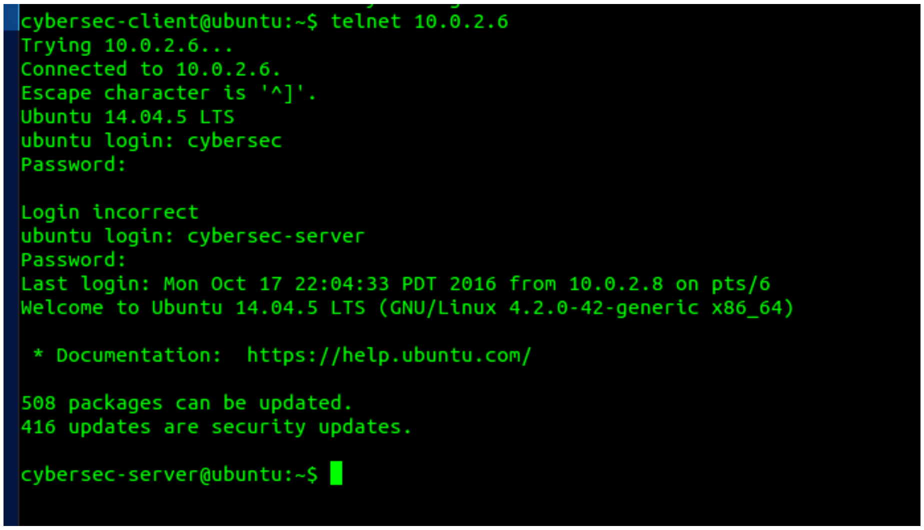
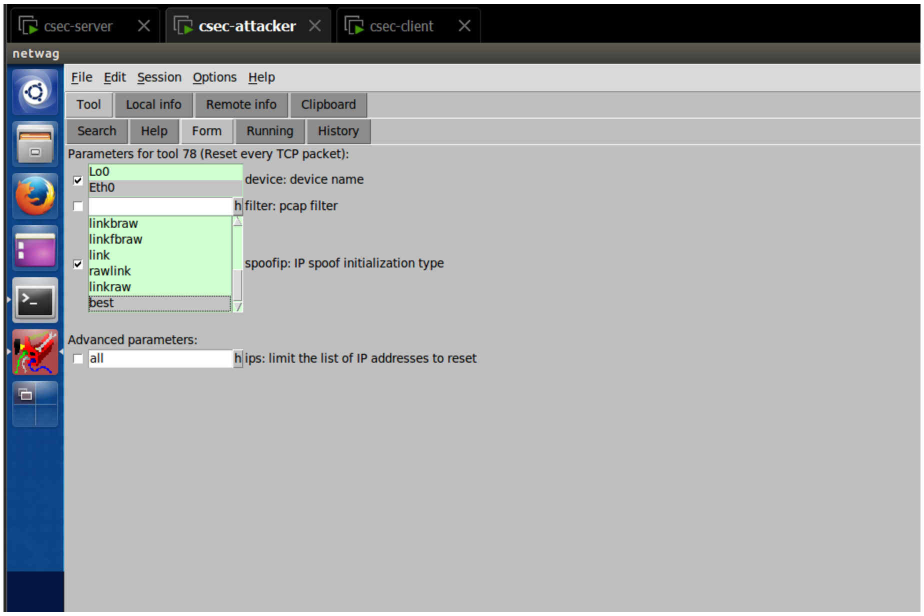
CSEC Week 06 Lab

Task 4 - TCP RST Attacks on Telnet and SSH Connections



```
cybersec-client@ubuntu:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 14.04.5 LTS
ubuntu login: cybersec
Password:

Login incorrect
ubuntu login: cybersec-server
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/

508 packages can be updated.
416 updates are security updates.

cybersec-server@ubuntu:~$ 
```


csec-server
csec-attacker
csec-client
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History

Parameters for tool 78 (Reset every TCP packet):

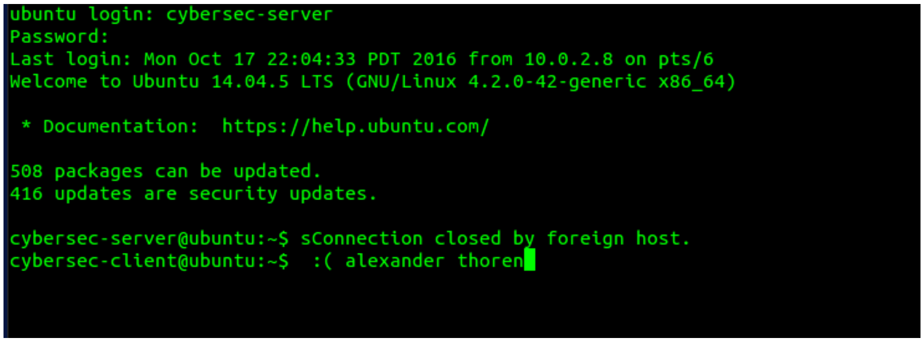
☑ Lo0 / Eth0 — device: device name

☐ h filter: pcap filter

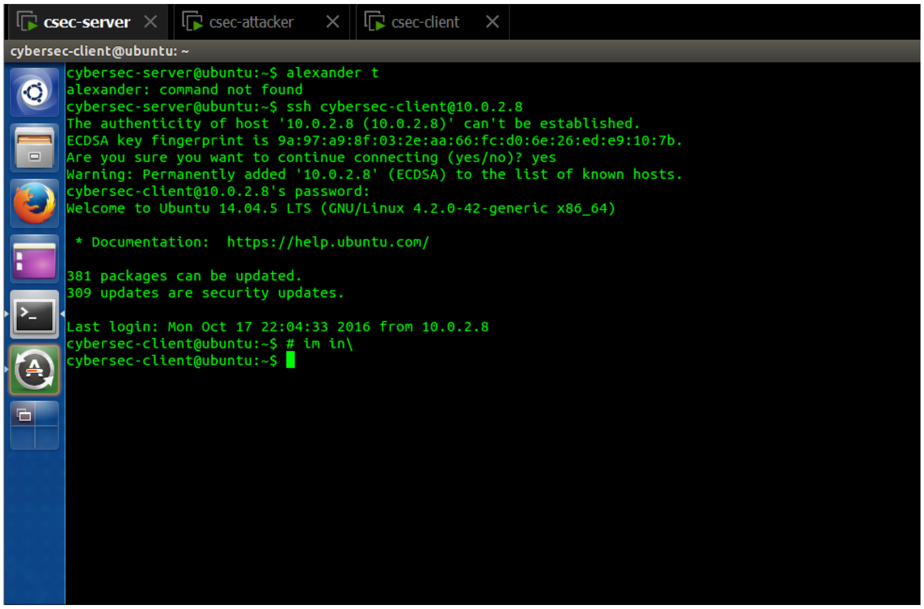
☑ linkbraw / linkfbraw / link / rawlink / linkraw / best — spoofip: IP spoof initialization type

