Protección de un servicio Web

1. Autenticación.
2. Gestión de usuarios y grupos.
3. Gestión de servicios.
4. Gestión de sistema de ficheros.
5. Firewall.
6. **Prevención con IDS.**
7. Código seguro.
8. Auditorias periódicas.
9. Sistemas de backup.

Que es un IDS

Los actuales sistemas de detección de intrusos, en adelante IDS63, nacieron cuando a las auditorías de seguridad se le aplicó el EDP4 (**Electronic Data-Processing)**, utilizando mecanismos de identificación de patrones y métodos estadísticos.

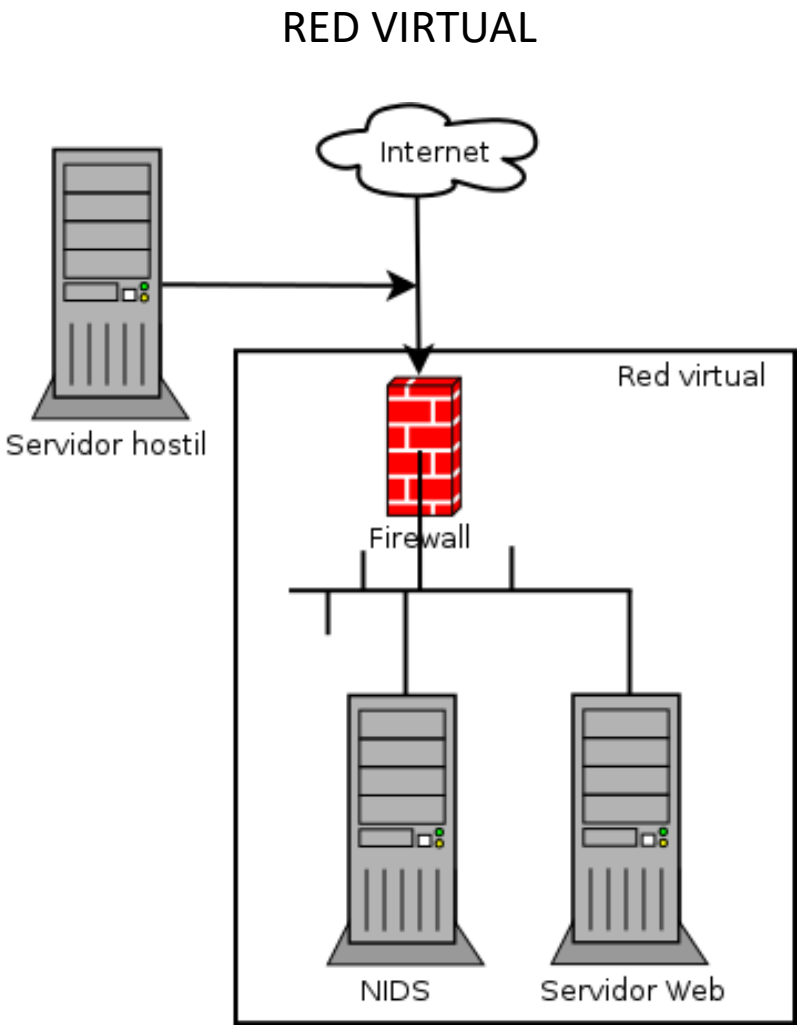
TIPOS de IDS	
HIDS (Host IDS)	Enfocados a garantizar la seguridad de un Host. En este caso el IDS intenta detectar modificaciones en el equipo afectado y realiza un informe de sus conclusiones.
NIDS (Network IDS)	Enfocados a garantizar la seguridad dentro de una red. En este caso el IDS intenta detectar ataques en toda la red capturando todo el tráfico que circula por la misma.
IDS Físicos	Enfocados a identificar amenazas a sistemas físicos. A menudo son vistos como controles físicos con el objetivo de asegurar un lugar o recurso, por ejemplo cámaras de seguridad, tarjetas de identificación, etc..
Prevención de intrusos	Permiten los mismos procesos de recogida e identificación de datos y comportamientos, con la capacidad adicional de bloquear una actividad.

