



Informe laboratorio 3

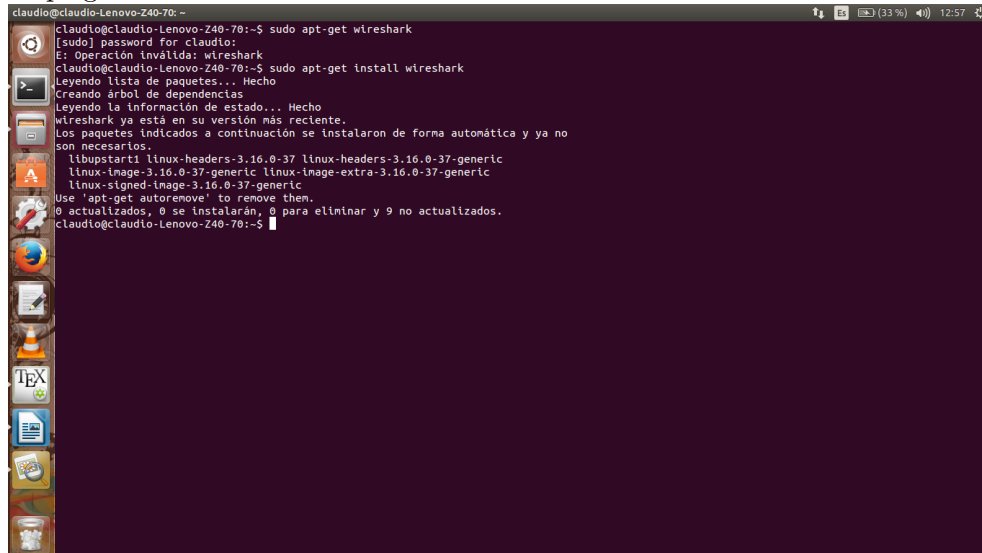
Claudio Carrillo, Martin Morice, Raul Flores.
Profesor: Jaime Alvarez—ayudante: Alexis Inzunza

