Tesina: Integración de herramientas de seguridad para redes informáticas

Autores: Matías Pagano y Einar Felipe Lanfranco

Director: Francisco Javier Díaz
Codirectora: Paula Venosa

Resumen

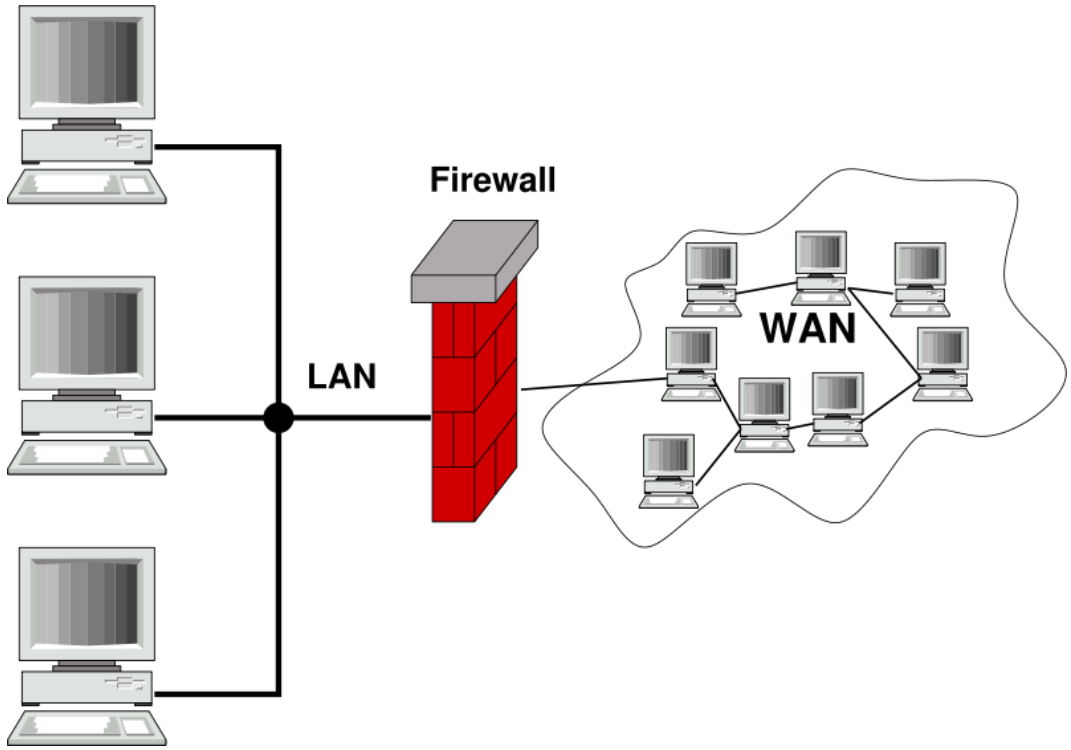
- Componentes a integrar
- Opciones analizadas y productos elegidos
- Integración
- Desarrollo
- Futuro
- Conclusiones

