

# Make Your Own Network Security Tools With Scapy



# Temario

- Introducción a Scapy
- Sniffing ARP
- ARP Discovery
- Man-In-The-Middle (MITM)
- ARP Spoofing
- IP Forwarding
- Sniffing HTTP
- Modificación de Tráfico HTTP

# Introducción a Scapy

1. Es una librería de Python (2.7.x y 3.4+)
2. Permite enviar, escuchar, analizar y crear paquetes de red
3. Soporta un modo de trabajo interactivo y también por scripts
4. Principalmente, hace dos cosas: envía paquetes, recibe respuestas
5. No interpreta, decodifica (ej: Puerto abierto vs TCP SYN/ACK)

# Introducción a Scapy

\*"You're free to put any value you want in any field you want and stack them like you want.\* \*You're an adult after all."\* From: Scapy Official Docs

# Inicio

```
# scapy3
```

```
                aSPY//YASa
      apyyyyCY/////////YCa
    sY////////YSpcs  scpCY//Pp
ayp ayyyyyyySCP//Pp      syY//C
AYAsAYYYYYYYY///Ps      cY//S
    pCCCCY//p      cSSps y//Y
    SPPPP///a      pP///AC//Y
        A//A      cyP///C
        p///Ac      sC///a
        P////YCpc      A//A
    scccccp///pSP///p      p//Y
sY/////////y  caa      S//P
cayCyayP//Ya      pY/Ya
    sY/PsY////YCc      aC//Yp
    sc  sccaCY//PCypaapyCP//YSs
        spCPY////////YPSps
            ccaacs
```

```
Welcome to Scapy
Version 2.4.0
```

```
https://github.com/secdev/scapy
```

```
Have fun!
```

```
Craft packets like it is your last
day on earth.
```

```
-- Lao-Tze
```

```
using IPython 5.5.0
```

```
>>>
```

# Nuestro Primer Paquete

```
:::py3
>>> l3 = IP(dst='8.8.4.4')
>>> l4 = ICMP()
>>> sr1(l3/l4)
```

Begin emission:

.Finished sending 1 packets.

\*

Received 2 packets, got 1 answers, remaining 0 packets

```
<IP  version=4 ihl=5 tos=0x0 len=28 id=11010 flags= frag=0 ttl=63 proto=icmp checksum=0x34c1
src=8.8.4.4 dst=10.0.2.15 options=[] |<ICMP  type=echo-reply code=0 checksum=0xffff id=0x0
seq=0x0 |<Padding  load='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' |>>
```

# ¿Qué es un "layer"?

```
:::py3
>>> l3.show()
####[ IP ]####
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 10.0.2.15
  dst= 8.8.4.4
  \options\

>>> l4.show()
####[ ICMP ]####
  type= echo-request
  code= 0
  chksum= None
  id= 0x0
  seq= 0x0
```

# ¿Qué es un "layer"? (2)

```
:::py3
>>> l3.show2()
####[ IP ]####
  version= 4
  ihl= 5
  tos= 0x0
  len= 20
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  checksum= 0x5ecb
  src= 10.0.2.15
  dst= 8.8.4.4
  \options\

>>> l4.show2()
####[ ICMP ]####
  type= echo-request
  code= 0
  checksum= 0xf7ff
  id= 0x0
  seq= 0x0
```



# Generando varios paquetes

```
:::py3
>>> l3 = IP(dst='8.8.4.4/30')
>>> ans,unans = sr(l3/l4, timeout=3)
Begin emission:
.Finished sending 4 packets.
*
Received 2 packets, got 1 answers, remaining 3 packets
>>> ans
<Results: TCP:0 UDP:0 ICMP:1 Other:0>
>>> unans
<Unanswered: TCP:0 UDP:0 ICMP:3 Other:0>
```