Advanced parameters:

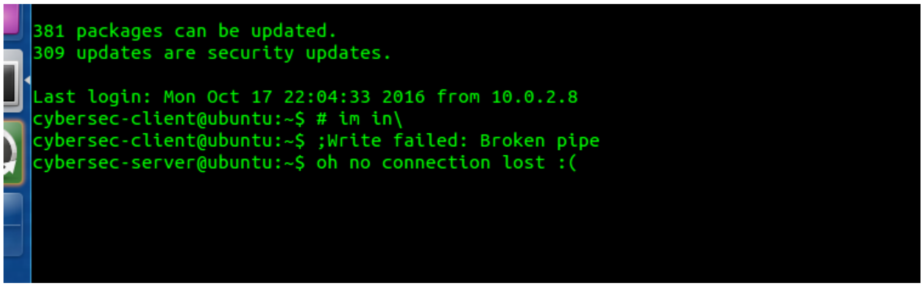
☐ all h ips: limit the list of IP addresses to reset



```
ubuntu login: cybersec-server
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/

508 packages can be updated.
416 updates are security updates.

cybersec-server@ubuntu:~$ sConnection closed by foreign host.
cybersec-client@ubuntu:~$  :( alexander thoren
```



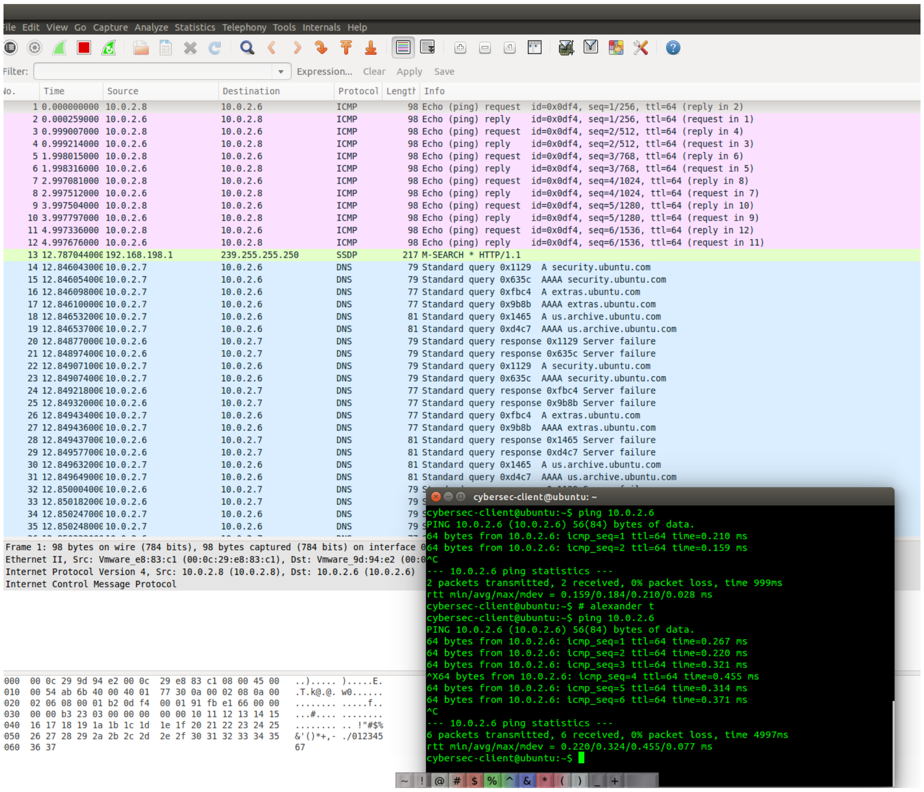
```
cybersec-server@ubuntu:~$ alexander t
alexander: command not found
cybersec-server@ubuntu:~$ ssh cybersec-client@10.0.2.8
The authenticity of host '10.0.2.8 (10.0.2.8)' can't be established.
ECDSA key fingerprint is 9a:97:a9:8f:03:2e:aa:66:fc:d0:6e:26:ed:e9:10:7b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.8' (ECDSA) to the list of known hosts.
cybersec-client@10.0.2.8's password:
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.

Last login: Mon Oct 17 22:04:33 2016 from 10.0.2.8
cybersec-client@ubuntu:~$ # im in\
cybersec-client@ubuntu:~$ 
```



