TP 4

Ex 1)

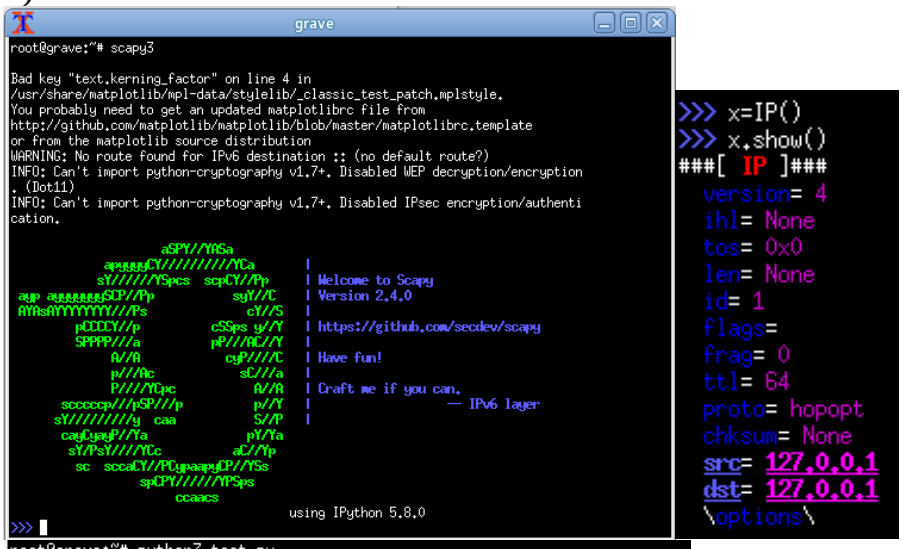
1)

```
root@immortal:~# tcpdump -i eth0
[  646.418720] device eth0 entered promiscuous mode
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
root@opeth:~# netstat -tupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:telnet          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:echo            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:daytime         0.0.0.0:*               LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
udp        0      0 0.0.0.0:echo            0.0.0.0:*
udp        0      0 0.0.0.0:daytime         0.0.0.0:*
```

Immortal espionne bien s'il y a un ping entre grave et syl ou opeth.

2)

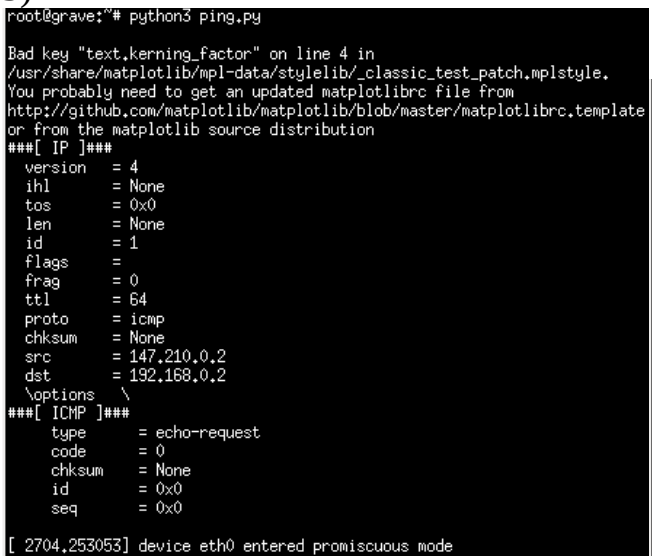


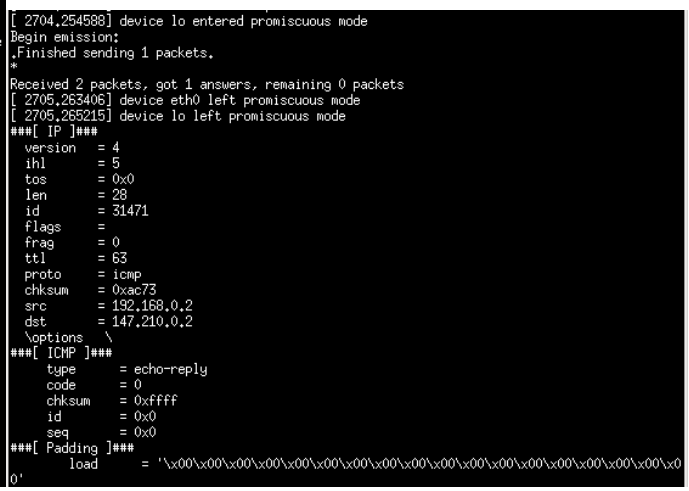

```
root@grave:~# python3 test.py

Bad key "text.kerning_factor" on line 4 in
/usr/share/matplotlib/mpl-data/stylelib/_classic_test_patch.mplstyle.
You probably need to get an updated matplotlibrc file from
http://github.com/matplotlib/matplotlib/blob/master/matplotlibrc.template
or from the matplotlib source distribution
###[ 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   \
```

