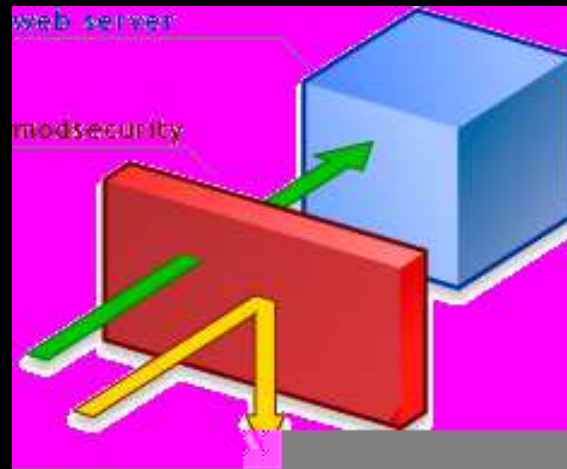


# Seguridad en portales

---



Ernesto Crespo

VELUG [www.velug.org.ve](http://www.velug.org.ve)

Debian Venezuela [www.debianvenezuela.org](http://www.debianvenezuela.org)

[ecrespo@debianvenezuela.org](mailto:ecrespo@debianvenezuela.org)

# Agenda

---

- Introducción
- ¿Como mejorar la seguridad?
- ¿Qué es mod-security?
- Ventajas
- Características
- Instalación
- Configuración Básica
- Mod-security+proxy inverso

# Introducción

---

- Las aplicaciones web son el punto más vulnerable en la infraestructura de una empresa
- Cada día son más los ataques en la capa HTTP:
  - Inyección SQL
  - XSS
  - Inyección de comandos
  - Buffer overflow
- Las vulnerabilidades crecen y las soluciones no
- La mayoría de los firewalls trabajan a nivel de capa de red

# ¿Como mejorar la seguridad?

---

- Definir esquema de particiones:
  - Partición /tmp con noexec y noexec
  - Colocar /usr sólo lectura
  - Crear una partición /boot
- Definir los usuarios que pueden administrar el portal remotamente
- Parchear el kernel de linux para soporte de grsecurity o selinux
- Límitar la cantidad de usuarios que puedan convertirse en root (dios)
- Utilizar herramientas de registro de eventos e IDS (snort,mod\_security,portsentry,logcheck)
- Prender un vela

# grub

---

## ■ Asegurando la seguridad del arranque (grub)

### ● Ejecutar:

- ▶ jewel:~# grub-md5-crypt
- ▶ Password:
- ▶ Retype password:
- ▶ \$1\$t18EM1\$fBCXycPjd.fnL8i9lcS6D0

### ● Agregar la clave en el archivo /boot/grub/menu.lst

- ▶ password --md5 \$1\$t18EM1\$fBCXycPjd.fnL8i9lcS6D0
- ▶ Esto evita que modifiquen el grub
- ▶ También se puede usar la opción password luego del título de un kernel y así se evita el arranque del equipo sin clave

# inittab

---

## ■ Definir que usuarios pueden ejecutar control+alt+del

### ● Editar el archivo /etc/inittab

- ▶ # what to do when CTRL-ALT-DEL is pressed
- ▶ ca::ctrlaltdel:/sbin/shutdown -a -r -t 4 now
- ▶ Con la opción -a se define el uso del archivo shutdown.allowed

root

bob

sarah

- ▶ Si se desea evitar que ejecuten ctrl-alt-del se cambia a:

ca::ctrlaltdel:

# vlock

---

## ■ Asegurando los terminales virtuales

- Para bloquear la consola se ejecuta:
  - `vlock -c`
- Para desbloquear la consola se pide la clave
- Para deshabilitar todos los terminales se ejecuta:
  - `vlock -a`

# login screen

---

- Es necesario quitar los mensajes de inicio de sesión tanto remoto como local
  - `clear > /etc/issue`
  - `clear > /etc/issue.net`
- Esto se hace para evitar que los atacantes tengan información que puedan usar en sus ataques
- El archivo `issue` contiene lo siguiente:
  - `cat /etc/issue`
  - Debian GNU/Linux testing

