

Actividad práctica numero 6:

Formato: Individual.

Asignatura: Seguridad en Sistemas Computacionales

Código: SSC 5501

**Titulo: Monitoreo de Seguridad con IDS SNORT**

1.- Inicie su computador en Windows 7.

2.- Cree una maquina virtual en Virtual Box con:

- Sistema Operativo: Linux, Other

- Memoria RAM: 512 MB

- Disco duro: 8GB

3.- Instale la máquina virtual Easy IDS provista por su profesor:



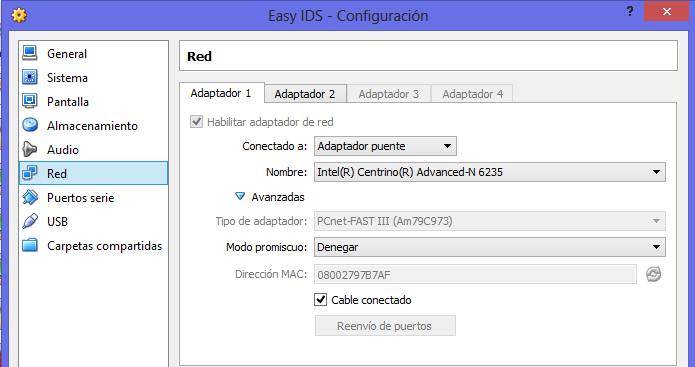
4.- Ejecute la instalación por defecto.

5.- Cree la password de root:



6.- Una vez finalizada la instalación, apague la máquina virtual y habilite las dos interfaces de red como se muestra en la figura:

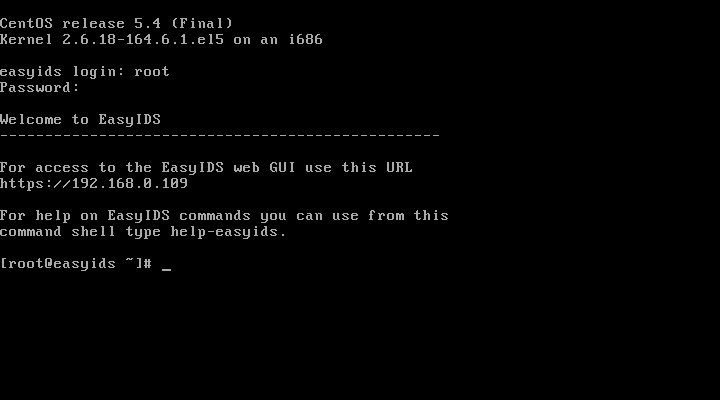
- Adaptador 1: modo puente



- Adaptador 2: modo anfitrión, modo promiscuo: permitir todo



7.- Inicie la máquina virtual con boot desde el disco duro, utilice la contraseña de root creada en el proceso de instalación.

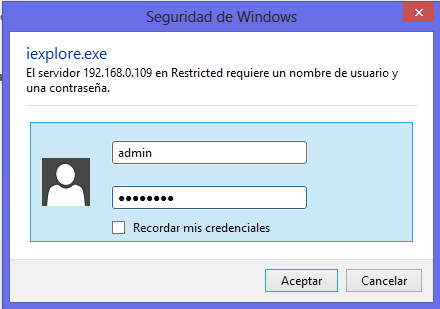


8.- Verifique que ambas interfaces están operativas, tal como se muestra en la figura:

