Modsecurity + GeoIP + Modsecurity-Console Install Ver1.0

2008 년 3 월 14 일 금요일

오전 11:06 박기혁

Modsecurity Install

[root@oops util]# ls

GeoLiteCity.dat.gz mod_security-2.5.0-jason.2.i386.rpm modsecurity-console_1_0_2_linux.rpm

아주 따끈따근하네요 mod_security-2.5.0-jason.2.i386.rpm 08 년 3 월 13 일 패치되었네요 ;;

[root@oops util]#

[root@oops util]# rpm -Uvh mod_security-2.5.0-jason.2.i386.rpm

[root@oops util]# rpm -ql mod_security-2.5.0

/etc/httpd/conf.d/mod_security.conf

/etc/httpd/modsecurity.d

/etc/httpd/modsecurity.d/blocking

/etc/httpd/modsecurity.d/blocking/modsecurity_crs_20_protocol_violations.conf

/etc/httpd/modsecurity.d/blocking/modsecurity_crs_21_protocol_anomalies.conf

/etc/httpd/modsecurity.d/blocking/modsecurity_crs_40_generic_attacks.conf

/etc/httpd/modsecurity.d/blocking/modsecurity_crs_42_comment_spam.conf

/etc/httpd/modsecurity.d/blocking/modsecurity_crs_42_tight_security.conf

/etc/httpd/modsecurity.d/blocking/modsecurity_crs_55_marketing.conf

/etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf

/etc/httpd/modsecurity.d/modsecurity_crs_20_protocol_violations.conf

/etc/httpd/modsecurity.d/modsecurity_crs_21_protocol_anomalies.conf

/etc/httpd/modsecurity.d/modsecurity_crs_23_request_limits.conf

/etc/httpd/modsecurity.d/modsecurity_crs_30_http_policy.conf

/etc/httpd/modsecurity.d/modsecurity_crs_35_bad_robots.conf

/etc/httpd/modsecurity.d/modsecurity_crs_40_generic_attacks.conf

/etc/httpd/modsecurity.d/modsecurity_crs_45_trojans.conf

/etc/httpd/modsecurity.d/modsecurity_crs_50_outbound.conf

/etc/httpd/modsecurity.d/modsecurity_localrules.conf

/usr/lib/httpd/modules/mod_security2.so

/usr/share/doc/mod_security-2.5.0

/usr/share/doc/mod_security-2.5.0/CHANGES
/usr/share/doc/mod_security-2.5.0/LICENSE
/usr/share/doc/mod_security-2.5.0/README.TXT
/usr/share/doc/mod_security-2.5.0/doc
/usr/share/doc/mod_security-2.5.0/doc/apache_request_cycle-modsecurity.jpg
/usr/share/doc/mod_security-2.5.0/doc/breach-logo-small.gif
/usr/share/doc/mod_security-2.5.0/doc/html-multipage
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/actions.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/apache_request_cycle-modsecurity.jpg
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/ar01s02.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/ar01s10.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/ar01s11.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/breach-logo-small.gif
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/configuration-directives.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/index.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/installation.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/introduction.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/modsecurity-reference.css
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/modsecurity.gif
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/operators.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/processing-phases.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/transformation-functions.html
/usr/share/doc/mod_security-2.5.0/doc/html-multipage/variables.html
/usr/share/doc/mod_security-2.5.0/doc/index.html
/usr/share/doc/mod_security-2.5.0/doc/migration-matrix.html
/usr/share/doc/mod_security-2.5.0/doc/migration-matrix.xml
/usr/share/doc/mod_security-2.5.0/doc/modsecurity-reference.css
/usr/share/doc/mod_security-2.5.0/doc/modsecurity.gif
/usr/share/doc/mod_security-2.5.0/doc/modsecurity2-apache-reference.html
/usr/share/doc/mod_security-2.5.0/doc/modsecurity2-apache-reference.pdf
/usr/share/doc/mod_security-2.5.0/doc/modsecurity2-apache-reference.xml
/usr/share/doc/mod_security-2.5.0/modsecurity.conf-minimal
[root@oops util]#
[root@oops util]# vi /etc/httpd/conf.d/mod_security.conf

LoadFile /usr/lib/libxml2.so.2

LoadModule security2_module modules/mod_security2.so
LoadModule unique_id_module modules/mod_unique_id.so

[root@oops util]# vi /etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf

SecServerSignature "Microsoft-IIS/5.0"

