

# Snort

Administración de Servidores Linux  
Universidad ORT  
Montevideo-Uruguay

Pablo Martinez Viberti  
[pdmartinez@adinet.com.uy](mailto:pdmartinez@adinet.com.uy)

# Sistemas IDS

- IDS : Intrusion Detection System
- Detecta y monitoriza eventos de la red
- Ataques de hackers, DoS, CGI, escaneos nmap
- Buscan patrones predefinidos característicos
- Aumentan prevención y alerta
- Proveen datos sobre el tráfico

# Tipos de IDS

- Host IDS (HIDS)
- Net IDS (NIDS)
- Distributed IDS (DIDS)

# Host IDS

- Protege un solo host
- Funciona de forma local. Interfaz de red en modo no promiscuo
- Carga menor de procesador
- Registra procesos y usuarios

# Net IDS

- Protección a nivel de red
- Sniffer de red
- Búsqueda de patrones de ataques
- Interfaz en modo promiscuo
- Trabajan a nivel de TCP/IP y a nivel de aplicación
- Análisis en tiempo real

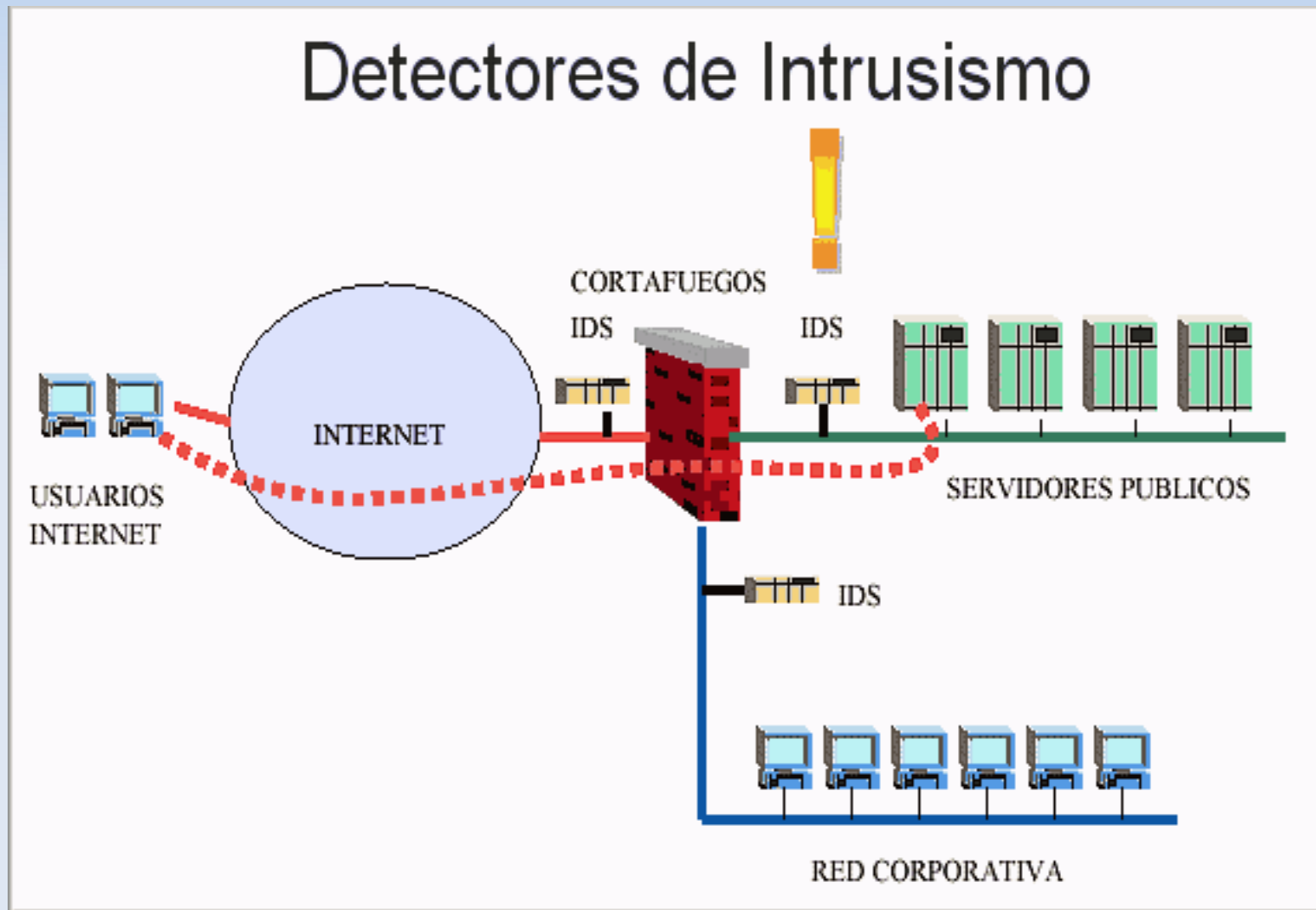
# Distributed IDS

- Basado en cliente – servidor
- Net IDS actuando como sensores
- Centralización de la información en base de datos
- Cada IDS tiene reglas específicas de cada segmento