Componentes a integrar

Componentes a integrar

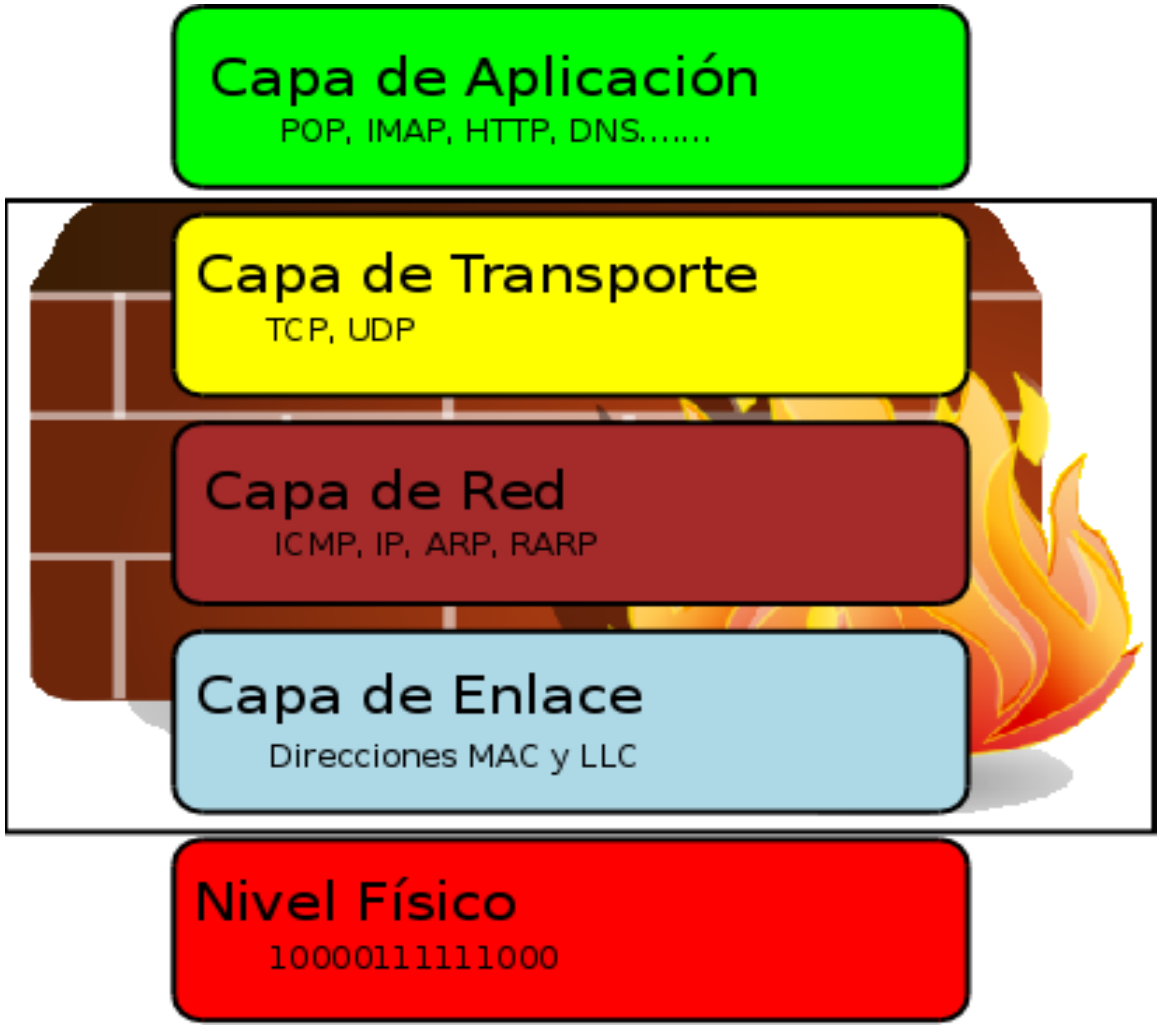
Firewall

- ¿Qué es un firewall?
  - Elemento que sirve para controlar las comunicaciones, permitiéndolas o prohibiéndolas, según las políticas definidas



Firewall

- En que capas trabaja



Componentes a integrar

IDS

- **¿Qué es un IDS?**
  Aplicación diseñada para examinar tráfico de red y/o archivos de logs en busca de comportamiento sospechoso.

- **¿Qué hace?**
  En su modo más simple de funcionamiento genera alertas.

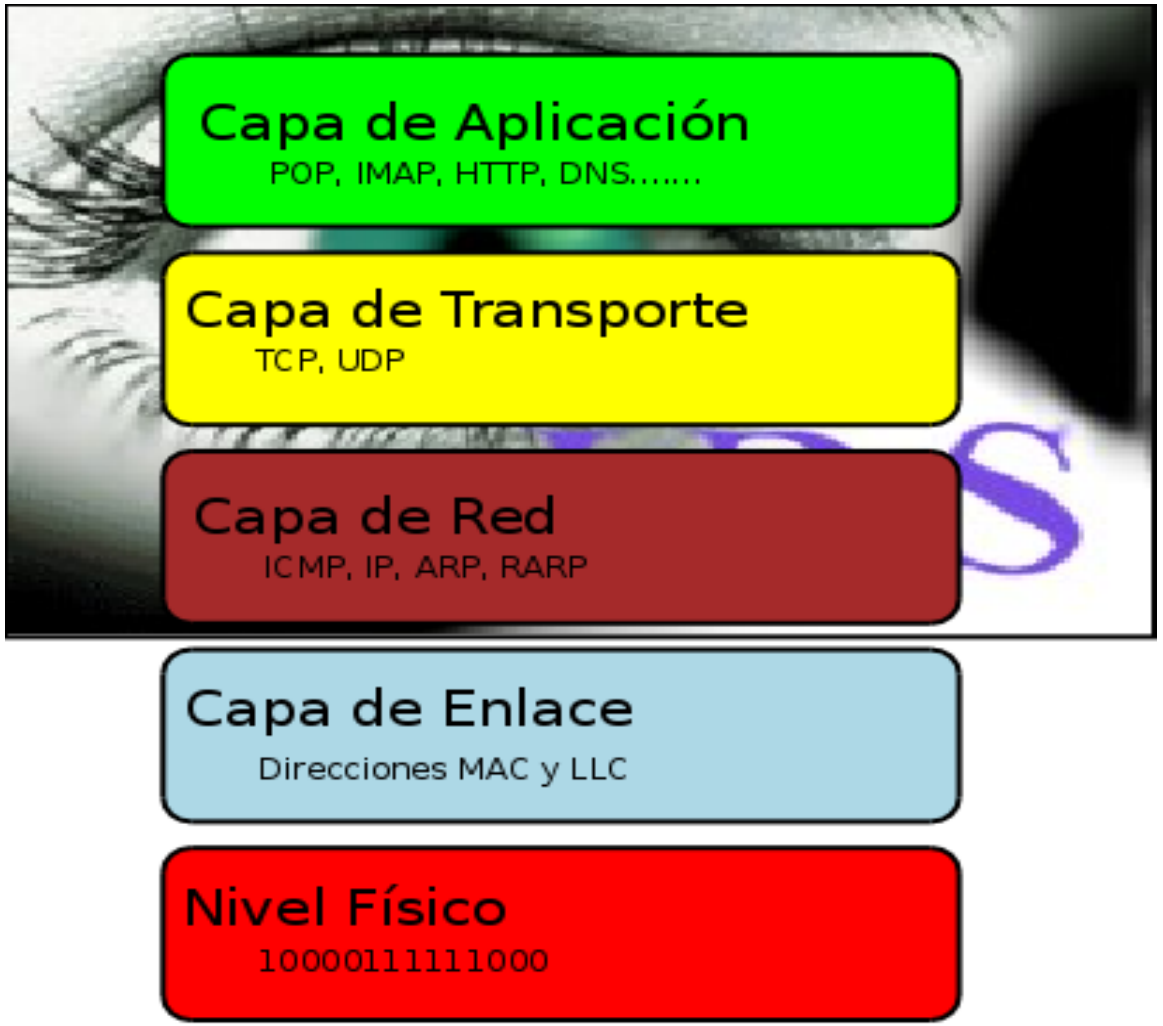
- **¿Para qué sirve?**
  Estas alertas permiten tomar las medidas necesarias para contrarrestar la actividad maliciosa o corregir los errores de configuración que se hayan detectado.