14 de abril de 2016

Parte I

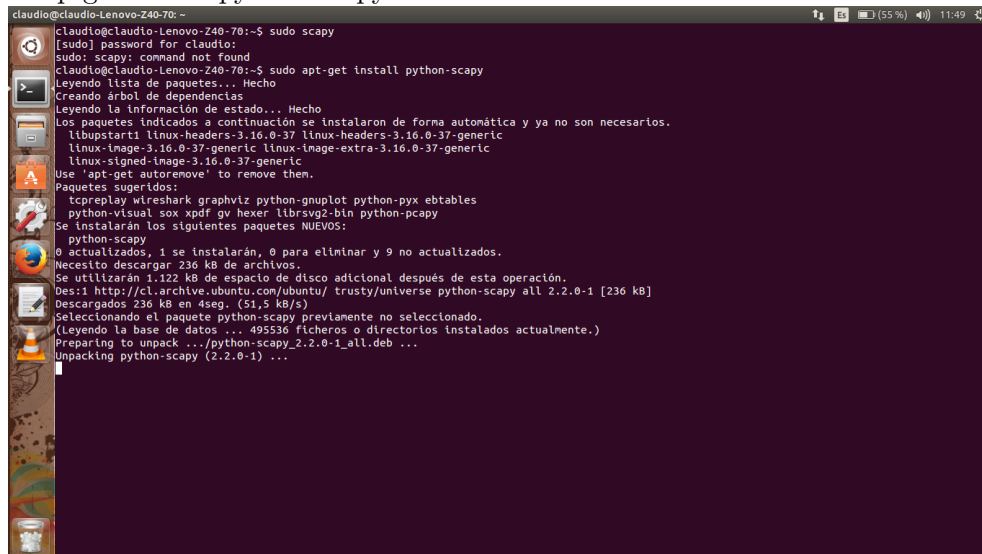
instalacion de scapy y wireshark

Para instalar whireshark en ubuntu es necesario abrir el terminal e ingresar el siguiente comando:
sudo apt-get install wireshark



```
claudio@claudio-Lenovo-240-70:~$ sudo apt-get install wireshark
[sudo] password for claudio:
E: Operación inválida: wireshark
claudio@claudio-Lenovo-240-70:~$ sudo apt-get install wireshark
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Wireshark ya está en su versión más reciente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
libpcap1 linux-headers-3.16.0-37 linux-headers-3.16.0-37-generic
linux-image-3.16.0-37-generic linux-image-extra-3.16.0-37-generic
linux-signed-image-3.16.0-37-generic
Use 'apt-get autoremove' to remove them.
0 actualizados, 0 se instalarán, 0 para eliminar y 9 no actualizados.
claudio@claudio-Lenovo-240-70:~$
```

luego para instalar scapy en una terminal se ingresa el siguiente comando
sudo apt-get install python-scapy



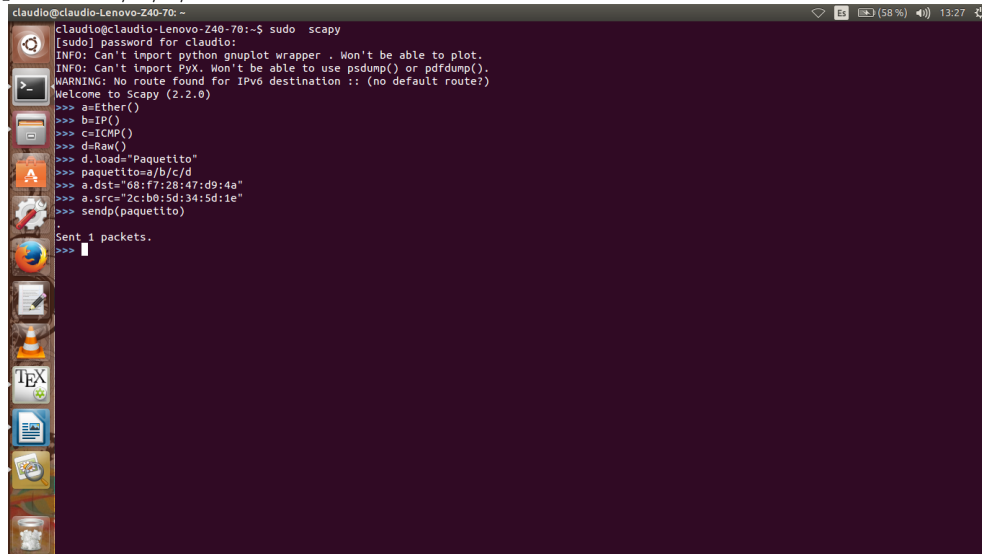
```
claudio@claudio-Lenovo-240-70:~$ sudo apt-get install python-scapy
[sudo] password for claudio:
E: scapy: command not found
claudio@claudio-Lenovo-240-70:~$ sudo apt-get install python-scapy
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
libpcap1 linux-headers-3.16.0-37 linux-headers-3.16.0-37-generic
linux-image-3.16.0-37-generic linux-image-extra-3.16.0-37-generic
linux-signed-image-3.16.0-37-generic
Use 'apt-get autoremove' to remove them.
Paquetes sugeridos:
tcpdump wireshark graphviz python-gnuplot python-pygments
python-virtualenv python-pygments python-pygments
se instalarán los siguientes paquetes NUEVOS:
python-scapy
0 actualizados, 1 se instalarán, 0 para eliminar y 9 no actualizados.
Necesito descargar 236 kB de archivos.
Se utilizarán 1.122 kB de espacio de disco adicional después de esta operación.
Des:1 http://cl.archive.ubuntu.com/ubuntu/ trusty/universe python-scapy all 2.2.0-1 [236 kB]
Descargados 236 kB en 4seg. (51,5 kB/s)
Seleccionando el paquete python-scapy previamente no seleccionado.
(Leyendo la base de datos ... 495536 ficheros o directorios instalados actualmente.)
Preparing to unpack .../python-scapy_2.2.0-1_all.deb ...
Unpacking python-scapy (2.2.0-1) ...
```

Parte II

creando un frame

procedemos a crear el frame

lo primero que hicimos fue asignar una variable a igualandola a la funcion ether(), para asi poder manipularla y poder darle nuestros propios valores, despues creamos otra variable de nombre b y le asignamos IP(), luego asignamos la variable c (que simula la capa de transporte) a el comando ICMP(), en segimiento asignamos a raw() la variable d, y agreagmos la direcion de destino y salida a la variable a, y por ultimo unimos el todas las variables al frame en si a traves de el siguiente comndo: `paquetito=a/b/c/d`.

