

## Task 1 : TCP RST attack on Telnet and SSH Connections

Screenshot 1 : Telnet Connection Details

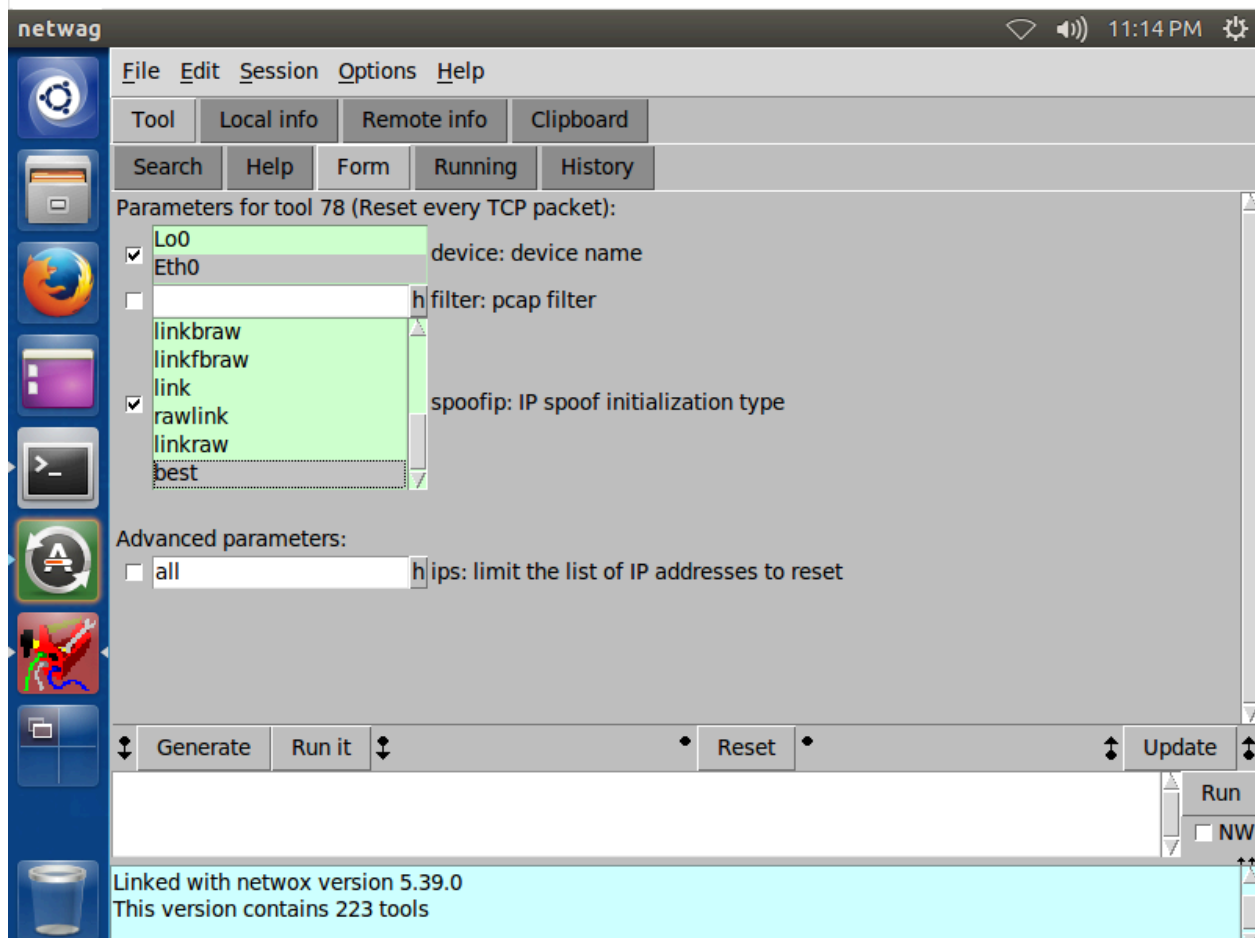
```
cybersec-server@ubuntu:~$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^]'.
Ubuntu 14.04.5 LTS
ubuntu login: cybersec-client
Password:
Last login: Mon Oct 17 22:04:33 PDT 2016 from 10.0.2.8 on pts/6
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.2.0-42-generic x86_64)

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

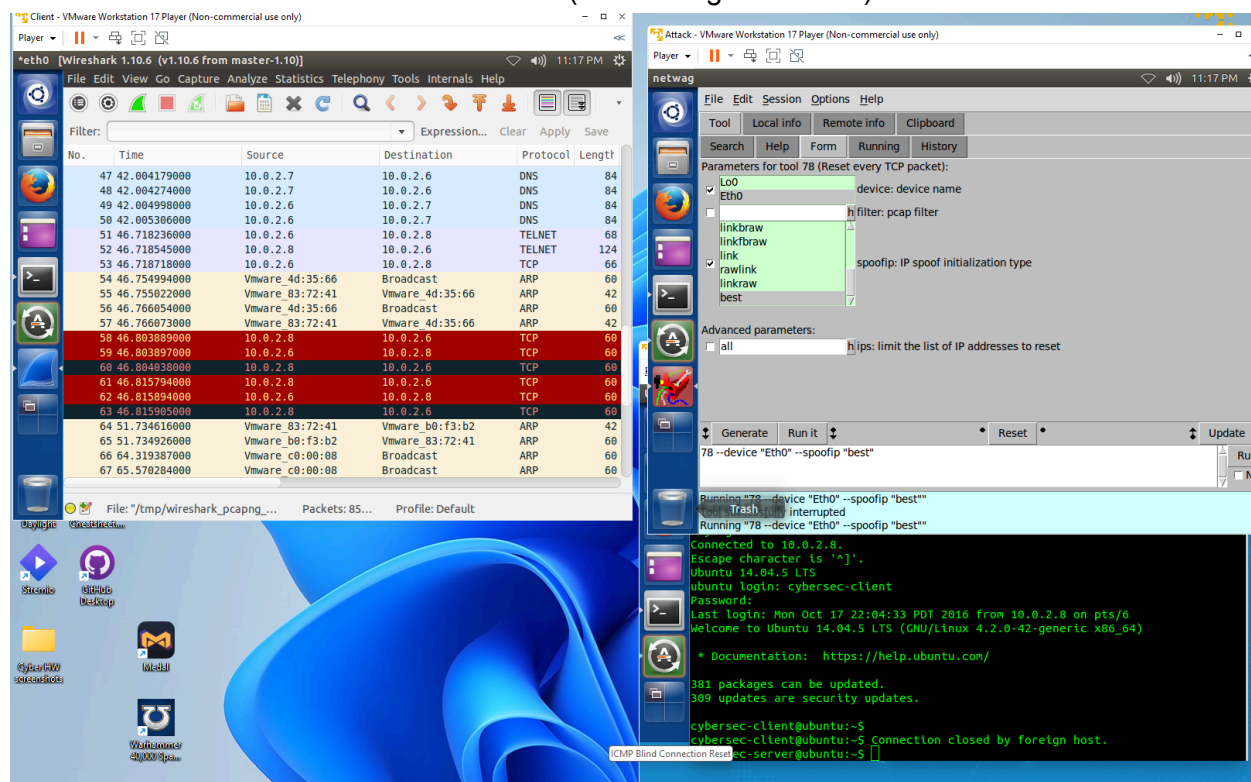
381 packages can be updated.
309 updates are security updates.

cybersec-client@ubuntu:~$
```

