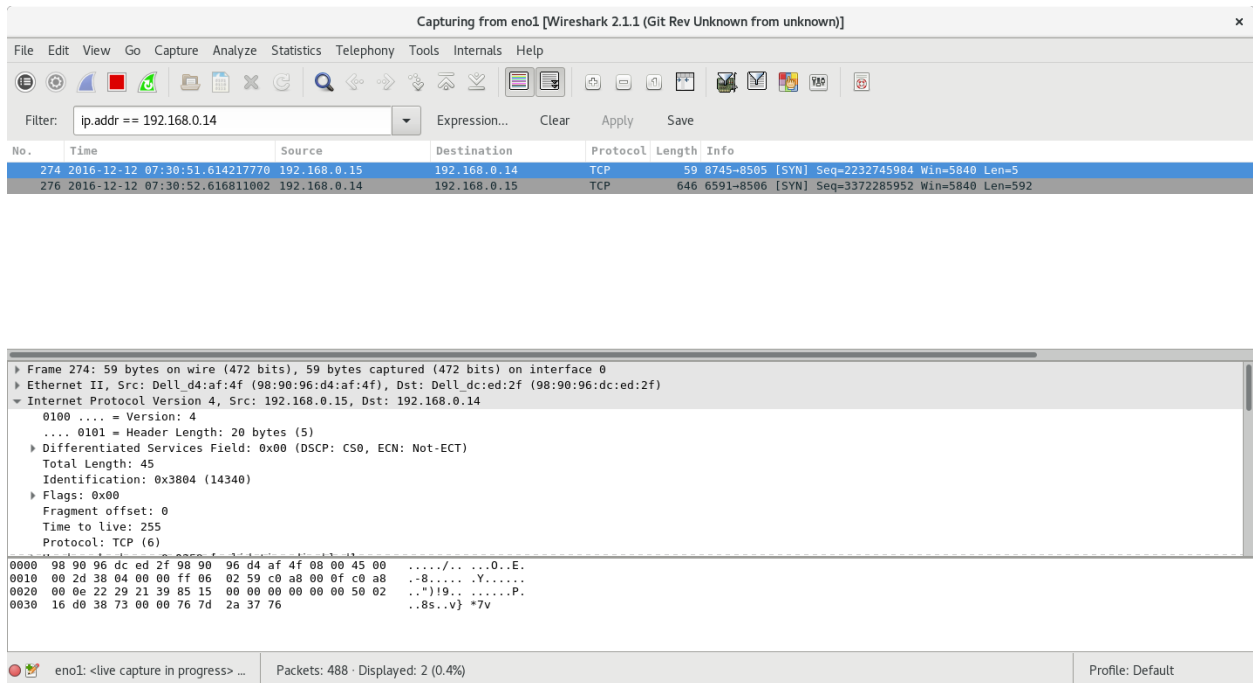


Figure 8 Exchange Victim and host

Victim

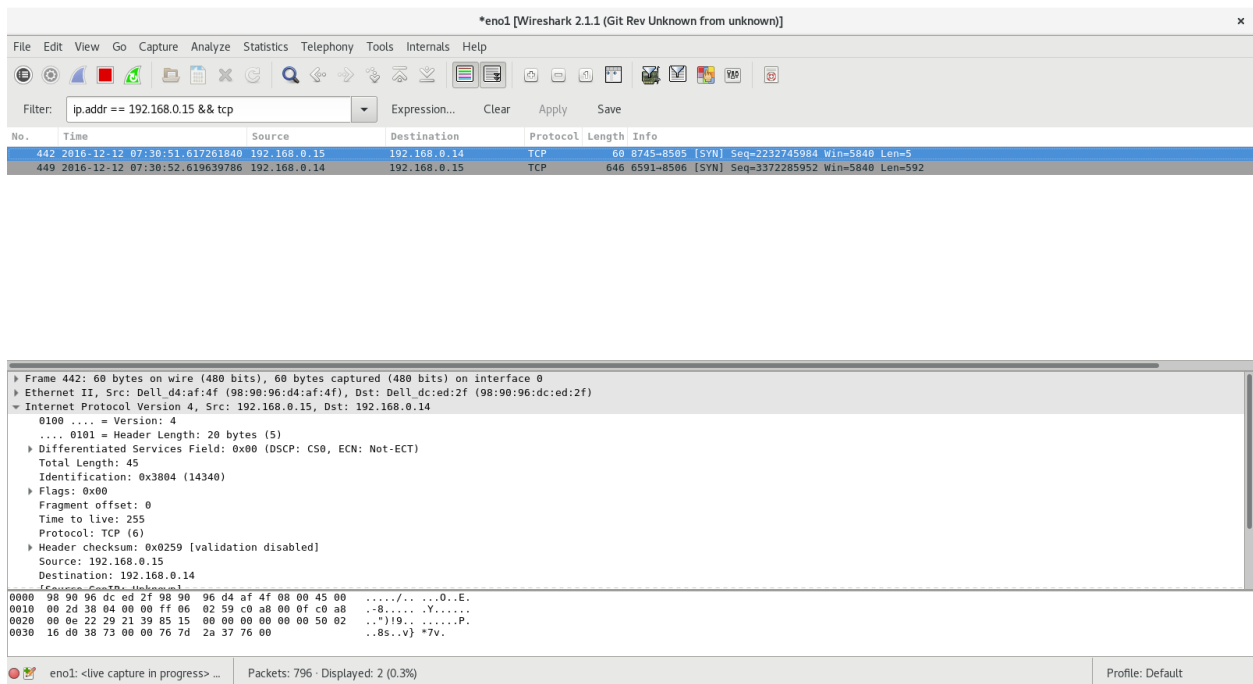


Figure 9 Exchange victim and host

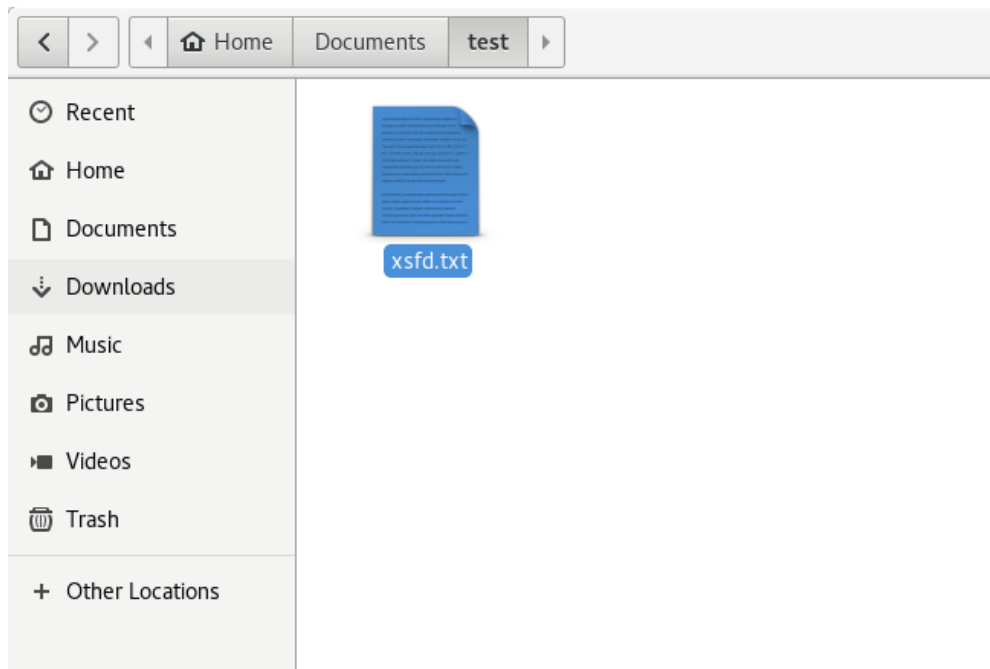


Figure 10 File to Transfer

Test 3

Host

```

root@datacomm:~/Documents/host
File Edit View Search Terminal Tabs Help
root@datacomm:~/Documents/host
Please input your command:
total 148
-rw-r--r-- 1 root root 190 Dec 12 06:13 config.txt
-rwxr-xr-x 1 root root 73536 Dec 12 07:26 covert
-rw-r--r-- 1 root root 4247 Dec 12 05:42 covert.cpp
-rw-r--r-- 1 root root 4419 Dec 12 06:49 exfilt.cpp
-rw-r--r-- 1 root root 8968 Dec 12 07:26 exfilt.o
-rw-r--r-- 1 root root 5909 Dec 12 06:11 headers.cpp
-rw-r--r-- 1 root root 3020 Dec 12 05:51 headers.h
-rw-r--r-- 1 root root 12152 Dec 12 07:26 headers.o
-rw-r--r-- 1 root root 250 Dec 11 22:50 Makefile
-rw-r--r-- 1 root root 6244 Dec 12 05:22 send_packet.cpp
-rw-r--r-- 1 root root 7120 Dec 12 07:26 send_packet.o
Knock on port: 7005
Knocks: 100
Knock on port: 8005
Knocks: 110
Knock on port: 323
Knocks: 111
Knocks: 000