A screenshot of a Linux terminal window. The window title is 'claudio@claudio-Lenovo-240-70: ~'. The user has run 'sudo scapy' and entered their password. The terminal shows the Scapy 2.2.0 welcome message and several commands being executed in a Python shell: 'a=Ether()', 'b=IP()', 'c=ICMP()', 'd=Raw()', 'd.load("Paquetito")', 'paquetito=a/b/c/d', 'a.dst="68:f7:28:47:d9:4a"', 'a.src="2c:b0:5d:34:5d:1e"', and 'sendp(paquetito)'. The output shows 'Sent 1 packets.' and a prompt for more commands. The terminal has a dark purple background. On the left side of the terminal window, there is a vertical dock with various application icons including a file manager, web browser, and office applications like LibreOffice and TeX.

Parte III

enviado y recepcion

luego en ocupamos el comando sendp para enviar el frame.

```
claudio@claudio-Lenovo-Z40-70:~$ sudo scapy
[sudo] password for claudio:
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> a=Ether()
>>> b=IP()
>>> c=ICMP()
>>> d=Raw()
>>> d.load="Paquetito"
>>> paquetito=a/b/c/d
>>> a.dst="68:f7:28:47:d9:4a"
>>> a.src="2c:b0:5d:34:5d:1e"
>>> sendp(paquetito)
Sent 1 packets.
>>> ls(a)
dst      : DestMACField      = '68:f7:28:47:d9:4a' (None)
src      : SourceMACField   = '2c:b0:5d:34:5d:1e' (None)
type     : XShortEnumField  = 0
a.dst    : 'ff:ff:ff:ff:ff:ff'
>>> sendp(paquetito)
Sent 1 packets.
>>> ls(a)
dst      : DestMACField      = 'ff:ff:ff:ff:ff:ff' (None)
src      : SourceMACField   = '2c:b0:5d:34:5d:1e' (None)
type     : XShortEnumField  = 0
a.dst    : '98:k5:12:32:p4:5d'
>>> sendp(paquetito)
Sent 1 packets.
>>>
```

aqui precentamos el envio del paquete

Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: icmp Expression... Clear Apply Guardar

