Monitoreo de Red con WireShark

Diseño y Evaluación de Configuraciones

Curso 2010-11

Miguel Telleria de Esteban

`telleriam AT unican.es`

Computadores y Tiempo Real

http://www.ctr.unican.es

Características de Wireshark

- Capturador y analizador de paquetes (sniffer) que entiende multitud de protocolos
  - Es visual e interactivo
- Utiliza la **librería pcap** al igual que *tcpdump* y otras herramientas
- Requiere permisos de root para capturar paquetes,
  - No es necesario ser root para analizarlos datos
- Multiplataforma (Linux / Windows).
  - En windows no se puede capturar localhost.
- Permite exportar datos de capturas a otros formatos (.csv, xml) para ser post-procesados.

Filtros de captura: Sintaxis TCPdump

- El filtro de captura comparte la sintaxis de tcpdump
  - [src | dst] host <direccion IP>
  - ether [src | dst] host <dirección MAC>
  - [udp| tcp] [src | dst] port <puerto TCP>
- Para ligarlas se usan operadores lógicos &&, || ! o en palabra and, or, not
- Ejemplos
  - Cualquier tráfico entre IP 192.168.2.34 y 192.168.2.43
    - (src host 192.168.2.34 && dst host 192.168.2.43) || (src host 192.168.2.43 && dest host 192.168.2.34)
  - Idem pero para puertos UDP 12000 y 12100
    - (src host 192.168.2.34 && dst host 192.168.2.43) || (src host 192.168.2.43 && dest host 192.168.2.34) && (udp port 12000 || udp port 121000)

Filtros de display

- Tienen una sintaxis más “matemática”
  - Usa operadores ==, !=, >
  - Los campos están ligados a los protocolos que se están filtrando (**ip.addr**, **udp.port**)
  - Si se quiere especificar una dirección addr se sustituye por src o dst
- Los ejemplos anteriores serían
  - Cualquier tráfico entre IP 192.168.2.34 y 192.168.2.43
    - (ip.src == 192.168.2.34 && ip.dst 192.168.2.43) || (ip.src == 192.168.2.43 && ip.dst == 192.168.2.34)
  - Idem pero para puertos UDP 12000 y 12100
    - ((ip.src == 192.168.2.34 && ip.dst 192.168.2.43) || (ip.src == 192.168.2.43 && ip.dst == 192.168.2.34)) && (udp.port == 12000 || udp.port == 12100

Uso de los filtros de display

- Se aplica el filtro en la ventana de los filtros
  - No olvidar dar al botón **apply**
- Los paquetes filtrados aparecen en las opciones de:
  - Guardar captura
  - Exportar captura
  - Estadísticas sumario

Modo de trabajo típico

- Recomendamos el siguiente procedimiento
  - Como root
    1. Lanzar una captura **global** aceptando todo el tráfico de la red
    2. Guardar la captura en **formato .pcap**
    3. Dejar el fichero .pcap accesible al usuario normal
       - chmod a+r <fichero>
       - chown usuario:usuario fichero
  - Como usuario normal
    1. Abrir el fichero .pcap e identificar los flujos de la aplicación
    2. Filtrar y aislar los flujos
    3. Seleccionar los intervalos de tiempo de confianza
    4. Guardar el contenido filtrado en **formato .pcap**
    5. Exportar los datos a formato .csv o XML para ser procesados externamente

Pequeños trucos de wireshark

- Por defecto Wireshark no muestra el tamaño de la trama ethernet en la lista de tramas
  - Sí se ve en el panel de detalles
  - Para mostrar este campo en la lista de tramas
    - Ir a **Edit->Preferences->Columns**
    - Seleccionar **Packet Length**
- Para seleccionar un rango de paquetes hay que usar el campo **frame.number**
  - frame.number >= (primera_trama) && frame.number <= (ultima_trama)

Estadísticas de Wireshark

- Summary
  - Muestra datos útiles de la captura y del filtrado de display
  - No muestra nada de interarrival de paquetes
- Packet length
  - Genera un histograma de los tamaños de los paquetes
- I/O graphs
  - Genera diagramas temporales de la captura

- Estas herramientas están bien para una primera visión, pero no se pueden exportar a ningún otro formato (salvo el diagrama de I/O graphs

Exportar a una hoja de cálculo

- Export → CSV

```
"No","Time","Size","Source","Destination","Protocol","Info"
"1","0.000000","16450","127.0.0.1","127.0.0.1","IP","Fragmented IP..."
"2","0.000026","9226","127.0.0.1","127.0.0.1","LLC","I P, N(R)=1, ..."
"3","1.004311","16450","127.0.0.1","127.0.0.1","IP","Fragmented IP ..."
"4","1.004336","9226","127.0.0.1","127.0.0.1","LLC","I P, N(R)=1, ..."
"5","2.007957","16450","127.0.0.1","127.0.0.1","IP","Fragmented IP ..."
"6","2.007981","9226","127.0.0.1","127.0.0.1","LLC","I P, N(R)=1, ..."
"7","3.003052","16450","127.0.0.1","127.0.0.1","IP","Fragmented IP ..."
"8","3.003080","9226","127.0.0.1","127.0.0.1","LLC","I P, N(R)=1, ..."
"9","4.004425","16450","127.0.0.1","127.0.0.1","IP","Fragmented IP ..."
"10","4.004447","9226","127.0.0.1","127.0.0.1","LLC","I P, N(R)=1, ..."
"11","5.003353","16450","127.0.0.1","127.0.0.1","IP","Fragmented IP ..."
"12","5.003376","9226","127.0.0.1","127.0.0.1","LLC","I P, N(R)=1, ..."
```

- En OpenOffice Calc seleccionar
  - Separador comma ON
  - Eliminar “campo citado como texto”

Otros postprocesos

- Exportar a PSML
  - Es una representación en XML del panel de lista de paquetes
- Exportar a PDML
  - Es una representación en XML de la captura **completa** con todos los campos
- Utilizar la librería pcap
  - Es una librería que parsea el formato nativo de Wireshark