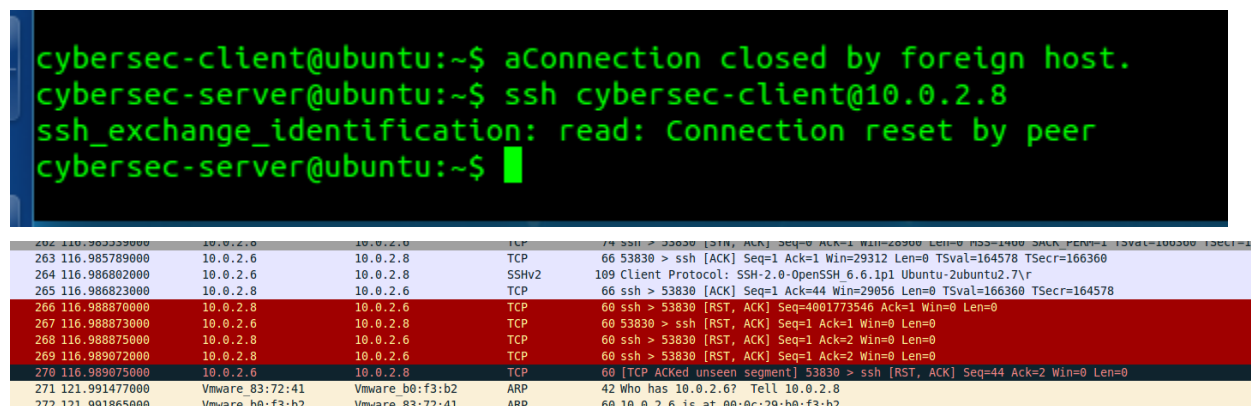
Screenshot 2 : Netswag (took 78) Interface with Details.



