Àdàkàdekè àwọn èdìdì ìsokọ́ra pẹ̀lú Scapy

Àdàkàdekè àwọn èdìdì isokọ́ra pẹ̀lú scapy

Scapy jẹ́ àkójọpọ̀ Python fún àdàkàdekè ìfiránṣẹ́ àti àgbàwọlé àwọn èdìdì ìsokọ́ra.

Ìmúlò àkọ́ọ̀lẹ̀ yìí

Àwọn ìmọ̀ ẹ̀rọ tó ṣe pàtàkì fún ìmúlò àkọ́ọ̀lẹ̀ yìí ni :

- Ìmọ̀ ẹ̀rọ ètò àkójọpọ̀ Python
- Ìmọ̀ ẹ̀rọ ìsókọ́ra kọ̀ńpútà

Lẹ́yìn ìgbà tí ẹ bá ka akọ́ọ̀lẹ̀ yìí, yóò rọrùn fún yín láti kọ ìtòlẹ́sẹẹsẹ̀ àwọn ohun èlò tí á wúlò fún yín àti fún ìmọ̀ ọ̀nà ìṣiṣẹ́ wọn.

Àgbékalẹ̀ àti ìmúlò

Àlàyé àgbékalẹ̀ pẹ̀lú Linux.
Ẹ lo ìlà àsẹ yìí fi ṣàgbékalẹ̀ scapy

$ sudo apt-get install python-scapy

Nígbà tí ẹ bá pinu láti lò Python ẹ ṣàgbékalẹ̀ ẹ̀yà 2.x(x >= 2.5). Ó ṣeé ṣe kí ẹ ṣàfikún agbára scapy pẹ̀lú àwọn àkójọpọ̀ mì ín.

Àgbékalẹ̀ ìjìnlẹ̀

Fún àgbékalẹ̀ tó jìnlẹ̀ ẹ lo àwọn ìlà àṣẹ:

$ sudo apt-get install python2.7 tcpdump graphviz imagemagick python-gnuplot python-crypto python-pyx nmap python-scapy

Àmúlò scapy

Ẹ lò àṣẹ láti olùtumọ̀ python:

$ sudo scapy

Àkíyèsí Láti lò scapy: Ẹ lo ìpele root.
Nígbà tí gbogbo èyí bá lọ bó ṣe tọ àfihàn ìsàlẹ̀ máa jáde:

```
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.1.0)
>>>
```

Àwọn ohun èlò scapy wà nínú ìtòlẹ́sẹẹsẹ̀ àkójọpọ̀ Python; ṣàfikún :

from scapy.all import

Àdàkàdekè àwọn èdìdì

Àdàkàdekè èdìdì ni ká fọwọ́ sínú ọ̀rọ̀fọ̀ fi ṣàkójọ rẹ̀. Nígbà tí ẹ bá lò ètòlẹ́sẹẹsẹ ìsọkọ́ra bíi ti ayélujára, méèlì, àwọn ètò máa ń ṣíṣàjọpín àwọn èdìdì, bíi àpẹẹrẹ, nígbà tí ẹ bá lo http://www.omoluwabi.org

Àkójọ ìwọ̀ (frame) Ethernet

Fún ṣíṣàjọpín àwọn èdìdì a yóò lò àwọn ìfẹ́nukò TCP, IP, HTTP
Ìbẹ̀rẹ̀ àkójọ àti àṣàfihàn ìwọ̀ Ethernet nínú onítúmọ̀ scapy.

```
>>> iwo_mi = Ether()
>>> iwo_mi.show()
###[ Ethernet ]###
WARNING: Mac address to reach destination not found. Using
broadcast.
  dst= ff:ff:ff:ff:ff:ff
  src= 00:00:00:00:00:00
  type= 0x0
```

Bíi a ṣe ri, a ṣàkójọ ohun ìwọ́ pẹ̀lú ọ̀wọ́ Ether().

Àtò ẹyọ kan ni a lò pẹ̀lú ìmúlò iṣẹ́ show(), iye àkùnàyàn ló wà nínú àwọn àfidámọ̀ dst, src àti type.

- A ṣàkójọ ìwọ́ ethernet ìpìlẹ̀, èyí tó túmọ̀ sí wípé a ò ní ìsọfúnni kan nínú rẹ̀, CRC máa ń fún wa ní àǹfààní láti ṣàkóso ìwọ́ ethernet tó péye. A lè ṣèyípadà ìwọ́ yìí pẹ̀lú àwọn ààtò 3 tó kù:
  - dst : Adírẹ́ẹ̀sì arídìmú àgbàsọfúnni
  - src : Adírẹ́ẹ̀sì arídìmú alátagbà
  - type : Irúfẹ́ ìfẹ́nukò (jẹmọ́ ẹ̀yà data tó jẹ́ òfo).

