Red de IDS

IRIS-CERT <cert@rediris.es>

22 de octubre de 2001

snort: funcionamiento

- Leer analizar todo el tráfico que circula por la red
- Comprobar el tráfico en función de patrones (cadenas significativas)
- Alertar de los posibles ataques que se producen

IDS: Ejemplo de funcionamiento

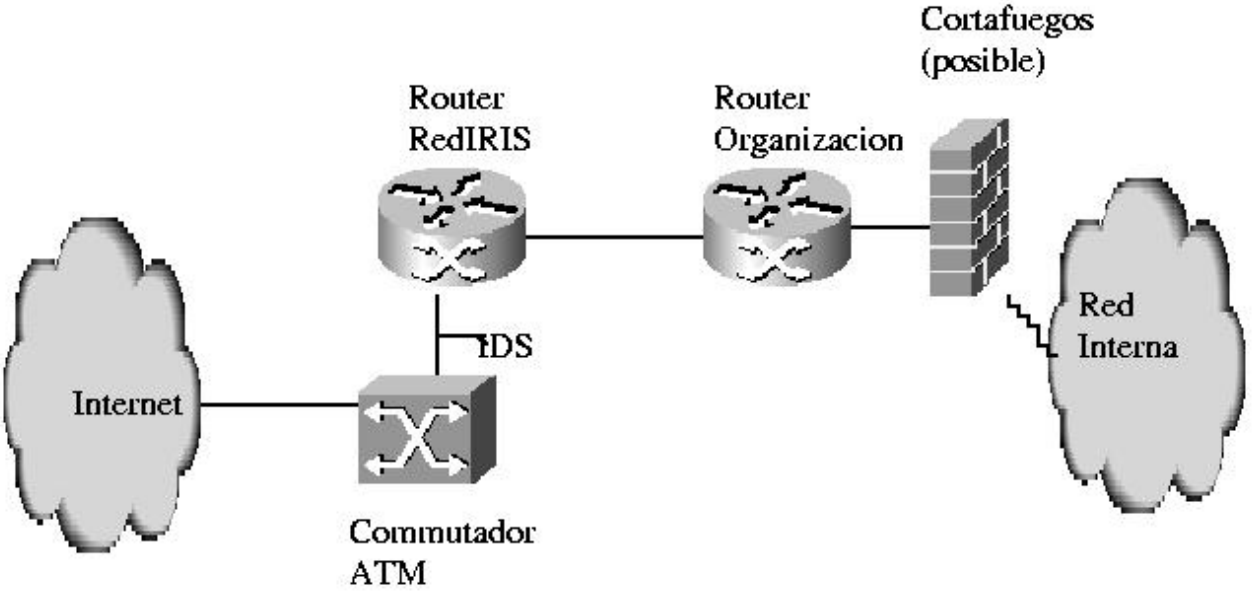
Reglas para la detección de ataques a otros servidores:

```
alert tcp any any -> $HOME_NET 110
   (msg:"QPOP Buffer Overflow!";
   content:"|E8 D9FF FFFF|";  flags: PA;)
alert tcp any any -> $HOME_NET 21
       (msg:"FTP Buffer Overflow-1!"; content:"|5057
        440A 2F69|"; flags: PA;)
alert tcp any any -> $HOME_NET 143
        (msg:"IMAP Buffer Overflow!";
        content:"|E8 C0FF FFFF|"; flags: PA;)
```

Proyecto

- IDS para análizar el tráfico en los nodos troncales de la red.
- Detectar y alertar sobre los ataques que se están produciendo en la red.
- colaboración con las instituciones para alertar y diseñar las alertas

