Trabajo Práctico N° 5

Sniffing

Fecha Límite de Entrega: 14 de junio a las 23:55
Profesor: Dr. Javier Echaiz
Auxiliar: Ing. Fernando Pap

Condiciones de Aprobación:

En líneas generales el trabajo debe dar evidencia del desarrollo realizado. En casos puntuales en los que sea conveniente, incluir un archivo `readme.txt` con notas correspondientes.
Entregas individuales subiendo contenido al directorio `ARS2018/Entregas/[nombre]` del Google Drive y enviando aviso al email fernandopap@gmail.com o al grupo de whatsapp. Se recomienda utilizar github/ Bitbucket/etc.
El trabajo debe ser entregado completo. Pasada la fecha límite de entrega se descontará un punto por cada día transcurrido.

Enunciados

1. Instalar el sniffer Snort (www.snort.org).

2. Buscar en internet un formulario en un sitio seguro (https) y realizar el análisis de paquetes ("sniffear") del envío de los datos del formulario. Localizar el contenido de los distintos campos y explicar lo encontrado.

3. Realizar el análisis de paquetes ("sniffear") del envío de los datos del formulario del sitio http://www.webs.com/s/login/relogin. Localizar el contenido de los distintos campos y explicar lo encontrado.

4. Realizar el análisis de paquetes ("sniffear") del envío de los datos del formulario del sitio http://www.apps.jsf2.com/xhtml/post-form.html. Localizar el contenido de los distintos campos y explicar lo encontrado.

5. Realizar el análisis de paquetes ("sniffear") mientras:
   a) La PC recibe comandos `ping` de otra PC
   b) La PC realiza comandos `ping` a otra PC

Localizar los paquetes relacionados con los comandos `ping` y explicar.

6. Explique para qué se puede utilizar el modo Network Intrusion Detection System (NIDS) de snort.

7. Explique por qué es inseguro utilizar hubs en una red.

8. ¿Es posible realizar un análisis de paquetes ("sniffing") de un switch?