[root@oops util]# curl --head 127.0.0.1

HTTP/1.1 400 Bad Request
Date: Fri, 14 Mar 2008 02:10:13 GMT
Server: Microsoft-IIS/5.0
Connection: close
Content-Type: text/html; charset=iso-8859-1

GeoIP Install

[root@oops util]# gzip -d GeoLiteCity.dat.gz
[root@oops util]# ls
GeoLiteCity.dat mod_security-2.5.0-jason.2.i386.rpm modsecurity-console_1_0_2_linux.rpm

[root@oops util]# mv GeoLiteCity.dat /usr/local/geo/data/
[root@oops util]# vi /etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf

SecGeoLookupDb /usr/local/geo/data/GeoLiteCity.dat
SecRule REMOTE_ADDR "@geoLookup" "chain,drop,msg:'Non-KR IP address'"
SecRule GEO:COUNTRY_CODE "!@streq KR" "t:none"

[root@oops util]# geoiplookup naver.com
GeoIP Country Edition: KR, Korea, Republic of
[root@oops util]#
[root@oops util]# geoiplookup yahoo.com
GeoIP Country Edition: US, United States
[root@oops util]#

geoiplookup 명령어는 이패키지를 깔아야 가능하다.

wget http://www.andreas-mueller.com/mrepo/centos5-i386/RPMS.epel/GeoIP-1.4.3-1.el5.i386.rpm

```
[root@gw ~]# rpm -Uvh GeoIP-1.4.3-1.el5.i386.rpm
경고: GeoIP-1.4.3-1.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID 217521f6
준비 중...                ########################################### [100%]
   1:GeoIP                ########################################### [100%]
[root@gw ~]# rpm -ql GeoIP-1.4.3-1
GeoIP-1.4.3-1 패키지가 설치되어 있지 않습니다
[root@gw ~]# rpm -ql GeoIP-1.4.3
/etc/GeoIP.conf
/etc/GeoIP.conf.default
/usr/bin/geoiplookup
/usr/bin/geoipupdate
/usr/lib/libGeoIP.so.1
/usr/lib/libGeoIP.so.1.4.3
/usr/lib/libGeoIPUpdate.so.0
/usr/lib/libGeoIPUpdate.so.0.0.0
/usr/share/GeoIP
/usr/share/GeoIP/GeoIP.dat
/usr/share/doc/GeoIP-1.4.3
/usr/share/doc/GeoIP-1.4.3/AUTHORS
/usr/share/doc/GeoIP-1.4.3/COPYING
/usr/share/doc/GeoIP-1.4.3/ChangeLog
/usr/share/doc/GeoIP-1.4.3/INSTALL
/usr/share/doc/GeoIP-1.4.3/LICENSE.txt
/usr/share/doc/GeoIP-1.4.3/README
/usr/share/doc/GeoIP-1.4.3/TODO
/usr/share/doc/GeoIP-1.4.3/fetch-geoipdata-city.pl
/usr/share/doc/GeoIP-1.4.3/fetch-geoipdata.pl
/usr/share/man/man1/geoiplookup.1.gz
/usr/share/man/man1/geoipupdate.1.gz
[root@gw ~]# ge
gedit                   generate-modprobe.conf  get_module              getfattr
getpcaps
```

```
gemtopbm                genhomedircon           getafm                  gethostip
getsebool
gemtopnm                genhostid               getconf                 getkey
gettext
gencat                  geoiplookup             getenforce              getkeycodes
gettext.sh
gencert                 geoipupdate             getent                  getopt
gex
gendiff                 geqn                    getfacl                 getopts
[root@gw ~]# geoiplookup naver.com
GeoIP Country Edition: KR, Korea, Republic of
[root@gw ~]#
```

만약 아파치에서 디렉토리별로 접근제어 사용하고 싶다면 요걸 설치한다

wget http://www.andreas-mueller.com/mrepo/centos5-i386/RPMS.epel/mod_geoip-1.2.0-1.el5.i386.rpm

```
[root@gw ~]# rpm -Uvh mod_geoip-1.2.0-1.el5.i386.rpm
경고: mod_geoip-1.2.0-1.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID 217521f6
준비 중...                ########################################### [100%]
   1:mod_geoip            ########################################### [100%]

[root@gw ~]# rpm -ql mod_geoip
/etc/httpd/conf.d/mod_geoip.conf
/usr/lib/httpd/modules/mod_geoip.so
/usr/share/doc/mod_geoip-1.2.0
/usr/share/doc/mod_geoip-1.2.0/Changes
/usr/share/doc/mod_geoip-1.2.0/INSTALL
/usr/share/doc/mod_geoip-1.2.0/README
/usr/share/doc/mod_geoip-1.2.0/README.php
[root@gw ~]# vi /etc/httpd/conf.d/mod_geoip.conf
```