Screenshot 3: Connection failed on server (Bottom Right Console) With wireshark results



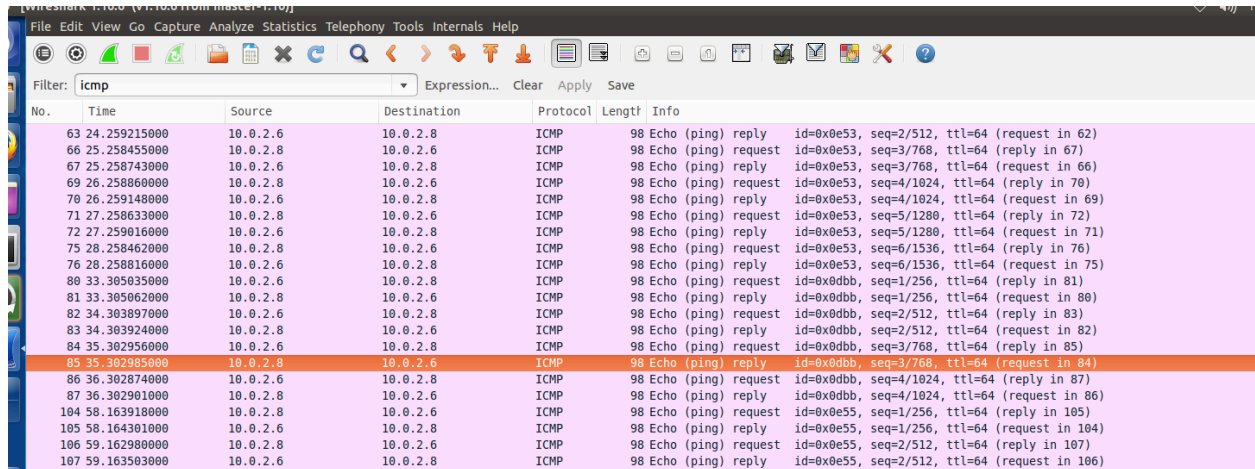
Screenshot 4 + 5 - SSH connection and SSH connection on wireshark.



