Cole Gottdank, Courtney Barbour, Eric Trudnak

We tried.

curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py
python get-pip.py
python -m pip install scapy --user

2.0 Using Tools to Sniff and Spoof Packets

```
node-0:~/codes> python mycode.py
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = hopopt
  chksum    = None
  src       = 127.0.0.1
  dst       = 127.0.0.1
  \options   \
```

Running python file

```
[node-0:~/codes> sudo python
Python 2.7.12 (default, Nov 12 2018, 14:36:49)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
[>>> from scapy.all import *
[a =>>> a = IP()
[>>> a.show()
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = hopopt
  chksum    = None
  src       = 127.0.0.1
  dst       = 127.0.0.1
  \options   \
```

Using python from CL

2.1 Sniffing Packets With Root Privilege

```
node-0:~/codes> sudo python sniffer.py
###[ Ethernet ]###
  dst       = c0:ea:e4:b1:b4:04
  src       = 02:51:d5:02:f7:3c
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0xc0
     len       = 576
     id        = 33080
     flags     =
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x3762
     src       = 155.98.37.88
     dst       = 185.254.68.170
     \options   \
###[ ICMP ]###
        type      = dest-unreach
        code      = port-unreachable
        chksum    = 0xb524
        reserved  = 0
        length    = 0
        nexthopmtu= 0
###[ IP in ICMP ]###
           version   = 4
           ihl       = 5
           tos       = 0x0
           len       = 671
           id        = 27741
           flags     =
           frag      = 0
           ttl       = 111
           proto     = udp
           chksum    = 0x1d8e
           src       = 185.254.68.170
           dst       = 155.98.37.88
           \options   \
###[ UDP in ICMP ]###
              sport     = 36794
              dport     = 4645
              len       = 651
              chksum    = 0x3c04
###[ Raw ]###
                 load      = 'OPTIONS sip:admin@155.98.37.88:4645;transport=udp;user=phone SIP/2.0\r\
nVia: SIP/2.0/UDP 185.254.68.170:36794;branch=z9hG4bK-107133-1---n83wge3koygvscnn;rport\r\nMax-Forwar
ds: 70\r\nContact: <sip:Annonymous@185.254.68.170:36794;transport=udp>\r\nTo: <sip:admin@155.98.37.88
:4645;transport=udp;user=phone>\r\nFrom: <sip:Annonymous@185.254.68.170:36794;transport=udp;user=phon
e>;tag=v7h3zkkg\r\nCall-ID: SkFRs3xTLDI7X8izkmXUOs..\r\nCSeq: 1 OPTIONS\r\nAllow: INVITE, ACK, CANCEL
, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE\r\nCont'
```

2.1 Sniffing Packets Without Root Privilege

```
^X^Cnode-0:~/codes> python sniffer.py
Traceback (most recent call last):
  File "sniffer.py", line 7, in <module>
    pkt = sniff(filter='icmp',prn=print_pkt)
  File "/usr/local/lib/python2.7/dist-packages/scapy-2.4.3.dev161-py2.7.egg/scapy/sendrecv.py", line
1022, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python2.7/dist-packages/scapy-2.4.3.dev161-py2.7.egg/scapy/sendrecv.py", line
890, in _run
    *arg, **karg)] = iface
  File "/usr/local/lib/python2.7/dist-packages/scapy-2.4.3.dev161-py2.7.egg/scapy/arch/linux.py", lin
e 467, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))  # noqa: E501
  File "/usr/lib/python2.7/socket.py", line 191, in __init__
    _sock = _realsocket(family, type, proto)
socket.error: [Errno 1] Operation not permitted
```

2.1 Sniffing Packets Without Root Privilege 1.1A

```
Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2019-11-12 07:30 MST
SENT (0.0077s) ICMP [155.98.37.87 > 192.168.1.2 Echo request (type=8/code=0) id=3766 seq=1] IP [ttl=6
4 id=19252 iplen=28 ]
RCVD (0.2030s) ICMP [192.168.1.2 > 155.98.37.87 Echo reply (type=0/code=0) id=3766 seq=1] IP [ttl=64
id=61402 iplen=28 ]

Max rtt: 195.123ms | Min rtt: 195.123ms | Avg rtt: 195.123ms
Raw packets sent: 1 (28B) | Rcvd: 1 (28B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.01 seconds
+ read line
++ echo 192.168.1.3 node-2-link-1 node-2-0 node-2
++ awk '{print $1}'
+ ip=192.168.1.3
+ '[' 192.168.1.3 '!=' 127.0.0.1 ']'
++ hostname
+ host=node-1.coleg-qv60341.secureedu.emulab.net
+ nping -c 1 --udp -p 9090 --data-string 'This is UDP message 9 from node-1.coleg-qv60341.secureedu.e
mulab.net to 192.168.1.3' -v-3 192.168.1.3
+ nping -c 1 --icmp 192.168.1.3
```

2.1 1.1B Sniffing Packets

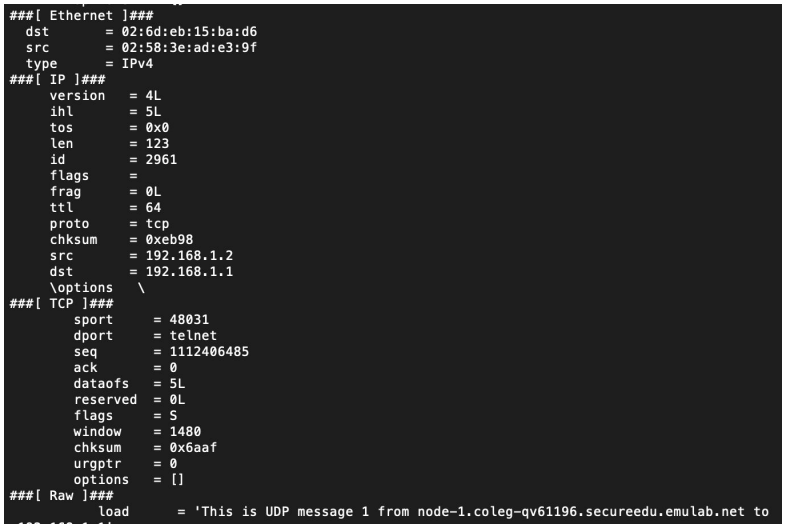
```
###[ Ethernet ]###
  dst       = c0:ea:e4:b1:b4:04
  src       = 02:51:d5:02:f7:3c
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 36
     id        = 18459
     flags     =
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x85b1
     src       = 155.98.37.88
     dst       = 54.248.181.90
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0x336d
        id        = 0x1f
        seq       = 0x2ae8
###[ Raw ]###
           load      = '\x15\xd7\x0e)\xda\n\xa3\x80'
```

```
pkt = sniff(filter='icmp', prn=print_pkt)
```

Attempting to sniff icmp packets

```
pkt = sniff(iface='eth1', filter='tcp port 23',prn=print_port)
```

Attempting to sniff TCP with port 23



Received TCP message even though the message says UDP, we just didn't update the message.