



Seguridad en Redes TP – Análisis de Protocolos con Wireshark

1. Objetivo

El objetivo de este trabajo práctico es proporcionar los elementos básicos de Wireshark para que el alumno pueda trabajar realizando análisis de protocolos en los trabajos prácticos posteriores de la materia.

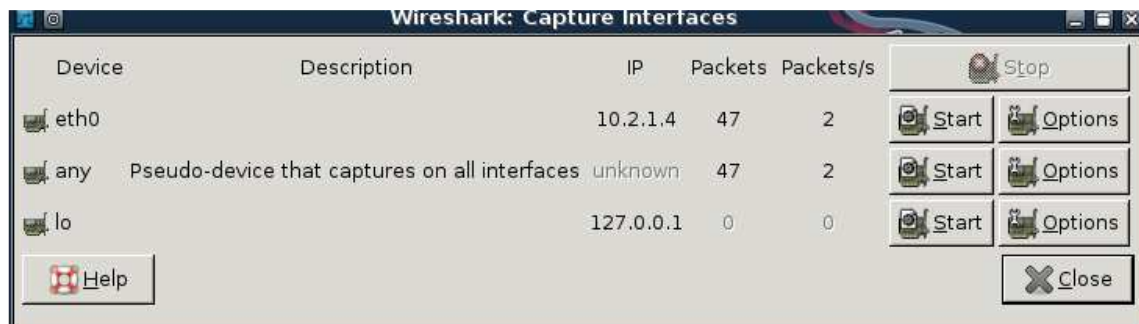
Wireshark

El *Wireshark* es un *sniffer*, es decir, un programa que al ejecutarse va copiando todos los frames que llegan a este host. Se encuentra incluido en la mayoría de las distribuciones de Linux, y también puede descargarse gratuitamente de www.wireshark.org

Este software nos resultará útil para la práctica de laboratorio, donde deberemos analizar protocolos de aplicación.

Para ilustrar su uso, realizaremos un ejemplo con el protocolo de aplicación POP.

Mediante el menú *Capture – Interfaces* podemos comenzar a “escuchar” la red y buscar la información que nos interesa. El programa presentará la siguiente pantalla:



Acá debemos seleccionar la interfaz sobre la que queremos trabajar (Ej: `eth0`) y presionar *Start* para comenzar.

Ahora se deberán iniciar las acciones correspondientes al protocolo que se quiere analizar. En este ejemplo nos conectamos al demonio POP que se encuentra corriendo en la misma máquina donde estamos, o sea, el *localhost* (127.0.0.1).

Al presionar el botón *Stop*,

No. .	Time	Source	Destination	Protocol	Info
167	14.585478	Cisco_69:cc:7a	PVST+	STP	Conf. Root = 24882
168	14.770160	10.1.9.172	10.3.106.120	TPKT	Continuation
169	14.797082	Cisco_69:cc:7a	PVST+	STP	Conf. Root = 24777
170	14.962554	10.3.106.120	10.1.9.172	TCP	54158 > ms-wbt-ser
171	14.968809	10.3.106.137	10.3.106.255	NBNS	Name querv NB S416

se obtiene la siguiente pantalla:

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	1186 > ipp [SYN] Seq=3225979958 Ack=0 Win=32767 Len=0
2	0.000032	127.0.0.1	127.0.0.1	TCP	ipp > 1186 [RST, ACK] Seq=0 Ack=3225979959 Win=0 Len=0
3	2.369983	127.0.0.1	127.0.0.1	TCP	1187 > pop3 [SYN] Seq=3242372805 Ack=0 Win=32767 Len=0
4	2.370024	127.0.0.1	127.0.0.1	TCP	pop3 > 1187 [SYN, ACK] Seq=3241238267 Ack=3242372806 Win=32767 Len=0
5	2.370052	127.0.0.1	127.0.0.1	TCP	1187 > pop3 [ACK] Seq=3242372806 Ack=3241238268 Win=32767 Len=0
6	2.378740	127.0.0.1	127.0.0.1	POP	Response: +OK POP3 intoxicada v2001.78rh server ready
7	2.378775	127.0.0.1	127.0.0.1	TCP	1187 > pop3 [ACK] Seq=3242372806 Ack=3241238313 Win=32767 Len=0
8	5.009975	127.0.0.1	127.0.0.1	TCP	1188 > ipp [SYN] Seq=3238539845 Ack=0 Win=32767 Len=0
9	5.010008	127.0.0.1	127.0.0.1	TCP	ipp > 1188 [RST, ACK] Seq=0 Ack=3238539846 Win=0 Len=0
10	7.032906	127.0.0.1	127.0.0.1	POP	Request: USER telnetuser
11	7.033048	127.0.0.1	127.0.0.1	TCP	pop3 > 1187 [ACK] Seq=3241238313 Ack=3242372823 Win=32767 Len=0
12	7.033191	127.0.0.1	127.0.0.1	POP	Response: +OK User name accepted, password please
13	7.033202	127.0.0.1	127.0.0.1	TCP	1187 > pop3 [ACK] Seq=3242372823 Ack=3241238354 Win=32767 Len=0
14	10.019969	127.0.0.1	127.0.0.1	TCP	1189 > ipp [SYN] Seq=3245453405 Ack=0 Win=32767 Len=0
15	10.020001	127.0.0.1	127.0.0.1	TCP	ipp > 1189 [RST, ACK] Seq=0 Ack=3245453406 Win=0 Len=0
16	11.392922	127.0.0.1	127.0.0.1	POP	Request: PASS telnetuser
17	11.407402	127.0.0.1	127.0.0.1	POP	Response: +OK Mailbox open, 3 messages

[x] Frame 1 (74 bytes on wire, 74 bytes captured)
 [x] Ethernet II, Src: 00:00:00:00:00:00, Dst: 00:00:00:00:00:00
 [x] Internet Protocol, Src Addr: 127.0.0.1 (127.0.0.1), Dst Addr: 127.0.0.1 (127.0.0.1)
 [x] Transmission Control Protocol, Src Port: 1186 (1186), Dst Port: ipp (631), Seq: 3225979958, Ack: 0, Len: 0

En cada línea de la parte superior podemos ver cada frame que Ethereal levanto de la interfase. Las columnas son: número de paquete, un *timestamp*, dirección de origen, dirección de destino, protocolo, y un resumen de la información que contiene el frame.

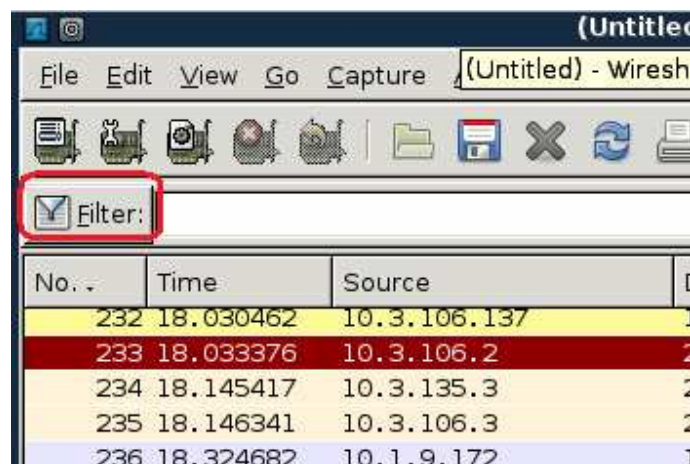
En la parte central observamos que hay cuatro o cinco líneas por cada frame seleccionado en la parte superior. Cada una de estas líneas corresponde a los protocolos usados de las distintas capas del modelo TCP/IP.

En nuestro caso sólo nos interesa la línea inferior, que es la que corresponde a la capa de aplicación (inmediatamente debajo de "TCP").

