

SCAPY Lab in Backtrack Linux – CSC 433

Use SCAPY to generate a custom packet and capture the packet:

- 1.) Create a packet in Scapy.
- 2.) Send your packet to either your loopback adapter or to another machine on your network.
- 3.) Capture the sent packet using a network sniffer such as Windump or Wireshark

Submit the following screen shots in this assignment:

- a.) A screenshot of the packet being sent from SCAPY
- b.) A screenshot of the captured packet

Backtrack Linux Screenshot shot in SCAPY Lab

```
root@bt: ~
File Edit View Terminal Help
>>> ls(IP)
version : BitField      = (4)
ihl     : BitField      = (None)
tos    : XByteField    = (0)
len    : ShortField    = (None)
id     : ShortField    = (1)
flags   : FlagsField    = (8)
frag    : BitField      = (0)
ttl     : ByteField     = (64)
proto   : ByteEnumField = (6)
chksum  : XShortField  = (None)
src    : Emph          = (None)
dst    : Emph          = ('127.0.0.1')
options : IPOptionsField = ('')
>>> i=IP(proto=6)
>>> ls(i)
version : BitField      = 4           (4)
ihl     : BitField      = None        (None)
tos    : XByteField    = 0            (0)
len    : ShortField    = None        (None)
id     : ShortField    = 1            (1)
flags   : FlagsField    = 0            (0)
frag    : BitField      = 0            (0)
ttl     : ByteField     = 64          (64)
proto   : ByteEnumField = 6           (0)
chksum  : XShortField  = None        (None)
src    : Emph          = '127.0.0.1' (None)
dst    : Emph          = '127.0.0.1' ('127.0.0.1')
options : IPOptionsField = ''          ('')
>>> i.src='5.5.5'
>>> ls(i)
version : BitField      = 4           (4)
ihl     : BitField      = None        (None)
tos    : XByteField    = 0            (0)
len    : ShortField    = None        (None)
id     : ShortField    = 1            (1)
flags   : FlagsField    = 0            (0)
frag    : BitField      = 0            (0)
ttl     : ByteField     = 64          (64)
proto   : ByteEnumField = 6           (0)
chksum  : XShortField  = None        (None)
src    : Emph          = '5.5.5'      (None)
dst    : Emph          = '127.0.0.1' ('127.0.0.1')
options : IPOptionsField = ''          ('')
>>>
```