IDS en los troncales



Un IDS en cada nodo troncal, tras el cambio de la red

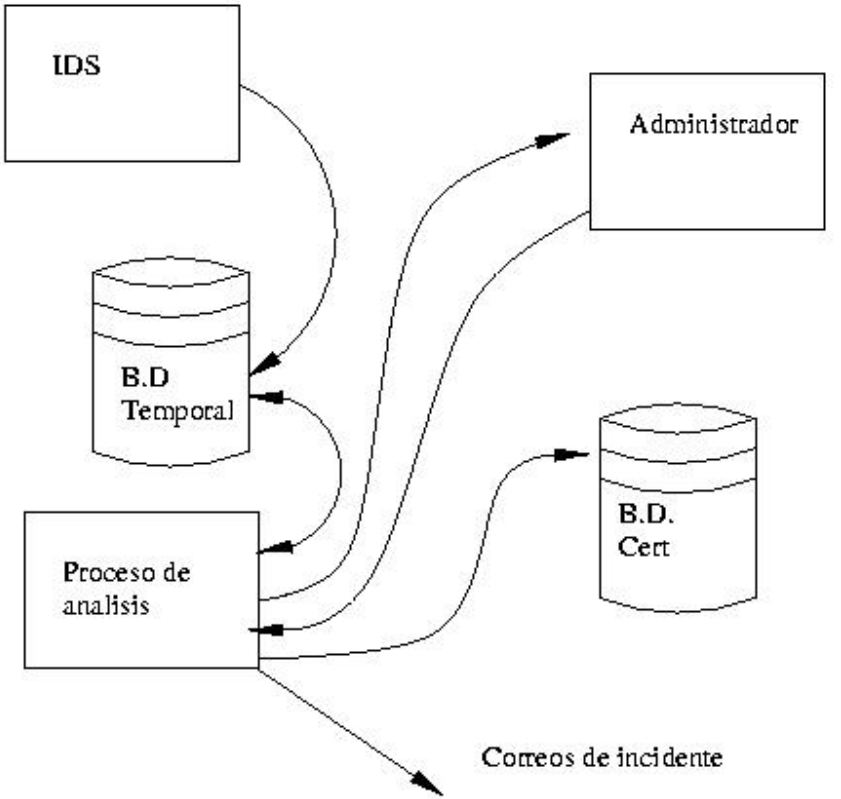
hay que analizar como incluir los IDS en el esquema.

- No interfiere con los filtros de las organizaciones.
- Detección de escaneos diriguidos a puertos filtrados.
- Protección de todos las instituciones.
- Centralización de las alerta, permite detectar nuevos tipos de ataques y equipos comprometidos.
- Generación de informes y sistema de seguimiento de incidencias por institución.

Inconvenientes

- Gran parte de los ataques “graves” se producen muchas veces desde exterior.
- Complejidad en la captura del tráfico, con diversos tipos de enlaces.
- Posible perdida de datos en algunos nodos (demasiado tráfico).

Funcionamiento



IDS

Software: snort.

- Captura el tráfico en modo raw, almacenandolos en ficheros rotados cada hora.

- Los ficheros rotados se añaden, con un proceso de bajar prioridad en la base de datos.

Se consigue capturar el tráfico, mientras que cuando no hay carga de máquina se añaden las alertas a la B.D.

Analisis

Proceso, en la misma máquina ejecutado 1 vez al día.

- Estudia, los logs diarios y genera “informes” y avisos de actividad.
- Estos informes de actividad son enviados via correo a los administradores
- Mueve datos de ataques a otra localización.

Administrador

Recibe correos con indicación de los incidentes que se han producido. Responde sistema "ok" a los

incidentes que se deban abrir.

Gestión incidentes

Para cada incidente "aprovado":

- Busca puntos de contacto.
- Genera un correo de queja.
- Emisión de ticket coordinado con los códigos de IRIS CERT
- envía el correo, con copia a IRIS CERT y a la organización.

RedIRIS

- No hay que generar ticket, ya que ya ha sido alertado el responsable.
- vision de conjunto de los problemas de seguridad.
- Coordinación entre incidentes similares de distintos centros.
- Simplificación de incidentes.

Estado del proyecto

1. Equipos: 5
2. Análisis de conexión IDS a los backbone (boletin 57).
3. Definición de reglas “mínimas” para no saturar el IDS.
4. Puesta en marcha de sistemas progresivamente.
5. Colaboración PTYOC de varios centros