## Task 2 : ICMP Blind Connection Reset and Source Quench Attacks

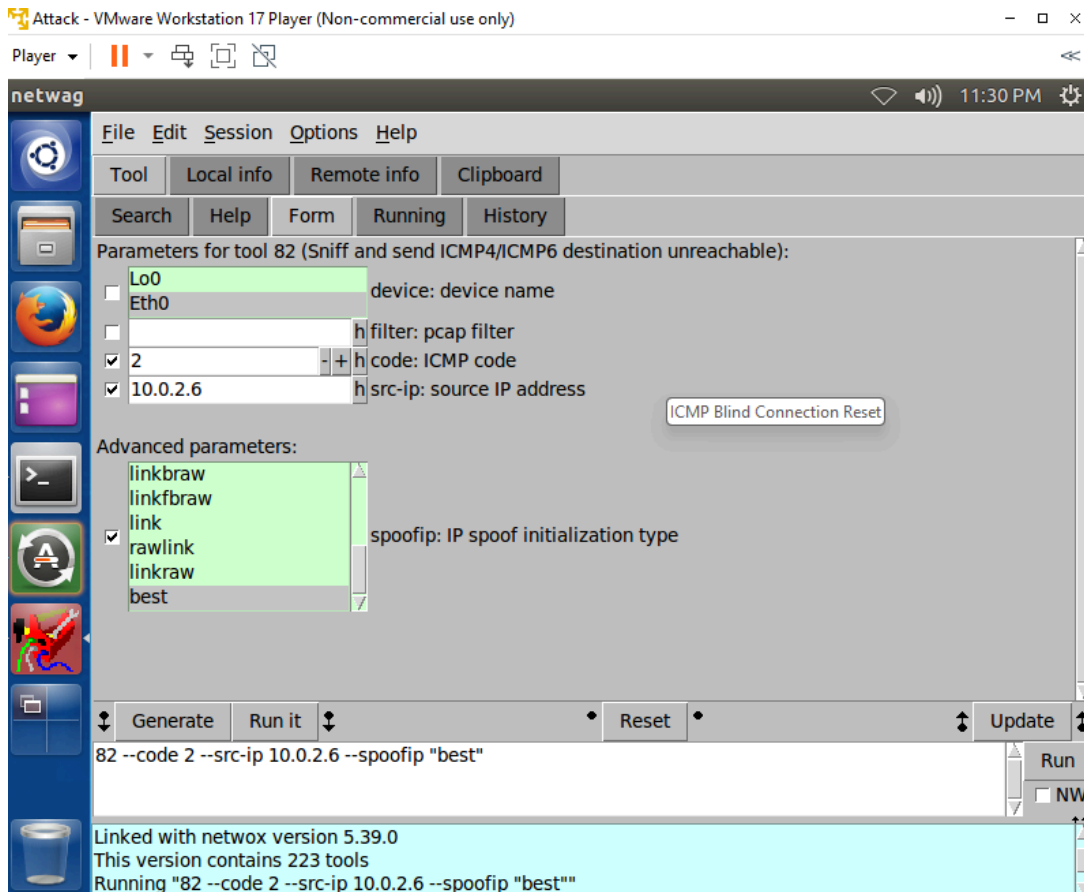
### Part 1 : Blind Connection-Reset

#### Screenshot 1 : Wireshark Capture (taken of the ping from client)



No.	Time	Source	Destination	Protocol	Length	Info
63	24.259215000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0xe53, seq=2/512, ttl=64 (request in 62)
66	25.258455000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0xe53, seq=3/768, ttl=64 (reply in 67)
67	25.258743000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0xe53, seq=3/768, ttl=64 (request in 66)
69	26.258860000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0xe53, seq=4/1024, ttl=64 (reply in 70)
70	26.259148000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0xe53, seq=4/1024, ttl=64 (request in 69)
71	27.258633000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0xe53, seq=5/1280, ttl=64 (reply in 72)
72	27.259016000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0xe53, seq=5/1280, ttl=64 (request in 71)
75	28.258633000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0xe53, seq=6/1536, ttl=64 (reply in 76)
76	28.258816000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0xe53, seq=6/1536, ttl=64 (request in 75)
80	33.305835000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0xdbb, seq=1/256, ttl=64 (reply in 81)
81	33.305862000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0xdbb, seq=1/256, ttl=64 (request in 80)
82	34.303897000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0xdbb, seq=2/512, ttl=64 (reply in 83)
83	34.303924000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0xdbb, seq=2/512, ttl=64 (request in 82)
84	35.302956000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0xdbb, seq=3/768, ttl=64 (reply in 85)
85	35.302985000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0xdbb, seq=3/768, ttl=64 (request in 84)
86	36.302874000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0xdbb, seq=4/1024, ttl=64 (reply in 87)
87	36.302901000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0xdbb, seq=4/1024, ttl=64 (request in 86)
104	58.163918000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0xe55, seq=1/256, ttl=64 (reply in 105)
105	58.164301000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0xe55, seq=1/256, ttl=64 (request in 104)
106	59.162908000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0xe55, seq=2/512, ttl=64 (reply in 107)
107	59.163503000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0xe55, seq=2/512, ttl=64 (request in 106)

#### Screenshot 2 : Netwag Interface (tool 82) with settings



### Screenshot 3 : Wireshark Capture after Netwag Tool Run.

Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e55, seq=108/27648, ttl=64 (reply in 2)
2	0.00035100	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e55, seq=108/27648, ttl=64 (request in 1)
3	0.01864300	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
4	0.01866700	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Host unreachable)
5	0.03854300	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
6	0.03856600	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Host unreachable)
7	1.00184000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e55, seq=109/27984, ttl=64 (reply in 8)
8	1.00221300	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e55, seq=109/27984, ttl=64 (request in 7)
9	1.00655100	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
10	1.00669000	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Host unreachable)
11	1.02622400	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
12	1.02625000	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Host unreachable)
13	2.00383400	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e55, seq=110/28160, ttl=64 (reply in 14)
14	2.00417700	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e55, seq=110/28160, ttl=64 (request in 13)
15	2.01449300	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
16	2.01451300	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Host unreachable)
17	2.04616900	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
18	2.04619500	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Host unreachable)
35	2.79427200	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
36	2.79428500	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Host unreachable)
37	2.79441200	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Host unreachable)