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

Last login: Mon Oct 17 22:04:33 2016 from 10.0.2.8
cybersec-client@ubuntu:~$ # im in\
cybersec-client@ubuntu:~$ ;Write failed: Broken pipe
cybersec-server@ubuntu:~$ oh no connection lost :(
```

Task 5 - ICMP Blind Connection-Reset and Source-Quench Attacks

(i) ICMP Blind Connection-Reset


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

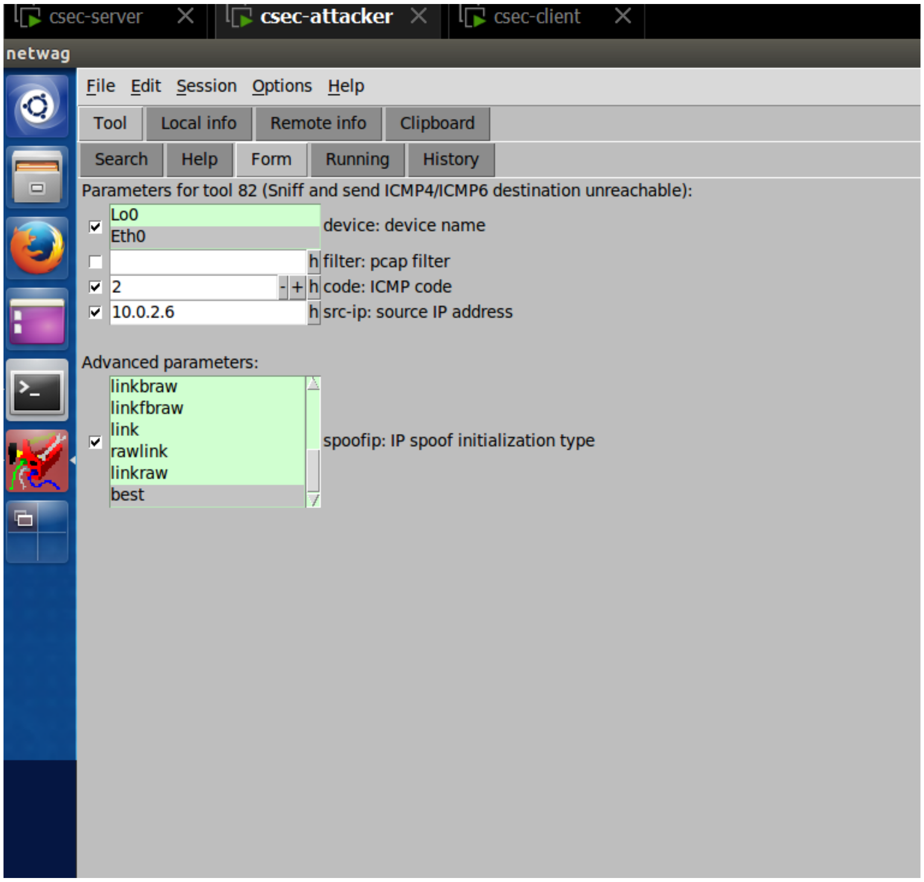
```
No.  Time         Source         Destination      Protocol Length Info
   1 0.000000000  10.0.2.8       10.0.2.6         ICMP       98 Echo (ping) request  id=0x0df4, seq=1/256, ttl=64 (reply in 2)
   2 0.000259000  10.0.2.6       10.0.2.8         ICMP       98 Echo (ping) reply    id=0x0df4, seq=1/256, ttl=64 (request in 1)
   3 0.999007000  10.0.2.8       10.0.2.6         ICMP       98 Echo (ping) request  id=0x0df4, seq=2/512, ttl=64 (reply in 4)
   4 0.999214000  10.0.2.6       10.0.2.8         ICMP       98 Echo (ping) reply    id=0x0df4, seq=2/512, ttl=64 (request in 3)
   5 1.998015000  10.0.2.8       10.0.2.6         ICMP       98 Echo (ping) request  id=0x0df4, seq=3/768, ttl=64 (reply in 6)
   6 1.998316000  10.0.2.6       10.0.2.8         ICMP       98 Echo (ping) reply    id=0x0df4, seq=3/768, ttl=64 (request in 5)
   7 2.997081000  10.0.2.8       10.0.2.6         ICMP       98 Echo (ping) request  id=0x0df4, seq=4/1024, ttl=64 (reply in 8)
   8 2.997512000  10.0.2.6       10.0.2.8         ICMP       98 Echo (ping) reply    id=0x0df4, seq=4/1024, ttl=64 (request in 7)
   9 3.997504000  10.0.2.8       10.0.2.6         ICMP       98 Echo (ping) request  id=0x0df4, seq=5/1280, ttl=64 (reply in 10)
  10 3.997797000  10.0.2.6       10.0.2.8         ICMP       98 Echo (ping) reply    id=0x0df4, seq=5/1280, ttl=64 (request in 9)
  11 4.997336000  10.0.2.8       10.0.2.6         ICMP       98 Echo (ping) request  id=0x0df4, seq=6/1536, ttl=64 (reply in 12)
  12 4.997676000  10.0.2.6       10.0.2.8         ICMP       98 Echo (ping) reply    id=0x0df4, seq=6/1536, ttl=64 (request in 11)
  13 12.78704400( 192.168.198.1  239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
  14 12.84604300( 10.0.2.7       10.0.2.6         DNS        79 Standard query 0x1129  A security.ubuntu.com
  15 12.84605400( 10.0.2.7       10.0.2.6         DNS        79 Standard query 0x635c  AAAA security.ubuntu.com
  16 12.84609800( 10.0.2.7       10.0.2.6         DNS        77 Standard query 0xfbc4  A extras.ubuntu.com
  17 12.84610000( 10.0.2.7       10.0.2.6         DNS        77 Standard query 0x9b8b  AAAA extras.ubuntu.com
  18 12.84653200( 10.0.2.7       10.0.2.6         DNS        81 Standard query 0x1465  A us.archive.ubuntu.com
  19 12.84653700( 10.0.2.7       10.0.2.6         DNS        81 Standard query 0xd4c7  AAAA us.archive.ubuntu.com
  20 12.84877000( 10.0.2.6       10.0.2.7         DNS        79 Standard query response 0x1129 Server failure
  21 12.84897400( 10.0.2.6       10.0.2.7         DNS        79 Standard query response 0x635c Server failure
  22 12.84907100( 10.0.2.7       10.0.2.6         DNS        79 Standard query 0x1129  A security.ubuntu.com
  23 12.84907400( 10.0.2.7       10.0.2.6         DNS        79 Standard query 0x635c  AAAA security.ubuntu.com
  24 12.84921800( 10.0.2.6       10.0.2.7         DNS        77 Standard query response 0xfbc4 Server failure
  25 12.84932000( 10.0.2.6       10.0.2.7         DNS        77 Standard query response 0x9b8b Server failure
  26 12.84943400( 10.0.2.7       10.0.2.6         DNS        77 Standard query 0xfbc4  A extras.ubuntu.com
  27 12.84943600( 10.0.2.7       10.0.2.6         DNS        77 Standard query 0x9b8b  AAAA extras.ubuntu.com
  28 12.84943700( 10.0.2.6       10.0.2.7         DNS        81 Standard query response 0x1465 Server failure
  29 12.84957700( 10.0.2.6       10.0.2.7         DNS        81 Standard query response 0xd4c7 Server failure
  30 12.84963200( 10.0.2.7       10.0.2.6         DNS        81 Standard query 0x1465  A us.archive.ubuntu.com
  31 12.84964900( 10.0.2.7       10.0.2.6         DNS        81 Standard query 0xd4c7  AAAA us.archive.ubuntu.com
  32 12.85000400( 10.0.2.6       10.0.2.7         DNS        79 S
  33 12.85018200( 10.0.2.6       10.0.2.7         DNS        79 S
  34 12.85024700( 10.0.2.7       10.0.2.6         DNS        79 S
  35 12.85024800( 10.0.2.7       10.0.2.6         DNS        79 S
```

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_e8:83:c1 (00:0c:29:e8:83:c1), Dst: Vmware_9d:94:e2 (00:0
Internet Protocol Version 4, Src: 10.0.2.8 (10.0.2.8), Dst: 10.0.2.6 (10.0.2.6)
Internet Control Message Protocol
```

```
000  00 0c 29 9d 94 e2 00 0c  29 e8 83 c1 08 00 45 00   ..)..... ).....E.
010  00 54 ab 6b 40 00 40 01  77 30 0a 00 02 08 0a 00   .T.k@.@. w0......
020  02 06 08 00 01 b2 0d f4  00 01 91 fb e1 66 00 00   ........ .....f..
030  00 00 b3 23 03 00 00 00  00 00 10 11 12 13 14 15   ...#.... ........
040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
060  36 37                                              67
```

cybersec-client@ubuntu: ~

```
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=0.210 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.159 ms
^C
--- 10.0.2.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.159/0.184/0.210/0.028 ms
cybersec-client@ubuntu:~$ # alexander t
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=0.267 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.220 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.321 ms
^X64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.455 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.314 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.371 ms
^C
--- 10.0.2.6 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4997ms
rtt min/avg/max/mdev = 0.220/0.324/0.455/0.077 ms
cybersec-client@ubuntu:~$ 
```