  Tí a bá fọwọ́ kan CRC ìwọ́ yìí kò tún wúlò mọ́.

Ìyípadà àwọn ààtò wọ̀nyìí rọrùn :

```
>>> iwo_mi.dst = '00:19:4b:10:38:79'
>>> iwo_mi.show()
###[ Ethernet ]###
  dst= 00:19:4b:10:38:79
  src= 00:00:00:00:00:00
  type= 0x0
>>>
```

A lè ṣàlàyé adírẹ́ẹ̀sì àgbàsọfúnni ní ìpìlẹ̀

>>> iwo_mi = Ether(dst='00:19:4b:10:38:79')

A lè ṣèyípadà àwọn àfidamọ̀, dst, src, àti type bó ṣe wù wa. Ẹ lè fi ìwọ́ kan ránṣẹ́ ní ìrọ̀rùn bíi ẹ̀yí tó jẹ́ ti ẹlòmíràn.

Ìfiránṣẹ́ ìwọ́ (frame)

Láti fi ìwọ̀ kan ránṣẹ́ a yóò lò iṣẹ́ **sendp()** ;

```
>>> sendp(iwo_mi)
.
Sent 1 packets.
>>>
```

Pẹ̀lú scapy "." fi ń yé wa wípé a ti sèfiránṣẹ́ èdìdì.

Báyìí ni a máa ṣèfiránṣẹ́ èdìdì pẹ̀lú adírẹ́ẹ̀sì rẹ̀.

Nǹkan tí a ṣe kó ní ìwúlò ẹyọ kan, òfoasán èdìdì tí a firánṣẹ́ kò wúlò àfi tó bá ní ìsọfúnni nínú, a yóò ṣé ìsúnkì ìfẹ́nukò.

Kínni ìsúnkì ?

Ìsúnkì nínú ìmọ̀ ìsokọ́ra ni kí a ki àwọn ìsọfúnni ìfẹ́nukò kan sínú omi.

Ìsúnkì àwọn protocole : Àpẹẹrẹ ping

Ping jẹ́ àṣẹ láti mọ̀ tí kọ́ńpútà kan pẹ̀lú adírẹ́ẹ̀sì rẹ̀ bá wà nínú ìsokọ́ra. ping máa fún wà ní àǹfààní láti ṣèfiránṣẹ́ èdìdì ICMP " echo-request" pẹ̀lú ìdápadà èdìdì "echo-reply".

Àdàkàdekè èdìdì ICMP "echo request"

```
>>> ping_mi = ICMP()
>>> ping_mi.show()
###[ ICMP ]###
  type= echo-request
  code= 0
  chksum= None
  id= 0x0
  seq= 0x0
>>>
```

A ri pé ní àkùnàyàn, ìṣẹ̀dá ọ̀wọ́ ICMP() fi àfidámọ̀ type sí echo_request a lè yípadà àti àwọn àfidámọ̀ tó kù.
A yóò ṣèsúnkì èdìdì ICMP sínú ìtòlẹ́sẹẹsẹ̀ ìsọfúnni (datagram) IP, inú èyí ni a máa ṣàlàyé adírẹ́ẹ̀sì IP agbàsọfúnni.
Nínú scapy àmì / ni a yóò lò fún ìsúnkí.

```
>>> ping_mi = Ether() / IP(dst='192.168.1.1') / ICMP()
>>> ping_mi.show()
###[ Ethernet ]###
  dst= 00:19:4b:10:38:79
  src= 00:26:5e:17:00:6e
  type= 0x800
###[ IP ]###
     version= 4
     ihl= None
     tos= 0x0
     len= None
     id= 1
     flags=
     frag= 0
     ttl= 64
     proto= icmp
     chksum= None
     src= 192.168.1.14
     dst= 192.168.1.1
     \options\
###[ ICMP ]###
        type= echo-request
        code= 0
        chksum= None
        id= 0x0
        seq= 0x0
>>>
```