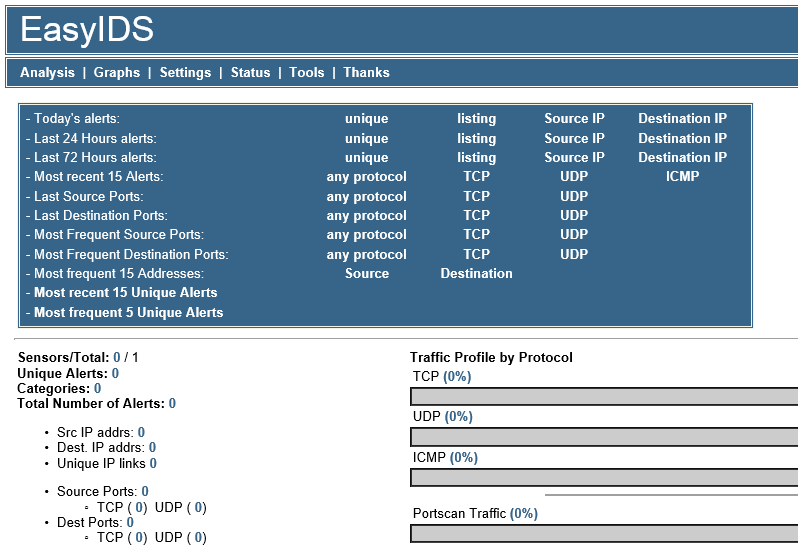


9.- Conéctese vía browser a la interfaz de administración desde su computador:

<https://direccionIP>eth0 usuario: admin password: password

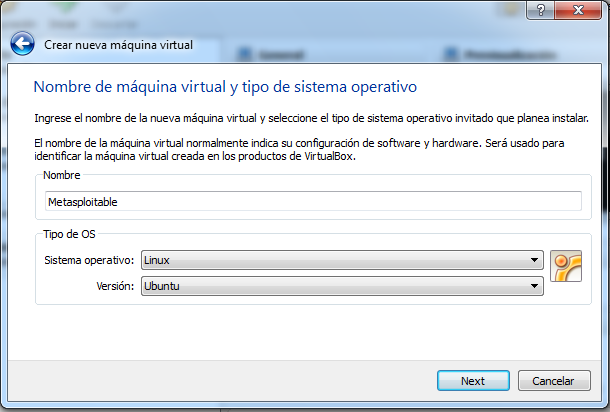


9.- Haga click en la opción Analysis > BASE para visualizar el tráfico monitoreado por el IDS.

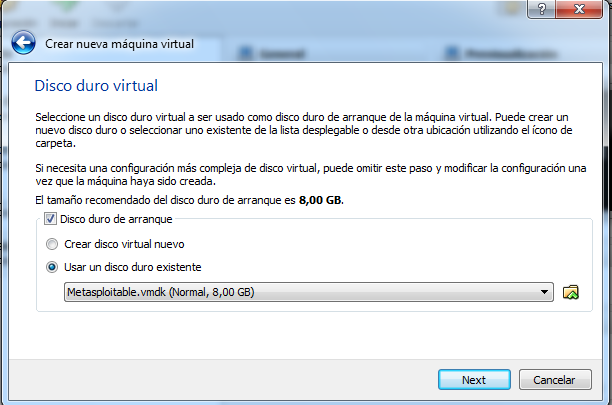


**Creación de la maquina "victima"**

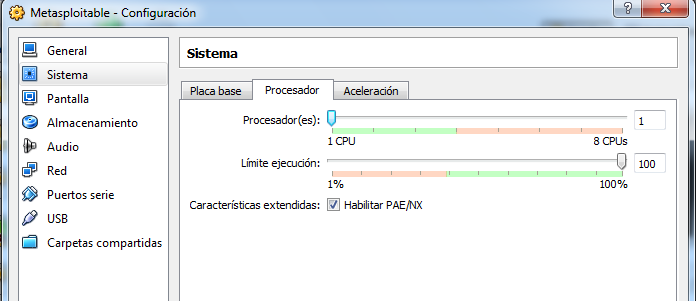
10.- Cree una nueva máquina virtual en Virtual Box, con Sistema Operativo Linux, Ubuntu y 512 MB de RAM.



11.- Instale la máquina virtual Metasploitable provista por su profesor.



12.- Configure la interfaz de red en modo “anfitrión”, el inicio (boot) desde el disco duro y en la opción Sistema > Procesador, habilite la opción PAE/NX.



13.- Inicie la máquina virtual e ingrese con:

- usuario: msfadmin

- password: msfadmin, y valide la dirección IP asignada.

**Instalación de la maquina "atacante":**

14.- Instale la máquina virtual Centos Nessus, provista por su profesor, con la interfaz de red en modo anfitrión

- Usuario: root

- password: duoc.2016



**Diagrama de red de laboratorio**

**Inicio de la sesión de monitoreo:**

15.- Ejecute desde la máquina Centos Nessus el siguiente comando para realizar un barrido de puertos a la maquina víctima:

#nmap ***ipvictima***

16.- Revise la interfaz de administración de EasyIDS para ver las alertas generadas.