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

☑ Lo0 / Eth0 — device: device name

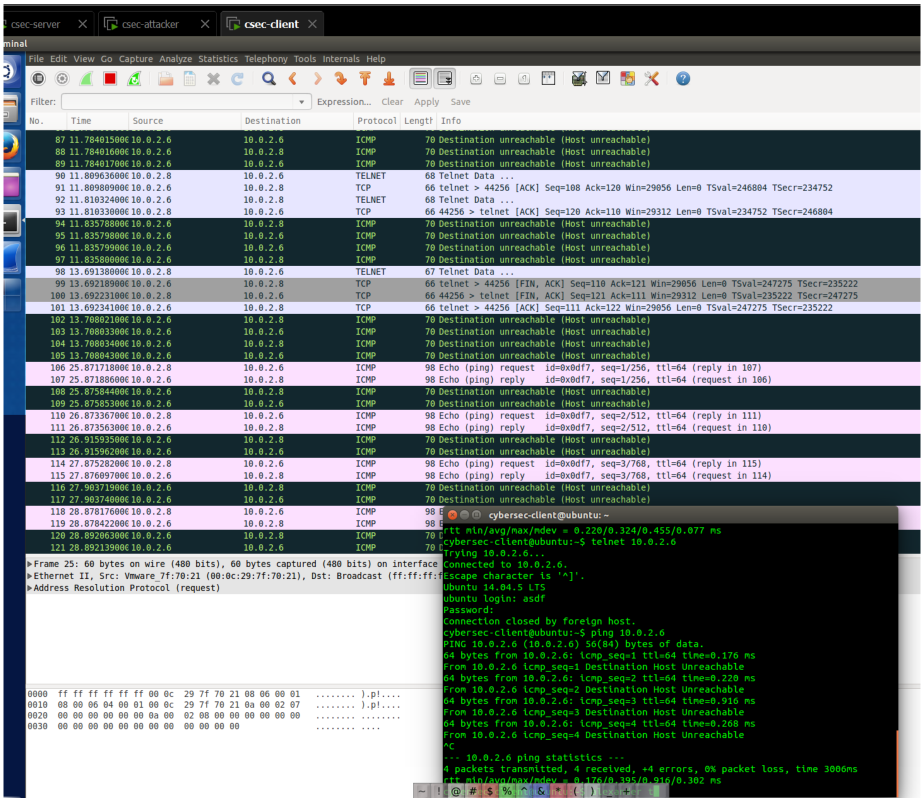
□ h filter: pcap filter

☑ 2 - + h code: ICMP code

☑ 10.0.2.6 h src-ip: source IP address

Advanced parameters:

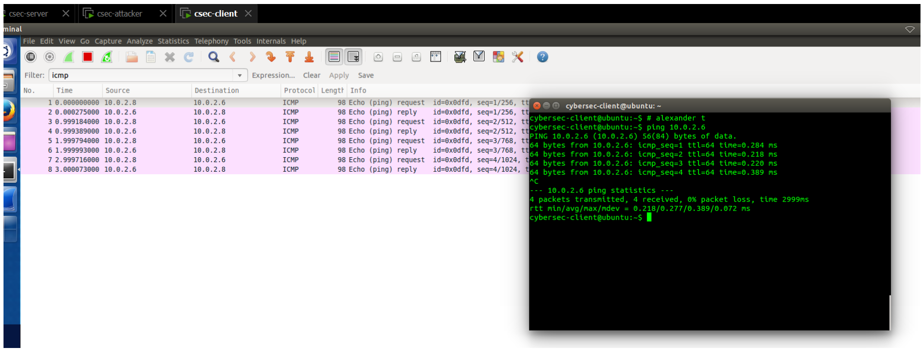
☑ linkbraw / linkfbraw / link / rawlink / linkraw / best — spoofip: IP spoof initialization type


csec-server
csec-attacker
csec-client
minal
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
cybersec-client@ubuntu: ~

```
No.  Time         Source    Destination Protocol Length Info
 87 11.784015000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
 88 11.784016000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
 89 11.784017000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
 90 11.809636000 10.0.2.8  10.0.2.6    TELNET   68 Telnet Data ...
 91 11.809809000 10.0.2.6  10.0.2.8    TCP      66 telnet > 44256 [ACK] Seq=108 Ack=120 Win=29056 Len=0 TSval=246804 TSecr=234752
 92 11.810324000 10.0.2.6  10.0.2.8    TELNET   68 Telnet Data ...
 93 11.810330000 10.0.2.8  10.0.2.6    TCP      66 44256 > telnet [ACK] Seq=120 Ack=110 Win=29312 Len=0 TSval=234752 TSecr=246804
 94 11.835788000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
 95 11.835798000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
 96 11.835799000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
 97 11.835800000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
 98 13.691380000 10.0.2.8  10.0.2.6    TELNET   67 Telnet Data ...
 99 13.692189000 10.0.2.6  10.0.2.8    TCP      66 telnet > 44256 [FIN, ACK] Seq=110 Ack=121 Win=29056 Len=0 TSval=247275 TSecr=235222
100 13.692231000 10.0.2.8  10.0.2.6    TCP      66 44256 > telnet [FIN, ACK] Seq=121 Ack=111 Win=29312 Len=0 TSval=235222 TSecr=247275
101 13.692341000 10.0.2.6  10.0.2.8    TCP      66 telnet > 44256 [ACK] Seq=111 Ack=122 Win=29056 Len=0 TSval=247275 TSecr=235222
102 13.708021000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
103 13.708033000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
104 13.708034000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
105 13.708043000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
106 25.871718000 10.0.2.8  10.0.2.6    ICMP     98 Echo (ping) request  id=0x0df7, seq=1/256, ttl=64 (reply in 107)
107 25.871886000 10.0.2.6  10.0.2.8    ICMP     98 Echo (ping) reply    id=0x0df7, seq=1/256, ttl=64 (request in 106)
108 25.875844000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
109 25.875853000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
110 26.873367000 10.0.2.8  10.0.2.6    ICMP     98 Echo (ping) request  id=0x0df7, seq=2/512, ttl=64 (reply in 111)
111 26.873563000 10.0.2.6  10.0.2.8    ICMP     98 Echo (ping) reply    id=0x0df7, seq=2/512, ttl=64 (request in 110)
112 26.915935000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
113 26.915962000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
114 27.875282000 10.0.2.8  10.0.2.6    ICMP     98 Echo (ping) request  id=0x0df7, seq=3/768, ttl=64 (reply in 115)
115 27.876097000 10.0.2.6  10.0.2.8    ICMP     98 Echo (ping) reply    id=0x0df7, seq=3/768, ttl=64 (request in 114)
116 27.903719000 10.0.2.6  10.0.2.8    ICMP     70 Destination unreachable (Host unreachable)
117 27.903740000 10.0.2.6  10.0.2.6    ICMP     70 Destination unreachable (Host unreachable)
118 28.878176000 10.0.2.8  10.0.2.6    ICMP     98 E
119 28.878422000 10.0.2.6  10.0.2.8    ICMP     98 E
120 28.892063000 10.0.2.6  10.0.2.8    ICMP     70 D
121 28.892139000 10.0.2.6  10.0.2.6    ICMP     70 D

▶Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
▶Ethernet II, Src: Vmware_7f:70:21 (00:0c:29:7f:70:21), Dst: Broadcast (ff:ff:ff:f
▶Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 7f 70 21 08 06 00 01   ........ ).p!....
0010  08 00 06 04 00 01 00 0c  29 7f 70 21 0a 00 02 07   ........ ).p!....
0020  00 00 00 00 00 00 0a 00  02 08 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

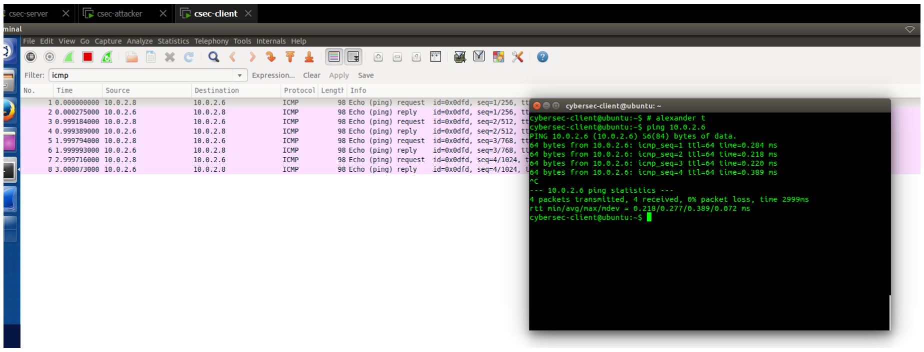
```
rtt min/avg/max/mdev = 0.220/0.324/0.455/0.077 ms
cybersec-client@ubuntu:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 14.04.5 LTS
ubuntu login: asdf
Password:
Connection closed by foreign host.
cybersec-client@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.176 ms
From 10.0.2.6 icmp_seq=1 Destination Host Unreachable
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.220 ms
From 10.0.2.6 icmp_seq=2 Destination Host Unreachable
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.916 ms
From 10.0.2.6 icmp_seq=3 Destination Host Unreachable
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.268 ms
From 10.0.2.6 icmp_seq=4 Destination Host Unreachable
^C
--- 10.0.2.6 ping statistics ---
4 packets transmitted, 4 received, +4 errors, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.176/0.395/0.916/0.302 ms
```

(ii) Source-Quench Attacks


csec-server
csec-attacker
csec-client
minal
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
Expression... Clear Apply Save
cybersec-client@ubuntu: ~