### Part 2 : Source-Quench Attacks

#### Screenshot 1 : Wireshak Capture (Ping server from client)

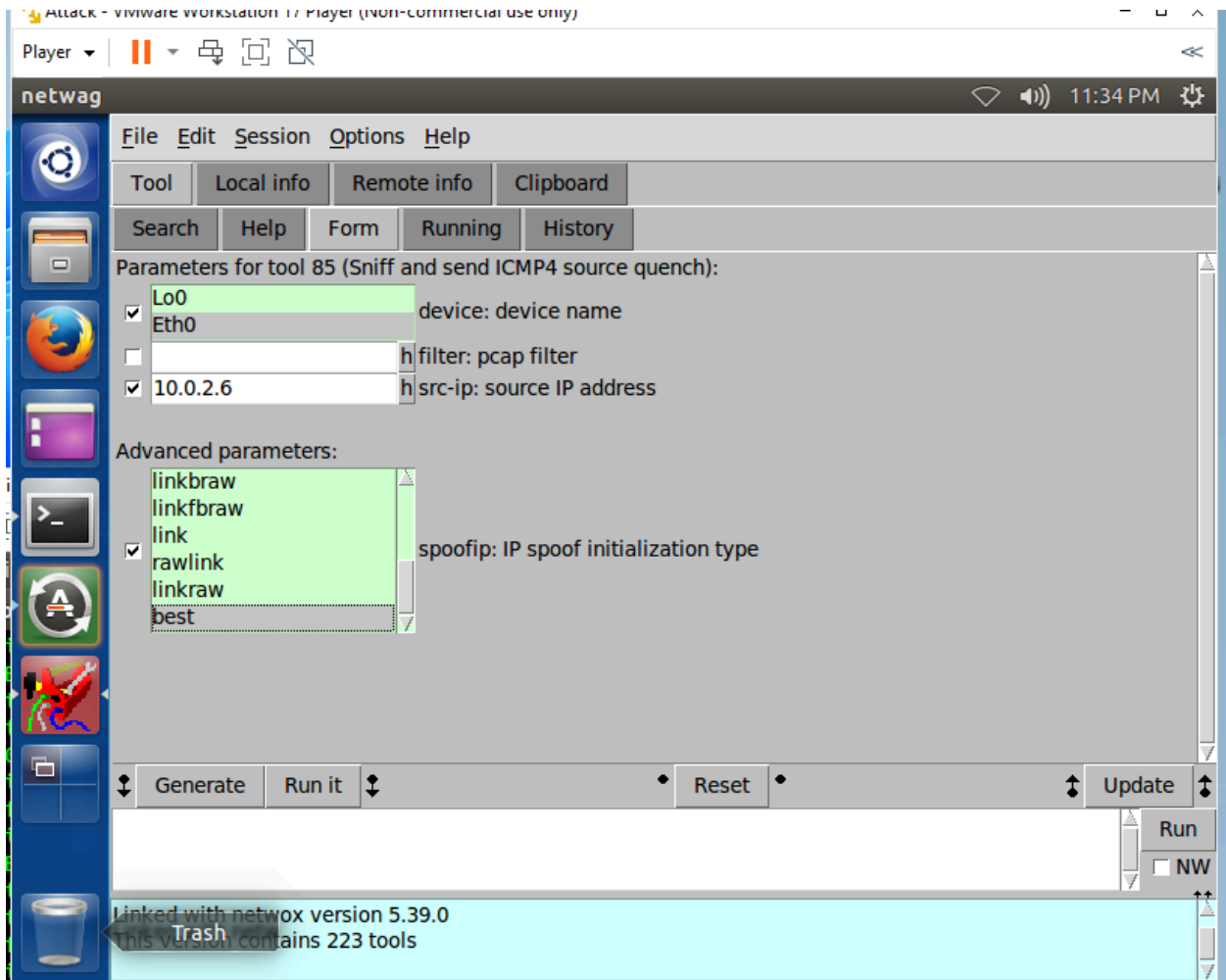
Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
99	24.20458200	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=108/27648, ttl=64 (reply in 2)
100	25.20399200	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=108/27648, ttl=64 (request in 99)
101	25.20466500	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=109/27984, ttl=64 (reply in 3)
102	26.20434400	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=109/27984, ttl=64 (request in 101)
103	26.20470100	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=110/28160, ttl=64 (reply in 4)
104	27.20411300	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=110/28160, ttl=64 (request in 103)
105	27.20448700	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=111/28480, ttl=64 (reply in 5)
106	28.20408700	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=111/28480, ttl=64 (request in 105)
107	28.20441200	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=112/28800, ttl=64 (reply in 6)
108	29.20415400	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=112/28800, ttl=64 (request in 107)
109	29.20454800	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=113/29120, ttl=64 (reply in 7)
110	33.47685800	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=113/29120, ttl=64 (request in 109)
111	33.47719500	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=114/29440, ttl=64 (reply in 8)
112	34.47598100	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=114/29440, ttl=64 (request in 111)
113	34.47632900	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=115/29760, ttl=64 (reply in 9)
114	35.47632900	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=115/29760, ttl=64 (request in 113)
115	35.47674300	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=116/30080, ttl=64 (reply in 10)
116	36.47606700	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=116/30080, ttl=64 (request in 115)
117	36.47641300	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=117/30400, ttl=64 (reply in 11)
118	37.47616400	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) reply id=0x0e55, seq=117/30400, ttl=64 (request in 117)
119	37.47649400	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) request id=0x0e55, seq=118/30720, ttl=64 (reply in 12)