```

Figure 11 Port Knocking

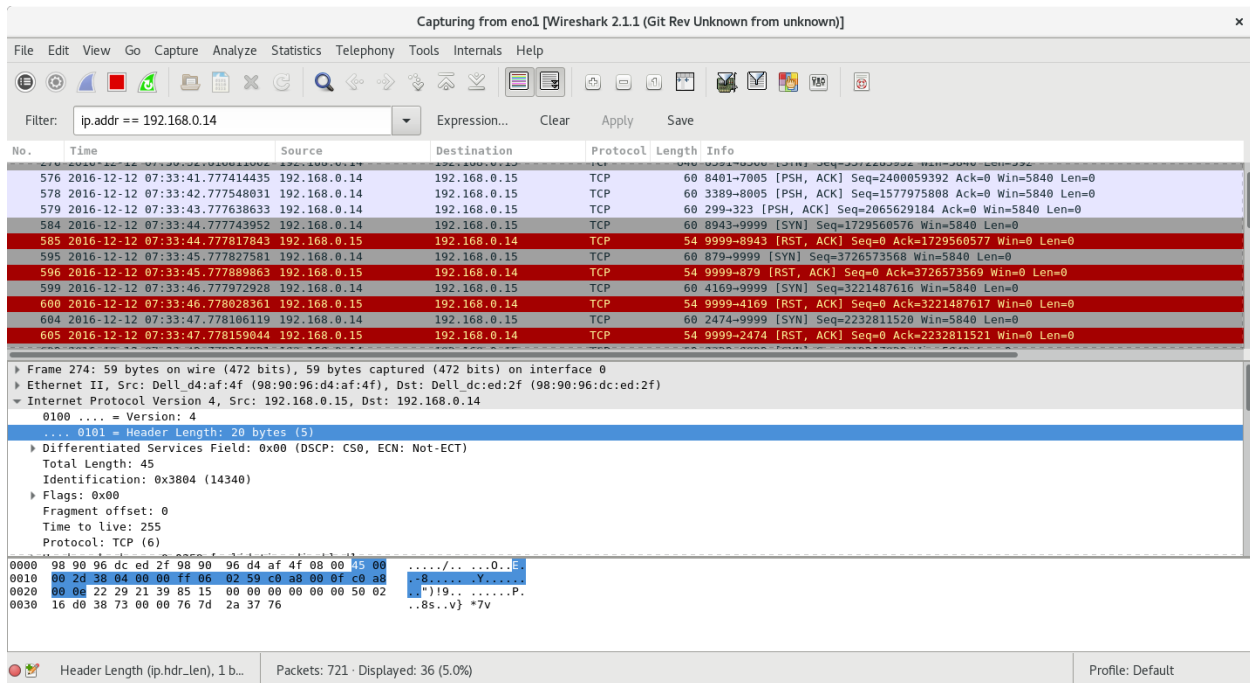


Figure 12 Exchange

Victim

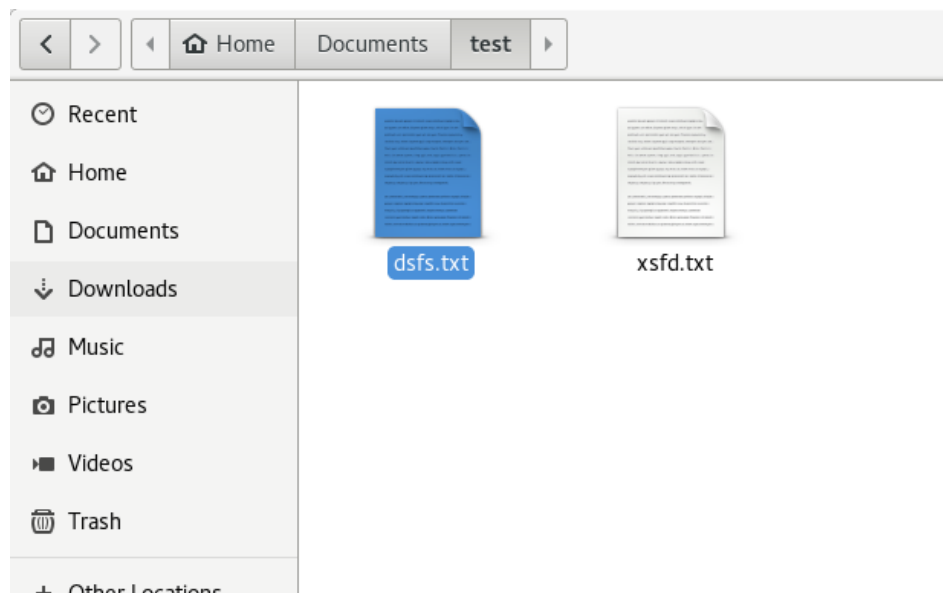


Figure 13 Files transferred

*eno1 [Wireshark 2.1.1 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr == 192.168.0.15 && tcp` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
854	2016-12-12 07:33:41.780126365	192.168.0.14	192.168.0.15	TCP	54	8401-7005 [PSH, ACK] Seq=2400059392 Ack=0 Win=5840 Len=0
856	2016-12-12 07:33:42.780232791	192.168.0.14	192.168.0.15	TCP	54	3389-8005 [PSH, ACK] Seq=1577975808 Ack=0 Win=5840 Len=0
857	2016-12-12 07:33:43.780340316	192.168.0.14	192.168.0.15	TCP	54	299-323 [PSH, ACK] Seq=2065629184 Ack=0 Win=5840 Len=0
863	2016-12-12 07:33:44.780439705	192.168.0.14	192.168.0.15	TCP	54	8943-9999 [SYN] Seq=1729560576 Win=5840 Len=0
864	2016-12-12 07:33:44.780675723	192.168.0.15	192.168.0.14	TCP	60	9999-8943 [RST, ACK] Seq=0 Ack=1729560577 Win=0 Len=0
873	2016-12-12 07:33:45.780537547	192.168.0.14	192.168.0.15	TCP	54	879-9999 [SYN] Seq=3726573568 Win=5840 Len=0
874	2016-12-12 07:33:45.780780036	192.168.0.15	192.168.0.14	TCP	60	9999-879 [RST, ACK] Seq=0 Ack=3726573569 Win=0 Len=0
881	2016-12-12 07:33:46.780657222	192.168.0.14	192.168.0.15	TCP	54	4169-9999 [SYN] Seq=3221487616 Win=5840 Len=0
882	2016-12-12 07:33:46.780918240	192.168.0.15	192.168.0.14	TCP	60	9999-4169 [RST, ACK] Seq=0 Ack=3221487617 Win=0 Len=0
886	2016-12-12 07:33:47.780780068	192.168.0.14	192.168.0.15	TCP	54	2474-9999 [SYN] Seq=2232811520 Win=5840 Len=0
887	2016-12-12 07:33:47.781047205	192.168.0.15	192.168.0.14	TCP	60	9999-2474 [RST, ACK] Seq=0 Ack=2232811521 Win=0 Len=0
891	2016-12-12 07:33:48.780906458	192.168.0.14	192.168.0.15	TCP	54	2329-9999 [SYN] Seq=219217920 Win=5840 Len=0
892	2016-12-12 07:33:48.781171560	192.168.0.15	192.168.0.14	TCP	60	9999-2329 [RST, ACK] Seq=0 Ack=219217921 Win=0 Len=0
894	2016-12-12 07:33:49.781027990	192.168.0.14	192.168.0.15	TCP	54	8616-9999 [SYN] Seq=4060807168 Win=5840 Len=0
895	2016-12-12 07:33:49.781257081	192.168.0.15	192.168.0.14	TCP	60	9999-8616 [RST, ACK] Seq=0 Ack=4060807169 Win=0 Len=0