# No-Respondidos vs Respondidos

```

:::py3
>>> for pkt in unans:
...:     print(pkt.summary())
...:
IP / ICMP 10.0.2.15 > 8.8.4.5 echo-request 0
IP / ICMP 10.0.2.15 > 8.8.4.6 echo-request 0
IP / ICMP 10.0.2.15 > 8.8.4.7 echo-request 0

>>> for s,pkt in ans:
...:     print(s.summary(), '|', pkt.summary())
...:
IP / ICMP 10.0.2.15 > 8.8.4.4 echo-request 0 | IP / ICMP 8.8.4.4 > 10.0.2.15 echo-reply 0 / Padding

```

# Sniffing



# Placa en estado promiscuo

Diccionario

promiscuo



## promiscuo, promiscua

*adjetivo*

1. Que está mezclado de forma confusa o indiferente.  
"apunta el psiquiatra que la tensión agresiva del paciente aumenta, debido a la suma de las agresividades patológicas individuales y a las que generan las presencias promiscuas e indeseadas de los otros"
2. Que denota promiscuidad sexual.  
"conducta sexual promiscua"

# ARP Discovery

arp						
No.	Time	Source	Destination	Protocol	Length	Info
177	21.63191...	IntelCor_da:40...	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.13
230	24.94750...	IntelCor_da:40...	Broadcast	ARP	42	Who has 192.168.0.3? Tell 192.168.0.13
231	25.00512...	Sagemcom_48:75...	IntelCor_da:40...	ARP	42	192.168.0.3 is at b0:b2:8f:48:75:ba
383	92.12674...	HonHaiPr_7d:76...	Broadcast	ARP	42	Who has 192.168.0.104? Tell 192.168.0.4

▶	Frame 230: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼	Ethernet II, Src: IntelCor_da:40:bc (18:5e:0f:da:40:bc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶	Destination: Broadcast (ff:ff:ff:ff:ff:ff)
▶	Source: IntelCor_da:40:bc (18:5e:0f:da:40:bc)
	Type: ARP (0x0806)
▼	Address Resolution Protocol (request)
	Hardware type: Ethernet (1)
	Protocol type: IPv4 (0x0800)
	Hardware size: 6
	Protocol size: 4
	Opcode: request (1)
	Sender MAC address: IntelCor_da:40:bc (18:5e:0f:da:40:bc)
	Sender IP address: 192.168.0.13
	Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
	Target IP address: 192.168.0.3