# Otras clasificaciones

- Pasivo: detecta una posible intrusión, envía la alerta que se almacena.  
NO ACTUA SOBRE EL ATACANTE
- Reactivo: responde a la actividad sospechosa reprogramando el firewall (Ej: bloqueando la conexión)

# Dónde colocar un IDS?



# Snort

- Monitoreo y detección de anomalías en el tráfico
- Detección de amplia variedad de ataques (CGI,DoS,escaneo de puertos,etc.)
- Sniffer de red
- Detector de intrusos
- Packet logger
- Basado en reglas
- Variedad de logs (Texto,binarios,syslog,Winpopup)
- Interfaz en modo promiscuo
- IDS reactivo o pasivo (FlexRep)

# Snort

- Decodificador de paquetes: captura y prepara paquetes
- Preprocesador: arreglan y modifican datos para el motor de detección. Buscan anomalías
- Motor de detección: responsables de la detección de anomalías en los paquetes
- Loggin y sist. alerta: loguea y registra las alertas
- Plugin de salida: envío de alertas por mail, syslog, base de datos, XML

# Instalación

- Desde repositorios
- Compilando ([www.snort.org](http://www.snort.org))
- Archivo configuración  
`/etc/snort/snort.conf`
- Reglas `/etc/snort/rules/*.rules`

# Puesta en marcha

- `snort [options] <filter options>`

- Modo IDS:

*snort -devl /var/log/snort -h 172.16.0.0/16 -c /etc/snort/snort.conf*

- Modo Sniffer:

*snort -dev*

- Packet logger:

*snort -devl /var/log/snort*

# Reglas

- Cabecera
  - Acción
  - Protocolo
  - IP y puerto origen
  - IP y puerto destino
- Opciones
  - Mensaje
  - Opciones de desición

# Ejemplo de reglas Cabecera

acción

protocolo

Origen  
IP/Puerto

Dirección

Destino  
IP/Puerto

# Ejemplo de reglas Cabecera

alert

protocolo

Origen  
IP/Puerto

Dirección

Destino  
IP/Puerto

# Ejemplo de reglas Cabecera

alert

tcp

Origen  
IP/Puerto

Dirección

Destino  
IP/Puerto

# Ejemplo de reglas Cabecera

alert

tcp

any

any

Dirección

Destino  
IP/Puerto

# Ejemplo de reglas Cabecera

alert

tcp

any

any

->

Destino  
IP/Puerto

# Ejemplo de reglas Cabecera

alert tcp any any -> 172.16.0.0/24 80

# Ejemplo de reglas Opciones

alert tcp any any -> 172.16.0.0/24 80 (mensaje opciones de decisión)

# Ejemplo de reglas Opciones

alert tcp any any -> 172.16.0.0/24 80 (msg:" "; opciones de decisión)

# Ejemplo de reglas Opciones

```
alert tcp any any -> 172.16.0.0/24 80 (msg:" ";content:"|00 86 a51|;)
```

# Otros ejemplos

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any  
  (msg:"escaneo ping con nmap";flag:A;ack:0;reference:  
  arachnids,28;classtype:attempted-recon;sid:628;rev:1;)
```

```
alert tcp $EXTERNAL_NET any ->$HOME_NET any  
  (msg:"atención:se esta descargando archivos  
  mpg";flags:AP;content:".mpg");)
```

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS  
  $HTTP_PORTS (msg:"WEB-CGI HyperSeek hsx.cgi  
  directory traversal attempt"; flow:to_server,established;  
  uricontent:"/hsx.cgi"; content:"../..//"; content:"%00";  
  distance:1; reference:bugtraq,2314; reference:cve,2001-  
  0253; reference:nessus,10602; classtype:web-  
  application-attack; sid:803; rev:11;)
```

# Referencias

- <http://www.snort.org>
- <http://www.whitehats.com>
- <http://www.incident.org/snortdb>

**FIN**