TP Wiretapping

Teoría de las Comunicaciones

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

04.09.2013

¿Cómo son los Trabajos Prácticos?

- 2 Trabajos Prácticos (3 entregas)
  1. TP1: Hacer tools en scapy
     a. TP1a: Wiretapping (Information Gathering)
     b. TP1b: ICMP (Rutas en Internet)
  2. TP2: Programación en *raw sockets*
- Objetivos
  1. Experimentar con la red. No siempre es lo que parece.
  2. Hacer análisis acerca de los comportamientos no esprados.
  3. Enmarcar el análisis en un informe.

¿Qué esperamos que hagan?

- Que reflexionen sobre lo que es una red.
- Que se vayan con herramientas prácticas para hacer diagnóstico.
- Que entiendan los conceptos teóricos de una manera aplicada.
- Que entreguen informes rigurosos sobre lo que ustedes descubrieron.

Dinámica de presentación y entrega.

- 3 o 4 integrantes.
- Fechas de entrega por mail.
  1. TP1a: 24/09/2013
  2. TP1b: 23/10/2013
  3. TP2: hasta el 19/11/2013
- ¡Defensa presencial!
  (a coordinar con el corrector - llevar impreso)
- Pautas para el informe.
  1. Tener en cuenta la estructura de informe científico.
  2. El código no es tan importante.
  3. Ojo con las figuras. Que sean claras y tengan leyendas.

Primera consigna

(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 del 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 (al menos 1 o 2).

Observación: tener en cuenta que se busca caracterizar los nodos de la red. Para esto deberán definir un modelos de fuentes de información adecuados a este proposito.

Tercera consigna

- Utilizando lo hecho en la consigna previa, graficar los datos encontrados y realizar un análisis de lo observado.
- Algunas sugerencias: histogramas de IPs solicitadas y/o grafos dirigidos de IPs (request $\rightarrow$ reply).
- ¡Pensar!

Escuchando

```
#! /usr/bin/python
from scapy.all import *

from math import log

ipssrc = {}
ipsdst = {}

def entropia(ips):
    N = sum(ips.values())
    Ps = [ k/N for k in ips.values() ]
    H = -sum([ p*log(p,2) for p in Ps ])
    return H

def arp_monitor_callback(pkt):
    if ARP in pkt and pkt[ARP].op in (1,2): #who-has or is-at
        src = pkt[ARP].psrc
        dst = pkt[ARP].pdst

        if not ipssrc.has_key(src): ipssrc[src] = 0.0
        ipssrc[src]+= 1
        if not ipsdst.has_key(dst): ipsdst[dst] = 0.0
        ipsdst[dst]+= 1

        return "H_src=%f, H_dst=%f" %(entropia(ipsdst), entropia(ipssrc))

sniff(prn=arp_monitor_callback, filter = "arp", store = 0)
```