Trabajos Prácticos

¿Cómo son los Trabajos Prácticos?

- 2 Trabajos Prácticos (2 entregas)
  1. TP1: Capturas en redes locales (ARP)
  2. TP2: Rutas en Internet (ICMP)
- Objetivos
  1. Experimentar con la red. No siempre es lo que parece.
  2. Hacer análisis acerca de los distintos comportamientos de los dispositivos (tanto los esperados como los no esperados).
  3. Enmarcar el análisis en un informe (o *tech rep*).

¿Qué esperamos que hagan?

- Que reflexionen sobre los distintos aspectos que componen las redes.
- Que se vayan con herramientas prácticas para hacer diagnóstico.
- Que profundicen la comprensión de los conceptos a partir de su aplicación.
- Que confeccionen informes sobre lo que experimentaron.

Dinámica de presentación y entrega.

- 3 o 4 integrantes.
- Fechas de entrega por mail.
  1. TP1: 19/09/2014
  2. TP2: 14/11/2014
- Entregables (attachment .zip):
  1. Informe.
  2. Herramienta que toma un `libpcap`.
- Pautas para los informes.
  1. Tener en cuenta la estructura de informe científico. *(introducción, métodos, resultados, conclusiones).*
  2. El código no es tan importante.
  3. Ojo con las figuras. Que sean claras y tengan **leyendas**.
  4. Template (*recomendado*): `http://mocha-java.uccs.edu/ieee/`

TP1: Introducción

- Sean $p_1..p_i$, paquetes que se capturan en un intervalo $[t_i, t_f]$.
- Fuente de información binaria de memoria nula $S = \{s_{BROADCAST}, s_{UNICAST}\}$.
- S emite $s_{BROADCAST}$ si $p.dst == \texttt{ff:ff:ff:ff:ff:ff}$, sino emite $s_{UNICAST}$.
- **Esta fuente distingue entre mensajes broadcast y unicast que aparecen en la red en ese intervalo.**

TP1: Primera consigna

1. Implementar una herramienta que escuche pasivamente los paquetes Ethernet de la red y muestre representativamente la fuente modelada S. Además, la herramienta debe proveer la opción de tomar un archivo en formato `libpcap`, en lugar de realizar la captura.

TP1: Primera consigna

1. Implementar una herramienta que escuche pasivamente los paquetes Ethernet de la red y muestre representativamente la fuente modelada S. Además, la herramienta debe proveer la opción de tomar un archivo en formato `libpcap`, en lugar de realizar la captura.
2. Adapte la herramienta anterior proponiendo un modelo de fuente de información de memoria nula $S1$ con el objetivo de distinguir, en lugar de tipos de destinos como hace S, los nodos (hosts) de la red.

TP1: Primera consigna

1. Implementar una herramienta que escuche pasivamente los paquetes Ethernet de la red y muestre representativamente la fuente modelada S. Además, la herramienta debe proveer la opción de tomar un archivo en formato `libpcap`, en lugar de realizar la captura.
2. Adapte la herramienta anterior proponiendo un modelo de fuente de información de memoria nula $S1$ con el objetivo de distinguir, en lugar de tipos de destinos como hace S, los nodos (hosts) de la red.
   - La distinción de S1 debe estar basada únicamente en las direcciones IP de paquetes ARP y en su tipo (`who-has` o `is-at`).
   - El criterio para el modelado lo deberá establecer cada grupo utilizando las herramientas teóricas provistas por la teoría de la información.
   - Se puede pensar que un símbolo es *distinguido* cuando sobresale del resto en términos de la información que provee.

TP1: Segunda consigna

- Utilizando estas herramientas, realizar experimentos analizando:
  - i) Los paquetes broadcast de la red.
  - ii) Los nodos distinguidos.
- Ver qué símbolos se distinguen en cada red, viendo la diferencia entre su información y la entropía de la fuente.
- Tantas capturas como cantidad de miembros tenga el grupo.
- Las capturas largas. $tf - ti > 10 minutos$
- *En la medida de lo posible, intentar capturar en al menos una red mediana/grande que no sea controlada (trabajo, shopping, etc).*

TP1: Segunda consigna (cont.)

El informe debe seguir la siguiente estructura:

- Introducción
- Métodos.
  - Condiciones de cada experimento.
  - Acá debe estar justificada la elección de modelo de fuente $S1$.
- Resultados
  - Figuras: Información, entropía y mensajes ARP.
  - Análisis: Respuestas a preguntas planteadas.
  - *(Ver preguntas en el enunciado)*
- Conclusión.
  - Análisis global entre las distintas redes.

Referencias

- RFC 826 (ARP) `http://tools.ietf.org/html/rfc826`
- Wireshark (página web oficial) `http://www.wireshark.org`
- Scapy (página web oficial) `http://www.secdev.org/projects/scapy/`
- OUI (IEEE) `http://standards.ieee.org/develop/regauth/oui/oui.txt`