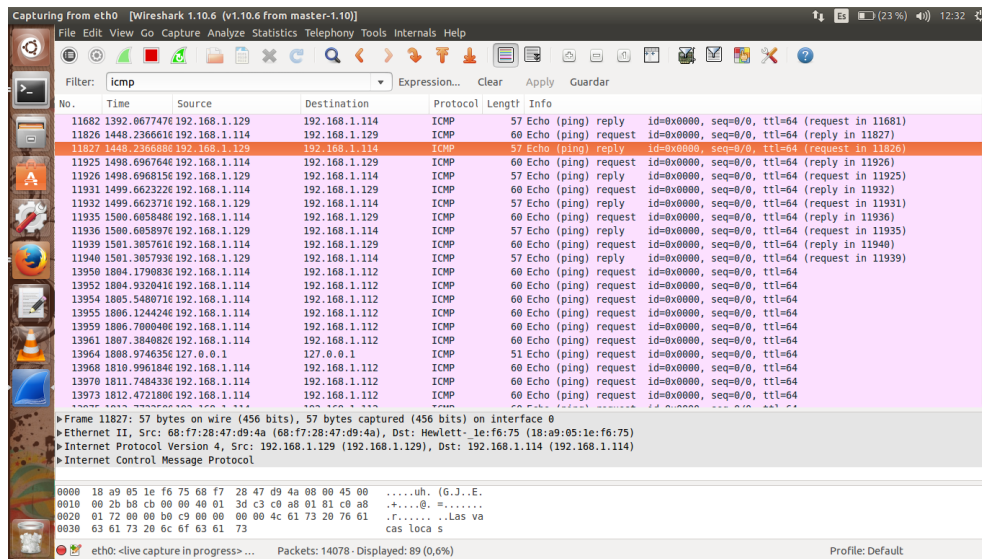
No.	Time	Source	Destination	Protocol	Length	Info
11925	1498.6967646	192.168.1.114	192.168.1.129	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 11926)
11926	1498.6968156	192.168.1.129	192.168.1.114	ICMP	57	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 11925)
11931	1499.6623226	192.168.1.114	192.168.1.129	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 11932)
11932	1499.6623716	192.168.1.129	192.168.1.114	ICMP	57	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 11931)
11935	1500.6058408	192.168.1.114	192.168.1.129	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 11936)
11936	1500.6059976	192.168.1.129	192.168.1.114	ICMP	57	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 11935)
11939	1501.3857616	192.168.1.114	192.168.1.129	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 11940)
11940	1501.3857936	192.168.1.129	192.168.1.114	ICMP	57	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 11939)
13950	1804.1790836	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13952	1804.9320416	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13954	1805.5480716	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13955	1806.1244248	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13959	1806.7000408	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13961	1807.3840826	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13964	1808.9746356	127.0.0.1	127.0.0.1	ICMP	51	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13968	1810.9961846	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13970	1811.7484336	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13973	1812.4721806	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13975	1813.7722506	192.168.1.114	192.168.1.112	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13982	1813.9922006	127.0.0.1	127.0.0.1	ICMP	51	Echo (ping) request id=0x0000, seq=0/0, ttl=64
13994	1822.2995936	127.0.0.1	127.0.0.1	ICMP	51	Echo (ping) request id=0x0000, seq=0/0, ttl=64

Frame 13982: 51 bytes on wire (408 bits), 51 bytes captured (408 bits) on interface 0
Ethernet II, Src: Netgear 34:5d:1e (2c:b0:5d:34:5d:1e), Dst: 68:f7:28:47:d9:4a (68:f7:28:47:d9:4a)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
Internet Control Message Protocol

0000 68 f7 28 47 d9 4a 2c b0 5d 34 5d 1e 08 00 45 00 h.(G.J.. [4]...E.
0010 00 25 00 01 00 00 40 01 7c d5 7f 00 00 01 7f 00 .%....@. |.....
0020 00 01 00 00 f8 3f 00 00 00 00 50 61 71 75 65 747... ..Paquet
0030 09 74 6f ito

eth0: <live capture in progress>... Packets: 14120 - Displayed: 89 (0,6%) Profile: Default

y aqui la recepcion de un paquete



0.1. por medio del hub

al enviarse un frame por medio del hub este le manda una copia a todos los computadores conectados a el, y el que tenga la mac de destino o puede abrir en los demas les llega pero no los pueden leer.

0.2. por medio del switch

la principal diferencia del switch con el hub es que el switch no replica el mensaje a todos los servidores conectados, solo lo envia al servidor con la mac de destino.

Parte IV

respuestas cuestionario

1- Se produce un envio broadcast que significa que la informacion de el paquete sera enviada a todos los canales de la red.

2-Depende de si la red tiene como nucleo central un switch o un hub, si es un switch el paquete sera enviado directamente al pc que tenga la mac de destino, por que el switch tiene identificados los pc y sus respectivas ip y mac, por lo que envia directamente.

Por otro lado si fuera un hub se utilizaria algo parecido a un broadcast, se enviaria a todos los pc hasta encontrar al que sea poseedor de la mac de destino.

3-Si uno envia algo a una mac inexistente en el sistema, el frame se envia igual sin poder llegar a el destino estimado.

Cualquier persona facilmente crear una mascara con la mac de destino del frame anterior y asi interceptar dicho frame.