test.py renvoie bien le même résultat que les commandes sur scapy.

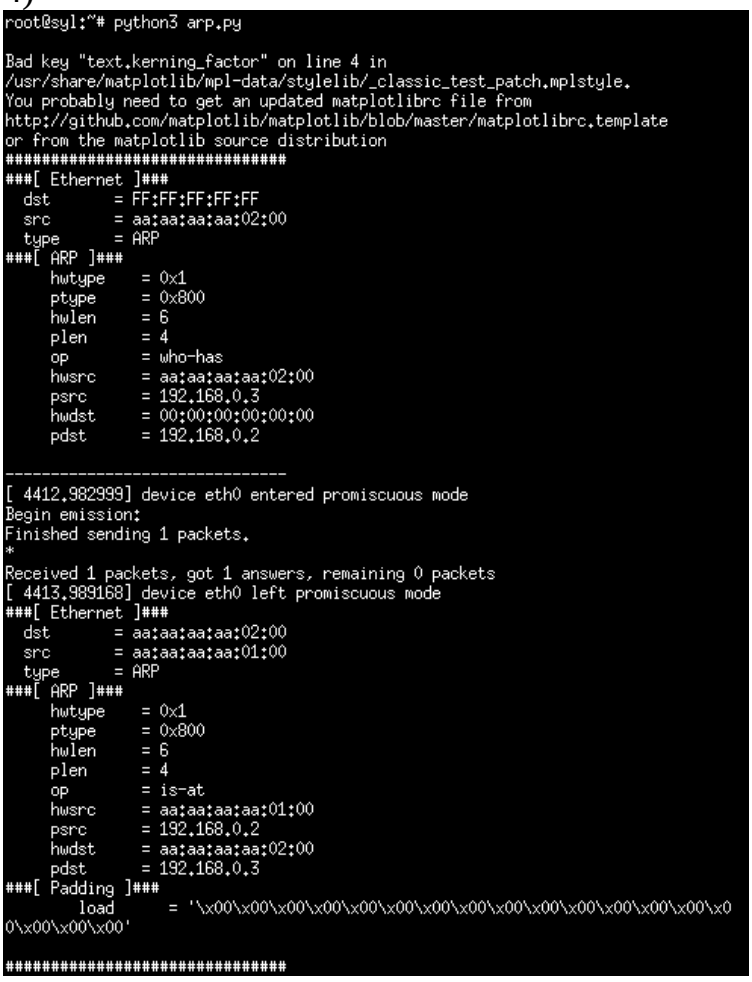
3)



