TALLER DE FUNDAMENTACION

CURSO AVANZADO DE HACKING ETICO

TECNICAS AVANZADAS DE ATAQUE Y DEFENSA.

TALLER - IDS

1. Uso de SNORT para trafico analizado

- Baje de la página de SNORT la versión del Mismo
- Instale el programa sobre su máquina virtual. Ejecute Snort_installer.exe o el respectivo.
- En un shell de comandos del sistema entre a el directorio SNORT **c:\sort>**
- Navegue sobre el directorio BIN cd bin **C:\snort\bin>**
- Ejecute el comando **Snort –dev** para la captura de paquetes en la máquina o la red.

- Si ud no ve captura de paquetes use **Snort –dev –i2** puede usar otros número i3 i4 i5 indicando con estos las interfaces por las cuales va a capturar paquetes o información.

- En este paso antes de parar la captura debe haber recolectado un numero de paquetes prudente que os deje ver actividades de ips, mac's,
- Después de la captura de paquetes pare Snort con **CTRL + C**

2. Realizar el proceso de instalación y de análisis de trafico de un ataque entre dos máquinas con NAGIOS.