Ìfiránṣẹ́ èdìdì

A á wò ó tí box bá máa dáhùn

```
>>> sendp(mon_ping)
.
Sent 1 packets.
>>>
```

Kò sí èsì kan ! , ó yẹ kó rí bẹ̀ẹ̀, ìfiránṣẹ́ nìkan ni iṣẹ́ sendp máa ń ṣé. A yóò lò àwọn iṣẹ́ srp() àti srp1() láti ṣèfiránṣẹ́ àti ṣègbàwọlé èsì.
srp() máa ń ṣèdápadà ọ̀wọ́ méjì: inú ọ̀wọ́ àkọ́kọ́ a yóò ri àwọn èdìdì tí a firánṣẹ́ pẹ̀lú èsì tó jẹ́ mọ́ wọn, inú èkèjì a yóò rí èdìdì tí kò níí èsì.

```
>>> rep,non_rep = srp(mon_ping)
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0
packets
>>> rep
<Results: TCP:0 UDP:0 ICMP:1 Other:0>
>>> non_rep
<Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>
>>>
```

Àmì “* “   kan fi hàn wa pé a ní èsì kan tó sì jẹ́ èdìdì ICMP echo-reply!

```
>>> rep.show()
0000 Ether / IP / ICMP 192.168.1.14 > 192.168.1.1 echo-request 0 ==> Ether / IP / ICMP
192.168.1.1 > 192.168.1.14 echo-reply 0
>>>
```

Nínú rep a ní àwọn àtòkọ èdìdì alákóméjì, níbi inú àtòkọ alákóméjì èdìdì kan ló wà nínú rep, a lè fihàn bíi ìdápìlẹ̀ gbogbo àtòkọ Python.

```
>>> rep[0]
(<Ether  type=0x800 |<IP  frag=0 proto=icmp dst=192.168.1.1 |<ICMP  |>>>, <Ether
dst=00:26:5e:17:00:6e src=00:19:4b:10:38:79 type=0x800 |<IP  version=4L ihl=5L tos=0x0
len=28 id=58681 flags= frag=0L ttl=64 proto=icmp chksum=0x1248 src=192.168.1.1
dst=192.168.1.14 options=[] |<ICMP  type=echo-reply code=0 chksum=0xffff id=0x0 seq=0x0 |
>>>)
```

Àwójúùtù jẹ́ alákóméjì. Fún àṣàfihàn èdìdì ìfiránṣẹ́ (ICMP echo-request wa) a lò rep[0][0].show(), fún èdìèdì èsì rep[0][1].show().

```
>>> rep[0][0].show()
###[ Ethernet ]###
  dst= 00:19:4b:10:38:79
  src= 00:26:5e:17:00:6e
  type= 0x800
###[ IP ]###
     version= 4
     ihl= None
     tos= 0x0
     len= None
     id= 1
     flags=
     frag= 0
     ttl= 64
     proto= icmp
     chksum= None
     src= 192.168.1.14
     dst= 192.168.1.1
     \options\
###[ ICMP ]###
        type= echo-request
        code= 0
        chksum= None
        id= 0x0
        seq= 0x0
```

```
>>> rep[0][1].show()
###[ Ethernet ]###
  dst= 00:26:5e:17:00:6e
  src= 00:19:4b:10:38:79
  type= 0x800
```

Láti mú gbogbo nǹkan rọrùn, a yóò lò iṣẹ́ srp1(), iṣẹ́ yìí máa ń ṣèyípadà ọ̀wọ́ ẹyọ kan.

```
>>> rep = srp1(mon_ping)
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> rep.show()
```

A kò yìí sàbá lò ẹ̀yà àkọ́sórí Ethernet scapy máa sàbá ṣètò rẹ̀ bó ṣe tọ, a yóò lò àwọn iṣẹ́ send(), sr(), àti sr1() tó dọ́gba mọ́ sendp(), srp() àti srp1(), lẹ́yìn pé wọ́n máa ń ṣàfikún àkọsórí ní aládáṣe.

```
>>> rep = sr1(IP(dst='192.168.1.1') / ICMP())
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> rep.show()
###[ IP ]###
```

Ká lò iṣẹ́ yìí sórí kọ̀ńpútà òfo.

```
>>> rep = sr1(IP(dst='192.168.1.2') / ICMP())
Begin emission:
.WARNING: Mac address to reach destination not found. Using broadcast.
Finished to send 1 packets.
....................^C
Received 22 packets, got 0 answers, remaining 1 packets
>>>
```

Mo dá ìfiránṣẹ́ dúró pẹ̀lú (Ctrl-c), lẹ́yìn 30 ìṣẹ́jú ààyá, oníyípadà rep gbà òdo nígbà tí “got 0 answers”. A lè ṣàfikún òpin ìgbà sórí iṣẹ́ sr1() ṣèdádúró ìfiránṣẹ́ pẹ̀lú timeout.

```
>>> rep = sr1(IP(dst='192.168.1.2') / ICMP(), timeout=0.5)
Begin emission:
WARNING: Mac address to reach destination not found. Using broadcast.
Finished to send 1 packets.
```

Ẹ lò help(sr1) fún ìrànlọ́wọ́.

