



**Curso: Sistemas Operativos II**  
**Plataforma: Linux**

## IDS

---

Cuando se desea dotar de seguridad a nuestra red, se hace necesaria la instalación y configuración de una herramienta que nos brinde la seguridad requerida, para este caso es la configuración de un Sistema de Detección de Intrusos el cual es utilizado para monitorear la red en donde se especifican un rango de direcciones donde se verifica a intrusos que no tienen los permisos de acceder al sistema, el IDS solo da una alerta sobre cualquier actividad maliciosa en la red.



# INDICE

---

TEMA	No. PAGINA
Introducción .....	3
Objetivos .....	4
Marco Teórico .....	5
Configuración .....	7
Conclusiones .....	11
Bibliografía .....	12
Recomendaciones .....	13



# INTRODUCCION

---

Debido al alto incremento de usuarios que cada día hacen uso de las redes informáticas surgen cada día nuevas amenazas, para ello es necesaria una herramienta que nos provea una detección de intrusos como lo es el IDS, el cual es el proceso de monitorear computadoras o redes, para detectar entradas no autorizadas, actividad o modificación de archivos.

Por ende un IDS puede también ser usado para monitorear trafico, así puede detectar si un sistema esta siendo un objetivo de un ataque de red como un DoS (denial of service).

Como toda herramienta posee ventajas y desventajas, dentro de una de las limitantes es que este genera únicamente alertas y no puede realizar acciones por si solo, como su nombre lo indica es un sistema de detección que además de ser un detector de intrusos nos da la posibilidad de usarlo como un Sniffer y poder capturar una serie de paquetes que se mueven en la red especificada al instalar un IDS, como por ejemplo SNORT.



# OBJETIVOS

---

## General:

- Configurar correctamente un IDS para proteger una red de intrusos.

## Específicos:

- Instalar y Configurar IDS SNORT.
- Aprender la sintaxis y funcionalidad del IDS.
- Configurar el SNORT para detectar intrusos en la red.



# IDS:

---

## Historia:

Un sistema de detección de intrusos surge por la necesidad de proteger nuestras redes y de proveer de funcionalidad de alertas en cuanto a amenazas se refiere, este es un programa usado para poder monitoriar y detectar accesos sin autorización a una PC específica o a una red, donde estos ataques generalmente son hecho por hackers.

El IDS provee una serie de sensores virtuales, entre ellos un snifer, monitoreando el tráfico, el IDS detecta anomalías y puede detectar la presencia de ataques informando con distintos tipos de alarma al administrador de la red.

[ 1 ]

## Funcionamiento:

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.

Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.



[ 2 ]

### **Tipos de IDS:**

Los principales tipos de IDS, son los que a continuación listamos:

**HIDS (HostIDS):** un IDS vigilando un único ordenador y por tanto su interfaz corre en modo no promiscuo. La ventaja es que la carga de procesado es mucho menor.

**NIDS (NetworkIDS):** un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.

**DIDS (DistributedIDS):** sistema basado en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN).

[ 2 ]



# CONFIGURACION

---

Se va explicar la instalación y configuración de SNORT en el sistema operativo LINUX con su distribución KUBUNTU:

Abrimos una Terminal en la cual debemos escribir el siguiente comando, el cual nos permitirá instalar el **SNORT**:

## SUDO APT-GET INSTALL SNORT

Deberíamos poder ver algo como la siguiente imagen:

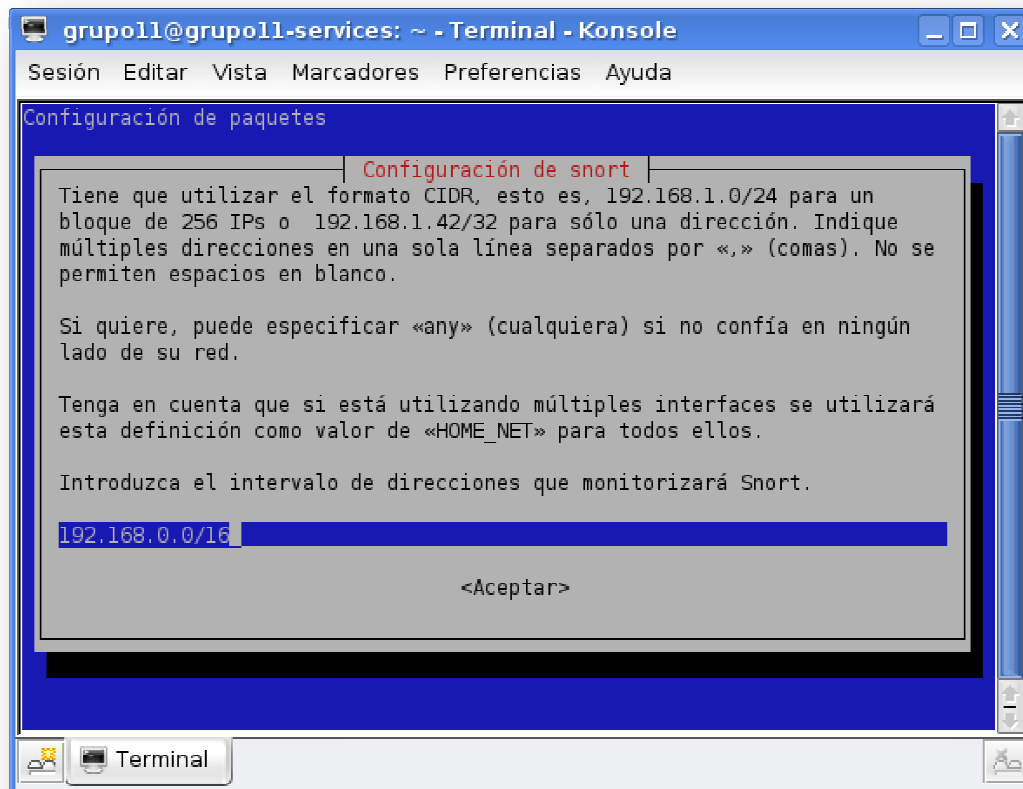
```
grupoll@grupoll-services: ~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
grupoll@grupoll-services:~$ sudo apt-get install snort
```

