Modsecurity 로그분석 및 고급 룰 설정

오늘과내일 홍석범

antihong@tt.co.kr

적용 여부 확인 방법

차단은 되는 것 같은데, 로그가 남지 않는다?

error_log : [Fri Oct 19 11:24:04 2007] [error] ModSecurity: ModSecurity requires mod_unique_id to be installed.

modsec_audit.log 에는 남지 않음

이러한 경우 httpd.conf 에서

LoadModule unique_id_module modules/mod_unique_id.so 확인

SecServerSignature를 IIS로 변경하여 설정했는데, 질의를 하면 헤더가 변경되지 않는다?

lynx -head -source http://127.0.0.1/

wget -S --spider http://127.0.0.1/

curl --head http://127.0.0.1/

httpd.conf 에서 ServerTokens **Prod** 를 **Full** 로 설정하여야 함

제로보드 관련 룰(1.9)

기존KISA 제공 룰

SecFilterSelective REQUEST_URI "/include/write₩.php₩?dir=(ftp|http):"
SecFilterSelective REQUEST_URI "/include/print_category₩.php₩?setup=1&dir=(ftp|http):"
SecFilterSelective REQUEST_URI "/zero_vote/error₩.php₩?dir=(ftp|http):"
SecFilterSelective REQUEST_URI "/outlogin₩.php₩?_zb_path=(ftp|http):"
SecFilterSelective REQUEST_URI "filename=₩|"
SecFilterSelective REQUEST_URI "check_user_id₩.php₩?user_id=<script>alert(document₩.cookie)"

추가룰

SecFilterSelective REQUEST_URI "/zero_vote/login₩.php₩?dir=(ftp|http):“
SecFilterSelective REQUEST_URI "/zero_vote/setup₩.php₩?dir=(ftp|http):“
SecFilterSelective REQUEST_URI "/zero_vote/ask_password₩.php₩?dir=(ftp|http):“

또는

#Generic PHP remote file inclusion attack signature with command
SecFilterSelective REQUEST_URI "₩.php₩?" chain
SecFilterSelective REQUEST_URI "(http|https|ftp)₩:/" chain
SecFilterSelective REQUEST_URI|REQUEST_BODY "(cd|₩;|perl |lynx |links |mkdir |cmd|pwd|wget |lwp-(download|request|mirror|rget) |id|uname||net(stat|cat) |curl |telnet |gcc |cc |rm ₩-[a-z|A-Z])"
2.x 에서는 SecFilterSelective ➔ Secrule

disable 해야 할 룰(1.9.x)

SecFilterSelective ARGS "-->" "msg:'XSS attack'"
SecRule ARGS "-->" "msg:'XSS attack'"
전송데이터에 --> 만 들어가도 공격으로 판단

mod_security-message: Access denied with code 403. Error processing request body: Multipart: final boundary missing [severity "EMERGENCY"]
➔ 파일업로드시 일부 발생, 1.9.x에만 발생 , SecFilterScanPOST On =>Off

mod_security-message: Access denied with code 403. Pattern match ";[[:space:]]*(ls|**id**|pwd|wget|cd)" at ARGS_VALUES("content") [msg "Command execution attack"] [severity "EMERGENCY"]
➔ ttp://www.example.com/example.php?board=public&**id=**1225 정상임

SecFilterSelective ARGS "alert[[:space:]]*\(“

```
<SCRIPT LANGUAGE="JAVASCRIPT">
function openerTr()
 {
  alert("팝업이 차단되었습니다!");
 }
</SCRIPT>
```

disable or 커스터마이징(1.9.x)

SecFilterSelective ARGS "http-equiv“
<meta http-equiv="Content-Type“

SecFilterSelective ARGS "style[[:space:]]*=“
<style type="text/css">

SecFilter "\.\./\.\."
SecFilter "\.\./\.\./"
SecFilter "/\.\./\.\./\.\./\.\./"
고도몰등 특정 프로그램이 작동 안 됨

WEB-CGI technote main.cgi file directory traversal attempt
SecFilterSelective THE_REQUEST "/technote/main\.cgi" chain
SecFilter "\.\./\.\./"

