Análisis de redes con WireShark

Jesús Espino García

Grupo de usuarios de Linux
Universidad Carlos III de Madrid.

10 de Marzo de 2009

Conceptos básicos de red

- Pila TCP-UDP/IP (Física,Enlace,IP,TCP,Aplicación)
- Hardware (Hub/Switch)
- Puerto.
- Protocolo.

¿Qué es?

- Sniffer de red.
- Es GPL.
- Multiplataforma.
- Reconoce mas de 480 protocolos.
- Capaz de seguir sesiones TCP.
- Soporta archivos de captura de otros sniffers.
- Compatible con tcpdump.

¿Por qué?

- Detección de errores.
- Detección de intrusiones.
- Detección de congestiones.
- Obtención de información privada.

¿Cómo?

- Usando wireshark.
- Usando tcpdump.

¿Dónde?

- Misma maquina.
- Misma red física (hubs).
- Mismo switch con puerto espejo.
- Mismo switch con cache poisoning.
- En ambas maquinas (origen y destino).

Obteniendo el trafico de red

Con wireshark

- Abrir WireShark como root.
- Ir a Capture ¿ Interface...
- Hacer click en start en la interfaz que nos interesa.
- Al terminar ir a Capture ¿ Stop.

Con tcpdump

- En un terminal como root ejecutar `tcpdump -w <fichero.pcap>`
- Abrir el fichero creado con WireShark.

Filtrando paquetes

En la captura

- Filtros que permiten capturar solo el trafico que nos interesa.
- Generan ficheros mas pequeños y manejables.
- Pueden perderse tramas interesantes para el diagnostico.

En el mostrado

- Ocultan los paquetes que no coinciden con el filtro.
- Maneja todos los datos, podemos diagnosticar con mas información.
- Los ficheros normalmente son mas grandes y mas pesados de manejar.

Filtrando paquetes

Expresiones

- Para poder filtrar mas fácilmente podemos usar el botón .Expresion...".
- Nos permite construir filtros de manera sencilla sin tener que acordarnos de todo.

Seguir tramas

- Hacemos click derecho sobre un paquete y seleccionamos "Follow TCP Stream".
- Nos crea automáticamente un filtro para esta trama.
- Ademas nos abre una ventana con la información intercambiada.

Modificando los tiempos

El formato

- Se pueden seleccionar diferentes formatos y precisiones para los tiempos.
- Formatos como, la fecha, la hora, el numero de segundos desde el principio de la captura...
- Precisiones desde segundos hasta nanosegundos.

La referencia

- También es interesante contar el tiempo a partir de un determinado paquete.
- WireShark permite seleccionar un paquete para que sea el segundo 0.

Ejemplos

- Telnet.
- IMAP.
- DNS.
- DHCP.
- Virus Slammer.
- WakeOnLan.

Referencias

- `man wireshark`: Pagina del manual de WireShark.
- `man tcpdump`: Pagina del manual de tcpdump.
- http://www.wireshark.org: Pagina oficial de WireShark.
- http://wiki.wireshark.org/SampleCaptures: Ejemplos de capturas.

Dudas

. . .

Fin