IDS

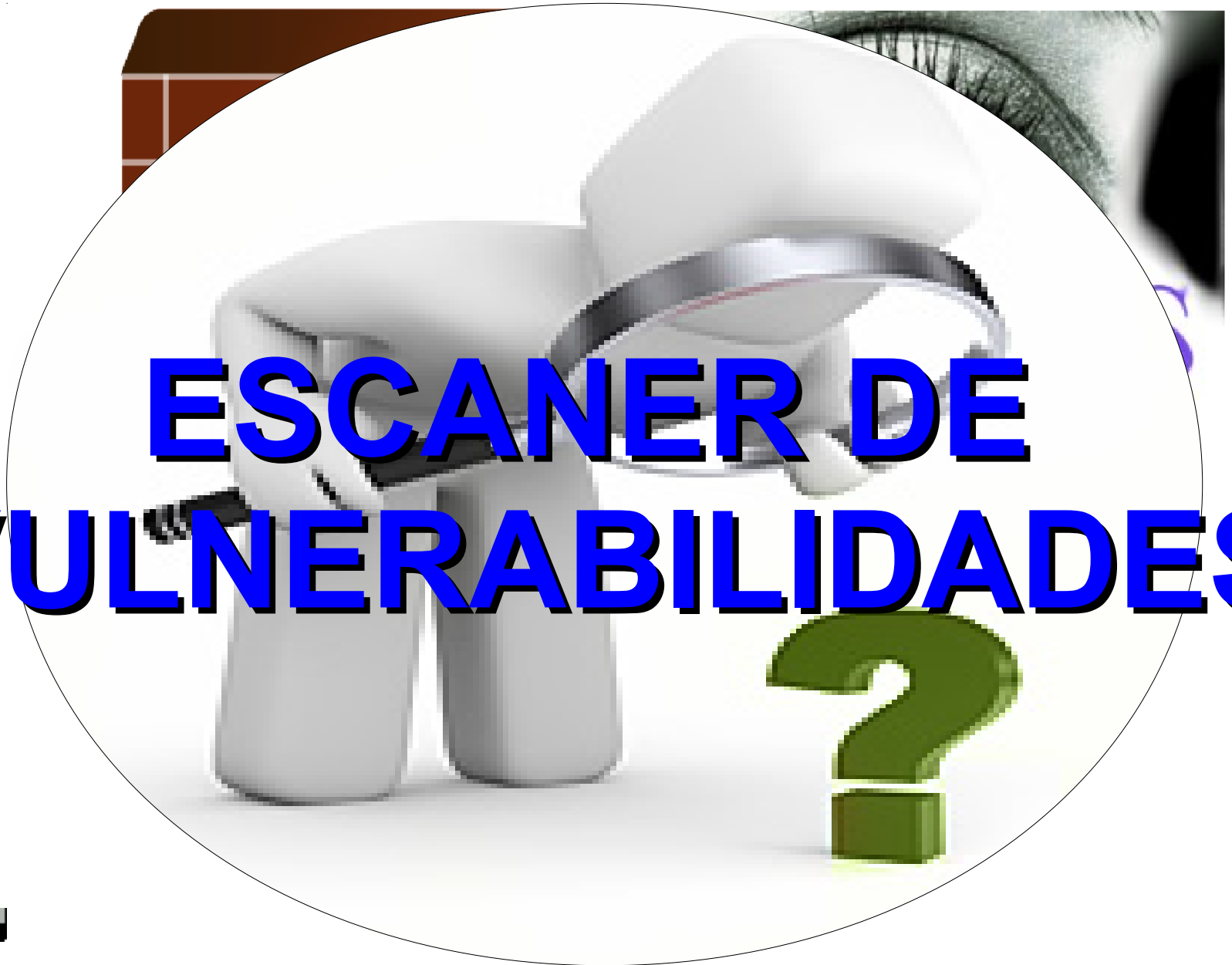
- Si ya se tiene un firewall, para qué se necesita un IDS?
  - Un sistema de detección de intrusiones funciona a manera de complemento del firewall.
  - Es un mecanismo de control que nos sirve para monitorear qué pasa dentro de nuestro entorno, una vez que se supera la barrera impuesta por el firewall.

IDS

- ¿En qué capas trabaja?



Componentes a integrar



Escaner de Vulnerabilidades

- **¿Qué es?**

  Un escaneador de vulnerabilidades es un programa diseñado para buscar fallas o debilidades en las aplicaciones o en su configuración.

- **¿Qué escanea?**

  Típicamente el ambiente de búsqueda es un host, un grupo de hosts en particular o todos los hosts de una red o subred dada.

Escaner de Vulnerabilidades

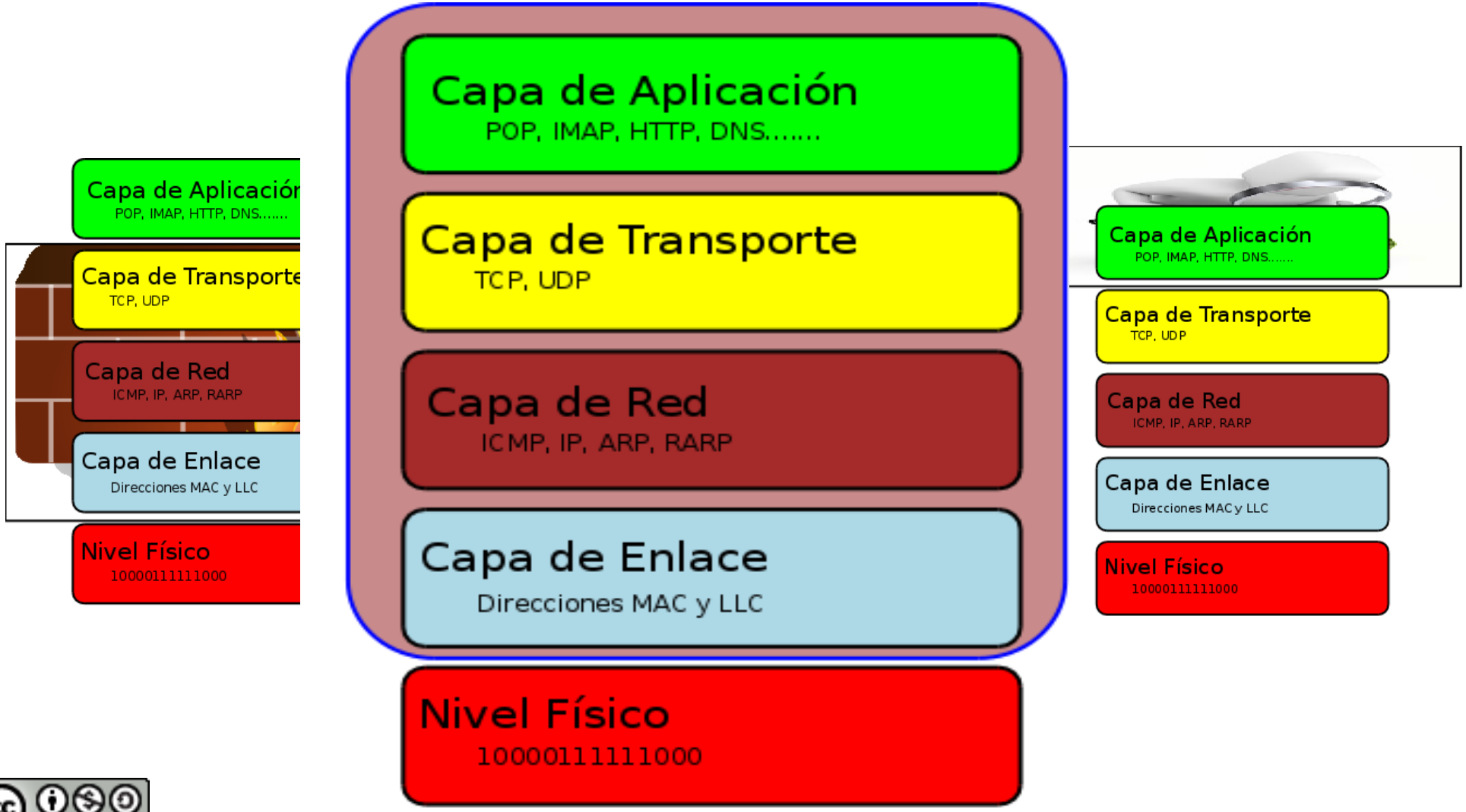
- **¿Cómo funciona?**
  - Busca direcciones IP activas
  - Intenta identificar los puertos abiertos
  - Intenta identificar qué sistema operativo y/o aplicaciones se están ejecutando
  - Finalmente intentará obtener la versión exacta de cada aplicación y cada sistema operativo para averiguar el nivel de actualización