# Acceso a usuarios

---

- Borrar los usuarios y grupos que no sean necesarios
- Verificar las claves que los usuarios usan, archivo `/etc/pam.d/password`:
  - `auth required pam_unix2.so nullok obscure min=6 max=11 md5`
- Habilitar el módulo `cracklib` para verificar la complejidad de las claves
- Habilitando el registro de los accesos positivos al sistema, archivo `/etc/login.defs`:
  - `LOG_OK_LOGINS yes`
- Activando el registro de accesos como root:
  - `SULOG_FILE /var/log/sulog`

# Contabilidad

---

- Registros de los comandos ejecutados por los usuarios.  
acct
  - Muestra los comandos ejecutados por los usuarios
    - sa -a
  - Contabilidad del acceso. sac
    - Este programa lee el archivo `/var/log/wtmp` mostrando la información de forma digerible

# Deshabilitando servicios que no se esten utilizando

---

- Eliminado paquetes que no sean necesarios:
  - Debian: `aptitude remove paquete`
- Desactivando servicios que no se esten utilizando
  - Debian: `update-rc.d -f servicio remove`
- Deshabilitar el reenvio de correos (exim):
  - `local_interfaces = "127.0.0.1"`

# ¿Qué es mod-security?

---

- Es un módulo de apache que brinda detección y prevención de intrusos para el servidor web apache
- Normalmente se llama firewall de aplicaciones
- Funcionamiento similar a un IDS que trabaja a nivel de HTTP
- Además de detectar previene si encuentra peticiones maliciosas

# Ventajas

---

- Protege complejas aplicaciones web
- Se puede utilizar para proteger foros, blogs, wikis, portales, etc
- Es Software Libre
- Fácil de configurar
- Curva de aprendizaje muy rápida
- Se puede evitar un alto número de ataques con pocas líneas de configuración
- Se pueden crear reglas muy específicas para optimizar el rendimiento de mod-security
- Se pueden usar las reglas del IDS snort

# Características

---

- Filtrado de peticiones
- Técnicas Anti-Evasión:
  - Elimina múltiples barras (//)
  - Elimina directorios referenciados por si mismos (./)
  - Tratamiento de / y Decodificación URL
  - Reemplazo de bytes nulos por espacios
- Comprensión de HTTP permitiendo filtrados más específicos
- Intercepta y analiza contenido transmitido por el método POST
- Genera Bitacoras
- Filtrado del protocolo HTTPS
- Filtrado de contenido comprimido

# Instalación

---

## ■ Instalando desde las fuentes:

- `wget http://www.modsecurity.org/download/modsecurity-1.8.7.tar.gz`
- `tar -pzxvf mod_security-1.8.7.tar.gz`
- Caso apache2:
  - `cd modsecurity-1.8.7/apache2`
  - `apxs -cia mod_security.c`
  - Copiar los módulos en `/usr/lib/apache2/modules/`

## ■ Instalación en debian

- `apt-get install libapache2-mod-security mod-security-common`

# Instalación (continuación)

---

## ■ Cargar módulos en apache:

- Desde las fuentes:

- Editar el archivo de configuración de apache2 y se agrega:

```
LoadModule security_module modules/mod_security.so
```

- Del paquete en debian:

- Hacer el enlace:

```
ln -s /etc/apache2/mods-available/mod-security.load /etc/apache2/mods-enabled/mod-security.load
```

## ■ Reiniciar apache

- /etc/init.d/apache2 restart

# Configuración

---

Agregar las siguientes líneas en el archivo de configuración de apache2

- Activar mod\_security
  - SecFilterEngine On
- Escanear el contenido de peticiones POST
  - SecFilterScanPOST On
- Escanear la respuesta de la petición
  - SecFilterScanOutput On
- Verificar codificación URL
  - SecFilterCheckURLEncoding On
- Verificar codificación Unicode
  - SecFilterUnicodeEncoding On
  - SecFilterCheckUnicodeEncoding Off
- Permitir solo cierto valores de los bytes
  - SecFilterForceByteRange 1 255

# Configuración (Continuación)

---

## Reglas:

- Loguear peticiones, solo las invalidas, para posterior análisis
  - SecAuditEngine RelevantOnly
  - SecAuditLog /var/log/apache2/audit\_log
- Por defecto, denegar las peticiones con mensaje de estado 500
  - SecFilterDefaultAction "deny,log,status:500"

