FIELD NOTE / CENTOS

Amankan Web Server dengan ModSecurity & Mod Evasive

Petruknisme · 25 May, 2016 · 6 min to read

Sekarang ini kita sering mendengar berita tentang peretasan situs pemerintahan Indonesia oleh orang yang mengatasnamakan dirinya adalah '*hacker*'. Tak lupa juga pesan yang selalu mereka tinggalkan untuk sang _web administrator _ataupun kritikan keburukan sistem yang ada. Banyak metode yang bisa dilakukan untuk menyerang suatu website dari mulai PHP Script, Web Server, Web Hosting dan masih banyak cara lainnya.

Mungkin diantara kita sudah tak asing lagi dengan istilah *SQL Injection*, _XSS, *Local File Inclusion* (*LFI*), _Remote File Inclusion(RFI) __dan lain-lain yang digunakan oleh _attacker _untuk mendapatkan akses terhadap website ataupun sistem itu sendiri dari celah yang ia temukan. Aplikasi yang bagus harus memperhatikan 3 hal, yaitu : Jaringan(Network), Aplikasi dan Manusia. Ketiga hal tersebut berkesinambungan dalam menjadikan aplikasi yang bagus–dalam artian keamanan–, karena seorang _attacker _akan melakukan serangan melalui 3 hal tersebut. Bisa jadi aplikasi yang dibuat sudah bagus dan jaringan pun bagus tapi ada celah pada manusia itu sendiri untuk dieksploitasi dengan _Social Engineering. _Seperti kata pepatah seorang *Social Engineer*

> *"If you cannot hack the machine, then hack the human"*

Dalam artikel ini akan membahas untuk melakukan pengamanan dari segi _web server. _Kita akan menggunakan ModSecurity sebagai Web Application Firewall(WAF) –atau bisa juga menjadi Intrusion Detection System(IDS)– yang berguna untuk melakukan proses *filtering* terhadap data yang masuk melalui protokol HTTP dan juga mampu melakukan tindakan tertentu sesuai dengan aturan(rules) yang sudah dibuat untuk menangani setiap proses data *filtering*. Sedangkan, Mod Evasive akan kita gunakan untuk DDoS Protection.

Apa yang bisa dilakukan ModSecurity?

- Real-time application security monitoring and access control
- Full HTTP traffic logging
- Web application hardening
- etc

Menggunakan ModSecurity membutuhkan rules tambahan agar lebih maksimal dalam mendeteksi serangan. Yang disebut sebagai Core Rule Set(CRS) dan kita masih bisa membuat rules sendiri.

Serangan apa yang bisa dideteksi oleh CRS?

- HTTP Protection – detecting violations of the HTTP protocol and a locally defined usage policy.

Licensed under CC BY-SA 4.0

- Real-time Blacklist Lookups – utilizes 3rd Party IP reputation.
- HTTP Denial of Service Protection – defense against HTTP flooding and slow HTTP DoS attacks.
- Common Web Attacks Protection – detecting common web application security attacks.
- Automation Detection – Detecting bots, crawlers, scanners and other surface malicious activity.
- Integration with AV Scanning for File Uploads – detects malicious files uploaded through the web application.
- Tracking Sensitive Data – Tracks credit card usage and blocks leakages.
- Trojan Protection – Detects trojan horses.
- Identification of Application Defects – alerts on application mis-configurations.
- Error Detection and Hiding – Disguising error messages sent by the server.

Sebelum memulai instalasi ModSecurity dan OWASP Core Rule Set, ada baiknya untuk melakukan pembaruan sistem. Saya disini menggunakan CentOS 7 dengan Apache 2 dan untuk distro lain bisa disesuaikan.

```
yum -y update
```

Beberapa _dependencies _diperlukan sebelum melakukan instalasi ModSecurity. Semua tergantung dari konfigurasi server dan paket yang mungkin sudah terinstal. Yum akan melakukan instalasi untuk paket yang belum terpasang dan akan menginformasikan bila sudah terpasang pada sistem

```
yum -y install httpd-devel git gcc make libxml2 pcre-devel libxml2-devel c
```

Unduh *source code* dari website ModSecurity. Versi stabil saat ini adalah 2.9.1

```
cd /opt/
wget https://www.modsecurity.org/tarball/2.9.1/modsecurity-2.9.1.tar.gz
```