여기 내용을 참조하면 모듈이 httpd.conf 에 올라가는것이 아니라 mod_geoip.conf 파일에 올라와 있는걸 알수 있다. 요즘 추세가 요런것 같다. httpd.conf 에 자동으로 올리는게

아니라 자신의 conf 파일에 모듈을 올려 사용하는걸 알 수 있다. modsecurity 모듈도 /etc/httpd/conf.d/mod_security.conf 에서 모듈정의를 하는것 처럼 말이다.

자 그럼 geoip 를 통한 아파치에서의 접근통제와 geoip 로 modsecurity 에서의 접근통제를 할수있다.

참고로 아파치 geoip 는 /usr/share/GeoIP/GeoIP.dat 를 사용하고
modsecurity 는 /usr/local/geo/data/GeoLiteCity.dat 를 LookupDB 로 사용한다.

.dat 파일은 주기적으로 업데이트 시켜주는게 좋다.

최신파일은 여기에서 다운받으면 된다.
http://www.maxmind.com/download/geoip/database/

Modsecurity-Console

modsecuriy console 은 JDK 가 설치되어있어야 한다.
http://java.sun.com/ 에서 최신버전의 JDK를 받을수있다..
modsecurity console 은
https://bsn.breach.com/ 에서 간단한 회원가입후 받을 수있다.

JDK 설치해보자
#cd /usr/local/
chmod 700 jdk-6u5-linux-i586.bin
./jdk-6u5-linux-i586.bin

동의하냐 라고 나오면 yes 라고 입력한다.

Java(TM) SE Development Kit 6 successfully installed.

Product Registration is FREE and provides many benefits:
* Notification of new versions, patches, and updates
* Special offers on Sun products, services and training
* Access to early releases and documentation

If your configuration supports a browser, the Sun Product Registration form for the JDK will be presented. You may also register your JDK later by opening the register.html file (located in the JDK installation directory) in a browser. For more information on what data Registration collects and how it is managed and used, see: http://java.sun.com/javase/registration/JDKRegistrationPrivacy.html

Press Enter to continue.....

Done.

설치가 정상적으로 끝났다. 이젠 자바변수 등록을 해주자.

#ln -s /usr/local/jdk1.6.0_05 /usr/local/java

vi /etc/profile

JAVA_HOME=/usr/local/java

PATH=$PATH:$JAVA_HOME/bin

source /etc/profile

java -version

export JAVA_HOME

modsecurity console install

#rpm -Uvh modsecurity-console_1_0_2_linux.rpm

#cd /opt/modsecurity-console/

TCP/8886 포트를 열어두자

#./modsecurity-console start

프로세스 확인

#ps axf

30000 pts/3 Sl 0:02 /usr/local/java/bin/java -server -Dinstall4j.jvmDir=/usr/local/java -Dinstall4j.appDir=/opt/modsecurity-console