Àdáṣe :

Pẹ̀lú àwọn àlàyé tí a ṣé ṣíwájú àti ìmọ̀ Ptyhon tí ẹ ní, yóò rọrùn fún yín láti kọ ètòlẹ́ṣẹ̀ẹ̀ṣẹ̀ tí á lè máa ṣé ping lórí àwọn àdírẹ́ẹ̀sì àtòpọ̀ kan.

òǹtẹ̀: Fún ìtọ́kasí àtòpọ̀ àdírẹ́ẹ̀sì, ẹ lò ‘192.168.1-15’ nínú àfidámọ̀ dst ti IP.

```
#! /usr/bin/python
from scapy.all import *

rang = '192.168.1.1-15'
rep,non_rep = sr( IP(dst=rang) / ICMP() , timeout=0.5 )
for elem in rep : # elem représente un couple (paquet émis, paquet reçu)
        if elem[1].type == 0 : # 0 <=> echo-reply
                print elem[1].src + ' a renvoye un echo-reply '
```

ls(edidi) máa ṣàfihàn èdìdì lọ́nà òǹkaye, tí yóò sì tún ṣàfihàn orúkọ, irúfẹ́ àti iye wọn ní àkùnàyàn.

```
>>> ls(IP(dst='192.168.1.1') / ICMP(type='echo-reply'))
version    : BitField        = 4          (4)
ihl        : BitField        = None       (None)
tos        : XByteField      = 0          (0)
len        : ShortField      = None       (None)
id         : ShortField      = 1          (1)
flags      : FlagsField      = 0          (0)
```

Àtòkọ àwọn èdìdì

Scapy máa ṣàlàyé fún àfidámọ̀ èdìdì kan àtòkọ iye, èyí yóò fi jẹ́ iye kan. Bíi a ṣe rí níwájú fún IP àgbàfúnni èyí lè ṣeé ṣe fún gbogbo àfidámọ̀.

Àtòkọ ní ráńpẹ́

Bíi àpẹẹrẹ a fẹ́ mọ̀ tí a lè lo apèsè web pẹ̀lú http àti https, a lè ṣàyẹ̀wò àwọn èbúté ní àkùnàyàn : 80 àti 443.

A yóò lò àtòkọ ráńpẹ́ èbúté pẹ̀lú dport = [80, 443].
a yóò lò àyẹ̀wò SYN : A máa ń ṣèfiránṣẹ́ èdìdì TCP lórí èbúté òkèrè pẹ̀lú àsia SYN láti fi mọ̀ tí ojú ìwọlé bá gbà àsopọ̀, ó máa ṣèyípadà èdìdì TCP pẹ̀lú àwọn àsia SYN àti ACK

```
>>> ls(TCP)
sport      : ShortEnumField       = (20)
dport      : ShortEnumField       = (80)
seq        : IntField             = (0)
ack        : IntField             = (0)
```

- Nígbà tí mo ṣàkójọ èdìdì mi, mo ṣàlàyé ojú ìkànpọ̀ orísùn àti ti èbúté, mo sì gbé àsia SYN sókè, mo sì fi èdìdì yìí ránṣẹ́.
  Inú àwójúùtù a ní èdìdì alákóméjì, èdìdì ìfiránṣẹ́/agbàsọfúnni.

  Èdìdì àkọ́kọ́ ti a gbà ni èyí tí firánṣẹ́ lórí ojú ìkànpọ̀. àwọn àsia ti fi sí ìpò òkè ni SYN àti ACK, ojú àkànpọ̀ ni ṣíṣí :