Screenshot 2: Netwag (Took 85 with settings)



Screenshot 3 : Wireshark Capture After Tool

No.	Time	Source	Destination	Protocol	Length	Info
345	116.529437000	10.0.2.6	10.0.2.6	ICMP	70	Source quench (flow control
346	117.486264000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0
347	117.486650000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0
348	117.517058000	10.0.2.6	10.0.2.8	ICMP	70	Source quench (flow control
349	117.517077000	10.0.2.6	10.0.2.6	ICMP	70	Source quench (flow control
350	118.488356000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0
351	118.488733000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0
352	118.505360000	10.0.2.6	10.0.2.8	ICMP	70	Source quench (flow control
353	118.505384000	10.0.2.6	10.0.2.6	ICMP	70	Source quench (flow control
354	119.489747000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0
355	119.490130000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0
356	119.493026000	10.0.2.6	10.0.2.8	ICMP	70	Source quench (flow control
357	119.493157000	10.0.2.6	10.0.2.6	ICMP	70	Source quench (flow control
359	120.491417000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0
360	120.491792000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0
361	120.533162000	10.0.2.6	10.0.2.8	ICMP	70	Source quench (flow control
362	120.533183000	10.0.2.6	10.0.2.6	ICMP	70	Source quench (flow control
364	121.493030000	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0
365	121.493455000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0
366	121.525491000	10.0.2.6	10.0.2.8	ICMP	70	Source quench (flow control
367	121.525515000	10.0.2.6	10.0.2.6	ICMP	70	Source quench (flow control

### Task 3 :TCP Session Hijacking

Screenshot 1 : Telnet connection

server - VMware Workstation 17 Player (Non-commercial use only)

Player ▾ | [Pause] [Full Screen] [Copy] [Paste]

Terminal 11:37 PM

```
cybersec-client@ubuntu: ~  
64 bytes from 10.0.2.8: icmp_seq=2 ttl=64 time=0.334 ms  
64 bytes from 10.0.2.8: icmp_seq=3 ttl=64 time=0.419 ms  
64 bytes from 10.0.2.8: icmp_seq=4 ttl=64 time=0.395 ms  
^C  
--- 10.0.2.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.334/0.407/0.480/0.052 ms  
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: Sun Sep 15 23:36:05 PDT 2024 from 10.0.2.8 on pts/3  
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.  
  
cybersec-client@ubuntu:~$  
cybersec-client@ubuntu:~$
```

Trash



Screenshot 2 : Last Telnet packet sent from Server to Client

Client - VMware Workstation 17 Player (Non-commercial use only)

Wireshark

Filter: telnet

No.	Time	Source	Destination	Protocol	Length	Info
168	95.774220000	10.0.2.6	10.0.2.8	TELNET	67	Telnet Data ...
170	95.843955000	10.0.2.6	10.0.2.8	TELNET	67	Telnet Data ...
172	96.040177000	10.0.2.6	10.0.2.8	TELNET	67	Telnet Data ...
174	96.142314000	10.0.2.6	10.0.2.8	TELNET	68	Telnet Data ...
176	96.144982000	10.0.2.8	10.0.2.6	TELNET	68	Telnet Data ...

254 174.871620000 10.0.2.6 10.0.2.8 TELNET 67 Telnet Data ...

Frame 254: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0

Ethernet II, Src: Vmware\_b0:f3:b2 (00:0c:29:b0:f3:b2), Dst: Vmware\_83:72:41 (00:0c:29:83:72:41)

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: 60574 (60574), Dst Port: telnet (23), Seq: 140, Ack: 489, Len: 1

Source port: 60574 (60574)

Destination port: telnet (23)

[Stream index: 0]

Sequence number: 140 (relative sequence number)

[Next sequence number: 141 (relative sequence number)]

Acknowledgment number: 489 (relative ack number)

Header length: 32 bytes

Flags: 0x018 (PSH, ACK)

Window size value: 229

We need to have absolute sequ...

0010 00 35 27 c9 40 00 40 06 fa dc 0a 00 02 06 0a 00 .5'.@.@. ....

0020 02 08 ec 9e 00 17 1c bf d0 f9 f7 ff 22 59 80 18 ..... "Y..

