

Instalar ModSecurity no Debian + Apache2

Autor: Luiz Cezar Quaquio

Convenções utilizadas neste documento:

- O símbolo "#" significa que o comando deve ser executado como root;

O ModSecurity (<http://www.modsecurity.org>) é um firewall de aplicação que é executado como um módulo do servidor Web Apache. O WAF (Web Application Firewall), ou firewall de aplicação, tem por objetivo bloquear diversos tipos de ataques, como o Cross-Site Scripting (XSS), SQL Injection, Command Injection, ASP e PHP Injection, Trojans & Backdoors Detection, dentre outros, que variam de acordo com as regras existentes. Instale o ModSecurity:

```
# aptitude install libapache2-modsecurity
```

Caso o pacote não esteja disponível, adicione o repositório "Backports". Após a instalação, crie o diretório abaixo:

```
# mkdir /etc/apache2/modsecurity
```

Crie o arquivo de configuração do ModSecurity que irá ser carregado pelo Apache:

```
# vi /etc/apache2/conf.d/modsecurity.conf
```

Adicione as duas linhas abaixo no arquivo:

```
## /etc/init.d/apache2/conf.d/modsecurity.conf
```

```
Include modsecurity/*.conf
```

Entre no diretório que nós criamos do ModSecurity para copiar as regras que por padrão já vem configuradas:

```
# cd /etc/apache2/modsecurity
```

```
# cp -R /usr/share/modsecurity-crs/base_rules/* .
```

Edite o arquivo de regra `modsecurity_crs_20_protocol_violations.conf` para corrigir um erro, antes de reiniciar o Apache2:

```
# vi /etc/apache2/modsecurity/modsecurity_crs_20_protocol_violations.conf
```

Edite a linha 90 e substitua a variável `REQBODY_ERROR`, por `REQBODY_PROCESSOR_ERROR`, ficará assim:

```
SecRule REQBODY_PROCESSOR_ERROR "!@eq 0" \
```

Inicie os módulos:

```
# a2enmod mod-security unique_id headers
```

Configure o Debug adicionando no arquivo `modsecurity_crs_10_config.conf`:

```
SecDebugLog /var/log/apache2/modsec_debug.log
```

```
SecAuditLog /var/log/apache2/logs/modsec_audit.log
```

Reiniciar o Apache:

```
# /etc/init.d/apache2 restart
```

Para verificar se o ModSecurity carregou com o Apache:

```
# cat /var/log/apache2/error.log | grep modsecurity
```

O retorno deve ser:

```
ModSecurity for Apache/2.5.13 (http://www.modsecurity.org/) configured.
```

Para testar crie o arquivo `test.php` com o conteúdo abaixo:

```
<?php
```

```
    $secret_file = $_GET['secret_file'];
```

```
    include ( $secret_file);
```

```
?>
```

Execute no seu navegador:

HTTP://seuip.com /test.php?secret_file=/etc/passwd

Se tudo estiver funcionando corretamente uma mensagem “403 Forbidden” deve aparecer!

Referências:

<http://allandc.wordpress.com/2010/10/04/instalar-modsecurity-no-debian-lenny/>

<http://www.grosseosterhues.com/2011/07/enabling-mod-security-protection-in-apache2-on-ubuntu/>