DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 1

Wiretapping

22 de septiembre de 2015 — Teoría de las comunicaciones

Integrante	LU	Correo electrónico
Ladelfa, Hernán Nahuel	318/04	nahueladelfa@gmail.com
González, Sergio Martín	723/10	sergiogonza90@gmail.com

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
http://www.exactas.uba.ar

Índice

1. Introducción

El primer paso del trabajo consiste en implementar una herramienta que, dada

$P_{t_i;t_f} = \{p_1 \cdots p_n\}$ siendo p_i el i-esimo paquete transmitido en la red entre los instantes de tiempo $[t_i, t_f]$

sea capas de generar las siguiente fuente de información:

$$S_{t_i;t_f} = \{s_1 \cdots s_n\} \text{ siendo } s_i = p_i.type/p_i \in P \text{ entre los instantes de tiempo } [t_i; t_f].$$

Y luego, adaptarla para poder obtener una fuente de información que nos permita encontrar hosts en la red, solo basándonos en paquetes ARP. Tomemos el siguiente subconjunto de P:

$$\overline{P}_{t_i;t_f} = \{\overline{p}_1 \cdots \overline{p}_n\} \; \forall \; \overline{p}_i \in \text{P} \; / \; \overline{p}_i.type = ARP \text{ entre los instantes de tiempo } [t_i; t_f].$$

Teniendo esto, la fuente de información que proponemos es la siguiente:

$S_1 = R_{t_i;t_f} = \{r_{ai} \mid r_{ai} = \overline{p}_i[ARP].ip\_origen\} \bigcup \{r_{bi} \mid r_{bi} = \overline{p}_i[ARP].ip\_destino\}$ entre los instantes de tiempo $[t_i; t_f]$.

Osea, nos quedamos con las ips origen y destino de la capa ARP. De esta forma, obtenemos una fuente de información que nos de los hosts de la red, y de esta manera podemos medir la cantidad de pedidos y respuestas que envía y recibe. Esta fuente de información podría ser utilizada, por ejemplo, para encontrar nodos distinguidos de la red.

2. Resumen de la herramienta

Para la simulación de las fuentes de información anteriormente presentadas. Desarrollamos una aplicación utilizando Scapy, la cual escucha pasivamente la red, captura los paquetes y vuelva la información pertinente en una serie de archivos. Los mismos son los siguientes:

- Un archivo que indica: El origen y el destino (MAC) de la capa Ethernet, el "type", y las IPs origen y destino (solo cuando es pertinente)
- Un archivo con la probabilidad de ocurrencia de cada "type", y la entropía de los "type"
- Un archivo con la probabilidad de ocurrencia de cada "host" (ip), y la entropía de los host (solo teniendo en cuenta paquetes ARP)
- Una imagen con un grafo indicando los "request" (who-has) y "replys" (is-at) que se enviaron los "host" entre si (opcional).

2.1. Ejecución

La ejecución del a herramienta debe ser realizada en un entorno Linux, y es necesario tener instalado: *Python 3.0* (o superior), *Scapy*, y si ademas se quiere realizar grafos, es necesario tener instalado *graphviz*.

Para ejecutar la herramienta, se debe abrir una consola en la carpeta "src" adjunta a este informe y ejecutar el comando:

```
$ sudo ./WiretappingTool.py
```

Esto comenzara a capturar, y volcara la informacion en los archivos configurados como default. Adicionalmente, la aplicacion cuenta con ciertos paramentos para personalizar la ejecucion de la captura. Por ejemplo:

```
$ sudo ./WiretappingTool.py -f salida.out -t 60 --console --arp
```

Esto realiza lo sigiuente:

- (-t o --timeout) indica un tiempo en segundos para finalizar la captura, en esta caso 60 segundos.
- (--arp) Captura solo paquetes ARP.
- (--console) Ademas de volcar el resultado de la captura a un archivo, se muestran los paquetes en la consola, en tiempo real.
- (-f) Vuelca la captura en *salida.out* en lugar del archivo configurado por defecto (out/sniff.out).

Si ademas de la captura, se desea realizar un grafo con los nodos de la red, junto con los "request" y "replys" realizados por los mismos, se debe pasar el parametro "–graph". Ejemplo:

```
$ sudo ./WiretappingTool.py -f salida.out --console --arp --graph
```

Al terminar la ejecucion, la imagen con el grafico se abrirá al instante.

Para ver con detalle cada uno de los parametros que dispone la aplicacion, se puede utilizar:

```
$ sudo ./WiretappingTool.py -h
```

3. Métodos

3.1. Primera Consigna: Caputando tráfico

3.2. Tercera Consigna: Gráficos y Análisis

4. Resultados

5. Conclusiones