0030 00 e5 48 38 00 00 01 01 08 0a 00 05 4d cd 00 05 ..H8.... .M...

0040 53 ea 7f S.

Client - VMware Workstation 17 Player (Non-commercial use only)

254 174.871620000 10.0.2.6 10.0.2.8 TELNET 67 Telnet Data ...

Frame 254: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0

Ethernet II, Src: Vmware\_b0:f3:b2 (00:0c:29:b0:f3:b2), Dst: Vmware\_83:72:41 (00:0c:29:83:72:41)

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: 60574 (60574), Dst Port: telnet (23), Seq: 482332921, Ack: 4160692825, Len:

Source port: 60574 (60574)

Destination port: telnet (23)

[Stream index: 0]

Sequence number: 482332921

[Next sequence number: 482332922]

Acknowledgment number: 4160692825

Header length: 32 bytes

Flags: 0x018 (PSH, ACK)

Window size value: 229

[Calculated window size: 29312]

[Window size scaling factor: 128]

Checksum: 0x4838 [validation disabled]

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

Telnet

Data: \177

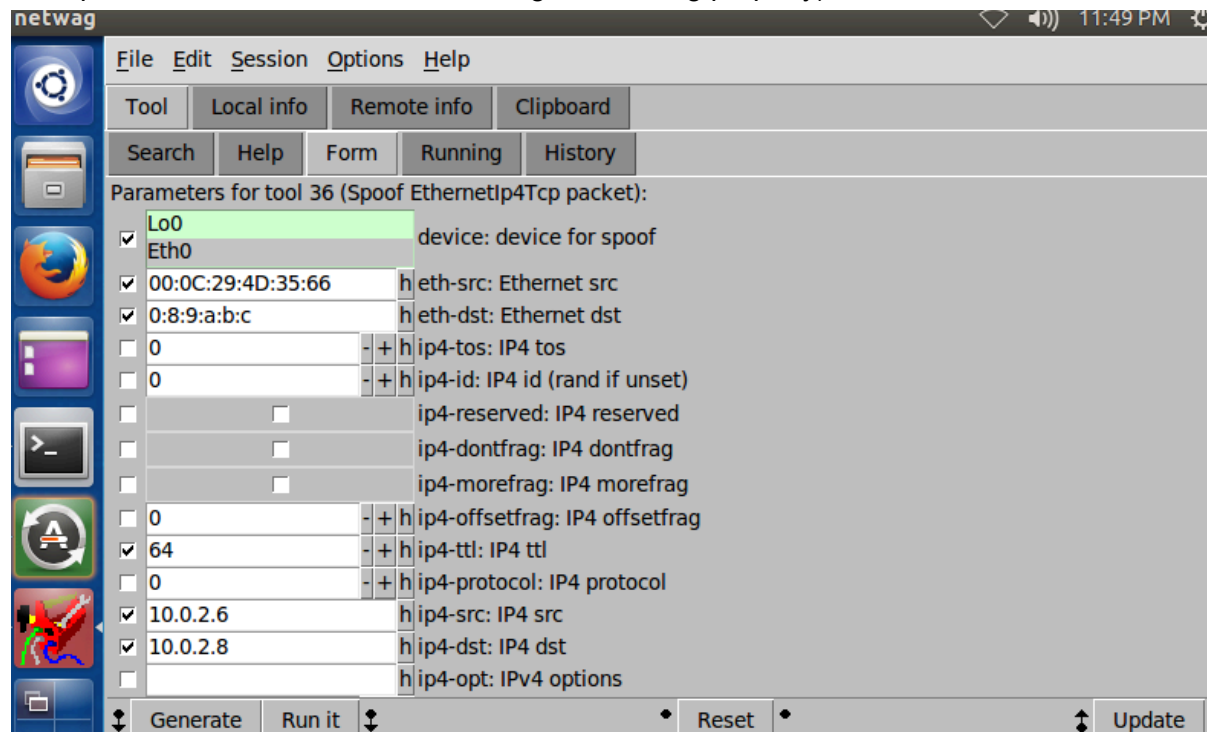
0000 00 0c 29 83 72 41 00 0c 29 b0 f3 b2 08 00 45 10 ..).rA.. )....E.

0010 00 35 27 c9 40 00 40 06 fa dc 0a 00 02 06 0a 00 .5'.@.@. ....

0020 02 08 ec 9e 00 17 1c bf d0 f9 f7 ff 22 59 80 18 ..... "Y..

0030 00 e5 48 38 00 00 01 01 08 0a 00 05 4d cd 00 05 ..H8.... .M...