Frame 442: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Dell d4:af:4f (98:90:96:dc:ed:2f), Dst: Dell dc:ed:2f (98:90:96:dc:ed:2f)
 Internet Protocol Version 4, Src: 192.168.0.15, Dst: 192.168.0.14
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 45
 Identification: 0x3804 (14340)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 255
 Protocol: TCP (6)
 Header checksum: 0x0259 [validation disabled]
 Source: 192.168.0.15
 Destination: 192.168.0.14
 (Capture length is 45 bytes)
 0000 00 00 06 dc ed 2f 98 90 96 d4 af 4f 00 00 45 00/.0..E.
 0010 00 2d 38 04 00 00 ff 06 02 59 c0 a0 00 0f c0 a8 ..8....Y.Y....
 0020 00 0e 22 29 21 39 85 15 00 00 00 00 00 50 02 ..")!9.....P.
 0030 16 d0 38 73 00 00 76 7d 2a 37 76 00 ..8s..v)*7v.

eno1: <live capture in progress> ... Packets: 967 - Displayed: 36 (3.7%) Profile: Default

Figure 14 Port Knock exchange

*eno1 [Wireshark 2.1.1 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr == 192.168.0.15 && tcp` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
854	2016-12-12 07:33:41.780126365	192.168.0.14	192.168.0.15	TCP	54	8401-7005 [PSH, ACK] Seq=2400059392 Ack=0 Win=5840 Len=0
856	2016-12-12 07:33:42.780232791	192.168.0.14	192.168.0.15	TCP	54	3389-8005 [PSH, ACK] Seq=1577975808 Ack=0 Win=5840 Len=0
857	2016-12-12 07:33:43.780340316	192.168.0.14	192.168.0.15	TCP	54	299-323 [PSH, ACK] Seq=2065629184 Ack=0 Win=5840 Len=0
863	2016-12-12 07:33:44.780439705	192.168.0.14	192.168.0.15	TCP	54	8943-9999 [SYN] Seq=1729560576 Win=5840 Len=0
864	2016-12-12 07:33:44.780675723	192.168.0.15	192.168.0.14	TCP	60	9999-8943 [RST, ACK] Seq=0 Ack=1729560577 Win=0 Len=0
873	2016-12-12 07:33:45.780537547	192.168.0.14	192.168.0.15	TCP	54	879-9999 [SYN] Seq=3726573568 Win=5840 Len=0
874	2016-12-12 07:33:45.780780036	192.168.0.15	192.168.0.14	TCP	60	9999-879 [RST, ACK] Seq=0 Ack=3726573569 Win=0 Len=0
881	2016-12-12 07:33:46.780657222	192.168.0.14	192.168.0.15	TCP	54	4169-9999 [SYN] Seq=3221487616 Win=5840 Len=0
882	2016-12-12 07:33:46.780918240	192.168.0.15	192.168.0.14	TCP	60	9999-4169 [RST, ACK] Seq=0 Ack=3221487617 Win=0 Len=0
886	2016-12-12 07:33:47.780780068	192.168.0.14	192.168.0.15	TCP	54	2474-9999 [SYN] Seq=2232811520 Win=5840 Len=0
887	2016-12-12 07:33:47.781047205	192.168.0.15	192.168.0.14	TCP	60	9999-2474 [RST, ACK] Seq=0 Ack=2232811521 Win=0 Len=0
891	2016-12-12 07:33:48.780906458	192.168.0.14	192.168.0.15	TCP	54	2329-9999 [SYN] Seq=219217920 Win=5840 Len=0
892	2016-12-12 07:33:48.781171560	192.168.0.15	192.168.0.14	TCP	60	9999-2329 [RST, ACK] Seq=0 Ack=219217921 Win=0 Len=0
894	2016-12-12 07:33:49.781027990	192.168.0.14	192.168.0.15	TCP	54	8616-9999 [SYN] Seq=4060807168 Win=5840 Len=0
895	2016-12-12 07:33:49.781257081	192.168.0.15	192.168.0.14	TCP	60	9999-8616 [RST, ACK] Seq=0 Ack=4060807169 Win=0 Len=0
898	2016-12-12 07:33:50.781171999	192.168.0.14	192.168.0.15	TCP	54	1156-9999 [SYN] Seq=672792576 Win=5840 Len=0
899	2016-12-12 07:33:50.781392156	192.168.0.15	192.168.0.14	TCP	60	9999-1156 [RST, ACK] Seq=0 Ack=672792577 Win=0 Len=0
908	2016-12-12 07:33:51.781291212	192.168.0.14	192.168.0.15	TCP	54	3491-9999 [SYN] Seq=1091436544 Win=5840 Len=0
909	2016-12-12 07:33:51.781528109	192.168.0.15	192.168.0.14	TCP	60	9999-3491 [RST, ACK] Seq=0 Ack=1091436545 Win=0 Len=0
911	2016-12-12 07:33:52.781410008	192.168.0.14	192.168.0.15	TCP	54	1400-9999 [SYN] Seq=1141309440 Win=5840 Len=0
912	2016-12-12 07:33:52.781642276	192.168.0.15	192.168.0.14	TCP	60	9999-1400 [RST, ACK] Seq=0 Ack=1141309441 Win=0 Len=0
916	2016-12-12 07:33:53.781532451	192.168.0.14	192.168.0.15	TCP	54	6108-9999 [SYN] Seq=2635661312 Win=5840 Len=0
917	2016-12-12 07:33:53.781779273	192.168.0.15	192.168.0.14	TCP	60	9999-6108 [RST, ACK] Seq=0 Ack=2635661313 Win=0 Len=0
923	2016-12-12 07:33:54.781654732	192.168.0.14	192.168.0.15	TCP	54	5917-9999 [SYN] Seq=874119168 Win=5840 Len=0
924	2016-12-12 07:33:54.781862467	192.168.0.15	192.168.0.14	TCP	60	9999-5917 [RST, ACK] Seq=0 Ack=874119169 Win=0 Len=0
925	2016-12-12 07:33:55.781810775	192.168.0.14	192.168.0.15	TCP	54	7259-9999 [SYN] Seq=3423141888 Win=5840 Len=0
926	2016-12-12 07:33:55.782071075	192.168.0.15	192.168.0.14	TCP	60	9999-7259 [RST, ACK] Seq=0 Ack=3423141889 Win=0 Len=0
933	2016-12-12 07:33:56.781934252	192.168.0.14	192.168.0.15	TCP	54	7165-9999 [SYN] Seq=454426624 Win=5840 Len=0