WEB-CGI technote print.cgi directory traversal attempt
SecFilterSelective THE_REQUEST "/technote/print\.cgi" chain
SecFilter "\x00"

Host 나 User-Agent가 없는 경우

Message: Warning. Operator EQ match: 0. [id "960008"] [msg "Request Missing a Host Header"] [severity "WARNING"]

HEAD / HTTP/1.0
Accept: */*
User-Agent: WhatsUp Professional/1.0

modsecurity_crs_21_protocol_anomalies.conf
SecRule &REQUEST_HEADERS:Host "@eq 0" \
"skip:1,log,auditlog,msg:'Request Missing a Host Header',,id:'960008',severity:'4'"
SecRule REQUEST_HEADERS:Host "^$" \
"log,auditlog,msg:'Request Missing a Host Header',,id:'960008',severity:'4'"

SecRule &REQUEST_HEADERS:User-Agent "@eq 0" \
"skip:1,log,auditlog,msg:'Request Missing a User Agent Header',,id:'960009',severity:'4'"
SecRule REQUEST_HEADERS:User-Agent "^$" \
"log,auditlog,msg:'Request Missing a User Agent Header',,id:'960009',severity:'4'"
SecFilterSelective HTTP_Host "^$" **(1.9.x)**
& : counting the number of variables
(1) 아예 헤더에 User-Agent가 없는 경우
(2) 헤더에 User-Agent는 있지만 데이터가 없는 경우

커스터마이징

Message: Access denied with code 400 (phase 2). Pattern match "^[\\d\\.]+$" at REQUEST_HEADERS:Host. [id "960017"] [msg "Host header is a numeric IP address"] [severity "CRITICAL"]

➔ 도메인이 아닌 IP 로 접속시 발생

modsecurity_crs_21_protocol_anomalies.conf

SecRule REQUEST_HEADERS:Host "^[\d\.]+$" "deny,log,auditlog,status:400,msg:'Host header is a numeric IP address', severity:'2',,id:'960017',"

파일에 특수문자 포함시

Message: Warning. Match of "rx ^[a-z]{3,10}₩₩s*(?:₩₩w{3,7}?₩₩:₩₩/₩₩/[₩₩w₩₩-₩₩.₩₩/]*)??₩₩/[₩₩w₩₩-₩₩.₩₩/~%:@&=+$,;]*(?:₩₩?[₩₩S]*)??₩₩s*http₩₩/₩₩d₩₩.₩₩d$" against "REQUEST_LINE" required. [id "960911"] [msg "Invalid HTTP Request Line"] [severity "CRITICAL"]

SecRule REQUEST_LINE "!^[a-z]{3,10}₩s*(?:₩w{3,7}?₩:₩/₩/[₩w₩-₩.₩/]*)??₩/[₩w₩-₩.₩/~%:@&=+$,;]*(?:₩?[₩S]*)??₩s*http₩/₩d₩.₩d$" ₩

"t:none,t:lowercase,deny,log,auditlog,status:400,msg:'Invalid HTTP Request Line',,id:'960911',severity:'2'"

==> GET /1181633664worldhistory(McGrawHill)cover.jpg HTTP/1.1

와 같이 파일이나 디렉토리 이름에 ()가 포함된 경우 또는 공란(space)이 있는 경우 등…

특정 IP/도메인을 제외할 때

특정한 IP에 대해서는 모니터링 하지 않을 때

SecRule REMOTE_ADDR "^192₩.168₩.1₩100$"
phase:1,nolog,allow,ctl:ruleEngine=Off,ctl:auditEngine=Off

* 특정 도메인(디렉토리)에 대해서는 modsecurity 설정을 해제하고자 할 때

.htaccess

SecFilterEngine Off # 기본 엔진 동작 정지

SecFilterScanPOST Off # POST 스캔 중지

SecFilterCheckURLEncoding Off # URL 인코딩 체크 중지

.htaccess 에 # 이 있을 경우 500 error가 발생하므로 그대로 복사할 경우
서비스가 되지 않을 수 있으므로 주석(#) 부분은 명기하지 않아야 함