_Extract _arsip ModSecurity

Licensed under CC BY-SA 4.0

```
tar zxvf modsecurity-2.9.1.tar.gz
cd modsecurity-2.9.1/
```

Konfigurasi dan lakukan proses kompilasi terhadap *source code*

```
./configure
make
make install
```

Salin konfigurasi bawaan ModSecurity dan file unicode mapping ke direktori Apache

```
cp modsecurity.conf-recommended /etc/httpd/conf.d/modsecurity.conf
cp unicode.mapping /etc/httpd/conf.d/
```

Konfigurasi Apache agar menggunakan modul ModSecurity

```
echo LoadModule security2_module modules/mod_security2.so >> /etc/httpd/co
```

Oke, sekarang *restart* Apache

```
systemctl restart httpd.service
```

Sebelum memasuki langkah selanjutnya, pastikan tidak menampilakan kesalahan saat *restart* _service _Apache. Bila tidak terjadi kesalahan, maka langkah selanjutnya unduh OWASP Core Rule Set

```
```

Licensed under CC BY-SA 4.0

```
cd /etc/httpd
git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git
```

Konfigurasi OWASP Core Rule Set

```
cd owasp-modsecurity-crs/
cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_config.conf
```

Selanjutnya, tambahkan ruleset ke konfigurasi Apache dengan menambahkan ruleset di */etc/httpd/conf/httpd.conf* agar ModSecurity terkonfigurasi sesuai acuan pada CRS.

/etc/httpd/conf/httpd.conf

```
Include owasp-modsecurity-crs/modsecurity_crs_10_config.conf
Include owasp-modsecurity-crs/base_rules/*.conf
```

Restart kembali Apache

```
systemctl restart httpd.service
```

Secara bawaan, ModSecurity berjalan dengan mode _detection-only. _Yang artinya akan melakukan log terhadap semua event tapi tidak akan ada tindakan. Setelah melakukan peninjauan terhadap log, maka selanjutnya kita memilih untuk membuat sebuah ruleset, memodifikasi ruleset yang sedang berjalan atau bahkan menonaktifkan ruleset dikarenakan oleh laporan yang tidak sesuai. Untuk melihat log bisa dengan menggunakan

```
tail -f /var/log/httpd/error_log
```

Ini adalah contoh laporan dari ModSecurity ketika mendapatkan masalah serangan dengan menggunakan sqlmap pada FreePBX

Licensed under CC BY-SA 4.0

```
[Wed May 25 02:05:34.479028 2016] [:error] [pid 8617] [client 127.0.0.1:33
HEADERS:User-Agent. [file "/etc/httpd/owasp-modsecurity-crs/base_rules/mod
st Indicates a Security Scanner Scanned the Site"] [data "sqlmap"] [severi
CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_1
mJvN1VzL9@UQAAAAE"]
[Wed May 25 01:36:01.538262 2016] [:error] [pid 7544] [client 192.168.88.2
[Wed May 25 01:36:01.538636 2016] [:error] [pid 7544] [client 192.168.88.2
[Wed May 25 01:36:01.645388 2016] [:error] [pid 7544] [client 192.168.88.2
```

Untuk merubah ModSecurity dari mode _detection-only _menjadi *protection*, cukup buka file _/etc/httpd/conf.d/modsecurity.conf _dan rubah

```
SecRuleEngine DetectionOnly
```

menjadi

```
SecRuleEngine On
```

Bila ingin melakukan perubahan terhadap ruleset yang ada atau menonaktifkan ruleset, bisa modifikasi file _/etc/httpd/owasp-modsecurity-crs/modsecurity_crs_10_config.conf . _Informasi lebih lanjut bisa melihat pada bagian referensi untuk melakukan konfigurasi ruleset.

Perlu dicatat, bagi yang menggunakan CodeIgniter sebagai web framework nya, sangat tidak disarankan untuk menampilkan _ci_session _di HTTP Header. Karena itu akan membuat ModSecurity memberikan laporan yang salah dengan isi dari _ci_session _yang mengandung karakter khusus yang sudah dikategorikan sebagai sebuah serangan. Karena apa yang ada pada CRS itu adalah data _pattern _yang bisa identik dengan serangan pada umumnya, diperlukan konfigurasi ulang bila memang menjumpai kasus yang berbeda.