# ARP Discovery (2)

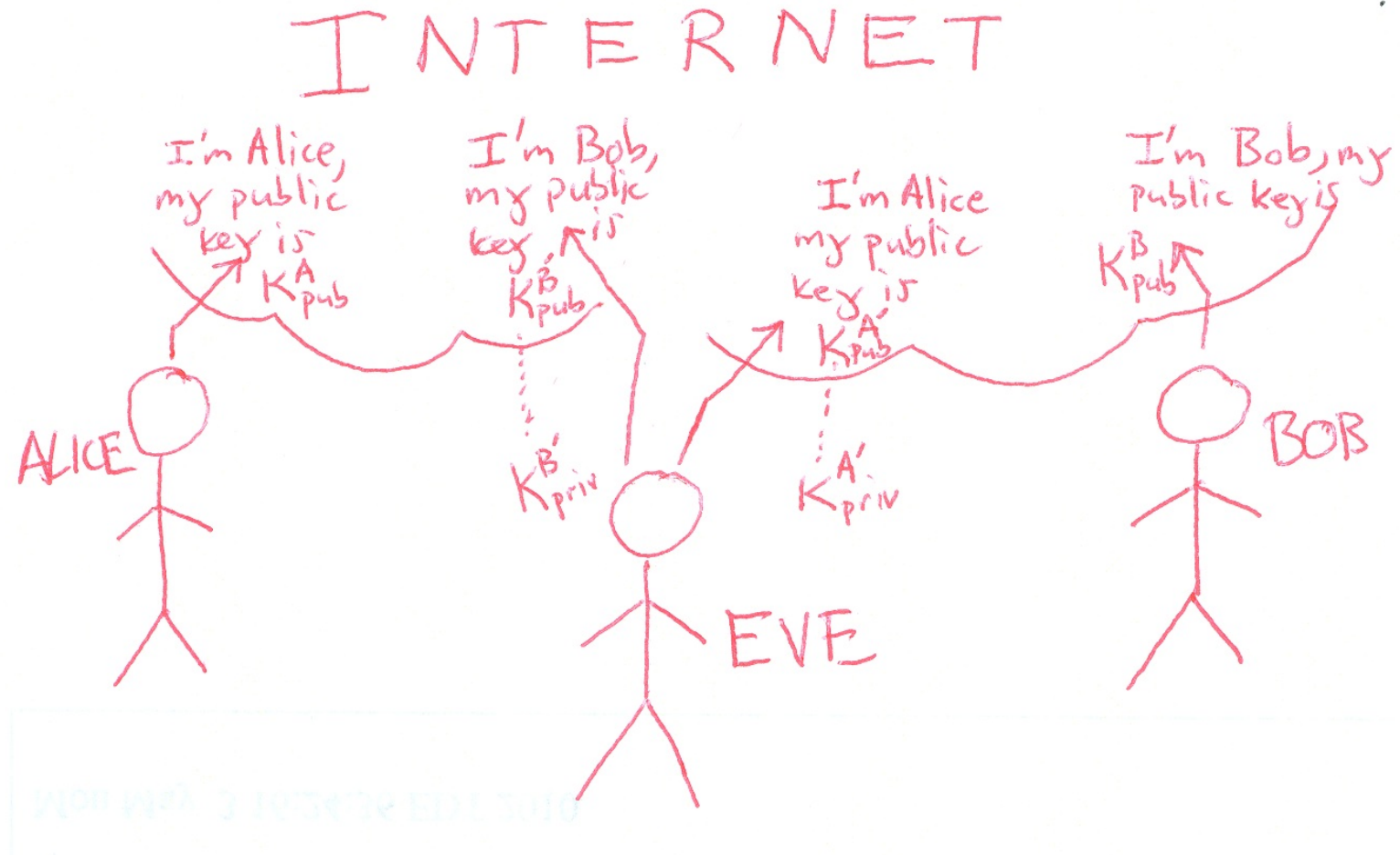
arp						
No.	Time	Source	Destination	Protocol	Length	Info
177	21.63191...	IntelCor_da:40...	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.13
230	24.94750...	IntelCor_da:40...	Broadcast	ARP	42	Who has 192.168.0.3? Tell 192.168.0.13
231	25.00512...	Sagemcom_48:75...	IntelCor_da:40...	ARP	42	192.168.0.3 is at b0:b2:8f:48:75:ba
383	92.12674...	HonHaiPr_7d:76...	Broadcast	ARP	42	Who has 192.168.0.104? Tell 192.168.0.4