```
No. Time        Source    Destination Protocol Length Info
  1 0.000000000 10.0.2.8  10.0.2.6    ICMP     98 Echo (ping) request  id=0x0dfd, seq=1/256, tt
  2 0.000275000 10.0.2.6  10.0.2.8    ICMP     98 Echo (ping) reply    id=0x0dfd, seq=1/256, tt
  3 0.999184000 10.0.2.8  10.0.2.6    ICMP     98 Echo (ping) request  id=0x0dfd, seq=2/512, tt
  4 0.999389000 10.0.2.6  10.0.2.8    ICMP     98 Echo (ping) reply    id=0x0dfd, seq=2/512, tt
  5 1.999794000 10.0.2.8  10.0.2.6    ICMP     98 Echo (ping) request  id=0x0dfd, seq=3/768, tt
  6 1.999993000 10.0.2.6  10.0.2.8    ICMP     98 Echo (ping) reply    id=0x0dfd, seq=3/768, tt
  7 2.999716000 10.0.2.8  10.0.2.6    ICMP     98 Echo (ping) request  id=0x0dfd, seq=4/1024, t
  8 3.000073000 10.0.2.6  10.0.2.8    ICMP     98 Echo (ping) reply    id=0x0dfd, seq=4/1024, t
```

```
cybersec-client@ubuntu:~$ # alexander t
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=0.284 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.389 ms
^C
--- 10.0.2.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.218/0.277/0.389/0.072 ms
cybersec-client@ubuntu:~$
```

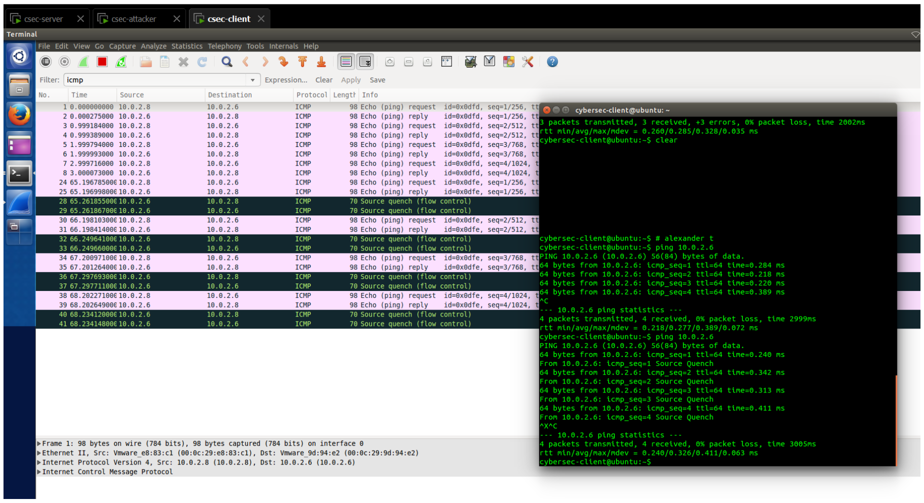


csec-server
csec-attacker
csec-client
minal
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
cybersec-client@ubuntu: ~

Filter: icmp

```
No.     Time        Source      Destination  Protocol Length Info
      1 0.000000000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=1/256, tt
      2 0.000275000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=1/256, tt
      3 0.999184000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=2/512, tt
      4 0.999389000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=2/512, tt
      5 1.999794000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=3/768, tt
      6 1.999993000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=3/768, tt
      7 2.999716000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=4/1024, t
      8 3.000073000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=4/1024, t
```