Escaner de Vulnerabilidades

- ¿En qué capas trabaja?

Resultado

- ¿En qué capas trabaja?



Software a integrar

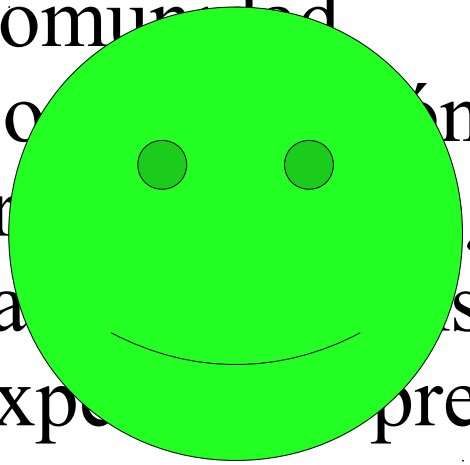
Criterios de selección:

- La licencia con la que se distribuye el software.
- La comunidad que lo utiliza.
- La documentación existente.
- Las pruebas realizadas cuando quisimos integrarlos.
- La facilidad de instalación.
- La experiencia previa en el uso de los mismos.

Elección de SO

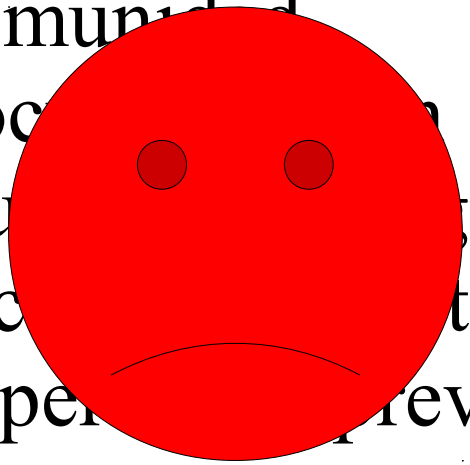
GNU/Linux

- ✔ Licencia
- ✔ Comunidad
- ✔ Documentación
- ✔ Programación
- ✔ Facilidad instalación
- ✔ Experiencia previa



BSD

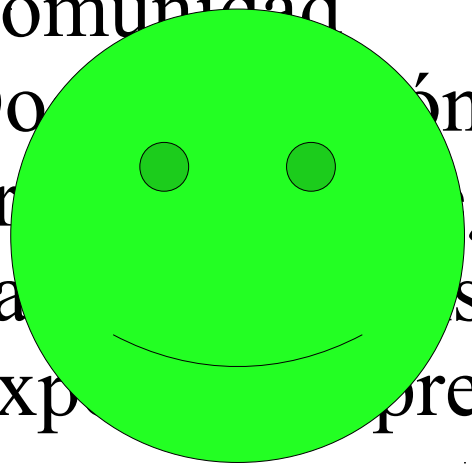
- ✔ Licencia
- ✔ Comunidad
- ✔ Documentación
- ✔ Programación
- ✔ Facilidad instalación
- ✗ Experiencia previa



