

Manual de usuario

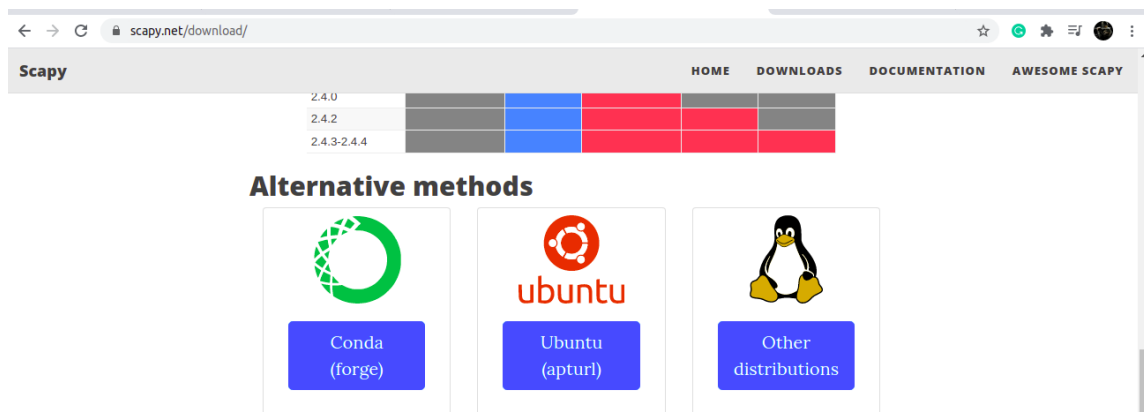
Punto 5. Captura de tramas

1. Requerimientos del programa:

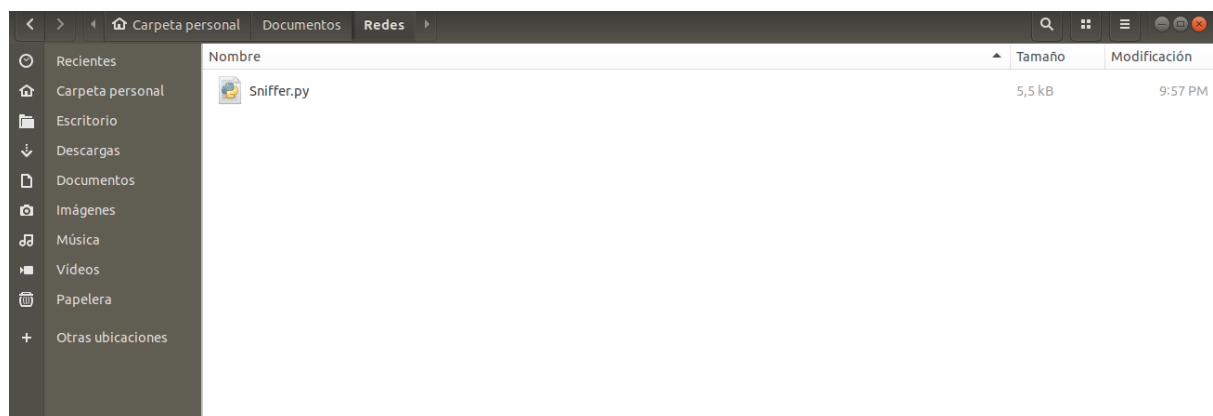
- Sistema operativo basado en Linux
- Scapy (herramienta de manipulación de paquetes para redes de computadoras)

2. Ejecución del programa:

- Para ejecutar el programa es importante tener instalado el programa de manipulación de paquetes “[Scapy](#)”
Instalaremos la versión que se acomode a nuestro sistema operativo basado en Linux



- A continuación descargamos el archivo “Sniffer.py” el cuál está anexo a este manual o directo desde el link de [github](#)



- Esta es una aplicación diseñada para la consola, entonces procedemos a entrar a la ubicación del archivo “Sniffer.py”

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$ ls
Sniffer.py
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$
```

- A continuación usando el comando << sudo -E python3 Sniffer.py >> ejecutaremos el archivo

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~$ cd Documentos/Redes/
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$ sudo -E python3
Sniffer.py
[sudo] contraseña para sebastian:
---Sniffer De Red---

Ingrese el nombre de la interfaz de red:
```

- Para este punto, el programa ya estará corriendo y listo para ser utilizado

3. Funcionamiento:

- El programa mostrará instrucciones paso a paso para el correcto funcionamiento del programa

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~$ cd Documentos/Redes/
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$ sudo -E python3
Sniffer.py
[sudo] contraseña para sebastian:
---Sniffer De Red---

Ingresa el nombre de la interfaz de red: █
```

- Aquí tendremos que ingresar el nombre de la interfaz de red a analizar, para obtener el nombre se recomienda usar el comando << ip link show >>

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
   group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
   de DEFAULT group default qlen 1000
    link/ether 8c:16:45:14:29:2a brd ff:ff:ff:ff:ff:ff
```