```
cybersec-client@ubuntu:~$ # alexander t
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=0.284 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.389 ms
^C
--- 10.0.2.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.218/0.277/0.389/0.072 ms
cybersec-client@ubuntu:~$
```



csec-server
csec-attacker
csec-client
Terminal
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
cybersec-client@ubuntu: ~

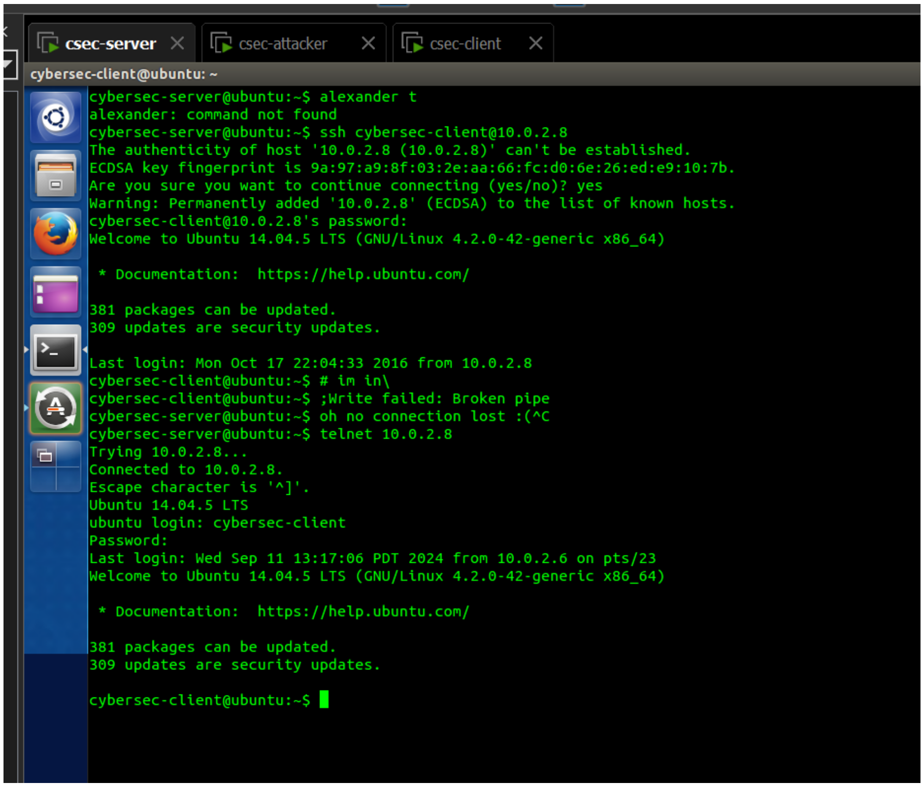
Filter: icmp

```
No.     Time        Source      Destination  Protocol Length Info
      1 0.000000000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=1/256, tt
      2 0.000275000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=1/256, tt
      3 0.999184000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=2/512, tt
      4 0.999389000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=2/512, tt
      5 1.999794000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=3/768, tt
      6 1.999993000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=3/768, tt
      7 2.999716000 10.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfd, seq=4/1024, t
      8 3.000073000 10.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfd, seq=4/1024, t
     24 65.19678500010.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfe, seq=1/256, tt
     25 65.19699800010.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfe, seq=1/256, tt
     28 65.26185500010.0.2.6    10.0.2.8     ICMP       70 Source quench (flow control)
     29 65.26186700010.0.2.6    10.0.2.6     ICMP       70 Source quench (flow control)
     30 66.19810300010.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfe, seq=2/512, tt
     31 66.19841400010.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfe, seq=2/512, tt
     32 66.24964100010.0.2.6    10.0.2.8     ICMP       70 Source quench (flow control)
     33 66.24966000010.0.2.6    10.0.2.6     ICMP       70 Source quench (flow control)
     34 67.20097100010.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfe, seq=3/768, tt
     35 67.20126400010.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfe, seq=3/768, tt
     36 67.29769300010.0.2.6    10.0.2.8     ICMP       70 Source quench (flow control)
     37 67.29771100010.0.2.6    10.0.2.6     ICMP       70 Source quench (flow control)
     38 68.20227100010.0.2.8    10.0.2.6     ICMP       98 Echo (ping) request  id=0x0dfe, seq=4/1024, t
     39 68.20264900010.0.2.6    10.0.2.8     ICMP       98 Echo (ping) reply    id=0x0dfe, seq=4/1024, t
     40 68.23412000010.0.2.6    10.0.2.8     ICMP       70 Source quench (flow control)
     41 68.23414800010.0.2.6    10.0.2.6     ICMP       70 Source quench (flow control)
```

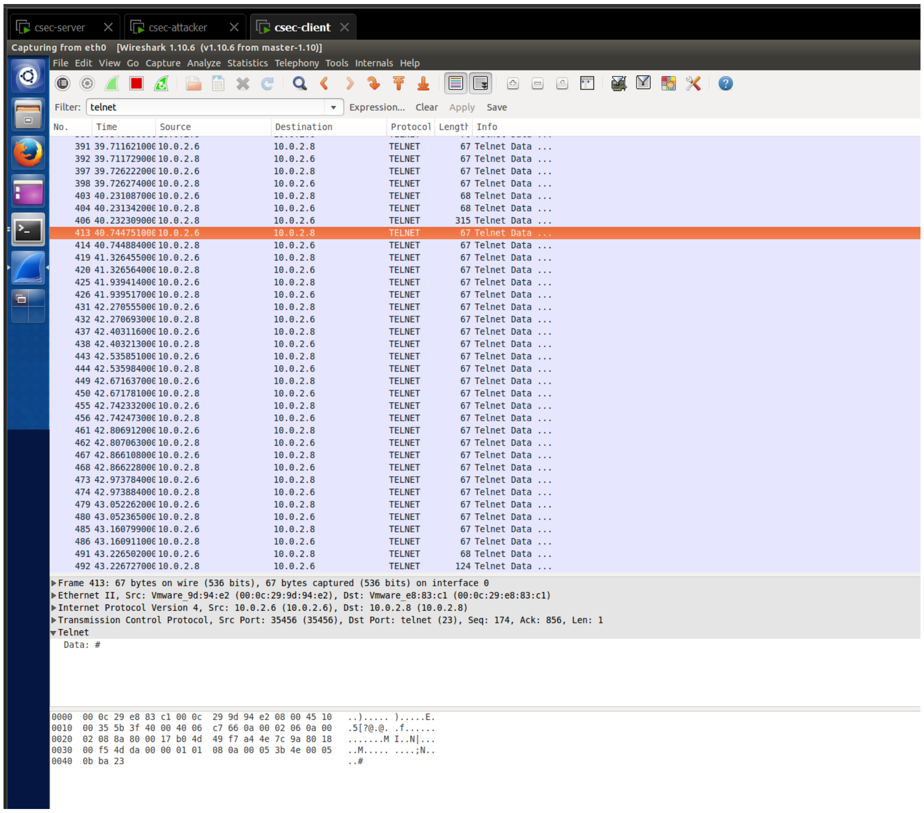
```
▶Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶Ethernet II, Src: Vmware_e8:83:c1 (00:0c:29:e8:83:c1), Dst: Vmware_9d:94:e2 (00:0c:29:9d:94:e2)
▶Internet Protocol Version 4, Src: 10.0.2.8 (10.0.2.8), Dst: 10.0.2.6 (10.0.2.6)
▶Internet Control Message Protocol
```