Elección de FW

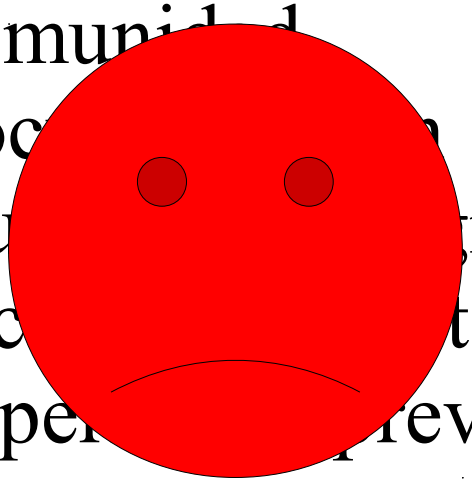
Netfilter/IPtables

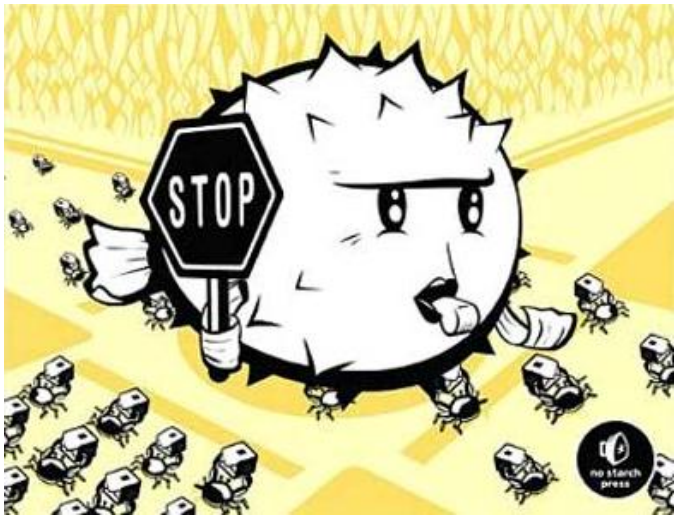
- ✔ Licencia
- ✔ Comunidad
- ✔ Do ón
- ✔ Pr gración
- ✔ Fa stalación
- ✔ Exp previa



PF/ BSD

- ✔ Licencia
- ✔ Comuni d
- ✔ Doc n
- ✔ Pru ración
- ✔ Fac talación
- ✗ Exper revia

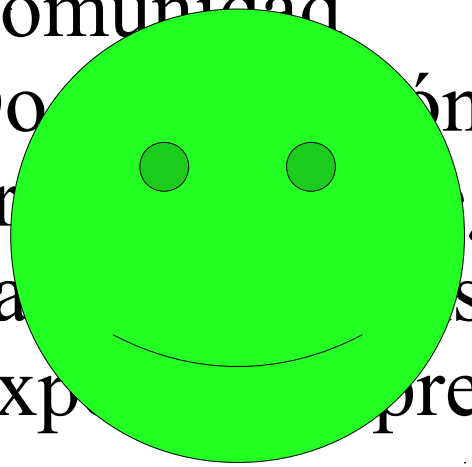




Elección de IDS

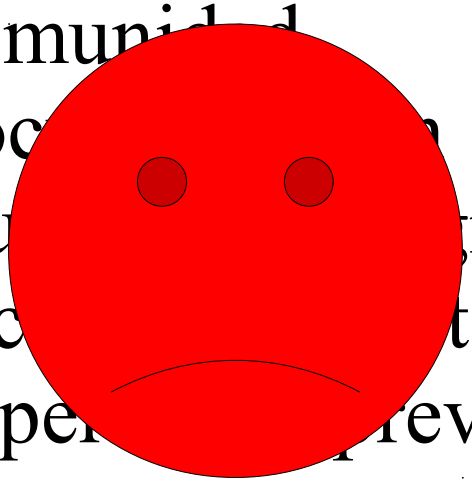
SNORT

- ✔ Licencia
- ✔ Comunidad
- ✔ Do ón
- ✔ Pr gración
- ✔ Fa stalación
- ✔ Exp previa



BRO - IDS

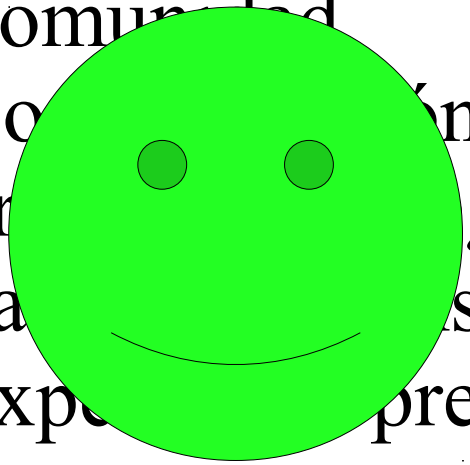
- ✔ Licencia
- ✔ Comuni d
- ✔ Doc n
- ✔ Pru ración
- ✗ Fac talación
- ✔ Exper revia



Elección de Escaner de Vuln.

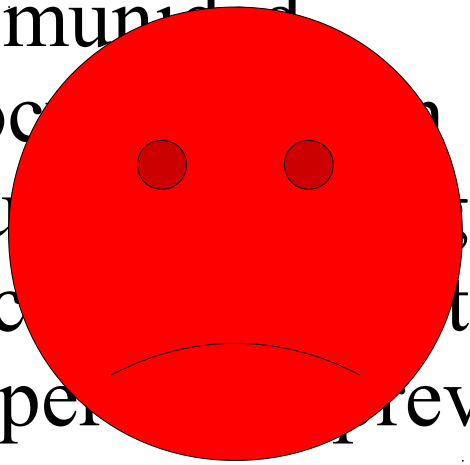
OpenVAS

- ✔ Licencia
- ✔ Comunidad
- ✔ Documentación
- ✔ Pruebas de integración
- ✔ Facilidad instalación
- ✔ Experiencia previa



Nessus

- ✗ Licencia
- ✔ Comunidad
- ✔ Documentación
- ✔ Pruebas de integración
- ✔ Facilidad instalación
- ✔ Experiencia previa