주의 : modsecurity 2.x 에서는 .htaccess를 지원하지 않음

Phpmyadmin등 예외사항

phpmyadmin 사용시, 제외하고자 할 때

SecRule REQUEST_URI ^/phpMyAdmin phase:1,allow,ctl:ruleEngine=off 또는

<LocationMatch "^/*phpMyAdmin*/">
  SecRuleEngine Off
</LocationMatch>

특정 룰을 주석처리하지 않고 disable하고자 할 때

Message: Warning. Pattern match "(?:\\b(?:\\.(?:ht(?:access|passwd|group)|www_?acl)|global\\.asa|httpd\\.conf|boot\\.ini)\\b|\\/etc\\/)" at REQUEST_FILENAME. [id "**950005**"] [msg "Remote File Access Attempt. Matched signature </etc/>"] [severity "CRITICAL"]

SecRuleRemoveById 950005 ➔ 룰의 선언위치가 중요 ,기선언된 룰의 뒤**(예:modsecurity_crs_80.conf)**에 선언해야 함

<VirtualHost 192.168.1.4>
  ServerAdmin webmaster@example.com
  DocumentRoot /home/example/public_html
  ServerName example.com
  SecRuleRemoveById 950005
</VirtualHost>

404는 로그에 남지 않도록 설정

apache-Error: [level 3] File does not exist: /var/www/html/favicon.ico

주로 사용하는 설정)
SecAuditLogRelevantStatus "^[45]"
권장 설정)
SecAuditLogRelevantStatus "^(?:5|4₩d[^4])“ ← 404는 포함하지 않음

파일명 또는 파라미터에 한글이 포함된 경우
예:/list.php?page=&addr1=강남구&grade=중학교.....
Message: Access denied with code 400 (phase 2). Invalid Unicode encoding: invalid byte value in character. [id "950801"] [msg "UTF8 Encoding Abuse Attack Attempt"] [severity "WARNING"]

SecFilterCheckUnicodeEncoding Off
SecFilterForceByteRange 0 255(기본값)
@validateUtf8Encoding, @validateByteRange, (2.x)

1.9.x에서 로그만 남도록 했는데, 차단되는 이유?

SecFilterDefaultAction "pass,log“ 로 설정해도 차단되는 이유?

SecFilterSignatureAction "msg:'Command execution attack'"
SecFilterSelective ARGS_VALUES ";[[:space:]]*(pwd|wget|curl)“ 와 같이 설정시 발생.

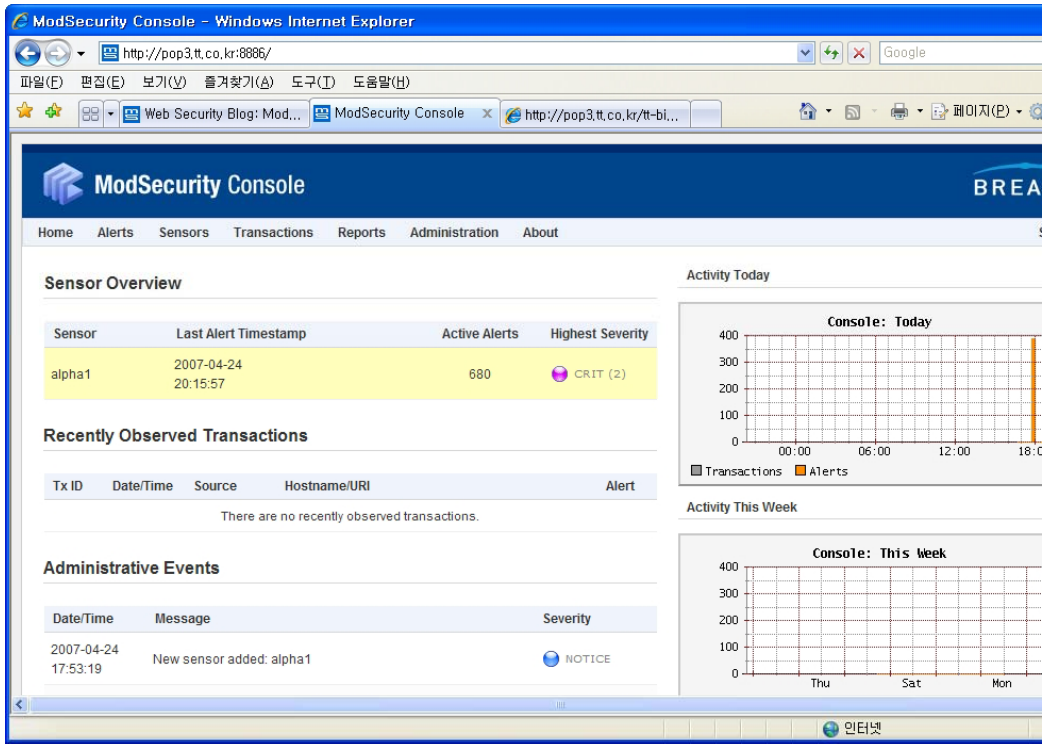
옳은 설정)
SecFilterSelective ARGS_VALUES ";[[:space:]]*(ls|id|pwd|wget|cd)" "msg:'Command execution attack'"