Snort como NIDS

- Implementa un lenguaje de creación de reglas flexibles, potente y sencillo
- provee de cientos de filtros o reglas para backdoor, ddos, finger, etc…
- Puede funcionar como sniffer o como un IDS normal.
- Está disponible bajo licencia GPL, gratuito.
- Funciona bajo plataformas Windows y UNIX/Linux.

Importancia de la ubicación de Snort

Zonas de la red	Aportación al IDS
ROJA	Al IDS le llega todo el tráfico externo a nuestra red, es por tanto una zona de alto riesgo
VERDE	El IDS se encuentra protegido detrás de un firewall y por ello debería ser configurado para tener una sensibilidad un poco mayor que en la zona roja, puesto que ahora, el firewall deberá ser capaz de filtrar algunos accesos definidos mediante la política de nuestra organización
AZUL	Esta es la zona de confianza. Cualquier tráfico anómalo que llegue hasta aquí debe ser considerado como hostil



Elementos de la red Virtual

- Cortafuegos. Smoothwall Express 3.1 Final
- NIDS. SNORT 2.9.8.2 sobre Ubuntu
- Servidor Web. Damn Vulnerable Web Application sobre Fedora

REFERENCIAS
http://www.smoothwall.org/
https://www.snort.org/
http://www.dvwa.co.uk/

Reglas usadas en Snort

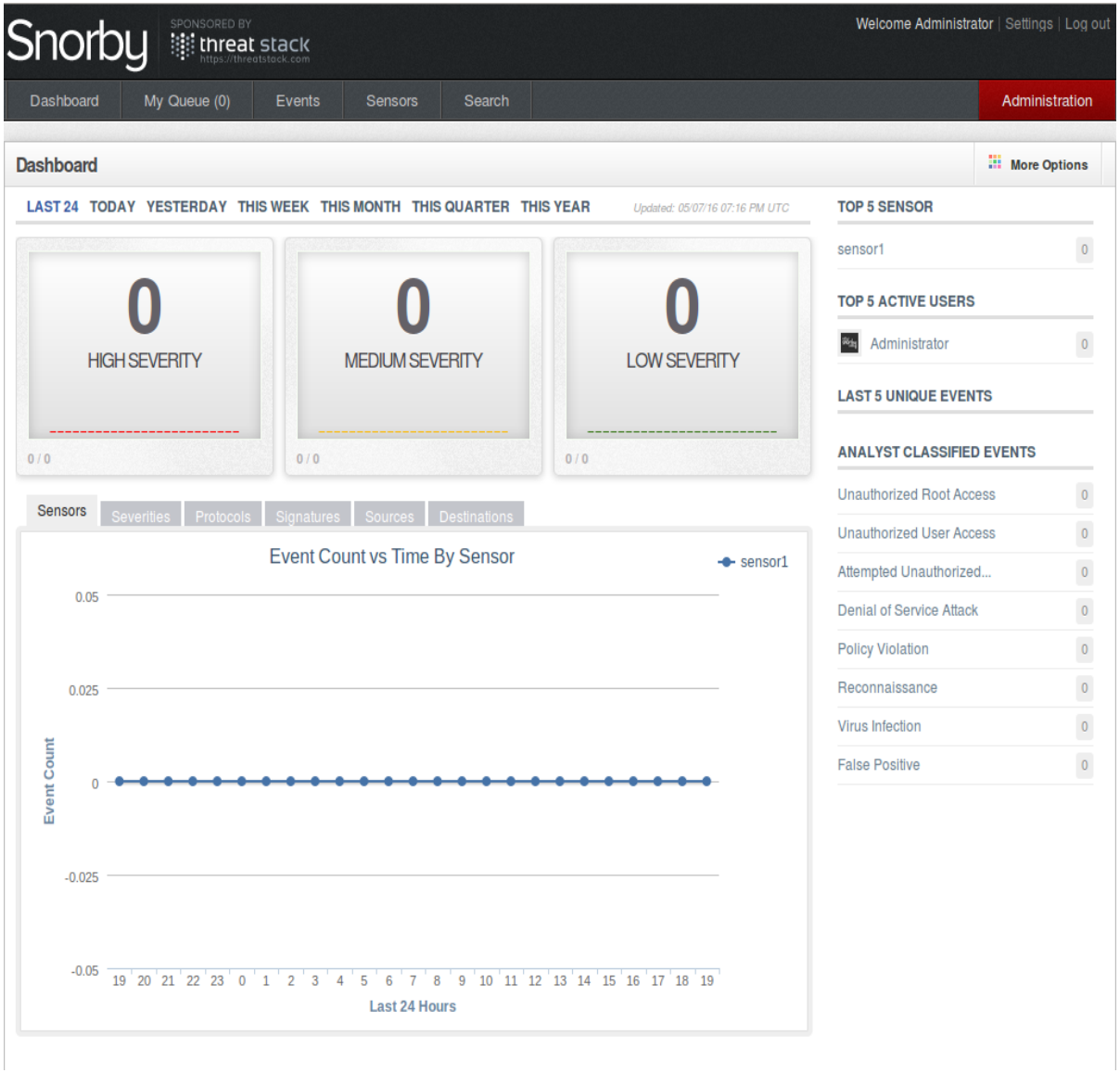
conjunto de reglas un poco mas completas utilizadas en versiones superiores a la 2.8.6, denominadas “emerging rules”. http://rules.emergingthreats.net/