Opciones analizadas y productos elegidos

Integrando

- Reglas Iptables:

```
# REGLAS PARA LIMPIAR EL FIREWALL
iptables -F TESIS;

#### REGLAS DEL SERVIDOR: Sitio Web Linti (163.10.10.13/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.13 -p TCP --dport 80 -m state --state NEW -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.13 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.13 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Distancia (163.10.10.21/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.21 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.21 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Lihuen (163.10.10.17/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.17 -p TCP --dport 7000 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.17 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.17 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Mail del LINTI (163.10.10.61/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 993 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Listas (163.10.10.22/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.22 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.22 -p TCP --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 163.10.53.122 -d 163.10.10.22 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 163.10.33.64 -d 163.10.10.22 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 163.10.20.0 -d 163.10.10.22 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

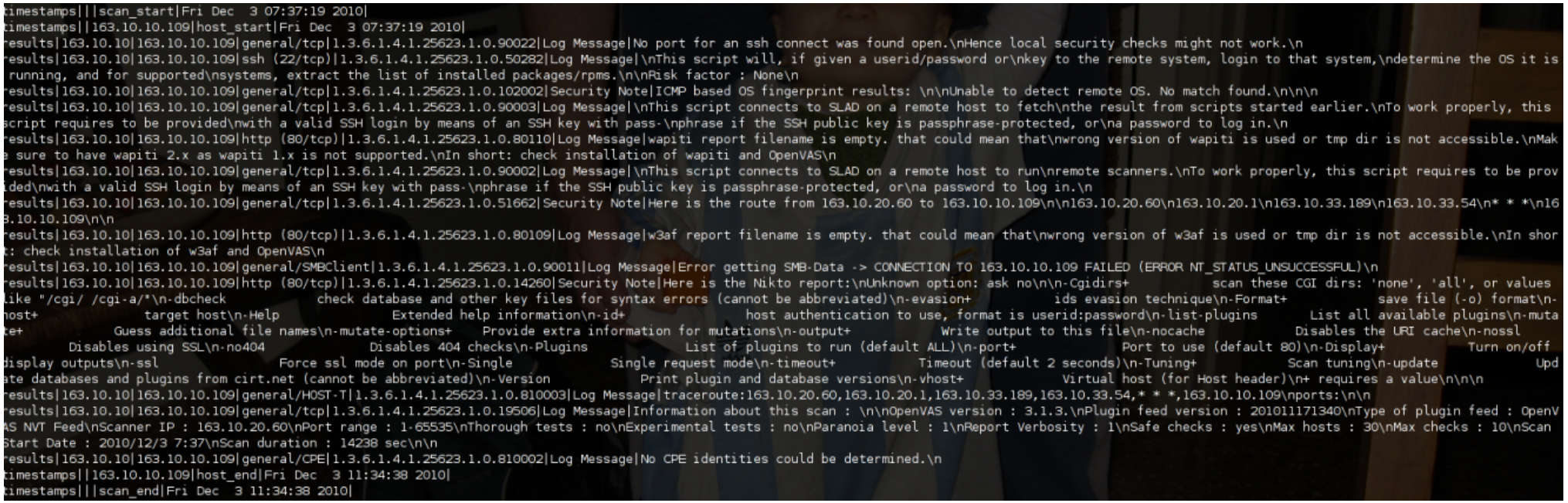
Integrando

- Alertas generadas por Snort:

```
[**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
05/15-08:20:54.377357 10.3.16.107 -> 10.3.9.152
ICMP TTL:57 TOS:0x0 ID:33363 IpLen:20 DgmLen:28
Type:8  Code:0  ID:22024   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS162]

[**] [122:1:0] (portscan) TCP Portscan [**]
[Priority: 3]
05/15-08:20:54.438127 10.3.16.107 -> 10.3.9.152
PROTO:255 TTL:0 TOS:0x0 ID:0 IpLen:20 DgmLen:157 DF

[**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
05/15-08:20:55.891333 10.3.16.107:41343 -> 10.3.9.152:705
TCP TTL:53 TOS:0x0 ID:45579 IpLen:20 DgmLen:44
******S* Seq: 0xC1DDAD5E  Ack: 0x0  Win: 0xC00  TcpLen: 24
TCP Options (1) => MSS: 1460
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0012][Xref => http://www.securi$

[**] [1:1420:11] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
05/15-08:20:59.097292 10.3.16.107:41343 -> 10.3.9.152:162
TCP TTL:48 TOS:0x0 ID:18580 IpLen:20 DgmLen:44
******S* Seq: 0xC1DDAD5E  Ack: 0x0  Win: 0x800  TcpLen: 24
TCP Options (1) => MSS: 1460
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0012][Xref => http://www.securi$