SecFilterSignatureAction의 기본값이 log,deny,status:403 이므로

(1) SecFilterSignatureAction을 사용하지 않거나
(2) SecFilterSignatureAction "log,pass,msg: 'Command execution attack '' 와 같이 변경

modsecurity console

-. 웹을 통해 실시간 통합 로그 관리가 가능한 패키지 프로그램(web+DB)
-. 1개의 콘솔에서 3개의 센서까지 무료로 제공
-. 상용버전(Enterprise Manager Console)은 breach를 통해 제공
-. JDK / JRE 1.4 이상에서 작동함
-. 메일등으로 알람(notify)기능
-. pdf로 보고서 작성 기능 제공



console 설치 방법

tar zxvfp modsecurity-console_1_0_2_unix.tar.gz
cd modsecurity-console
./modsecurity-console
No suitable Java Virtual Machine could be found on your system.
The version of the JVM must be at least 1.4.
Please define INSTALL4J_JAVA_HOME to point to a suitable JVM.
You can also try to delete the JVM cache file /root/.install4j

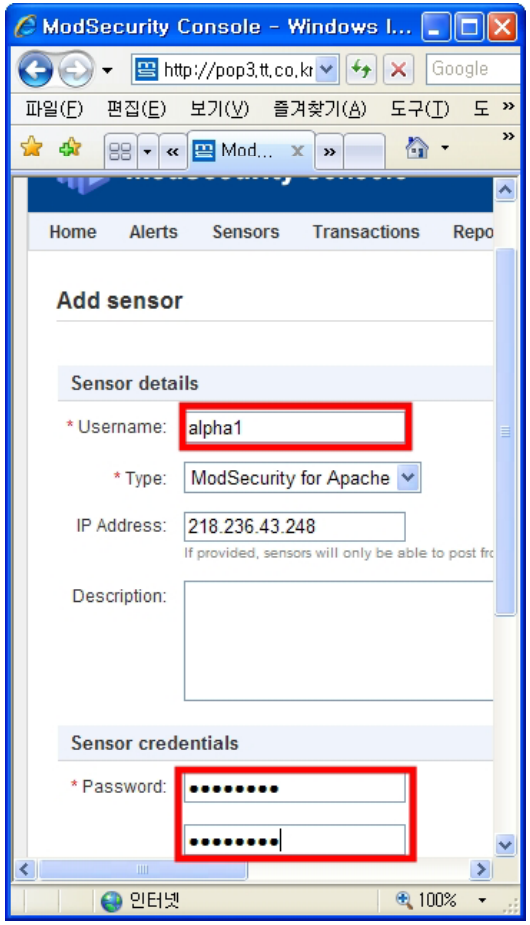
에러메시지

http://java.sun.com/ 에서 jdk1.5 다운로드 및 설치
./jdk-1_5_0_09-linux-i586.bin ← 엔터만 입력

export INSTALL4J_JAVA_HOME=/usr/local/src/modsecurity-console/jdk1.5.0_09
./modsecurity-console start ← 8886/tcp 리슨 확인