Setelah proses instalasi dan konfigurasi ModSecurity, sekarang kita lanjutkan proses tahap instalasi Mod Evasive untuk DDoS/DoS Protection.

Mod Evasive

Mod_evasive adalah sebuah _evasive *modul yang disediakan oleh Apache untuk menangani sebuah serangan* _seperti HTTP DoS, DDoS dan *brute force* pada Apache _Server. _ Modul ini bekerja dengan membuat _internal dynamic hash table _untuk IP Adress dan URI, dan melakukan penolakan *request* bila sesuai dengan kriteria berikut:

- Melakukan _request _pada halaman yang sama berkali-kali dalam jangka waktu yang singkat
- Membuat lebih dari 50 _request _bersamaan pada proses yang sama per detik
- Membuat *request* ketika status masih dalam *blacklist*

Sebelum melakukan instalasi, kita diharuskan sudah memasang EPEL Repo pada sistem bila menggunakan CentOS.

Untuk CentOS 7:

```
1 sudo rpm -ivh http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release
```

Untuk CentOS 6:

```
1 sudo rpm -ivh http://download.fedoraproject.org/pub/epel/6/x86_64/epel-rel
```

Oke, sekarang kita lakukan instalasi untuk modul mod_evasive

```
1 sudo yum install mod_evasive -y
```

Lakukan pengecekan terlebih dahulu untuk mengetahui bahwa mod_evasive sudah ter-_load _oleh Apache

```
1 sudo  httpd -M | grep evasive
```

Bila sudah terpasang, maka akan tampil seperti ini

```
1 evasive20_module (shared)
```

Licensed under CC BY-SA 4.0

Konfigurasi mod_evasive

Sekarang saat nya melakukan proses konfigurasi untuk mod_evasive agar berjalan sesuai dengan kondisi yang kita inginkan. Semua konfigurasi berada di */etc/httpd/conf.d/mod_evasive.conf* . Maka, kita buka file tersebut

```
sudo nano /etc/httpd/conf.d/mod_evasive.conf
```

Saya akan jelaskan masing-masing kegunaan parameter yang terdapat pada file konfigurasi

```
DOSPageCount
```

_DOSPageCount _untuk menentukan jumlah batasan per _request _pada halaman yang sama dalam jangka waktu 1 detik oleh IP Address. Ketika _request _menyentuh batas dari yang ditentukan, maka IP akan dimasukkan kedalam _blocked list _karena dianggap tidak wajar. Kita bisa mengatur sesuai dengan kebutuhan masing-masing, misal menjadi 20 atau 30.

```
DOSSiteCount
```

_DOSSiteCount _hampir sama dengan _DOSPageCount, _hanya saja ini berhubungan dengan berapa banyak _request _keseluruhan yang bisa dilakukan sesuai dengan interval *DOSSiteInterval.*

```
DOSBlockingPeriod
```

_DOSBlockingPeriod _untuk menentukan durasi setiap IP yang terblokir dalam satuan detik.

```
DOSEmailNotify
```

_Uncomment _#DOSEmailNotify untuk mengaftikan pemberitahuan melalui email setiap ada serangan.

```
DOSSystemCommand
```

Licensed under CC BY-SA 4.0

_Uncomment #DOSSystemCommand _untuk menggabungkan mod_evasive dengan perintah lain. Seperti menggabungkan mod_evasive dengan fail2ban.

```
DOSLogDir
```

_Uncomment #DOSLogDir _untuk mengaktifkan _logging _pada setiap aktivitas yang terjadi di Apache. Contoh, kita akan menggunakan _/var/log/mod_evasive _sebagai direktori tempat penyimpanan. Maka lakukan hal berikut:

```
sudo mkdir /var/log/mod_evasive
```

Lalu, berikan hak akses kepada user apache

```
sudo chown -R apache:apache /var/log/mod_evasive
```

Maka, _set *DOSLogDir* _ke direktori yang sudah kita buat sebelumnya

```
DOSLogDir           "/var/log/mod_evasive"
```

Bila sudah, sekarang kita harus _restart service _Apache agar modul mod_evasive terpasang.

```
systemctl restart httpd.service
```