Èdìdì èkèjì ti a gbà ni èyí tó sì 443 àwọn àsia ní SYN àti ACK RESET àti ACK : ojú àkànpọ̀ wà ní títì.

```
>>> mon_paquet = IP(dst='192.168.1.10') / TCP(sport=12345, dport=(80,443), flags='S')
>>> rep,non_rep = sr(mon_paquet)
Begin emission:
.*************************************************************************************
**************************************************************************************
**************************************************************************************
**************************************************************************************
*********************************************************Finished to send 364 packets.
*
Received 365 packets, got 364 answers, remaining 0 packets
>>>
```

```
>>> for emis,recu in rep :
...     if recu[1].flags==18 : # 18 <=> SYN+ACK
...         print 'port ouvert : ', recu[1].sport
...
port ouvert :  80
port ouvert :  111
>>>
```

Àdáṣe : Ìṣètòlẹ́ṣẹ̀ẹ̀ṣẹ traceroute

Àṣe traceroute máa ń fún wa ní àǹfààní láti mọ̀ àwọn ọ̀nà tí èdìdì gbà fi dé èbúté, fún ìdí èyí a yóò lò ttl (time to live) àkọ́sórí IP. Iye yìí máa ń díkan ní gbogbo gbà tó bá gbanu alànà, tí iye bá dé 0, ó máa kù tí yóò sì padà wá. a yóò lò àfidámọ̀ rẹ̀ src àkosórí IP rẹ̀, fi mọ̀ àdírẹ́ẹ̀sì ibi tó kù sí.

```
>>> rep,non_rep=sr( IP(dst='209.85.143.100', ttl=(1,25)) / TCP(), timeout=1 )
Begin emission:
********Finished to send 25 packets.
***..
Received 13 packets, got 11 answers, remaining 14 packets
>>> for emis,recu in rep:
...     print emis.ttl, recu.src
...
1 192.168.1.1
2 90.45.115.1
3 10.125.164.10
4 193.253.93.105
5 81.253.130.14
6 193.252.100.42
7 193.251.254.18
8 72.14.232.211
9 209.85.251.190
10 209.85.253.125
11 209.85.143.100
>>>
```

Àdírẹ́ẹ̀sì IP 209.85.143.100 ní a lò fún èbúté. Mo sèsúnkì TCP sínú IP, ó ṣeé ṣe kó jẹ́ I
ICMP àti UDP tàbí kí a máa tún lò nǹkan kan. Àwọn ogiri iná lè dá àwọn ìfẹ́nukò mì ín dùró. A ṣàyípadà tt1 láti 1 dé 25 àmọ́ a rí wípé lẹ́yìn ìfòsókè 11. Àwọn alànà Livebox àti àwọn alànà Orange àti Google.

Iṣẹ́ Sniff()

A mọ̀ bí tí a ṣé ń ṣèfiránṣẹ́ tàbí gbà wọn wọlé, àwọn èdìdì. Àmọ́ láti tẹ̀ síwájú pẹ̀lú ìmọ̀ àwọn ohun èlò ìsokọ́rà, Ó yẹ kí a ṣèpínsíwẹ́wẹ́ àwọn ṣíṣàjọpín àwọn èdìdì. Bíi àpẹẹrẹ báwo ni àṣẹ ping ṣé n ṣiṣẹ́.láti sàyẹ̀wò ojú àkànpọ̀, báwo ni firefox láti www.omoluwa.oẹg ìbẹ̀ ni a yóò lò sniff() ti scapy.

Àgbékalẹ̀-ètò

sniff(filter="", count=0, prn=None, lfilter=None, timeout=None, iface=All)
Ó máa ń ṣẹ̀firánṣẹ́ àtòkọ èdìdì (bíi àfiwé, sr() máa ń ṣèfiránṣẹ́ àtòkọ̀ èdìdì méjì)

Àwọn ààtò

Count : Iye àwọn èdìdì tí a fẹ́ gélọgan, 0: àìlópin
timeout : Ìfimúnfínlẹ̀ máa dópin lẹ́yìn ìgbà mélòó kan.

Iface : àtọkùn tí a fẹ́ lò fún ìfimúfínlẹ̀, pẹ̀lú àṣẹ ifconfig a lè ṣàfihàn àwọn àtọkùn tí a ń lò.
filtre : Asẹ àwọn èdìdì tí a fẹ́ ṣàṣàyàn pẹ̀lú àsòpọ̀ ìró.
Àpẹẹre : filter = “port = “port 80” àwọn èdìdì tí wọ́n jẹmọ́ port 80.

lfilter : lfilter = lambda x: x[1].src == ‘192.168.1.14’ máa ń ṣàṣàyàn

- filter máa ń lò aṣẹ BPF. asẹ “(port 80 or 443) and dst 192.168.1.14” máa ń ṣàṣàyàn àwọn èdìdì ìfiránṣẹ́ (dst) sí èmi náà (host 192.168.1.14) tó jẹmọ́ àwọn ojú àkànpọ̀ http tàbí https (port 80 or port 443)

Ìfimúnfínlẹ̀
Kínni iṣẹ́ ping ?