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 0000 00 00 06 dc ed 2f 98 90 96 d4 af 4f 00 00 45 00/.0..E.
 0010 00 2d 38 04 00 00 ff 06 02 59 c0 a0 00 0f c0 a8 ..8....Y.Y....
 0020 00 0e 22 29 21 39 85 15 00 00 00 00 00 50 02 ..")!9.....P.
 0030 16 d0 38 73 00 00 76 7d 2a 37 76 00 ..8s..v)*7v.

eno1: <live capture in progress> ... Packets: 988 - Displayed: 36 (3.6%) Profile: Default

Test 4

Host

```

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# make covert
make: 'covert' is up to date.
[root@datacomm host]# make clean
rm -f *.o core covert
[root@datacomm host]# make covert
g++ -c send_packet.cpp
^[[Ag++ -c headers.cpp
g++ -c recv_packet.cpp
g++ -o covert covert.cpp recv_packet.o send_packet.o headers.o -lpcap -lpthread
[root@datacomm host]# ./covert MARIO config.txt
Please input your command:
Knock on port: 7005
Knocks: 100
Knock on port: 8005
Knocks: 110
Knock on port: 323
Knocks: 111
Knocks: 000
[]

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
[root@datacomm host]#

```

Figure 15 Default

```

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# ./covert MARIO config.txt
Please input your command:
Knock on port: 7005
Knocks: 100
Knock on port: 8005
Knocks: 110
Knock on port: 323
Knocks: 111
Knocks: 111
[]

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
[root@datacomm host]# iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination
ACCEPT    tcp  --  anywhere              tcp dpt:distinct
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
[root@datacomm host]#

```

Figure 16 Port Knocking Successful


```

root@datacomm: ~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# ./covert MARIO config.txt
Please input your command:
Knock on port: 7005
Knocks: 100
Knock on port: 8005
Knocks: 110
Knock on port: 323
Knocks: 111
Knocks: 000
[]

root@datacomm: ~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# iptables -L
Chain INPUT (policy DROP)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
[root@datacomm host]# iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:distinct

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
[root@datacomm host]# iptables -L
Chain INPUT (policy DROP)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
[root@datacomm host]#

```

Figure 17 IP tables rules again set to drop

Victim

Capturing from eno1 [Wireshark 2.1.1 (Git Rev Unknown from unknown)]

Filter: `ip.addr == 192.168.0.14` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1185	2016-12-12 07:38:00.184886027	192.168.0.15	192.168.0.14	TCP	54	9999->935 [RST, ACK] Seq=0 Ack=2316828673 Win=0 Len=0
1189	2016-12-12 07:38:01.184948254	192.168.0.14	192.168.0.15	TCP	60	265->9999 [SYN] Seq=623181824 Win=5840 Len=0
1190	2016-12-12 07:38:01.184994982	192.168.0.15	192.168.0.14	TCP	54	9999->265 [RST, ACK] Seq=0 Ack=623181825 Win=0 Len=0
1192	2016-12-12 07:38:02.185047696	192.168.0.14	192.168.0.15	TCP	60	1577->9999 [SYN] Seq=975044608 Win=5840 Len=0
1193	2016-12-12 07:38:02.185103570	192.168.0.15	192.168.0.14	TCP	54	9999->1577 [RST, ACK] Seq=0 Ack=975044609 Win=0 Len=0
1196	2016-12-12 07:38:03.185188943	192.168.0.14	192.168.0.15	TCP	60	5022->9999 [SYN] Seq=3541958656 Win=5840 Len=0
1197	2016-12-12 07:38:03.185248602	192.168.0.15	192.168.0.14	TCP	54	9999->5022 [RST, ACK] Seq=0 Ack=3541958657 Win=0 Len=0
1200	2016-12-12 07:38:04.185301120	192.168.0.14	192.168.0.15	TCP	60	4420->9999 [SYN] Seq=2283798528 Win=5840 Len=0
1201	2016-12-12 07:38:04.185362791	192.168.0.15	192.168.0.14	TCP	54	9999->4420 [RST, ACK] Seq=0 Ack=2283798529 Win=0 Len=0
1205	2016-12-12 07:38:05.185418613	192.168.0.14	192.168.0.15	TCP	60	5509->9999 [SYN] Seq=4079026176 Win=5840 Len=1
1206	2016-12-12 07:38:05.185475340	192.168.0.15	192.168.0.14	TCP	54	9999->5509 [RST, ACK] Seq=0 Ack=4079026178 Win=0 Len=0
1207	2016-12-12 07:38:05.185486911	192.168.0.14	192.168.0.15	TCP	60	2677->7005 [PSH, ACK] Seq=3055419392 Ack=0 Win=5840 Len=0

