## **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 EN1OMB (Ethernet), capture size 262144 bytes
root@opeth:~# netstat -tupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address
                                                         Foreign Address
              Ó
                       0 0.0.0.0;ssh
                                                                                        LISTEN
                                                         0.0.0.0:*
                                                         0.0.0.0:*
tcp
              Û
                       0 0.0.0.0;telnet
                                                                                        LISTEN
                                                         0.0.0.0:*
0.0.0.0:*
[::]:*
[::]:*
                       0 0.0.0.0;echo
0 0.0.0.0;daytime
              0
                                                                                        LISTEN
tcp
tcp
              0
                                                                                        LISTEN
                       0 [::]:http
0 [::]:ssh
0 0.0.0.0;echo
tcp6
              0
                                                                                        LISTEN
              0
                                                                                        LISTEN
tcp6
              0
                                                         0.0.0.0:*
udp
                       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)

```
Bad key "text.kerning_factor" on line 4 in
/usr/share/matplotlib/mpl-data/stylelib/_classic_test_patch.mplstyle.
/usr/share/matplotlib/mpl-data/stylelib/_classic_test_patch.mplstyle.
/usr/shably need to get an updated matplotlibrc file from
/ttp://github.com/matplotlib/matplotlib/blob/master/matplotlibrc.template
/r from the matplotlib source distribution
/MRNING: No route found for IPv6 destination :: (no default route?)
//TWO: Can't import python-cryptography v1.7+. Disabled WEP decryption/encryption
//TWO: Can't inport python-cryptography v1.7+. Disabled WEP decryption/encryption
//TWO: Can't inport python-cryptography v1.7+.
                                                                                                                                                                                            >>> x=IP()
                                                                                                                                                                                            >>> x.show()
                                                                                                                                                                                            ###[ IP ]###
                                                                                                                                                                                                             sion= 4
 INFO: Can't import python-cryptography v1.7+. Disabled IPsec encryption/authenti
                                                                                                                                                                                                    ihl= None
                                                                                                                                                                                                     0x0 = cot
                                                                                                                                                                                                      en= None
                                                                                     Welcome to Scapy
Version 2.4.0
                                                                                                                                                                                                    id= 1
                                                                                                                                                                                                     frag= 0
                                                                                     Have fun!
                                                                                                                                                                                                    proto= hopopt
chksum= None
                                                                                                                                                                                                   src= 127,0,0,1
                                                                                                                                                                                                   dst= 127,0,0,1
                                                                             using IPython 5.8.0
  oot@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
ihl
                          = 4
                             = None
     tos
   id
flags
frag
ttl
                              = 64
                             = hopopt
= None
= 127.0.0.1
= 127.0.0.1
   proto
chksum
   src
dst
      \options
```

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

3)

```
oot@grave:~# python3 ping.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 matplotlibro file from
http://github.com/matplotlib/matplotlib/blob/master/matplotlibro.template
or from the matplotlib source distribution
###[ IP ]###
version = 4
ihl = None
tos = 0%0
                                                                                                                                                                            Begin emission:
                                                                                                                                                                           Received 2 packets, got 1 answers, remaining 0 packets

[ 2705,283406] device eth0 left promiscuous mode

[ 2705,285215] device lo left promiscuous mode

###[ |P ]###
                                                                                                                                                                            Finished sending 1 packets.
                                                                                                                                                                           ### [P] | ###

version = 4
ihl = 5
tos = 0
len = 2
id = 3
flags = 6
frag = 0
ttl = 6
proto = 1
chksum = 0
src = 1
dot = 1
\options \
type
code
chksum
id
seq
     tos
len
                            = 0x0
                            = None
    id
flags
                           = icmp
= None
= 147.210.0.2
= 192.168.0.2
    proto
chksum
     dst
  \options \
###[ ICMP ]###
            type
                                  = echo-request
                                                                                                                                                                                                       = echo-reply
= 0
= 0xfffff
= 0x0
= 0x0
           code
chksum
                                  = 0
                                  = None
                                  = 0x0
= 0x0
                                                                                                                                                                            seq = (
###[ Padding ]###
load
            seq
                                                                                                                                                                                                             2704,253053] device ethO entered promiscuous mode
```