Ìmúlò snifff fi ṣíṣàṣàyàn lórí ping 192.168.1.10

```
>>> rep = sniff(filter="host 192.168.1.10")
```

Mo máa rí àwọn èdìdì ìfimúnfínlẹ̀

```
>>> rep.show()
0000 Ether / IP / ICMP 192.168.1.14 > 192.168.1.10 echo-request 0 / Raw
0001 Ether / IP / ICMP 192.168.1.10 > 192.168.1.14 echo-reply 0 / Raw
>>>
```

Kínni ó wà nínú Raw.
Raw jẹ àwọn ìsọfúnni tó wúlò (playload), àwọn ìsọfúnni láì ní àkọsórí, bíi

àpẹẹrẹ, nígbà tí a bá ń ṣègbàsílẹ̀ àwọn fáìlì tó tóbi a yóò ṣèpínsíwẹwẹ fáìlì yìí àwọn èdìdì tí a máa kójọ ní ìgbẹ̀yìn.

```
>>> rep[0].show()
###[ Ethernet ]###
  ....
  blabla
  ....
###[ Raw ]###
        load= 'B\xdd\xa5N\x14\xf7\x02\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'
>>>
```

Látarí ìsọfúnni yìí a yóò mọ̀ tí ping bá wa sórí kọ̀ńpútà.

Kínni nmap máa ń ṣé ?

A yóò lò (scan) àyẹ̀wò SYN ojú àkànpọ̀ 80 ti 192.168.1.10

```
$ sudo nmap -sS -p 80 192.168.1.10
```

Àwọn èdìdì ìfimúnfínlẹ̀ :

```
>>> rep.show()
0000 Ether / ARP who has 192.168.1.10 says 192.168.1.14
0001 Ether / ARP is at 00:16:17:e3:ed:88 says 192.168.1.10 / Padding
0002 Ether / IP / TCP 192.168.1.14:50662 > 192.168.1.10:www S
0003 Ether / IP / TCP 192.168.1.10:www > 192.168.1.14:50662 SA / Padding
0004 Ether / IP / TCP 192.168.1.14:50662 > 192.168.1.10:www R
>>>
```

Nínú ẹ̀yà scan SYN yìí, àwọn èdìdì pẹ̀lú àsia S SA nìkan ni a ní. A tún ní àwọn èdìdì ARP fi mọ̀ adírẹ́ẹ̀sì MAC èbúté. scapy máa ń ṣèsúnki láàyè wa.
A ò ṣàkíyèsí ìfiránṣẹ́ èdìdì RESET. Nígbà tí kúró Linux gbà èdìdì SYN + ACK tí kò sí mọ̀ pé ṣcapy ti béèrè fun, kúró máa ṣèfiránṣẹ́ èdìdì RESET láti ti àsòpọ̀ tó rò pé kò wáyé. A yóò dá RESET dúró pẹ̀lú àṣẹ:

$ sudo iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP nmap ṣé bíi wa.

Kínni firefox máa ń ṣé

Mo lo http://lalitte.com/anciensite/double.html nínú firefox:

```
>>> r = sniff(filter="host 192.168.1.14")
^C>>> r
<Sniffed: TCP:28 UDP:4 ICMP:0 Other:2>
>>> r.show()
0000 Ether / IP / UDP / DNS Qry "lalitte.com."
0001 Ether / IP / UDP / DNS Ans "88.191.135.63"
```

Ẹ jẹ́ ká wò nǹkan tó ṣẹlẹ̀ ?

- Àwọn èdìdì 0 àti 1 jẹ́ èdìdì DNS méjì, wọ́n máa ń fún firefoxe láàǹfààní láti adíẹ́ẹ̀sì IP ti lalitte.com
- Àwọn èdìdì 2, 3, 4 jẹ́ handshak TCP, tí gbogba bá lọ ṣe yẹ (látari àwọn àsia S/ SA /A)
- Èdìdì 5 jẹ́ ìbéèrè HTTP ti firefox ìjẹ́rìí.

```
>>> r[5].show()
###[ Ethernet ]###
  dst= 00:19:4b:10:38:79
  src= 00:26:5e:17:00:6e
  type= 0x800
###[ IP ]###
     version= 4L
```