Frame 274: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
 Ethernet II, Src: Dell d4:af:4f (98:90:96:d4:af:4f), Dst: Dell dc:ed:2f (98:90:96:dc:ed:2f)
 Internet Protocol Version 4, Src: 192.168.0.15, Dst: 192.168.0.14
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 45
 Identification: 0x3804 (14340)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 255
 Protocol: TCP (6)

0000 98 90 96 dc ed 2f 98 90 96 d4 af 4f 08 00 15 000...
 0010 00 2d 38 04 00 00 ff 06 02 59 c0 a8 00 0f c0 a8 ..8.....Y.....
 0020 00 0e 22 29 21 39 85 15 00 00 00 00 00 50 02 ..")19.....P..
 0030 16 d0 38 73 00 00 76 7d 2a 37 76 ..8s..v} *7v

Header Length (ip.hdr.len), 1 b... Packets: 1274 · Displayed: 185 (14.5%) Profile: Default

Figure 18 Exchange between Host and Victim

Test 5

Host

```

config.txt — /root/Documents
File Edit View Selection Find Packages Help
▼ host
  config.txt
  covert
  covert.cpp
  dsfs.txt
  headers.cpp
  headers.h
  headers.o
  Makefile
  recv_packet.cpp
  recv_packet.o
  send_packet.cpp
  send_packet.o
1 protocol udp
2 src_host 192.168.0.15
3 dst_host 192.168.0.14
4 ip_id 1080
5 password 10
6 dst_port 8505
7 src_port 8506
8 knock_1 7005
9 knock_2 8005
10 knock_3 323
11 tcp_port 9999
12

```

Figure 19 Configuration file for UDP

```

root@datacomm:~/Documents/host
File Edit View Search Terminal Help
[root@datacomm host]# ./covert MARIO config.txt
Please input your command:
Knock on port: 7005
Knocks: 100
Knock on port: 8005
Knocks: 110
Knock on port: 323
Knocks: 111
Knocks: 000
^C
[root@datacomm host]# ./covert MARIO config.txt
Please input your command:
ls -l
udp
sending datagram
Please input your command:
total 148
-rw-r--r-- 1 root root 190 Dec 12 07:39 config.txt
-rwxr-xr-x 1 root root 73536 Dec 12 07:26 covert
-rw-r--r-- 1 root root 4247 Dec 12 05:42 covert.cpp
-rw-r--r-- 1 root root 4419 Dec 12 06:49 exfilt.cpp
-rw-r--r-- 1 root root 8968 Dec 12 07:26 exfilt.o
-rw-r--r-- 1 root root 5909 Dec 12 06:11 headers.cpp
-rw-r--r-- 1 root root 3020 Dec 12 05:51 headers.h
-rw-r--r-- 1 root root 12152 Dec 12 07:26 headers.o
-rw-r--r-- 1 root root 250 Dec 11 22:50 Makefile
-rw-r--r-- 1 root root 6244 Dec 12 05:22 send_packet.cpp
-rw-r--r-- 1 root root 7120 Dec 12 07:26 send_packet.o

```

Figure 20 Results of UDP

root@datacomm:~/Documents/host										
File	Edit	View	Search	Terminal	Help					
root		24	0.0	0.0	0	0 ?	S	Dec11	0:00	[watchdog/2]
root		25	0.0	0.0	0	0 ?	S	Dec11	0:00	[migration/2]
root		26	0.0	0.0	0	0 ?	S	Dec11	0:00	[ksoftirqd/2]
root		28	0.0	0.0	0	0 ?	S<	Dec11	0:00	[kworker/2:0H]
root		29	0.0	0.0	0	0 ?	S	Dec11	0:06	[rcuos/2]
root		30	0.0	0.0	0	0 ?	S	Dec11	0:00	[rcuob/2]
root		31	0.0	0.0	0	0 ?	S	Dec11	0:00	[cpuhp/3]
root		32	0.0	0.0	0	0 ?	S	Dec11	0:00	[watchdog/3]
root		33	0.0	0.0	0	0 ?	S	Dec11	0:00	[migration/3]
root		34	0.0	0.0	0	0 ?	S	Dec11	0:00	[ksoftirqd/3]
root		36	0.0	0.0	0	0 ?	S<	Dec11	0:00	[kworker/3:0H]
root		37	0.0	0.0	0	0 ?	S	Dec11	0:04	[rcuos/3]
root		38	0.0	0.0	0	0 ?	S	Dec11	0:00	[rcuob/3]
root		39	0.0	0.0	0	0 ?	S	Dec11	0:00	[kdevtmpfs]
root		40	0.0	0.0	0	0 ?	S<	Dec11	0:00	[netns]
root		41	0.0	0.0	0	0 ?	S	Dec11	0:00	[oom_reaper]
root		42	0.0	0.0	0	0 ?	S<	Dec11	0:00	[writeback]
root		43	0.0	0.0	0	0 ?	S	Dec11	0:00	[kcompactd0]
root		44	0.0	0.0	0	0 ?	SN	Dec11	0:00	[ksmd]
root		45	0.0	0.0	0	0 ?	SN	Dec11	0:00	[khugepaged]
root		46	0.0	0.0	0	0 ?	S<	Dec11	0:00	[crypto]
root		47	0.0	0.0	0	0 ?	S<	Dec11	0:00	[kintegrityd]
root		48	0.0	0.0	0	0 ?	S<	Dec11	0:00	[bioset]
root		49	0.0	0.0	0	0 ?	S<	Dec11	0:00	[kblockd]
root		50	0.0	0.0	0	0 ?	S<	Dec11	0:00	[ata_sff]
root		51	0.0	0.0	0	0 ?	S<	Dec11	0:00	[md]
root		52	0.0	0.0	0	0 ?	S<	Dec11	0:00	[devfreq_wq]
root		53	0.0	0.0	0	0 ?	S<	Dec11	0:00	[watchdogd]
root		56	0.0	0.0	0	0 ?	S	Dec11	0:00	[kswapd0]
root		57	0.0	0.0	0	0 ?	S<	Dec11	0:00	[vmstat]
root		103	0.0	0.0	0	0 ?	S<	Dec11	0:00	[kthrotld]
root		105	0.0	0.0	0	0 ?	S<	Dec11	0:00	[acpi_thermal_pm]
root		106	0.0	0.0	0	0 ?	S	Dec11	0:00	[scsi_eh_0]
root		107	0.0	0.0	0	0 ?	S<	Dec11	0:00	[scsi_tm_f_0]
root		108	0.0	0.0	0	0 ?	S	Dec11	0:00	[scsi_eh_1]
root		109	0.0	0.0	0	0 ?	S<	Dec11	0:00	[scsi_tm_f_1]
root		110	0.0	0.0	0	0 ?	S	Dec11	0:00	[scsi_eh_2]
root		111	0.0	0.0	0	0 ?	S<	Dec11	0:00	[scsi_tm_f_2]
root		112	0.0	0.0	0	0 ?	S	Dec11	0:00	[scsi_eh_3]
root		113	0.0	0.0	0	0 ?	S<	Dec11	0:00	[scsi_tm_f_3]
root		114	0.0	0.0	0	0 ?	S	Dec11	0:00	[scsi_eh_4]
root		115	0.0	0.0	0	0 ?	S<	Dec11	0:00	[scsi_tm_f_4]
root		116	0.0	0.0	0	0 ?	S	Dec11	0:00	[scsi_eh_5]
root		11								