```
3 packets transmitted, 3 received, +3 errors, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.260/0.285/0.328/0.035 ms
cybersec-client@ubuntu:~$ clear









cybersec-client@ubuntu:~$ # alexander t
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=0.284 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.389 ms
^C
--- 10.0.2.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.218/0.277/0.389/0.072 ms
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=0.240 ms
From 10.0.2.6: icmp_seq=1 Source Quench
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.342 ms
From 10.0.2.6: icmp_seq=2 Source Quench
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.313 ms
From 10.0.2.6: icmp_seq=3 Source Quench
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.411 ms
From 10.0.2.6: icmp_seq=4 Source Quench
^X^C
--- 10.0.2.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.240/0.326/0.411/0.063 ms
cybersec-client@ubuntu:~$
```

Task 6 - TCP Session Hijacking



```
cybersec-server@ubuntu:~$ alexander t
alexander: command not found
cybersec-server@ubuntu:~$ ssh cybersec-client@10.0.2.8
The authenticity of host '10.0.2.8 (10.0.2.8)' can't be established.
ECDSA key fingerprint is 9a:97:a9:8f:03:2e:aa:66:fc:d0:6e:26:ed:e9:10:7b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.8' (ECDSA) to the list of known hosts.
cybersec-client@10.0.2.8's password:
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.

Last login: Mon Oct 17 22:04:33 2016 from 10.0.2.8
cybersec-client@ubuntu:~$ # im in\
cybersec-client@ubuntu:~$ ;Write failed: Broken pipe
cybersec-server@ubuntu:~$ oh no connection lost :(^C
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: Wed Sep 11 13:17:06 PDT 2024 from 10.0.2.6 on pts/23
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:~$ 
```


csec-server
csec-attacker
csec-client
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

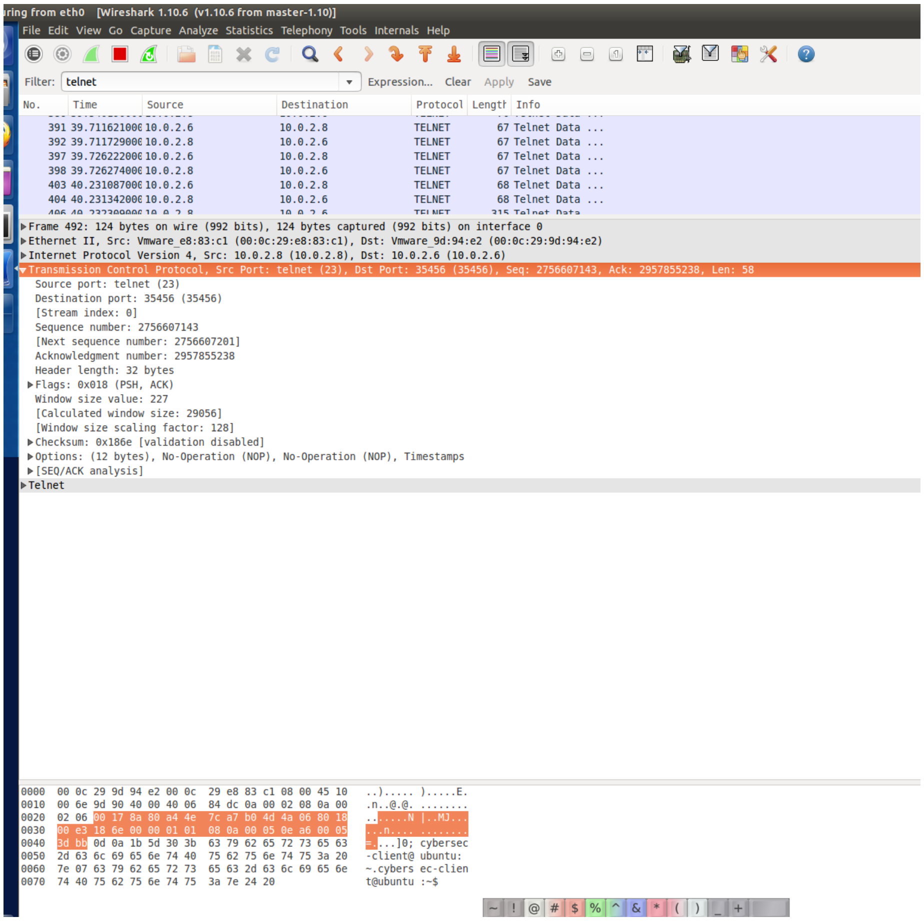
Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: telnet

```
No.   Time         Source          Destination     Protocol  Length Info
  391 39.71162100 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  392 39.71172900 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  397 39.72622200 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  398 39.72627400 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  403 40.23108700 10.0.2.6        10.0.2.8        TELNET      68 Telnet Data ...
  404 40.23134200 10.0.2.8        10.0.2.6        TELNET      68 Telnet Data ...
  406 40.23230900 10.0.2.8        10.0.2.6        TELNET     315 Telnet Data ...
  413 40.74475100 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  414 40.74488400 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  419 41.32645500 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  420 41.32656400 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  425 41.93941400 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  426 41.93951700 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  431 42.27055500 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  432 42.27069300 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  437 42.40311600 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  438 42.40321300 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  443 42.53585100 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  444 42.53598400 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  449 42.67163700 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  450 42.67178100 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  455 42.74233200 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  456 42.74247300 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  461 42.80691200 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  462 42.80706300 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  467 42.86610800 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  468 42.86622800 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  473 42.97378400 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  474 42.97388400 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  479 43.05226200 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  480 43.05236500 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  485 43.16079900 10.0.2.6        10.0.2.8        TELNET      67 Telnet Data ...
  486 43.16091100 10.0.2.8        10.0.2.6        TELNET      67 Telnet Data ...
  491 43.22650200 10.0.2.6        10.0.2.8        TELNET      68 Telnet Data ...
  492 43.22672700 10.0.2.8        10.0.2.6        TELNET     124 Telnet Data ...
```

```
▶Frame 413: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▶Ethernet II, Src: Vmware_9d:94:e2 (00:0c:29:9d:94:e2), Dst: Vmware_e8:83:c1 (00:0c:29:e8:83:c1)
▶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: 35456 (35456), Dst Port: telnet (23), Seq: 174, Ack: 856, Len: 1
▼Telnet
   Data: #
```