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~$ cd Documentos/Redes/
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$ sudo -E python3
Sniffer.py
[sudo] contraseña para sebastian:
---Sniffer De Red---

Ingrese el nombre de la interfaz de red: enp1s0
La red "enp1s0" será analizada

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: █
```

- En este punto podremos ver el menú principal donde podremos escoger si queremos salir de la aplicación o acceder a alguna de las funciones que tiene el programa

3.1 Opción 1 - Sniffing de paquetes por protocolo

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
---Sniffer De Red---

Ingrese el nombre de la interfaz de red: enp1s0
La red "enp1s0" será analizada

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: 1

Protocolos aceptados:
  Ethernet (ether)
  Wireless LAN (wlan)
  Internet protocolo (ip)
  IPv6 (ip6)
  Address Resolution Protocol (arp)
  Reverse ARP (rarp)
  Transmission Control Protocol (tcp)
  User Datagram Protocol (udp)
  Internet Control Message Protocol (icmp)

Ingresa el protocolo que desees filtrar: █
```

- Esta función nos permitirá filtrar los paquetes de un protocolo específico de nuestra elección. Lo primero que se verá al seleccionar esta opción es una lista de los protocolos disponibles para analizar; aquí tendremos que escribir el acrónimo del protocolo que queramos observar

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
Ingrese el nombre de la interfaz de red: enp1s0
La red "enp1s0" será analizada

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: 1

Protocolos aceptados:
  Ethernet (ether)
  Wireless LAN (wlan)
  Internet protocolo (ip)
  IPv6 (ip6)
  Address Resolution Protocol (arp)
  Reverse ARP (rarp)
  Transmission Control Protocol (tcp)
  User Datagram Protocol (udp)
  Internet Control Message Protocol (icmp)

Ingresa el protocolo que desees filtrar: tcp
Quieres ver toda la información de cada paquete? (Y/N):
```

- En este punto nos dará a escoger si queremos una versión resumida o una versión completa de los detalles del paquete. A manera de ejemplo veremos primero la versión resumida de paquetes del protocolo **tcp**.

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: 1

Protocolos aceptados:
  Ethernet (ether)
  Wireless LAN (wlan)
  Internet protocolo (ip)
  IPv6 (ip6)
  Address Resolution Protocol (arp)
  Reverse ARP (rarp)
  Transmission Control Protocol (tcp)
  User Datagram Protocol (udp)
  Internet Control Message Protocol (icmp)

Ingresa el protocolo que desees filtrar: tcp
Quieres ver toda la información de cada paquete? (Y/N): N
Se analizarán 50 paquetes, quieres cambiar ese número? (Y/N):
```

- Después (sin importar la opción que escojamos) se nos preguntará cuántos paquetes se quieren analizar. De manera predeterminada, se analizarán 50 paquetes pero se puede escoger una cantidad personalizada.

Luego se mostrará los resultados del análisis de paquetes:

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
Address Resolution Protocol (arp)
Reverse ARP (rarp)
Transmission Control Protocol (tcp)
User Datagram Protocol (udp)
Internet Control Message Protocol (icmp)

Ingresa el protocolo que desees filtrar: tcp

Quieres ver toda la información de cada paquete? (Y/N): N

Se analizarán 50 paquetes, quieres cambiar ese número? (Y/N): Y
Ingresa el número de paquetes que quieres analizar: 10
Ether / IP / TCP 192.168.0.36:56666 > 142.250.78.3:https A
Ether / IP / TCP 192.168.0.36:54208 > 142.250.78.142:https PA / Raw
Ether / IP / TCP 192.168.0.36:54208 > 142.250.78.142:https PA / Raw
Ether / IP / TCP 192.168.0.36:54208 > 142.250.78.142:https PA / Raw
Ether / IP / TCP 192.168.0.36:54208 > 142.250.78.142:https PA / Raw
Ether / IP / TCP 192.168.0.36:54208 > 142.250.78.142:https PA / Raw
Ether / IP / TCP 142.250.78.142:https > 192.168.0.36:54208 A
Ether / IP / TCP 142.250.78.142:https > 192.168.0.36:54208 A
Ether / IP / TCP 142.250.78.142:https > 192.168.0.36:54208 PA / Raw
Ether / IP / TCP 142.250.78.142:https > 192.168.0.36:54208 A
<Sniffed: TCP:10 UDP:0 ICMP:0 Other:0>
```

- Funciona de manera similar si queremos ver la versión completa de los detalles de los paquetes. Simplemente tendremos que escoger “Y” cuando nos pregunten si queremos ver la información completa de cada paquete.

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
Address Resolution Protocol (arp)
Reverse ARP (rarp)
Transmission Control Protocol (tcp)
User Datagram Protocol (udp)
Internet Control Message Protocol (icmp)

Ingresa el protocolo que desees filtrar: udp

Quieres ver toda la información de cada paquete? (Y/N): Y

Se analizarán 50 paquetes, quieres cambiar ese número? (Y/N): Y
Ingresa el número de paquetes que quieres analizar: 1
###[ Ethernet ]###
  dst      = e0:88:5d:d8:d8:bb
  src      = 8c:16:45:14:29:2a
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 61
  id       = 30498
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = udp
  chksum   = 0xa8b9
  src      = 192.168.0.36
  dst      = 172.217.173.46
  options  \
###[ UDP ]###
  sport    = 34676
  dport    = 443
  len      = 41
  chksum   = 0x1b0f
###[ Raw ]###
  load     = b'\\\xe4_0\xb5\xf4)\xbel\x1aa\xd8`Qs\xc5&\x07b\x0f\xac\xaa\x01A:\x9b\x81\xdfV \xcd`8'
<Sniffed: TCP:0 UDP:1 ICMP:0 Other:0>
```