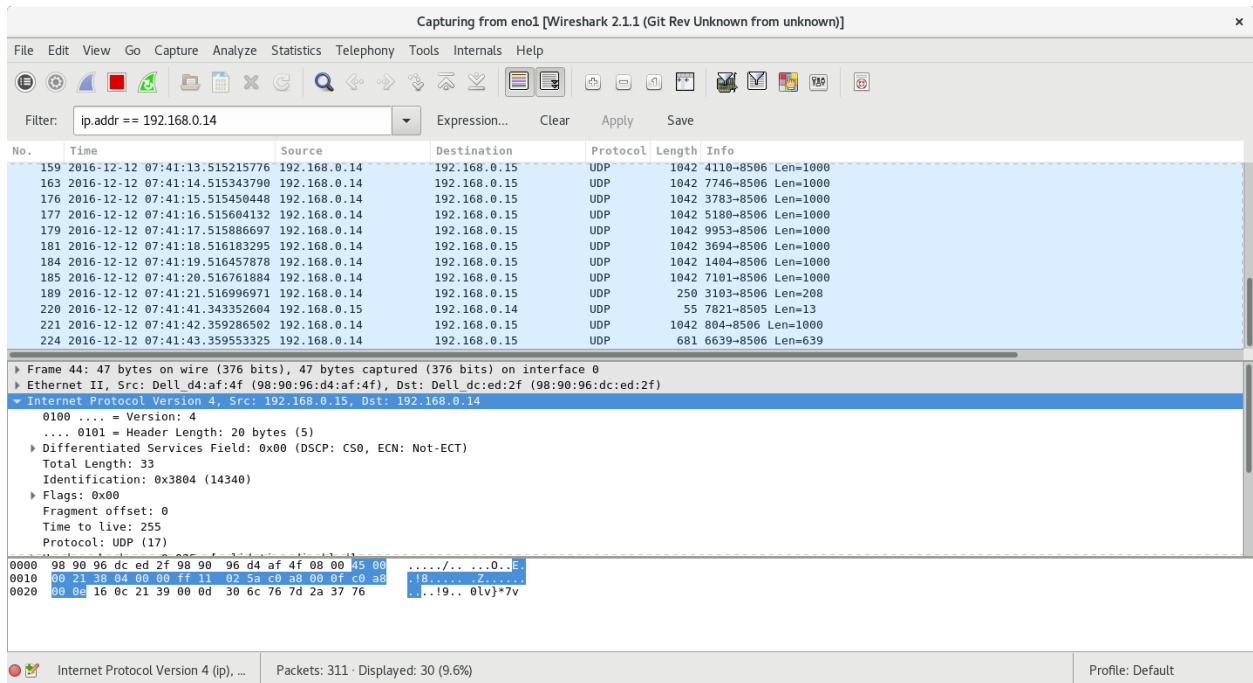


Figure 21 Exchange UDP

Victim

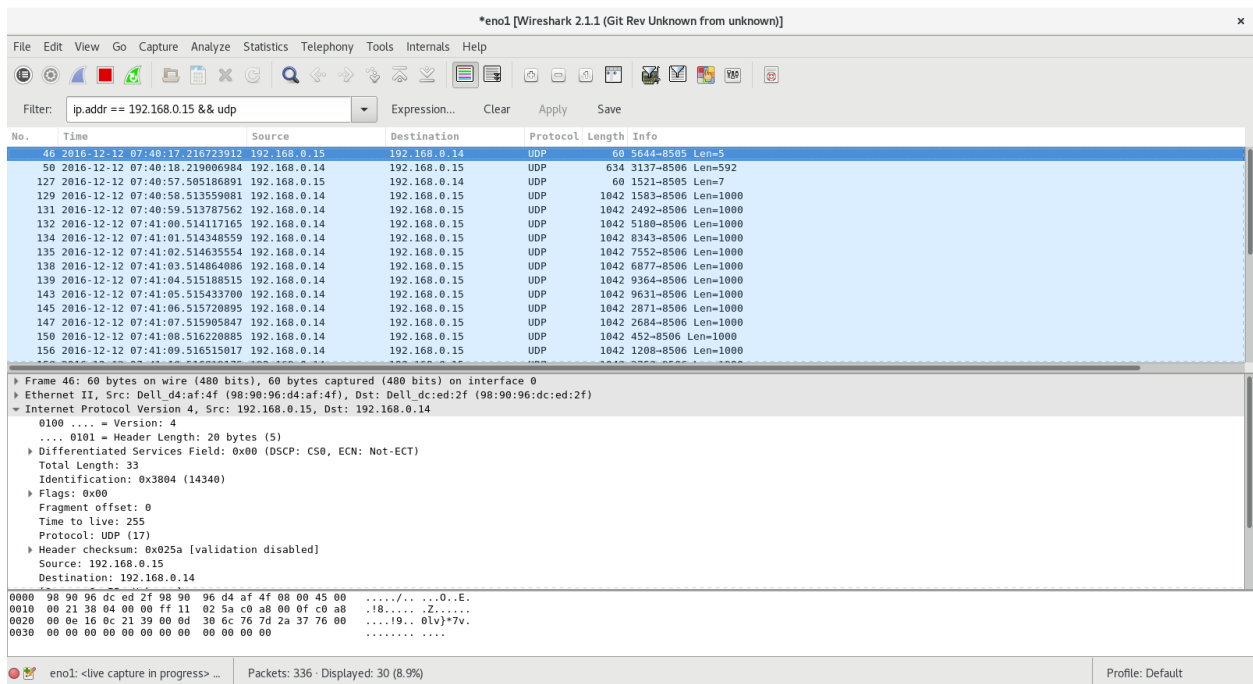


Figure 22 UDP results

Observations

- By default, inotify may have trouble depending on how the file is modified or created. Gedit on Linux can be troublesome because it creates and modifies over a temporal file.
- Port knocking allows us to set the firewall as a filter, as it can allow only raw sockets directed to a specific port to get to us.

Pseudocode

Victim Machine

Include libraries

Main Function

 Open Configuration file

 Read Configuration file

 Assign values

 Create interruption handler

 Start Thread Function Capture

 Start Thread Function Ex-filtration

 Join

 Exit

End of Main

Capture Function, receives Filter parameters, password

 Start libpcap filter to capture packets from host machine directed to an specific port

 Grab payload contents

Authenticate payload by using Decrypt function

Use Decrypt Function to Decrypt rest of payload

Execute Command

Encrypt Command Results with Encrypt Function

While there are still command result values

 Send result values using Craft_packet

End of While

End of Capture

Ex-filtration Function receives directory to watch, host parameters

 Set Function to detect changes of selected file directory

 Set select function to detect the changes on the directory

 if there is a change in the directory

 Get Filename

 Port knock host machine

 Establish connection with host machine

 Encrypt Filename and contents with Encrypt Function

 Use Craft_packet to send contents of Filename

 Port Knock if neccessary and repeat sending

 End if

End of Ex-filtration

Craft_packet Function receives message, host parameters

 Set IP header parameters

 if TCPs protocol, set TCP header parameters

```

    if UDP protocol, set UDP header parameters

    Create pseudo-header

    Copy Packet parameters

    Perform Checksum

    Send Packet

    if TCP selected, wait for ack

        if ack is not received resend packets

        end if

    end if

End of Craft_packet Function

```

Decrypt Function, receives message and password

```

    Generate Key from password

    Decrypt message with Key

End of Decrypt Function

```