console 설정 방법

Sensors => Add Sensor 클릭



httpd.conf 에 아래 설정 추가

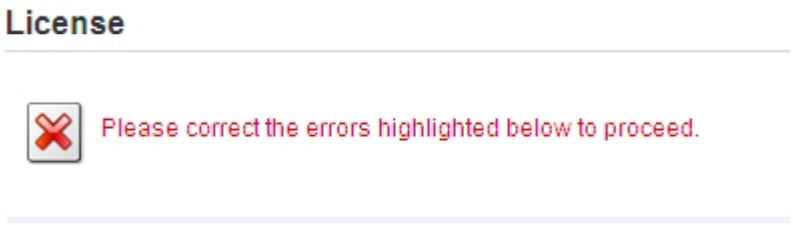
```
SecAuditEngine RelevantOnly
SecAuditLogRelevantStatus "^(?:5|4₩d[^4])"
SecAuditLogType Concurrent
SecAuditLogParts ABCDEFGHZ
SecAuditLogStorageDir /usr/local/apache2/logs/data/
SecAuditLog /usr/local/apache2/logs/modsec-audit.log
SecAuditLog "|/usr/local/apache2/bin/modsec-auditlog-collector.pl ₩
/usr/local/apache2/logs/data/ /usr/local/apache2/logs/modsec-audit.log"
```

http://xx.xx.xx.xx:8886/static/modsec-auditlog-collector 파일 저장

```
my $CONSOLE_HOST = "218.236.xx.xxx";
my $CONSOLE_PORT = "8886";
my $CONSOLE_USERNAME = "alpha1";
my $CONSOLE_PASSWORD = "sensor1";
```

라이센스 입력

The licence key is missing, invalid, or expired. Please configure a valid licence key to unlock the full functionality