다음과 같은 파일 하나를 만든다

vi /usr/local/bin/modsec-auditlog-collector.pl

아래를 붙여서 넣으세요

==========

```
#!/usr/bin/perl
#
# ModSecurity for Apache (http://www.modsecurity.org)
# Copyright (c) 2002-2006 Thinking Stone (http://www.thinkingstone.com)
#
# $Id: modsec-auditlog-collector.pl,v 1.1.2.3 2006/01/31 11:27:45 ivanr Exp $
#
# This is a proof-of-concept script that listens to the
# audit log in real time and submits the entries to
# a remote HTTP server. This code is not suitable for
# non-trivial production use since it can only submit
# one audit log entry at a time, plus it does not handle
# errors gracefully.
#
# Usage:
#
# 1) Enter the correct parameters $CONSOLE_* below
#
# 2) Configure ModSecurity to use this script for
#       concurrent audit logging index:
#
#       SecAuditEngine RelevantOnly
#       SecAuditLogType Concurrent
#       SecAuditLogParts ABCDEFGHZ
#       SecAuditLogStorageDir /path/to/auditlog/data/
#       SecAuditLog "|/path/to/modsec-auditlog-collector.pl \
#             /path/to/auditlog/data/ \
#             /path/to/auditlog/index"
#
# 3) Restart Apache.
```

```
use MIME::Base64();
use IO::Socket::INET;

my $CONSOLE_URI = "/rpc/auditLogReceiver";
my $CONSOLE_HOST = "127.0.0.1";
my $CONSOLE_PORT = "8886";
my $CONSOLE_USERNAME = "test";
my $CONSOLE_PASSWORD = "sensor";

# ------------------------------------------------

my $logline_regex = "";

# hostname
$logline_regex .= "^(\\S+)";
# remote host, remote username, local username
$logline_regex .= "\\ (\\S+)\\ (\\S+)\\ (\\S+)";
# date, time, and gmt offset
$logline_regex .= "\\ \\[([^:]+):(\\d+:\\d+:\\d+)\\ ([^\\]]+)\\]";
# request method + request uri + protocol (as one field)
$logline_regex .= "\\ \"(.*)\"";
# status, bytes out
$logline_regex .= "\\ (\\d+)\\ (\\S+)";
# referer, user_agent
$logline_regex .= "\\ \"(.*)\"\\ \"(.*)\"";
# uniqueid, sessionid
$logline_regex .= "\\ (\\S+)\\ \"(.*)\"";
# filename, offset, size
$logline_regex .= "\\ (\\S+)\\ (\\d+)\\ (\\d+)";
# hash
$logline_regex .= "\\ (\\S+)";
# the rest (always keep this part of the regex)
$logline_regex .= "(.*)\$";

my $therequest_regex = "(\\S+)\\ (.*?)\\ (\\S+)";
```

```
sub send_entry {
    my ($file_name, $file_offset, $file_size, $hash, $summary) = @_;
    my $buffer;

    if (!open(F, $file_name)) {
        print LOG "> Could not open file $file_name.\n";
        return;
    }

    binmode F;

    $socket = IO::Socket::INET->new(Proto => 'tcp', PeerAddr => $CONSOLE_HOST, PeerPort =>
$CONSOLE_PORT, Timeout => 10);
    binmode $socket;

    if (!$socket) {
        print LOG "> Failed to open socket.\n";
        return;
    }

    $socket->autoflush(1);

    my $credentials = MIME::Base64::encode($CONSOLE_USERNAME . ":" .
$CONSOLE_PASSWORD);
    chomp($credentials);

    print $socket "PUT $CONSOLE_URI HTTP/1.0\r\n";
    print $socket "Content-Length: " . $file_size . "\r\n";
    print $socket "Authorization: Basic " . $credentials . "\r\n";
    print $socket "X-ForensicLog-Summary: " . $summary . "\r\n";
    print $socket "X-Content-Hash: " . $hash . "\r\n";
    print $socket "\r\n";

    # send file contents
    while (
        read(F, $buffer, 8192)
```

```
        and print $socket $buffer
    ) {};
    close(F);

    my $status = 0;
    while(<$socket>) {
        # print "> $_";
        if (($status == 0) && (/^HTTP\/[0-9]\.[0-9] ([0-9]+).+$/)) {
            $status = $1;
        }
    }

    print LOG "> Status: " . $status . "\n";
    close($socket);
}

# -- Main ----------------------------------------------------------------

if (@ARGV != 2) {
        print "Usage: modsec-auditlog-collector auditlog-folder auditlog-index\n";
        exit;
}

my($folder, $index) = @ARGV;

open(LOG, ">>$index") || die("Failed to open: $index\n");
$| = 1, select $_ for select LOG;


while(<STDIN>) {
        # print LOG "Line: $_";

        chomp();
        my $summary = $_;

        next if (/^$/);
```

```
my @parsed_logline = /$logline_regex/x;
if (@parsed_logline == 0) {
        print LOG "> Failed to parse line: " . $_ . "\n";
} else {
   (
          $request{"hostname"},
          $request{"remote_ip"},
          $request{"remote_username"},
          $request{"username"},
          $request{"date"},
          $request{"time"},
          $request{"gmt_offset"},
          $request{"the_request"},
          $request{"status"},
          $request{"bytes_out"},
          $request{"referer"},
          $request{"user_agent"},
          $request{"unique_id"},
          $request{"session_id"},
          $request{"filename"},
          $request{"file_offset"},
          $request{"file_size"},
          $request{"hash"},
          $request{"the_rest"}
   ) = @parsed_logline;

   $_ = $request{"the_request"};
   my @parsed_therequest = /$therequest_regex/x;
   if (@parsed_therequest == 0) {
      $request{"invalid"} = "1";
      $request{"request_method"} = "";
      $request{"request_uri"} = "";
      $request{"protocol"} = "";
   } else {
      (
```

```
            $request{"request_method"},
            $request{"request_uri"},
            $request{"protocol"}
        ) = @parsed_therequest;
        }

    print LOG ($summary . "\n");
    send_entry($abs_file_name = $folder . "/" . $request{"filename"}, $request{"file_offset"},
$request{"file_size"}, $request{"hash"}, $summary);
  }
}

close(LOG);
```

http://서버IP:8886 접속해보자

초기접속시 ID=admin PW=admin 이다.
접속확인후 바로 admin 패스워드를 변경해주자.