Testing mod_evasive

Setelah kita melalui tahap instalasi dan juga konfigurasi, sekarang saat nya kita melakukan uji coba terhadap sistem yang sudah diterapkan. Kita akan melakukan uji coba dengan hal yang sangat sederhana. Yaitu menggunakan *test script* yang diberikan oleh mod_evasive untuk melakukan uji coba terhadap konfigurasi. Kita diharuskan untuk memasang Perl terlebih dahulu

Licensed under CC BY-SA 4.0

```
sudo yum install -y perl
```

_Test script _sudah terpasang di _/usr/share/doc/mod_evasive-1.10.1/test.pl . _Seperti berikut:

test.pl

```
#!/usr/bin/perl

# test.pl: small script to test mod_dosevasive's effectiveness

use IO::Socket;
use strict;

for(0..100) {
  my($response);
  my($SOCKET) = new IO::Socket::INET( Proto   => "tcp",
                                      PeerAddr=> "127.0.0.1:80");
  if (! defined $SOCKET) { die $!; }
  print $SOCKET "GET /?$_ HTTP/1.0\n\n";
  $response = <$SOCKET>;
  print $response;
  close($SOCKET);
}
```

Rubah nilai 100 menjadi nilai yang lebih besar untuk melakukan uji coba *request*. Misal kita ingin merubah menjadi 500. Simpan dan kemudian jalankan script tersebut

```
sudo perl /usr/share/doc/mod_evasive-1.10.1/test.pl
```

Kita akan mendapatkan tampilan yang menandakan bahwa _request _tersebut sudah ditolak seperti berikut:

```
HTTP/1.1 302 Found
HTTP/1.1 403 Forbidden
```

Licensed under CC BY-SA 4.0

```
3   HTTP/1.1 403 Forbidden
4   HTTP/1.1 403 Forbidden
5   HTTP/1.1 403 Forbidden
```

Untuk melihat log aktivitas nya cukup menggunakan perintah berikut

```
1   sudo tailf /var/log/messages
```

Maka, akan tampil seperti berikut

```
1   May 25 13:01:02 localhost mod_evasive[18866]: Blacklisting address 127.0.0
```

Kesimpulan

ModSecurity dan mod_evasive cukup bagus untuk langkah pencegahan dari serangan yang banyak terjadi. Dengan adanya fitur Web Application Firewall, Intrusion Detection System, dan DoS/DDoS Protection sangat membantu dalam mengamankan Web Server ataupun Web Application. Tapi, tidak menutup kemungkinan adanya serangan lain yang bisa saja masuk dengan berbagai cara. Yang perlu diingat bahwa “No System is safe” .

Akhir kata, semoga artikel ini bermanfaat.

Referensi

- https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-Frequently-Asked-Questions-(FAQ) (https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-Frequently-Asked-Questions-(FAQ))
- https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#OWASP_ModSecurity_Core_Rule_Set_CRS_Project (https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#OWASP%5C_ModSecurity%5C_Core%5C_Rule%5C_Set%5C_CRS%5C_Project)
- http://www.owasp.org (http://www.owasp.org)
- http://resources.infosecinstitute.com/avoiding-mod-security-false-positives-white-listing/ (http://resources.infosecinstitute.com/avoiding-mod-security-false-positives-white-listing/)
- http://ezine.echo.or.id/ezine19/e19.010.txt (http://ezine.echo.or.id/ezine19/e19.010.txt)
- Social Engineering: The Art of Human Hacking
- https://www.vultr.com/docs/modsecurity-and-owasp-on-centos-6-and-apache2 (https://www.vultr.com/docs/modsecurity-and-owasp-on-centos-6-and-apache2)

Licensed under CC BY-SA 4.0

- http://www.zdziarski.com/blog/?page_id=442 (http://www.zdziarski.com/blog/?page_id=442)
- https://www.digitalocean.com/community/tutorials/how-to-protect-against-dos-and-ddos-with-mod_evasive-for-apache-on-centos-7 (https://www.digitalocean.com/community/tutorials/how-to-protect-against-dos-and-ddos-with-mod_evasive-for-apache-on-centos-7)

CentOS # Linux # Security # Tutorial

Licensed under CC BY-SA 4.0