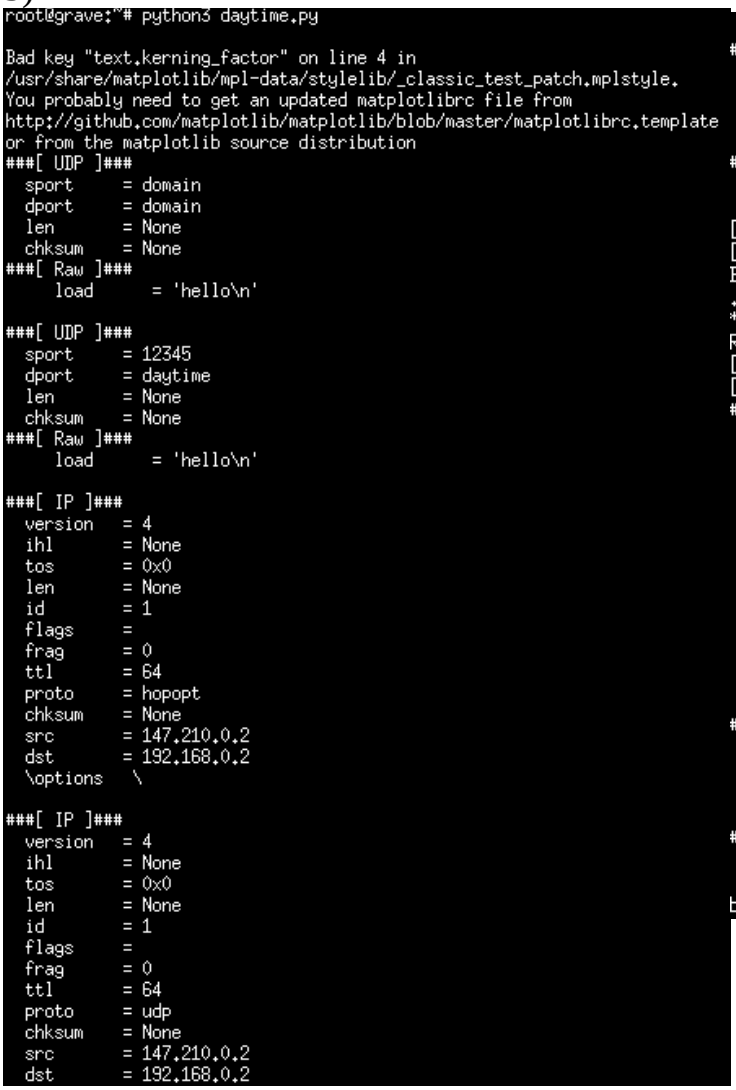


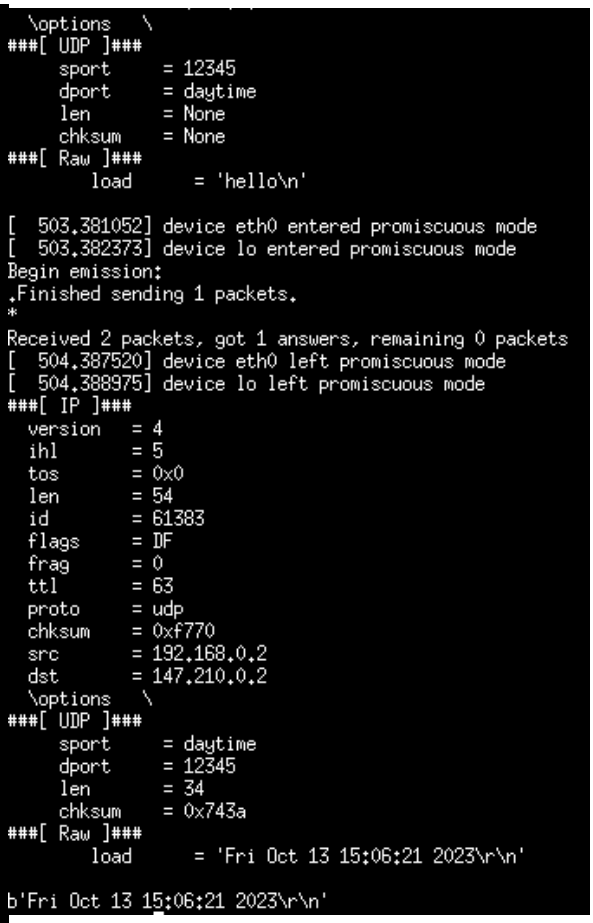
Le ping (séparé ici en deux images) vers opeth marche un peu différemment d'une commande ping normal mais montre de nombreuses informations sur les deux machines et la liaison entre elles

4)



5)





Il revoit la date et l’heure auxquelles la commande à été renvoyé.