3.2 Opción 2 - Sniffing de todos los paquetes

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~$ cd Documentos/Redes/
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$ sudo -E python3
Sniffer.py
[sudo] contraseña para sebastian:
---Sniffer De Red---

Ingresa el nombre de la interfaz de red: enp1s0
La red "enp1s0" será analizada

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: 2

Quieres ver toda la información de cada paquete? (Y/N):
```

- Esta función muestra todos los paquetes sin importar el protocolo. De manera similar a la función vista anteriormente, en este punto se nos dará a escoger si queremos una versión resumida o una versión completa de los detalles de los paquetes.

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda
sebastian@sebastian-Lenovo-ideapad-320-15IKB:~/Documentos/Redes$ sudo -E python3
Sniffer.py
---Sniffer De Red---

Ingresa el nombre de la interfaz de red: enp1s0
La red "enp1s0" será analizada

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: 2

Quieres ver toda la información de cada paquete? (Y/N): N

Se analizarán 50 paquetes, quieres cambiar ese número? (Y/N): Y
Ingresa el número de paquetes que quieres analizar:
```

- Después (sin importar la opción que escojamos) se nos preguntará cuántos paquetes se quieren analizar. De manera predeterminada, se analizarán 50 paquetes pero se puede escoger una cantidad personalizada. Luego se mostrará los resultados del análisis de paquetes:

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: 2

Quieres ver toda la información de cada paquete? (Y/N): N

Se analizarán 50 paquetes, quieres cambiar ese número? (Y/N): Y
Ingresa el número de paquetes que quieres analizar:10
Ether / IP / TCP 192.168.0.36:44170 > 172.217.172.14:https A
Ether / IP / UDP 192.168.0.36:35710 > 142.250.78.14:443 / Raw
Ether / IP / UDP 192.168.0.36:35710 > 142.250.78.14:443 / Raw
Ether / IP / UDP 192.168.0.36:35710 > 142.250.78.14:443 / Raw
Ether / IP / UDP 192.168.0.36:35710 > 142.250.78.14:443 / Raw
Ether / IP / UDP 192.168.0.36:35710 > 142.250.78.14:443 / Raw
Ether / IP / UDP 192.168.0.36:35710 > 142.250.78.14:443 / Raw
Ether / IP / TCP 172.217.172.14:https > 192.168.0.36:44170 A
Ether / IP / UDP 142.250.78.14:443 > 192.168.0.36:35710 / Raw
Ether / IP / UDP 142.250.78.14:443 > 192.168.0.36:35710 / Raw
<Sniffed: TCP:2 UDP:8 ICMP:0 Other:0>
```

- Al igual que en la función anterior, si queremos ver la versión completa de los detalles de los paquetes. Simplemente tendremos que escoger “Y” cuando nos pregunten si queremos ver la información completa de cada paquete.

```
sebastian@sebastian-Lenovo-ideapad-320-15IKB: ~/Documentos/Redes
Archivo Editar Ver Buscar Terminal Ayuda

Selecciona una opción:
  1. Analizar paquetes de un protocolo en específico
  2. Analizar todos los paquetes de cualquier protocolo
  3. Salir

Escoge una opción: 2

Quieres ver toda la información de cada paquete? (Y/N): Y

Se analizarán 50 paquetes, quieres cambiar ese número? (Y/N): Y
Ingresa el número de paquetes que quieres analizar: 1
###[ Ethernet ]###
  dst      = e0:88:5d:d8:d8:bb
  src      = 8c:16:45:14:29:2a
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 61
  id       = 34464
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = udp
  checksum = 0x6bc3
  src      = 192.168.0.36
  dst      = 173.194.217.189
  \options \
###[ UDP ]###
  sport    = 60033
  dport    = 443
  len      = 41
  checksum = 0x4887
###[ Raw ]###
  load     = b'S\xc2\xed\x87C\x9a\x8f\x70\xadt*\xde\x99\xe8\xf1I\xdf\x02\xa5\xb8\xe2bb3a\xacV\xb4g?'
<Sniffed: TCP:0 UDP:1 ICMP:0 Other:0>
```