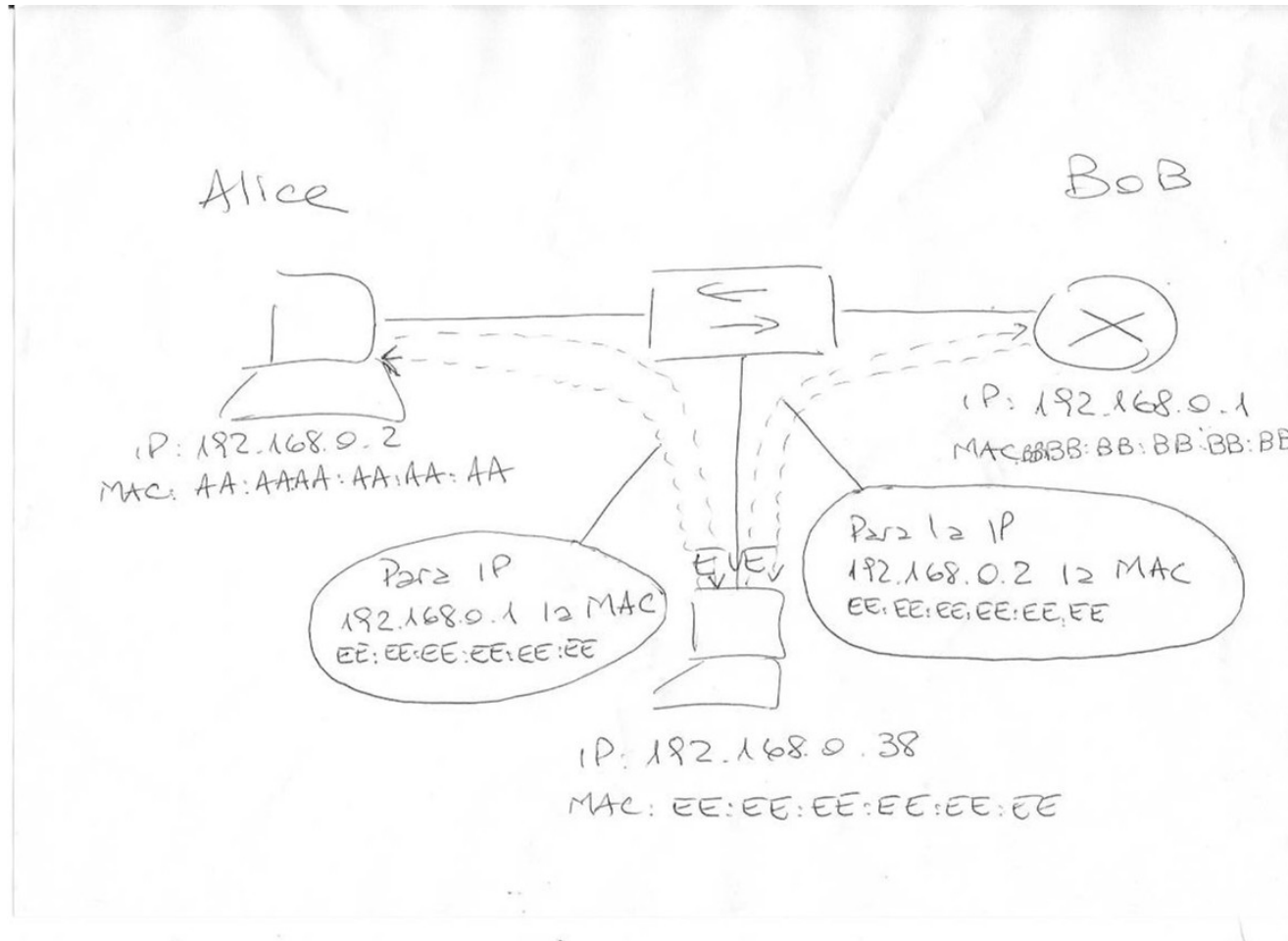
▶	Frame 231: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼	Ethernet II, Src: Sagemcom_48:75:ba (b0:b2:8f:48:75:ba), Dst: IntelCor_da:40:bc (18:5e:0f:da:40:bc) <ul style="list-style-type: none"><li>▶ Destination: IntelCor_da:40:bc (18:5e:0f:da:40:bc)</li><li>▶ Source: Sagemcom_48:75:ba (b0:b2:8f:48:75:ba)</li><li>Type: ARP (0x0806)</li></ul>
▼	Address Resolution Protocol (reply) <ul style="list-style-type: none"><li>Hardware type: Ethernet (1)</li><li>Protocol type: IPv4 (0x0800)</li><li>Hardware size: 6</li><li>Protocol size: 4</li><li>Opcode: reply (2)</li><li>Sender MAC address: Sagemcom_48:75:ba (b0:b2:8f:48:75:ba)</li><li>Sender IP address: 192.168.0.3</li><li>Target MAC address: IntelCor_da:40:bc (18:5e:0f:da:40:bc)</li><li>Target IP address: 192.168.0.13</li></ul>



# Man-In-The-Middle (MITM)



# ARP Spoofing





# Modificación de Tráfico HTTP