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)

```
root@syl:~# python3 arp.py
###[ Ethernet ]###
dst = FF:FF:FF:FF:00
            = aa:aa:aa:aa:02:00
= ARP
  src
type =
###[ ARP ]###
     hwtype
                = 0x1
                = 0x800
= 6
= 4
     ptype
hwlen
     plen
                = who-has
     OP
                = aa;aa;aa;02;00
= 192,168,0,3
= 00;00;00;00;00;00
     hwsrc
     psrc
hwdst
                = 192,168,0,2
     pdst
  4412.982999] device eth0 entered promiscuous mode
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets [ 4413.989168] device eth0 left promiscuous mode ###[ Ethernet ]###
  dst
            = aa;aa;aa;aa;02:00
  src
               aa;aa;aa;aa;01;00
###[ ARP ]###
     hwtype
                = 0x1
     ptype
hwlen
                = 0x800
     plen
                = 4
                = is-at
                = aa;aa;aa;aa;01;00
= 192,168,0,2
     hwsrc
     psrc
     hwdst
                = aa;aa;aa;aa;02;00
pdst = 1
###[ Padding ]###
load
                = 192,168,0,3
                   00x/00x/00x/0
**************************
```

```
root@grave:~# python3 daytime.py
                                                                                                                      \options '
###[ UDP ]###
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
###[ UDP ] ###
sport __domain
                                                                                                                               sport
                                                                                                                                                = 12345
                                                                                                                               dport
                                                                                                                                                = daytime
                                                                                                                               len
                                                                                                                                                = None
                                                                                                                               chksum
                                                                                                                                                = None
                                                                                                                      ###[ Raw ]###
    sport
                   = domain
                                                                                                                                                    = 'hello\n'
                                                                                                                                   load
                   = domain
= None
    dport
                                                                                                                           503,381052] device eth0 entered promiscuous mode 503,382373] device lo entered promiscuous mode
    len
                   = None
    chksum
###[ Raw ]###
                                                                                                                      Begin emission:
.Finished sending 1 packets.
        load
                        = 'hello\n'
                                                                                                                      Received 2 packets, got 1 answers, remaining 0 packets [ 504.387520] device eth0 left promiscuous mode [ 504.388975] device lo left promiscuous mode ###[ IP ]###
###[ UDP ]###
   sport
dport
                   = 12345
                   = daytime
= None
    len
    chksum
                   = None
                                                                                                                                        = 4
= 5
###[ Raw ]###
                                                                                                                         version
                                                                                                                          ihl
                        = 'hello\n'
        load
                                                                                                                                          = 0x0
                                                                                                                         tos
                                                                                                                         len
                                                                                                                                          = 54
###[ IP ]###
                                                                                                                                          = 61383
    version
                  = 4
                                                                                                                          id
    ihl
                   = None
= 0x0
                                                                                                                          flags
                                                                                                                                          = DF
                                                                                                                         frag
    tos
                                                                                                                                          = 0
    len
                   = None
                                                                                                                         ttl
                                                                                                                                          = 63
    id
flags
                                                                                                                                          = udp
= 0xf770
= 192,168,0,2
= 147,210,0,2
                                                                                                                         proto
chksum
    frag
ttl
                                                                                                                          src
                   = 64
                                                                                                                         dst
    proto
                    = hopopt
                                                                                                                      \options \
###[ UDP ]###
                   = None
= 147,210,0,2
= 192,168,0,2
    chksum
                                                                                                                                               = daytime
= 12345
= 34
                                                                                                                               sport
    dst
                                                                                                                               dport
    \options
                                                                                                                               len
                                                                                                                                                = 0x743a
                                                                                                                               chksum
###[ IP ]###
                                                                                                                      ###[ Raw ]###
   version
ihl
                                                                                                                                   load
                                                                                                                                                    = 'Fri Oct 13 15:06:21 2023\r\n'
                      None
                    = 0 \times 0
    tos
                      None
                                                                                                                      b'Fri Oct 13 15:06:21 2023\r\n'
    len
    id
flags
    frag
ttl
                      64
   proto
                    = udp
    .
chksum
                      None
                      147.210.0.2
192.168.0.2
    src
dst
```