REGLAS APLICADAS	
emerging-attack_response	Reglas para capturar los resultados de un ataque exitoso
emerging-dos	Permite capturar actividad asociada a ataques de denegación de servicio
emerging-icmp e icmp_info	Asociadas al uso de paquetes icmp de forma fraudulenta
emerging-sql	Detecta ataques SQL inyection, y relacionados
attack_response...emerging-web_ (cliente, server, specific).	ataque o vulnerabilidad en servicios Web
emerging-scan	Alertas para detectar el sondeo de puertos

GUIs para Snort

Aplicación	Pros	Contras
BASE	Muy usado como GUI para Snort.	Interfaz simple y anticuado. El panel de control solo informa del tráfico.
OSSIM	Se puede integrar con otras herramientas, además de Snort, como: p0f, arpwatch, pads, nessus, ntop, nagios.	Herramienta muy compleja de uso (gran curva de aprendizaje).
Place	Rapidez a la hora de gestionar muchos datos.	Instalación compleja. En desuso, su sitio Web oficial no esta online.
SGUIL	Permite agregar datos de distintas fuentes. Incluye análisis automáticos de los datos para detectar falsos positivos.	Enfocado a la minería de datos. No dispone de un cliente Web.
Snorby	**Dispone de una interfaz Web de las más actuales. Dispone de documentación completa para integrarse con Snort.**	**No es tan potente como otros sistemas.**
SQueRT	Dispone de una interfaz Web para consultar los datos. Proporcionar contexto adicional a los eventos a través del uso de metadatos, representaciones de series de tiempo y ponderados y conjuntos de resultados agrupados de forma lógica	Necesita de una BD con el formato de Sguil.
FirePower	Agrupa muchas características en un sistema extremadamente complejo mediante una intuitiva y fácil de navegar interfaz gráfica de usuario.Es perfecto para grandes redes.	Es una aplicación comercial.
Snez	Instalación y configuración simple.Permite crear filtros para descartar alertas de forma automática.	Interfaz Web muy simple.
IDS Policy Manager	Permite establecer múltiples sensores en entornos distribuidos.Permite administrar las reglas en forma de políticas por sensor.	Esta orientada a entornos Windows.

Snorby



Ventajas
Web 2.0
Buena documentación
Integración con Snort
Facilita la monitorización
Clasifica las alertas
Múltiples sensores
Acceso a fuentes externas