Taller de Wiretapping

Teoría de las Comunicaciones
Departamento de Computación
FCEN - UBA

16.04.2013

1. Introducción

En este taller vamos a abordar en forma práctica algunas nociones de nivel de enlace, poniendo fundamentalmente el foco en el vínculo con la capa superior y desarrollando un acercamiento analítico. El objetivo será analizar de manera interactiva el protocolo ARP [1] y sacar algunas conclusiones de cómo se comportan los hosts en un segumento de red determinado. Para ello, sugerimos el uso de dos herramientas modernas de manipulación y análisis de paquetes: Wireshark [2] y Scapy [3].

2. Normativa

- Fecha de entrega: 07.05.2013
- El código deberá haber sido enviado por correo para esa fecha con el siguiente formato:
  to: tdc-doc at dc uba ar
  subject: debe tener el prefijo [tdc-wiretapping]
  body: nombres de los integrantes y las respectivas direcciones de correo electrónico
  attachment: el código fuente desarrollado.
- Se deberá entregar el informe impreso y abrochado con la lista de integrantes y los respectivos correos electrónicos (los mismos que fueran enviados por mail).

3. Enunciado

Cada grupo deberá resolver las consignas que siguen a continuación, tomando como referencia lo explicado en la clase de taller de la fecha que figura en el título.

3.1. Primera consigna: implementación de un cliente ARP

(a) Implementar un cliente ARP sencillo: definir una función en Scapy (u otro lenguaje a elección con soporte para networking) que, dada una dirección IP, realice un pedido por la dirección física asociada y reciba y muestre la respuesta en caso de que ésta sea recibida.

(b) Analizar qué ocurre al suministrarle distintas direcciones de la red local:

- Una dirección inexistente,
- La misma dirección de la máquina origen,
- etc.

3.2. Segunda consigna: capturando tráfico

(a) Implementar una función para escuchar pasivamente en la red local por un lapso de tiempo dado y capturar cada mensaje ARP encontrado.

(b) Analizar la entropía de la red en base a los mensajes ARP observados. Para esto deberán:

- Definir un modelo para la fuente de información.
- Definir el conjunto de símbolos. (Ver observación, no necesariamente es un caracter).
- Calcular las frecuencias relativas de cada evento y determinar la entropía de cada fuente de información.

Observación: tener en cuenta que se busca caracterizar los nodos de la red. Para esto deberán definir un modelo adecuado para la fuente de información.

3.3. Tercera parte: gráficos y análisis

Utilizando lo hecho en la consigna previa, graficar los datos encontrados y realizar un análisis de lo observado. Sugerimos, entre otros, histogramas de IPs solicitadas o grafos dirigidos de IPs (donde existirá un eje entre la IP x y la IP y sii se observó un request ARP con source IP x y target IP y) y analizar que IPs son estadísticamente significativas en la LAN analizando la información de cada símbolo con respecto a la entropía de su respectiva fuente.

Se valorará especialmente en esta consigna la creatividad y el análisis propuesto. Recomendamos, pués, pensar cómo resultará más efectivo presentar la información recopilada.

Referencias

[1] RFC 826 (ARP) `http://tools.ietf.org/html/rfc826`

[2] Wireshark (página web oficial) `http://www.wireshark.org`

[3] Scapy (página web oficial) `http://www.secdev.org/projects/scapy/`

[4] OUI (IEEE) `http://standards.ieee.org/develop/regauth/oui/oui.txt`