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

6)

```
root@grave:~# python3 syn_scan.py
                                                                                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
                                                                               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
or from the matplotlib source distribution
****************************
###[ IP ]###
                                                                                ###[ IP ]###
   version = 4
                                                                                  version
ihl
   ihl
                = None
                                                                                                = None
   tos
                 = 0x0
                                                                                                   0 \times 0
                                                                                  tos
   len
                 = None
                                                                                  len
                                                                                                   None
   id
                 = 1
                                                                                                   1
                                                                                  id
   flags
                                                                                  flags
                                                                                                 Н
   frag
ttl
                 = 0
                                                                                                   Ô
                                                                                  frag
                 = 64
                                                                                  ttl
                                                                                                   64
                = tcp
   proto
                                                                                  proto
                                                                                                   tcp
                = None
= 147,210,0,2
= 192,168,0,2
   chksum
                                                                                  .
chksum
                                                                                                   None
   src
                                                                                                = 147,210,0,2
= 192,168,0,2
                                                                                  src
   dst
                                                                                  dst
   \options
                                                                                \options \
###[ TCP ]###
###[ TCP ]###
                     = ftp_data
      sport
                                                                                                     = ftp_data
                                                                                      sport
       dport
                     = http
                                                                                                     = 81
                                                                                      dport
                     = 0
      seq
                                                                                                     = 0
                                                                                      seq
                     = 0
       ack
                                                                                                     = 0
                                                                                       ack
       dataofs
                     = None
      reserved = 0
flags = S
                                                                                       dataofs
                                                                                                    = None
                                                                                      reserved
                                                                                                        0
                                                                                      flags
                                                                                                        S
       window
                     = 8192
                                                                                                        8192
                                                                                      window
      chksum
                     = None
                     = 0
= []
                                                                                                    = None
                                                                                      chksum
      urgptr
      options
                                                                                      urgptr
                                                                                                     = []
                                                                                       options
  2721,069481] device eth0 entered promiscuous mode 2721,070813] device lo entered promiscuous mode
                                                                                  2616.446825] device eth0 entered promiscuous mode 2616.448048] device lo entered promiscuous mode
Begin emission:
.Finished sending 1 packets.
                                                                                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
                                                                                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
ihl
               = 4
                                                                                 ###[ IP ]###
                = 5
                                                                                  version
   tos
                 = 0x0
                                                                                  ihl
                                                                                                 = 5
   len
                 = 44
                                                                                                   0x0
                                                                                  tos
   id
                                                                                                 = 40
                                                                                  len
                 = DF
   flags
                                                                                  id
                                                                                                   53293
                 = 0
   frag
                                                                                  flags
                                                                                                   DF
                = 63
   t.t.l
                                                                                  frag
ttl
                                                                                                Н
                 = tcp
   proto
                                                                                                   63
                = 0xe74d
= 192,168,0,2
= 147,210,0,2
   chksum
                                                                                                   tcp
0x1724
                                                                                  proto
   src
                                                                                  chksum
   dst
                                                                                                   192,168,0,2
                                                                                  src
   \options
                                                                                                   147,210,0,2
                                                                                  dst
###[ TCP ]###
                                                                               \options \
###[ TCP ]###
      sport
                     = http
                    = ftp_data
= 3226606667
       doort.
                                                                                                     = 81
                                                                                      sport
       seq
                                                                                                     = ftp_data
                                                                                      dport
                     = 1
       ack
                                                                                      seq
       dataofs
                     = 6
      reserved = 0
flags = SA
                                                                                      ack
                                                                                       dataofs
                                                                                                        5
                     = SA
= 29200
                                                                                       reserved
                                                                                                        0
       window
                                                                                       flags
                                                                                                        RΑ
                     = 0xf484
       chksum
                                                                                      window
                                                                                                        0
      urgptr
                     = 0
                                                                                                     = 0x5aec
                                                                                      chksum
options = |
###[ Padding ]###
                    = [('MSS', 1460)]
                                                                                                    = 0
= []
                                                                                      urgptr
                                                                               options = |
###[ Padding ]###
                         = '\x00\x00'
           load
                                                                                           load
                                                                                                         = '\x00\x00\x00\x00\x00\x00'
```

```
###[ IP ]###
   version = 4
ihl = No
                = None
                   0x0
   tos
   len
                = None
   id
flags
                = 1
   frag
                = 0
   ttl
                = 64
                = tcp
= None
= 147,210,0,2
= 192,168,0,2
   proto
chksum
   src
   dst
\options \
###[ TCP ]###
                    = ftp_data
= 100
       sport
       dport
                    = 0
      seq
       ack
                    = 0
       dataofs
                    = None
       reserved = 0
flags = S
                    = 8192
      window
                    = None
      chksum
                    = 0
= []
      urgptr
       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
                = 0x0
= 40
   tos
   len
   id
flags
                = 6853
                = DF
                = 0
   frag
                = 63
   ttl
   proto
                = tcp
   chksum
                = 0xcc8c
                = 192,168,0,2
= 147,210,0,2
   src
dst
\options \
###[ TCP ]###
       sport
                    = 100
       dport
                    = ftp_data
                   = 0
= 1
= 5
       seq
       ack
       dataofs
      reserved = 0
flags = RA
                    = ŘA
= 0
       window
                    = 0x5ad9
       chksum
                    = 0
       urgptr
options = [
###[ Padding ]###
load
                        = '\x00\x00\x00\x00\x00\x00'
```