6)

```
root@grave:~# python3 syn_scan.py

Bad key "text.kerning_factor" on line 4 in
/usr/share/matplotlib/mpl-data/stylelib/_classic_test_p
You probably need to get an updated matplotlibrc file f
http://github.com/matplotlib/matplotlib/blob/master/mat
or from the matplotlib source distribution
###############################
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 147.210.0.2
  dst       = 192.168.0.2
  \options   \
###[ TCP ]###
     sport     = ftp_data
     dport     = http
     seq       = 0
     ack       = 0
     dataofs   = None
     reserved  = 0
     flags     = S
     window    = 8192
     chksum    = None
     urgptr    = 0
     options   = []

------------------------------
[ 2721.069481] device eth0 entered promiscuous mode
[ 2721.070813] device lo entered promiscuous mode
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
[ 2722.080774] device eth0 left promiscuous mode
[ 2722.082218] device lo left promiscuous mode
###[ IP ]###
  version   = 4
  ihl       = 5
  tos       = 0x0
  len       = 44
  id        = 0
  flags     = DF
  frag      = 0
  ttl       = 63
  proto     = tcp
  chksum    = 0xe74d
  src       = 192.168.0.2
  dst       = 147.210.0.2
  \options   \
###[ TCP ]###
     sport     = http
     dport     = ftp_data
     seq       = 3226606667
     ack       = 1
     dataofs   = 6
     reserved  = 0
     flags     = SA
     window    = 29200
     chksum    = 0xf484
     urgptr    = 0
     options   = [('MSS', 1460)]
###[ Padding ]###
        load      = '\x00\x00'

###############################
```

```
root@grave:~# python3 syn_scan.py

Bad key "text.kerning_factor" on line 4 in
/usr/share/matplotlib/mpl-data/stylelib/_classic_test_p
You probably need to get an updated matplotlibrc file f
http://github.com/matplotlib/matplotlib/blob/master/mat
or from the matplotlib source distribution
###############################
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 147.210.0.2
  dst       = 192.168.0.2
  \options   \
###[ TCP ]###
     sport     = ftp_data
     dport     = 81
     seq       = 0
     ack       = 0
     dataofs   = None
     reserved  = 0
     flags     = S
     window    = 8192
     chksum    = None
     urgptr    = 0
     options   = []

------------------------------
[ 2616.446825] device eth0 entered promiscuous mode
[ 2616.448048] device lo entered promiscuous mode
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
[ 2617.456898] device eth0 left promiscuous mode
[ 2617.458187] device lo left promiscuous mode
###[ IP ]###
  version   = 4
  ihl       = 5
  tos       = 0x0
  len       = 40
  id        = 53293
  flags     = DF
  frag      = 0
  ttl       = 63
  proto     = tcp
  chksum    = 0x1724
  src       = 192.168.0.2
  dst       = 147.210.0.2
  \options   \
###[ TCP ]###
     sport     = 81
     dport     = ftp_data
     seq       = 0
     ack       = 1
     dataofs   = 5
     reserved  = 0
     flags     = RA
     window    = 0
     chksum    = 0x5aec
     urgptr    = 0
     options   = []
###[ Padding ]###
        load      = '\x00\x00\x00\x00\x00\x00'
```

```
###############################
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 147.210.0.2
  dst       = 192.168.0.2
  \options   \
###[ TCP ]###
     sport     = ftp_data
     dport     = 100
     seq       = 0
     ack       = 0
     dataofs   = None
     reserved  = 0
     flags     = S
     window    = 8192
     chksum    = None
     urgptr    = 0
     options   = []

------------------------------
[ 3052.634398] device eth0 entered promiscuous mode
[ 3052.635732] device lo entered promiscuous mode
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
[ 3053.645898] device eth0 left promiscuous mode
[ 3053.647159] device lo left promiscuous mode
###[ IP ]###
  version   = 4
  ihl       = 5
  tos       = 0x0
  len       = 40
  id        = 6853
  flags     = DF
  frag      = 0
  ttl       = 63
  proto     = tcp
  chksum    = 0xcc8c
  src       = 192.168.0.2
  dst       = 147.210.0.2
  \options   \
###[ TCP ]###
     sport     = 100
     dport     = ftp_data
     seq       = 0
     ack       = 1
     dataofs   = 5
     reserved  = 0
     flags     = RA
     window    = 0
     chksum    = 0x5ad9
     urgptr    = 0
     options   = []
###[ Padding ]###
        load      = '\x00\x00\x00\x00\x00\x00'

###############################
```