```
0000  00 0c 29 e8 83 c1 00 0c  29 9d 94 e2 08 00 45 10   ..)..... ).....E.
0010  00 35 5b 3f 40 00 40 06  c7 66 0a 00 02 06 0a 00   .5[?@.@. .f......
0020  02 08 8a 80 00 17 b0 4d  49 f7 a4 4e 7c 9a 80 18   .......M I..N|...
0030  00 f5 4d da 00 00 01 01  08 0a 00 05 3b 4e 00 05   ..M..... ....;N..
0040  0b ba 23                                           ..#
```

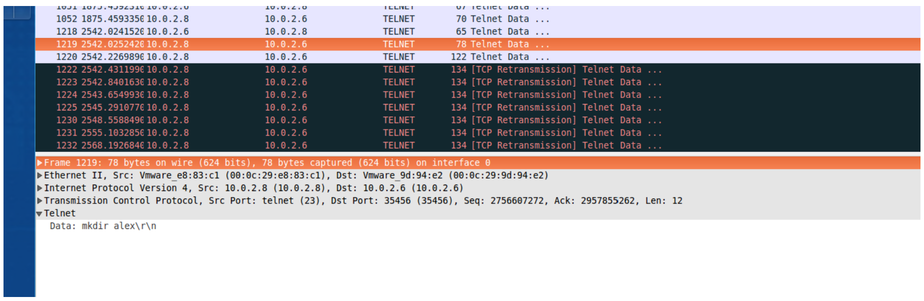

ring from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
~ ! @ # $ % ^ & * ( ) _ +

Filter: telnet

```
No.   Time          Source       Destination   Protocol Lengtł Info
  391 39.71162100( 10.0.2.6      10.0.2.8      TELNET     67 Telnet Data ...
  392 39.71172900( 10.0.2.8      10.0.2.6      TELNET     67 Telnet Data ...
  397 39.72622200( 10.0.2.6      10.0.2.8      TELNET     67 Telnet Data ...
  398 39.72627400( 10.0.2.8      10.0.2.6      TELNET     67 Telnet Data ...
  403 40.23108700( 10.0.2.6      10.0.2.8      TELNET     68 Telnet Data ...
  404 40.23134200( 10.0.2.8      10.0.2.6      TELNET     68 Telnet Data ...
```

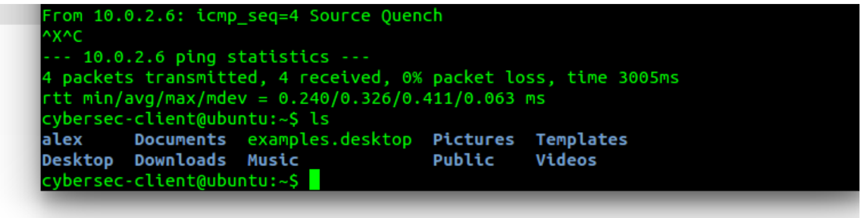
```
▶Frame 492: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
▶Ethernet II, Src: Vmware_e8:83:c1 (00:0c:29:e8:83:c1), Dst: Vmware_9d:94:e2 (00:0c:29:9d:94:e2)
▶Internet Protocol Version 4, Src: 10.0.2.8 (10.0.2.8), Dst: 10.0.2.6 (10.0.2.6)
▼Transmission Control Protocol, Src Port: telnet (23), Dst Port: 35456 (35456), Seq: 2756607143, Ack: 2957855238, Len: 58
  Source port: telnet (23)
  Destination port: 35456 (35456)
  [Stream index: 0]
  Sequence number: 2756607143
  [Next sequence number: 2756607201]
  Acknowledgment number: 2957855238
  Header length: 32 bytes
 ▶Flags: 0x018 (PSH, ACK)
  Window size value: 227
  [Calculated window size: 29056]
  [Window size scaling factor: 128]
 ▶Checksum: 0x186e [validation disabled]
 ▶Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 ▶[SEQ/ACK analysis]
▶Telnet
```

```
0000  00 0c 29 9d 94 e2 00 0c  29 e8 83 c1 08 00 45 10   ..)..... ).....E.
0010  00 6e 9d 90 40 00 40 06  84 dc 0a 00 02 08 0a 00   .n..@.@. ........
0020  02 06 00 17 8a 80 a4 4e  7c a7 b0 4d 4a 06 80 18   .......N |..MJ...
0030  00 e3 18 6e 00 00 01 01  08 0a 00 05 0e a6 00 05   ...n.... ........
0040  3d bb 0d 0a 1b 5d 30 3b  63 79 62 65 72 73 65 63   =....]0; cybersec
0050  2d 63 6c 69 65 6e 74 40  75 62 75 6e 74 75 3a 20   -client@ ubuntu:
0060  7e 07 63 79 62 65 72 73  65 63 2d 63 6c 69 65 6e   ~.cybers ec-clien
0070  74 40 75 62 75 6e 74 75  3a 7e 24 20               t@ubuntu :~$
```



```
1052 1875.459335( 10.0.2.8   10.0.2.6   TELNET    70 Telnet Data ...
1218 2542.024152( 10.0.2.6   10.0.2.8   TELNET    65 Telnet Data ...
1219 2542.025242( 10.0.2.8   10.0.2.6   TELNET    78 Telnet Data ...
1220 2542.226989( 10.0.2.8   10.0.2.6   TELNET   122 Telnet Data ...
1222 2542.431199( 10.0.2.8   10.0.2.6   TELNET   134 [TCP Retransmission] Telnet Data ...
1223 2542.840163( 10.0.2.8   10.0.2.6   TELNET   134 [TCP Retransmission] Telnet Data ...
1224 2543.654993( 10.0.2.8   10.0.2.6   TELNET   134 [TCP Retransmission] Telnet Data ...
1225 2545.291077( 10.0.2.8   10.0.2.6   TELNET   134 [TCP Retransmission] Telnet Data ...
1230 2548.558849( 10.0.2.8   10.0.2.6   TELNET   134 [TCP Retransmission] Telnet Data ...
1231 2555.103285( 10.0.2.8   10.0.2.6   TELNET   134 [TCP Retransmission] Telnet Data ...
1232 2568.192684( 10.0.2.8   10.0.2.6   TELNET   134 [TCP Retransmission] Telnet Data ...
```

```
▶Frame 1219: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶Ethernet II, Src: Vmware_e8:83:c1 (00:0c:29:e8:83:c1), Dst: Vmware_9d:94:e2 (00:0c:29:9d:94:e2)
▶Internet Protocol Version 4, Src: 10.0.2.8 (10.0.2.8), Dst: 10.0.2.6 (10.0.2.6)
▶Transmission Control Protocol, Src Port: telnet (23), Dst Port: 35456 (35456), Seq: 2756607272, Ack: 2957855262, Len: 12
▼Telnet
  Data: mkdir alex\r\n
```



```
From 10.0.2.6: icmp_seq=4 Source Quench
^X^C
--- 10.0.2.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.240/0.326/0.411/0.063 ms
cybersec-client@ubuntu:~$ ls
alex      Documents  examples.desktop  Pictures  Templates
Desktop   Downloads  Music             Public    Videos
cybersec-client@ubuntu:~$
```