그다음 위부분의 Sensors 클릭 --> Add Sensor 클릭

Username IP 패스워드 부분을 적어주자

적어줬으면 Submit 클릭 --> 적용클릭

또한 도메인당 Sensors 는 3 개까지 가능하다. 센서당 라이선스가 부여되는데
아래사이트를 가서 라이선스를 부여 받자.
https://bsn.breach.com/ 부여방은 키는 http://서버IP:8886 접속하여
Administration 클릭 오른쪽 밑에의 Licence Management 들어가서 적용시켜주자.

또한 리포트도 받아보자 .Administration 클릭 Email Connectivity 클릭
자신에 맞게 설정 후 Apply Configuration 클릭
Reports 클릭 New Report 클릭
Name 부분은 메일 받을때 제목 부분이다.
Author/Contact 에는 메일 주소를

추가 참조메일주소가 있으면 Recipients 에 추가시켜주자
매일 받도록 Daily 로 Sensors 선택하고 섹션 선택해주고 Submit & Apply

다음으로 위에 적어주웠던 Username IP 패스워드 부분을 아래파일에 수정해주자
#vi /usr/local/bin/modsec-auditlog-collector.pl

my $CONSOLE_HOST = "서버 IP";
my $CONSOLE_PORT = "8886";
my $CONSOLE_USERNAME = "이름";
my $CONSOLE_PASSWORD = "패스워드";

modsecurity 설정파일을 열어 아래내용을 추가 및 수정해주자.
vi /etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf

SecAuditLogType Concurrent
SecDataDir /tmp
SecAuditLogStorageDir /tmp
SecAuditLog "|/usr/local/bin/modsec-auditlog-collector.pl \
/tmp/ /etc/httpd/logs/modsec_audit.log"

이와 같이 설정 및 저장하고 아파치 restart
콘솔 또한 stop & start

로그가 /tmp/20080314/ ... 여기에 생성될것이다. 확인해보자

[root@oops tmp]# curl --head 127.0.0.1
HTTP/1.1 400 Bad Request
Date: Fri, 14 Mar 2008 05:39:05 GMT
Server: Microsoft-IIS/5.0
Connection: close
Content-Type: text/html; charset=iso-8859-1

[root@oops tmp]# ll /tmp
합계 120

drwxr-x--- 3 apache apache 4096 3 월 14 14:39 20080314

마치며..

동작 방식은 /tmp 내용을 가져가는것 같다. 원래는 /etc/httpd/logs/mod_audit/ 를 스토리지 디렉토리로 하려 했는데 로그가 쌓이지가 않아서 할 수 없이 찝찝하게 /tmp 로 하였다.
별짓을 해도 안쌓이더군요. 또한 /etc/httpd/modsecurity.d/ 에 보면 룰 파일들이 많이있다.
룰의 적용 순서는 crs_10 ~ crs_50 까지 순차적으로 적용되므로 허용할 IP 대역이 있으면 보통 crs10 이나 15 에 적용해준다. 15 파일은 없으나 마이그레션파일을 하나 만들면 될것같다.
당연히 만들면 modsecurity.conf 파일에 라인 추가 시켜줘야 할 것이다.
마이그레이션 파일은 우리나라 실정에 맞게 키사에서 제공하는 룰정도면 충분할것 같다.
Block IP 가 있으면 crs 50 이나 그이후에 적용을 해주면 된다.

그리고 많은 분들이 정말 좋은 기능의 modsecurity 를 설치와 관심을 가졌으면 좋겠습니다.
또한 이기본틀을 가지고 계속 버전업을 할 계획입니다.
시간내서 스샷도 첨부하고 수정부분도 찾고 덧붙일 부분도 찾고 할려구요. 혹시 도움을 주실분 korea.oops@gmail.com 으로 부탁해욤

아마 룰 마이그레이션부분하고 modsecurity-console 에서 DB 및 여러가지모니터링에 대한 버전업이 될꺼 같네요. 특히 console 은 자료가 많지 않아 문제네욤.