[**] [1:1418:11] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
05/15-08:21:00.498347 10.3.16.107:41343 -> 10.3.9.152:161
TCP TTL:56 TOS:0x0 ID:51164 IpLen:20 DgmLen:44
******S* Seq: 0xC1DDAD5E  Ack: 0x0  Win: 0x800  TcpLen: 24
```

Integrando

- Reporte de escaneo de OpenVAS:

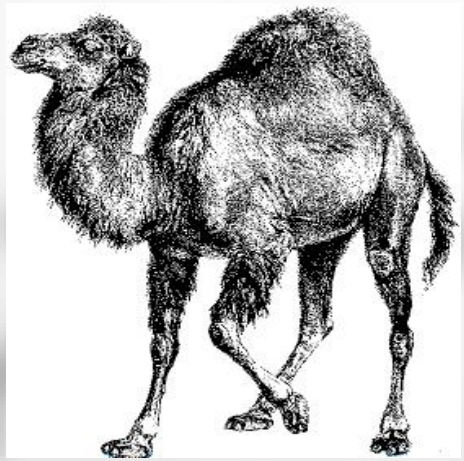


El producto

- **¿Qué buscamos?**
  - Integrar las herramientas con el fin de que lo que una produzca lo pueda utilizar el resto.
  - Unificar y congregar los resultados y la administración de cada una de estas herramientas
  - SIMPLIFICAR !!!!!!!
    - AHORRAR RECURSOS
    - DETECTAR Y MINIMIZAR ERRORES
    - DETECTAR Y RESPONDER RAPIDAMENTE A EVENTOS

El producto final

El producto final



MySQL®

catalyst
Web Framework

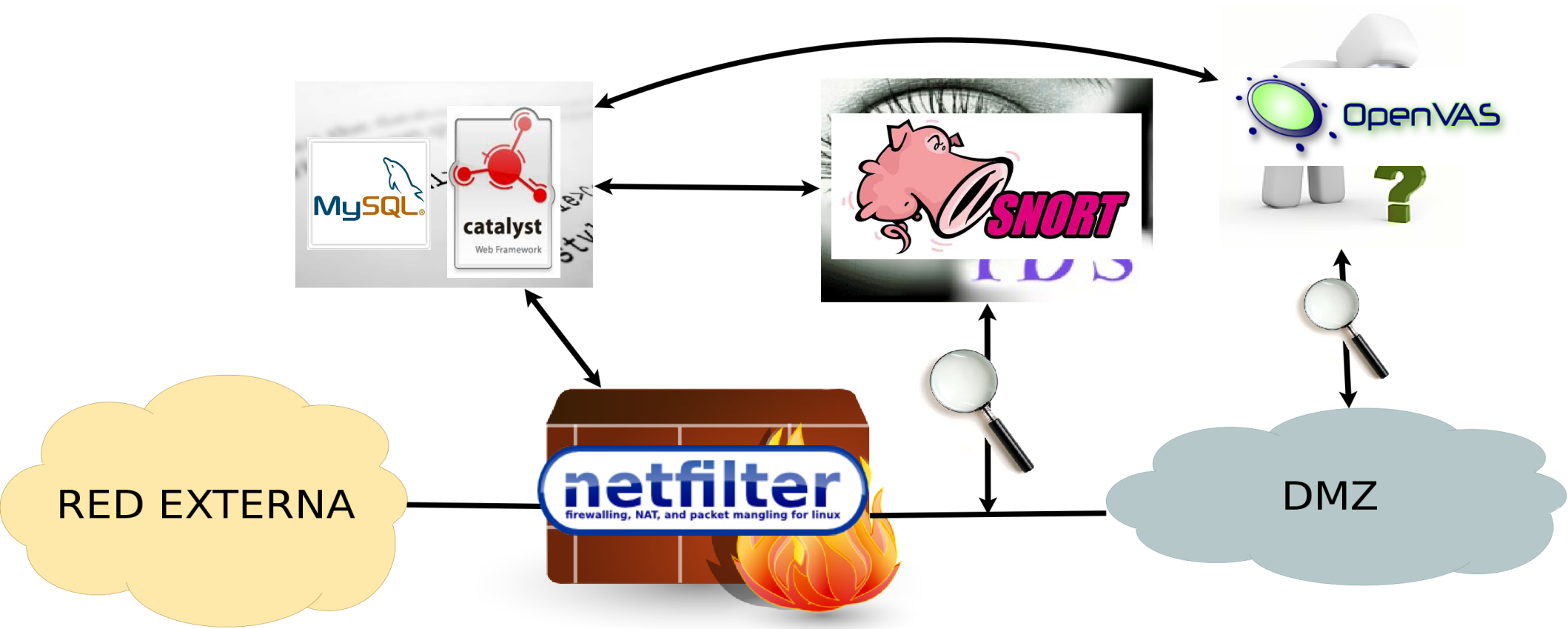
El producto final

- Respeta Model View Controller
- Dont Repeat Yourself
- Desarrollo Orientado a Objetos
- Aprueba validaciones de W3C (XHTML 1.0 Strict y CSS 2.1)
- Desarrollo distribuido usando Subversion

El producto final

- Algunas cifras sobre el trabajo realizado:
  - Más de 350 commits al repositorio
  - Cerca de 3000 líneas de código
  - Unos 100 archivos diferentes
  - 82 clases
  - 39 tablas en la base de datos

Producto final - Funcionamiento



Integración del Firewall:

- Tráfico a un servidor:

Tráfico: Sitio Web Linti (163.10.10.13/255.255.255.255)

Tráfico Entrante

PROTOCOLO	PUERTO	IP ORIGEN	MASCARA ORIGEN	ESTADO	HABILITADO	ACCION
TCP	80	0.0.0.0	255.255.255.255	NEW		
TCP	80	0.0.0.0	0.0.0.0	NEW,ESTABLISHED,RELATED		
TCP	443	0.0.0.0	0.0.0.0	NEW,ESTABLISHED,RELATED		

Tráfico Saliente

PROTOCOLO	PUERTO	IP DESTINO	MASCARA DESTINO	ESTADO	HABILITADO	ACCION

Tráfico Entrante Bloqueado

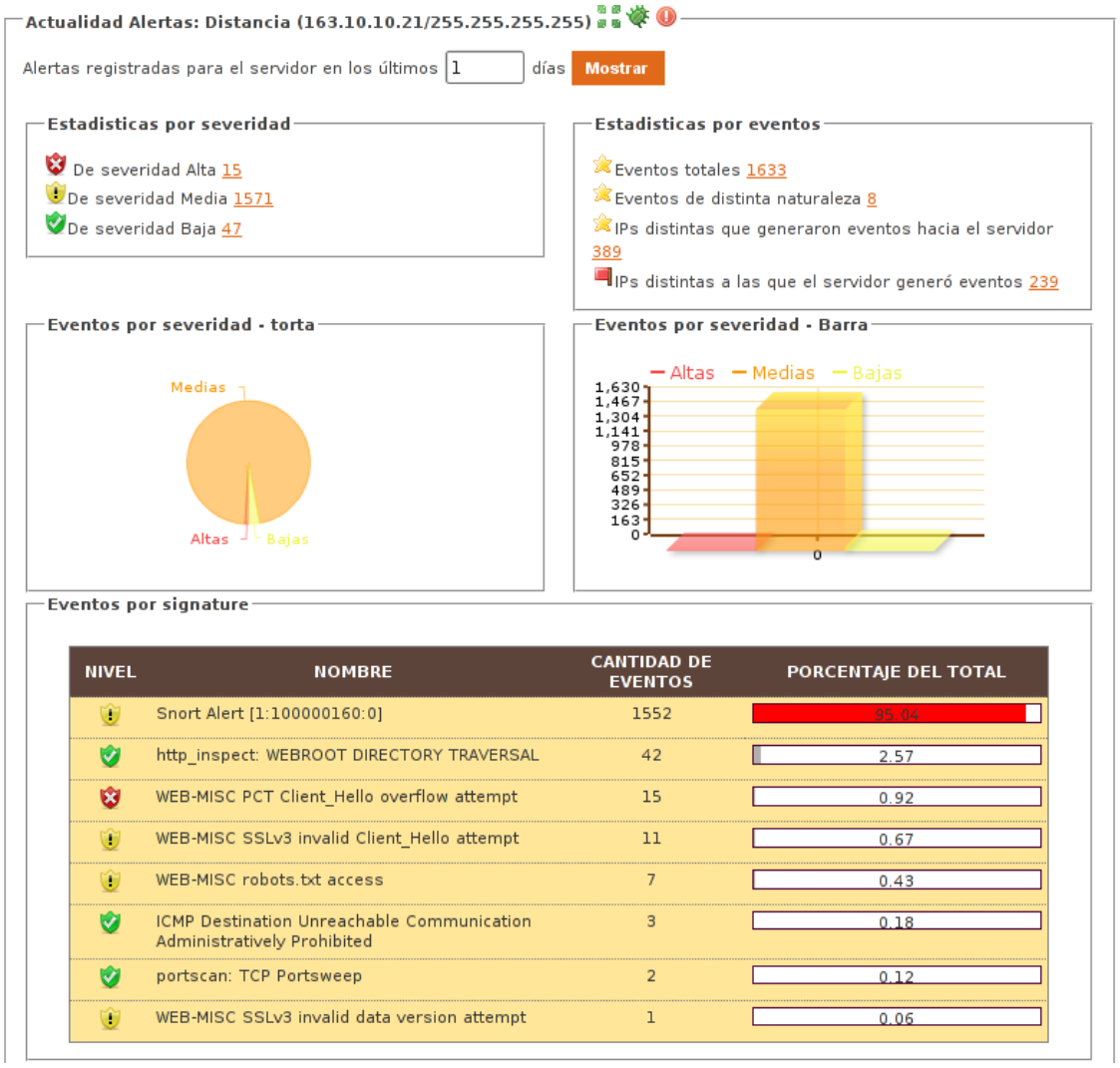
PROTOCOLO	PUERTO	IP ORIGEN	MASCARA ORIGEN	ESTADO	ACCION

Tráfico Saliente Bloqueado

PROTOCOLO	PUERTO	IP DESTINO	MASCARA DESTINO	ESTADO	ACCION

Integración del IDS:

- Alertas de un servidor:



Actualidad Alertas: Distancia (163.10.10.21/255.255.255.255)

Alertas registradas para el servidor en los últimos 1 días **Mostrar**

Estadisticas por severidad

- De severidad Alta 15
- De severidad Media 1571
- De severidad Baja 47

Estadisticas por eventos

- Eventos totales 1633
- Eventos de distinta naturaleza 8
- IPs distintas que generaron eventos hacia el servidor 389
- IPs distintas a las que el servidor generó eventos 239

Eventos por severidad - torta

Eventos por severidad - Barra

Eventos por signature

NIVEL	NOMBRE	CANTIDAD DE EVENTOS	PORCENTAJE DEL TOTAL
	Snort Alert [1:100000160:0]	1552	95.04
	http_inspect: WEBROOT DIRECTORY TRAVERSAL	42	2.57
	WEB-MISC PCT Client_Hello overflow attempt	15	0.92
	WEB-MISC SSLv3 invalid Client_Hello attempt	11	0.67
	WEB-MISC robots.txt access	7	0.43
	ICMP Destination Unreachable Communication Administratively Prohibited	3	0.18