En la parte inferior se encuentra el *dump* del frame tanto en hexadecimal como en ASCII.

Tal como se encuentra, la captura realizada presenta la información que no nos es de utilidad en este momento:

FILTRO: Si sólo nos interesa ver la información correspondiente al protocolo POP, podemos aplicar un filtro de información. Al presionar el botón *Filter*, que se encuentra en la esquina superior izquierda.



se abre la siguiente ventana:



Acá podemos escribir filtros complejos, usando expresiones lógicas e información de los protocolo/s que queramos analizar.

Sin embargo, nosotros sólo necesitamos filtrar el protocolo POP. Para esto alcanza con completar la caja de texto que está al lado del botón **Filter** en la pantalla principal con la expresión "pop"

(sin las comillas y con minúscula) y presionar el botón `Apply`. Así obtendremos la siguiente información:

No. -	Time	Source	Destination	Protocol	Info
6	2.378740	127.0.0.1	127.0.0.1	POP	Response: +OK POP3 intoxicada v2001.78rh server ready
10	7.052606	127.0.0.1	127.0.0.1	POP	Request: USER telnetuser
12	7.053191	127.0.0.1	127.0.0.1	POP	Response: +OK User name accepted, password please
16	11.392922	127.0.0.1	127.0.0.1	POP	Request: PASS telnetuser
17	11.407402	127.0.0.1	127.0.0.1	POP	Response: +OK Mailbox open, 3 messages
19	13.424464	127.0.0.1	127.0.0.1	POP	Request: LIST
20	13.424658	127.0.0.1	127.0.0.1	POP	Response: +OK Mailbox scan listing follows
24	17.355250	127.0.0.1	127.0.0.1	POP	Request: QUIT
25	17.356384	127.0.0.1	127.0.0.1	POP	Response: +OK Sayonara

.....

Frame 10 (83 bytes on wire, 83 bytes captured)
 Ethernet II, Src: 00:00:00:00:00:00, Dst: 00:00:00:00:00:00
 Internet Protocol, Src Addr: 127.0.0.1 (127.0.0.1), Dst Addr: 127.0.0.1 (127.0.0.1)
 Transmission Control Protocol, Src Port: 1187 (1187), Dst Port: pop3 (110), Seq: 3242372806, Ack: 3241238313, Len: 17
 Post Office Protocol
 Request: USER
 Request Arg: telnetuser

Expandiendo la quinta línea, como se muestra en la figura, podemos ver la información correspondiente al protocolo que queremos analizar.

CONSEJOS:

Tal vez necesite filtrar paquetes por dirección IP de origen y destino además de por protocolo.

Si se quiere hacer el seguimiento de una conexión

Se puede configurar rápidamente la opción “Conversation Filter” o la opción “Follow TCP Stream

1	0.000000	10.3.106.120	10.1.9.172	CP	54158 > ms-wbt
2	0.190597	10.3.135.3	10.1.9.172	HSRP	Hello (state S
3	0.191431	10.3.106.3	10.1.9.172	HSRP	Hello (state S
4	0.363542	10.3.106.2	10.1.9.172	IMv2	Assert
5	0.365559	10.3.106.3	10.1.9.172	IMv2	Assert
6	0.368512	10.1.9.172	10.1.9.172	PKT	Continuation
7	0.522452	10.3.135.2	10.1.9.172	Ethernet	state Ar
8	0.537621	Cisco_69:cc:7	10.1.9.172	IP	pot = 2
9	0.560359	10.3.106.120	10.1.9.172	TCP	ms-wbt:
10	0.806387	10.1.9.172	10.1.9.172	UDP	ation
11	0.843397	Cisco_69:cc:7	10.1.9.172	UDP	pot = 2
12	0.997784	10.3.106.120	10.1.9.172	PN-CBA Server	ms-wbt:

Filtros por MAC `eth.addr == 00:78:AC:...`