TP1a: Wiretapping

Teoría de las Comunicaciones
Departamento de Computación
FCEN - UBA

04.09.2013

1. Introducción

En este taller vamos a abordar el desarrollo de tools de diagnóstico de red. 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: 24.09.2013
- El informe 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 coordinará una defensa presencial con el corrector. Se deberá llevar el informe impreso y abrochado con la lista de integrantes.

3. Enunciado

Cada grupo deberá resolver las consignas que siguen a continuación, tomando como referencia lo explicado en clase.

3.1. Primera consigna: capturando tráfico

(a) Implementar una *tool* para escuchar pasivamente en la red local.

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

- Definir la fuente de información (el conjunto de símbolos).
- Adapte la tool de inciso (a) para estimar las probabilidades de dicha fuente en función de los paquetes ARP observados y calcular la entropía.

(c) Realizar capturas sobre distintas LANs (al menos 2 o 3).

(d) Proponer otros modelos de fuente de información (al menos 1 o 2).

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.

3.2. Segunda consigna: gráficos y análisis

Utilizando lo hecho en la consigna previa, graficar los datos encontrados y realizar un análisis de los nodos distinguidos. Sugerimos, entre otros, histogramas de IPs solicitadas o grafos dirigidos de IPs con pesos en los nodos (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`