	portscan: TCP Portsweep	2	0.12
	WEB-MISC SSLv3 invalid data version attempt	1	0.06

Integración del Escaner de Vulnerabilidades:

- Reporte de escaneo :

Resultado de Escaneo

Actualidad Escaneo: Sitio Web Linti (163.10.10.13/255.255.255.255)

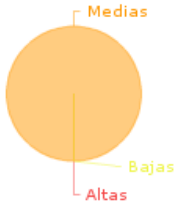
Detalle

Servidor: **163.10.10.13/255.255.255.255**
Frecuencia: **Diario**
Estado: **Fin**
Último Escaneo: **06/12/2010**

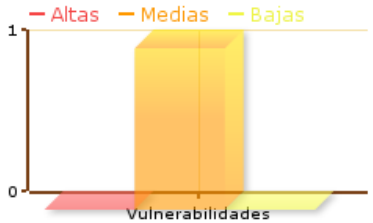
Estadisticas por severidad

De severidad Alta 0
De severidad Media 1
De severidad Baja 0

Vulnerabilidades por severidad - Torta



Vulnerabilidades por severidad - Barras



Resultado del Último Escaneo (06/12/2010)

IP	PUERTO	OID	TIPO	RIESGO	CVE	
		DE SEVERIDAD MEDIA				
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.100153	Security Warning	Medium	CVE-2008-5161	+
		INFORMACIÓN				
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.50282	Log Message	None		+
163.10.10.13	http (80/tcp)	1.3.6.1.4.1.25623.1.0.10386	Security Note	None		+
163.10.10.13	general/tcp	1.3.6.1.4.1.25623.1.0.80091	Security Note	None		+
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.100259	Security Note	None		+
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.10330	Security Note	-		+
163.10.10.13	http (80/tcp)	1.3.6.1.4.1.25623.1.0.10330	Security Note	-		+
163.10.10.13	https (443/tcp)	1.3.6.1.4.1.25623.1.0.10330	Security Note	-		+

Trabajos a Futuro

- Retribuir a la comunidad del software libre
- ~~Instalar el software en un ambiente producción~~
- Mejorar la documentación
- Empaquetar la aplicación para facilitar su distribución
- ~~Desarrollar una guía de instalación.~~
- ~~Agregar la posibilidad de reglas por defecto para el Firewall~~
- Mejorar la parte de auditoría del sistema
- Exportar alertas del Snort y resultados de escaneos a varios formatos
- Subir reportes de escaneos antiguos con fines estadísticos
- Desarrollar un módulo de reportes vía mail
- Agregar el soporte para IPV6.
- Agregar la posibilidad de utilizar múltiples IDS

Ambiente en producción

DEMO!!!!

Conclusiones

- El software que planteamos inicialmente como un prototipo hoy es un sistema puesto en producción en un ambiente real.
- No es necesario ser un experto para manejar el sistema.
- El sistema integra eficazmente herramientas de distinta naturaleza cubriendo casi todas las capas del modelo TCP-IP.
- Respeta los estándares de desarrollo web de la W3C y sigue buenas técnicas de programación como MVC y DRY.

Conclusiones

- Consideramos que el texto resultante es un buen punto de partida para introducirse en los temas de seguridad involucrados.
- El trabajo se realizó íntegramente utilizando aplicaciones de Software Libre, desde la propuesta hasta el desarrollo de esta presentación.

¿Preguntas?