Screenshot 3 : Netwag Tool (36) With information (Note: Some fields were changed as multiple attempts were taken after screenshot to get it working properly)





netwag 11:49 PM

File Edit Session Options Help

Tool Local info Remote info Clipboard

Search Help Form Running History

<input checked="" type="checkbox"/>	45828	- + h	tcp-src: TCP src
<input checked="" type="checkbox"/>	23	- + h	tcp-dst: TCP dst
<input checked="" type="checkbox"/>	3780513243	- + h	tcp-seqnum: TCP seqnum (rand if unset)
<input checked="" type="checkbox"/>	1111218671	- + h	tcp-acknum: TCP acknum
<input type="checkbox"/>			tcp-reserved1: TCP reserved1
<input type="checkbox"/>			tcp-reserved2: TCP reserved2
<input type="checkbox"/>			tcp-reserved3: TCP reserved3
<input type="checkbox"/>			tcp-reserved4: TCP reserved4
<input type="checkbox"/>			tcp-cwr: TCP cwr
<input type="checkbox"/>			tcp-ece: TCP ece
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	tcp-urg: TCP urg
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	tcp-ack: TCP ack
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	tcp-psh: TCP psh
<input type="checkbox"/>			tcp-rst: TCP rst
<input type="checkbox"/>			tcp-syn: TCP syn

Generate Run it Reset Update

netwag 11:49 PM

File Edit Session Options Help

Tool Local info Remote info Clipboard

Search Help Form Running History

<input type="checkbox"/>			tcp-rst: TCP rst
<input type="checkbox"/>			tcp-syn: TCP syn
<input type="checkbox"/>			tcp-fin: TCP fin
<input checked="" type="checkbox"/>	229	- + h	tcp-window: TCP window
<input type="checkbox"/>	0	- + h	tcp-urgptr: TCP urgptr
<input type="checkbox"/>			tcp-opt: TCP options
<input checked="" type="checkbox"/>	72 20 68 65 6c 6c 6f 0a	- + h	tcp-data: mixed data

Terminal

Advanced parameters:

<input type="checkbox"/>	2048	- + h	eth-type: Ethernet type
<input type="checkbox"/>	5	- + h	ip4-ihl: IP4 ihl
<input type="checkbox"/>	0	- + h	ip4-totlen: IP4 totlen
<input type="checkbox"/>	0	- + h	ip4-checksum: IP4 checksum
<input type="checkbox"/>	0	- + h	tcp-doff: TCP data offset
<input type="checkbox"/>	0	- + h	tcp-checksum: TCP checksum

Generate Run it Reset Update

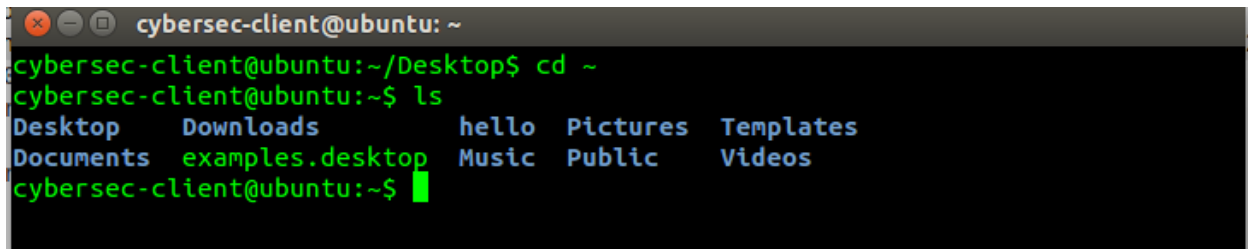
Run NW

Screenshot 4: Wireshark capture of telnet

255 174.871766000	10.0.2.8	10.0.2.6	TELNET	70 Telnet Data ...
721 887.472277000	10.0.2.6	10.0.2.8	TELNET	66 Telnet Data ...



Bonus Screenshot. Home Directory Created due to Injection of code / Hijack

A terminal window titled 'cybersec-client@ubuntu: ~' with standard window controls. The terminal shows a sequence of commands and their output. The user starts in the Desktop directory, navigates to the home directory with 'cd ~', and then runs 'ls'. The output of 'ls' lists the contents of the home directory, including standard Ubuntu directories and a file named 'hello'.

```
cybersec-client@ubuntu:~/Desktop$ cd ~
cybersec-client@ubuntu:~$ ls
Desktop    Downloads      hello  Pictures  Templates
Documents  examples.desktop Music   Public    Videos
cybersec-client@ubuntu:~$
```