TP1: Wiretapping

Teoría de las Comunicaciones

Departamento de Computación
FCEN - UBA

08.04.2015

1. Introducción

El objetivo de este trabajo es utilizar técnicas provistas por la teoría de la información para distinguir diversos aspectos de la red de manera analítica. 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: 29.04.2015
- 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 informe y el código desarrollado.

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

1. Implementar una herramienta para escuchar pasivamente en la red local.
2. La siguiente fuente de información distingue los protocolos que se encapsulan en todos los paquetes ethernet de una red:

   $$S = \{s_1 \cdots s_n\} \text{ siendo } s_i \text{ el valor del campo } \textit{type} \text{ del frame de capa 2.}$$

   A partir de ello se pide:

   (a) Proponga una nueva fuente S_1 con el objetivo de distinguir nodos de la red en base *solamente* al tráfico ARP. Esto significa que los símbolos de S_1 tienen que estar conformados por campos del paquete ARP.

   (b) Adapte la *tool* del inciso (a) para estimar las probabilidades de las fuentes S y S_1 en función de los paquetes observados y calcular la entropía de cada fuente.

   (c) Utilizando la herramienta realizar capturas (lo más extensas posibles) de paquetes en alguna red de accesso compartido. En la medida de lo posible, intentar capturar en una red que no sea controlada (en el trabajo, en un shopping, etc.). Debe haber exactamente una captura por cada integrante del grupo.

3.2. Segunda consigna: gráficos y análisis

Utilizando lo hecho en la consigna previa realizar un análisis que permita, para cada una de las redes estudiadas:

(a) Determinar los protocolos distinguidos y analizar el overhead impuesto por ARP.

(b) Determinar los nodos distinguidos.

Los resultados de esta consigna deben estar basados en la teoría de la información. O sea, deben analizar qué símbolos son estadísticamente significativos en cada LAN analizando la información de cada símbolo con respecto a la entropía de su respectiva fuente. La presentación de los resultados debe efectuarse mediante gráficos y su correspondiente análisis. Sugerimos, entre otros, histogramas (de IPs y protocolos) con cortes en los valores de entropía. De todos modos, se valorará 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`