### **Nota:**

La instalación puede hacerse de forma gráfica en kubuntu con su manejador de paquetes Adept Manager o si se quiere descargando de la página de snort [www.snort.org](http://www.snort.org)

Al estar instalando se nos mostrará una pantalla en el cual se nos solicitará, que introduzcamos el intervalo de direcciones que analizará el IDS.

Por lo cual debemos ingresar un rango de IP que corresponda a la red que deseamos proteger, luego debemos aceptar dichos cambios para continuar con la instalación.



Únicamente con estos pasos tendremos instalado y configurado **Snort** .

## SNORT Como detector de Intrusos

Para utilizar SNORT como un detector de intrusos será necesario configurar el archivo “**snort.conf**” que se encuentra en **/etc/snort/**, ya que aquí se guardan las reglas y configuraciones mas avanzadas de detección de intrusos y filtros de puertos y lo hacemos mediante el siguiente comando:

```
# SNORT -DEV -L ./LOG -H 192.168.0.4/16 -C ../ETC/SNORT.CONF -D
```



Luego de crear la carpeta donde se guardan los logs, con la opción **-c** indicamos que será utilizado como detector de intrusos, será para la IP **192.168.0.4** y con la opción **D**, estamos indicando que **snort**, funcionará como un servicio, la opción **-l** sirve para indicar que en **/log** se guardarán un historial.

## Alertas

Existen varias formas de generar alertas y son:

- Línea de órdenes
- Completo
- Rápido
- Socket
- Syslog
- Smb
- Consola
- Ninguno

La configuración de las alertas se modifica en el archivo alerts.ids

## Ejemplos de Alertas:

### Alerta Rapida

Únicamente nos devolverá información de tiempo, mensaje de alerta su clasificación IP y su origen y destino del puerto y lo realizamos mediante el siguiente comando:

```
#SNORT -A FAST -DEV -L ./LOG -H 192.168.0.4/16 -C ../ETC/SNORT.CONF
```

Al ejecutar dicho comando obtendremos la siguiente salida:

```
Running in IDS mode

Initializing Network Interface eth0
OpenPcap() device eth0 network lookup:
  eth0: no IPv4 address assigned

  == Initializing Snort ==
Initializing Output Plugins!
Decoding Ethernet on interface eth0
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file /etc/snort.conf

+++++
Initializing rule chains...
```



### Alerta Completa

Nos devolverá información mas completa, todas las de alerta rápida y las cabeceras de los paquetes que están registrados con el siguiente comando:

**#SNORT -A FULL ...**



# CONCLUSIONES

---



En base a lo anteriormente expuesto se concluye lo siguiente:

- Que un IDS debe ser confiable, robusto, escalable y que pueda diferenciar entre un ataque y un comportamiento normal en la red, que sea seguro y que tenga compatibilidad con un firewall, para que aumente la seguridad del sistema.
- Que un sistema de protección IDS puede ser implementado en sistemas LINUX tanto en modo gráfico así como por medio de la consola dependiendo de la distribución.
- Que un IDS solamente brinda la funcionalidad de generar alertas y por ende debe de complementarse con un sistema secundaria que si pueda generar acciones por si solo.



# TUTORIAL DESARROLLADO POR

---

	<b>Carlos Enrique Rodas Gálvez</b>	<b>2002-12383</b>
	<b>Miguel Enrique Guerra Connor</b>	<b>2002-17739</b>
	<b>Vinicio Rodolfo Miranda Orozco</b>	<b>2002-12355</b>

## BIBLIOGRAFIA

---

La sección conceptual de este documento fue investigada bajo las siguientes fuentes bibliográficas.

### Motor de Búsqueda:

[www.google.com.gt](http://www.google.com.gt)

### Sitios Virtuales Consultados:

[1] [http://en.wikipedia.org/wiki/Intrusion-detection\\_system](http://en.wikipedia.org/wiki/Intrusion-detection_system)

[2] [http://es.wikipedia.org/wiki/Sistema\\_de\\_detecci%C3%B3n\\_de\\_intrusos](http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos)



## RECOMENDACIONES

---

En base a la experiencia que se deriva del equipo de implementación se plantean unas recomendaciones básicas que deben ser tomadas en cuenta para tener una óptima configuración e implementación.

- Puede convertirse en un error llegar a instalar un IDS en las maquinas cliente.
- Utilizar el SNORT no solamente para detectar intrusos sino para realizar monitoreos o administración en la red.
- Se debe pensar en un detector de intrusos que sea compatible con un firewall y que se pueda unir la inteligencia de un IDS con la capacidad que tiene un firewall de bloquear tráfico no seguro.