DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 1

Wiretapping

19 de abril de 2016 — Teoría de las comunicaciones

Integrante	LU	Correo electrónico
Interlandi, Daniel	Barbeito, Nicolás/147/10	danielinterlandi@gmail.com
Ladelfa, Hernán Nahuel	318/04	nahueladelfa@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. Resumen

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. Además, sugerimos el uso de dos herramientas modernas de manipulación y análisis de paquetes frecuentemente usadas en el dominio de las redes de computadoras: Wireshark y Scapy.

2. Introducción

Se modelaron las redes analizadas como dos fuentes, S y S_1. La primera tiene como objetivo examinar los protocolos presentes y su importancia en la misma, se toma

$$S = \{s_1 ... s_n\}$$

donde s_i es $p_i.type$, con p_i el i-ésimo paquete capturado.
El segundo modelo es

$$S_1 = \{s_{1,1} ... s_{1,n}\}$$

donde $s_{1,i}$ es $p_i.pdst$ (dirección IP destino), con p_i el i-ésimo paquete del protocolo ARP capturado. Este es utilizado para analizar la importancia de los nodos dentro de la red.
Usando estos modelos y los conceptos de información y entropía podemos detectar símbolos destacados en las fuentes (nodos o protocolos según la fuente). La información que otorga un símbolo s_i en una fuente se define como

$$I(s_i) = log(1/P(s_i))$$

y nos ayuda a detectar que tan frecuente es la emisión de ese símbolo por la fuente. La entripía de una fuente $S = \{s_1 ... s_n\}$ se define como

$$\sum_S P(s_i) I(s_i) \forall s_i \in S$$

este número da la información media emitida por la fuente. Indica que tan desordenada es la aparición de los símbolos.

Un concepto fundmental es el del protocolo ARP. Este sirve para relacionar direcciones de nivel de red (IP) con direcciones de nivel de enlace (MAC). Cuando un equipo desea mandar un paquete a una dirección IP dada, necesita ubicar el mismo a nivel de enlace, entonces envía un ARP-request mediante broadcast requiriendo una respuesta del poseedor de la dirección IP, luego, si existe, el nodo que tenga esa IP responderá usando un paquete ARP reply a quién realizó la consulta con su dirección MAC. De esta manera, interceptando paquetes ARP se puede detectar qué nodos activos hay en una red.

3. Conclusiones

3.1. Instructivo

3.2. Ejecución

¿sudo ./sniffer.py ¡timeout¿
Filtrado por protocolo ARP:
¿sudo ./sniffer.py ¡timeout¿arp