Encrypt Function, receives message and password

```

    Generate Key from password

    Encrypt message with Key

End of Encrypt Function

```

Host Machine

```

Include libraries

```

```

Main Function

```

```
    Open Configuration file
    Read Configuration file
    Assign values
    Create interruption handler
    Start Thread Function Command
    Start Thread Function Receive_File
    Start Thread Function Capture
    Join
    Exit
End of Main

Command Function
    While True
        Prompt user Input
        Create and send packet using Craft_packet function
        Wait for Response
        Print Result
    End While
End of Command Function

Receive_File Function
    While true
        Wait until start of port knocking
```



```
        If Port Knocking sequence is correct drop Firewall rules

            Establish connection with victim machine

            Receive File data from the covert channel

            If necessary receive port knocking sequence again

            Decrypt File using Decrypt function

            Write File in Directory

        End if

    End While

End Receive_File

Craft_packet Function receives message, host parameters

    Set IP header parameters

    if TCPs protocol, set TCP header parameters

    if UDP protocol, set UDP header parameters

    Create pseudo-header

    Copy Packet parameters

    Perform Checksum

    Send Packet

    if TCP selected, wait for ack

        if ack is not received resend packets

        end if

    end if

End of Craft_packet Function
```

Capture Function, receives Filter parameters, password

Start libpcap filter to capture packets from host machine directed to an specific port

Grab payload contents

Authenticate payload by using Decrypt function

Use Decrypt Function to Decrypt rest of payload

Execute Command

Encrypt Command Results with Encrypt Function

While there are still command result values

Send result values using Craft_packet

End of While

End of Capture

Decrypt Function, receives message and password

Generate Key from password

Decrypt message with Key

End of Decrypt Function

Encrypt Function, receives message and password

Generate Key from password

Encrypt message with Key

End of Encrypt Function