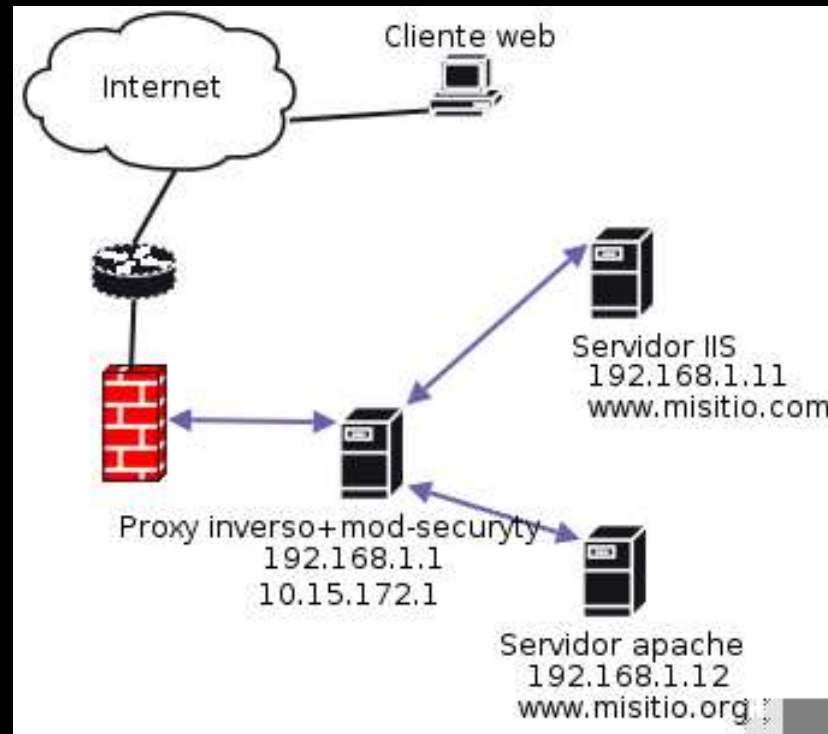
# Configuración (Continuación)

---

## Reglas:

- Define que el servidor es un Microsoft IIS
  - SecServerSignature "Microsoft IIS/1.0"
  - SecServerResponseToken Off
- Protección contra buffer overflow
  - SecFilterSelective ARG\_nombre ".{6,}" "redirect:http://www.google.es"
- Se prohíbe subir archivos
  - SecFilterSelective "HTTP\_CONTENT\_TYPE" multipart/form-data)"
- Si alguien quiere acceder al administrador se redirige a [www.google.com](http://www.google.com)
  - Secfilter ?/admin/administrar.php? redirect:http://www.google.com

# Proxy inverso+mod-security



- Mod-security con un proxy inverso puede resguardar 1 o más servidores
- Un solo punto de control
- Ocultamiento de la topología de la red
- Mejor rendimiento al descargar el servidor web del filtrado

# Proxy inverso + mod-security (cont...)

---

- Añade complejidad al sistema y es un único punto de fallas
- Requerimientos:
  - Apache
  - mod\_proxy y mod\_proxy\_http
  - mod\_security
  - mod\_ssl

# Proxy inverso + mod-security (cont...)

---

## ■ Configuración de virtual host

- <VirtualHost www.misitio.com>
- ServerName www.misitio.com
- #Rechazamos peticiones de proxy, para que no sea un proxy abierto
- ProxyRequests Off
- ProxyPass / http://192.168.1.11/
- ProxyPassReverse / http://192.168.1.11/
- ServerName www.misitio.org
- ProxyRequests Off
- ProxyPass / http://192.168.1.12/
- ProxyPassReverse / http://192.168.1.12/
- </VirtualHost>

# Proxy inverso + mod-security (cont...)

---

- Se heredan las reglas del mod-security anterior
- No funciona la definición de IIS para los servidores web
- Se tiene que instalar mod\_headers y se agrega lo siguiente en apache:
  - Header set Server ?Microsoft IIS/1.0?

# Conclusiones

---

- La seguridad es lo más importante
- Configuración simple
- Alto aporte en la seguridad de la infraestructura
- Cada día se agregan nuevas funcionalidades

# Referencias

---

- <http://www.debian-administration.org/articles/65>
- <http://www.onlamp.com/lpt/a/5917>
- <http://www.securityfocus.com/infocus/1739>
- [http://www.eth0.us/mod\\_security](http://www.eth0.us/mod_security)