https://bsn.breach.com/ 접속후 **Licensing** 클릭하여 발급

발급된 라이센스로 업데이트 시행

라이센스 입력

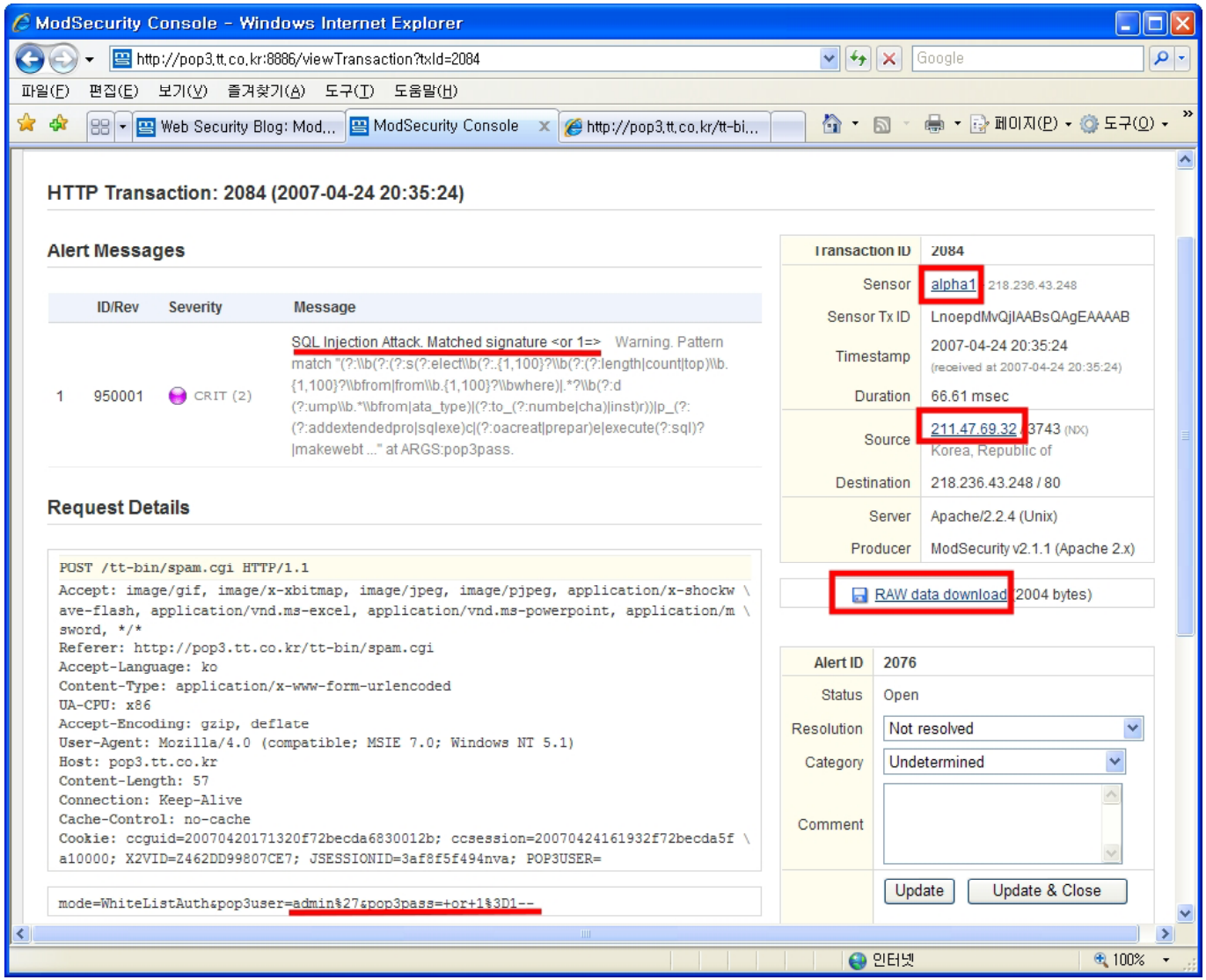
LS0tLS1CRUdJTiBGSUxFLS0tLS0KcHJvZHVjdE5hbWUgPSBNb2RTZWN1cmI0eSBDb25zb2xlCnBy
b2R1Y3RWZXJzaW9uID0gMS4wLjIKcHJvZHVjdFVyaSA9IGh0dHA6Ly93d3cubW9kc2VjdXJpdHku
b3JnL3Byb2pIY3RzL2NvbnNvbGUvCnByb2R1Y3RWZW5kb3IgPSBCcmVhY2ggU2VjdXJpdHkKcHJv
ZHVjdFZlbmRvclVyaSA9IGh0dHA6Ly93d3cuYnJlYWNoLmNvbQoKbGIjZW5jZURlc2NyaXB0aW9u
ID0gTW9kU2VjdXJpdHkgQ29uc29sZSBGcmVlIENvbW11bmI0eSBMaWNlbmNlCmxpY2VuY2VHZW5l
cmF0ZWRPbiA9IDIwMDcvMTAvMjUKbGIjZW5jZVZhbGlkVW50aWwgPSA5OTk5LzAxLzAxCgpsaWNl
bmNlZU5hbWUgPSBUb2RheQpsaWNlbmNlZVVyaSA9IGh0dHA6Ly9jb2Z3LnR0LmNvLmtyLwpsaWNl
bmNlZUVtYWlsID0gYW50aWhvbmdAdHQuY28ua3IKICAgICAgICAgICAgICAKYWxsb3dlZFNlbnNvcnMgPSAz
Ci0tLS0tQkVHSU4gU0lHTkFUVVJFLS0tLS0KTUN3Q0ZIdjduUGxPUjJmMlJEMTJGL3o0L0hhWHdT
amlBaFJYeVlhMXF4ZncvdFRRcFQyTklQOXNZRy81V0E9PQ0KLS0tLS1FTkQgU0lHTkFUVVJFLS0t LS0K

Console 설정후에는 **modsec_audit.log**가 다음과 같이 보임

cofw.tt.co.kr 192.168.69.32 - - [26/Oct/2007:17:52:28 +0900] "GET /etc/passwd HTTP/1.1" 501 293 "-" "-" eG72FdrsK0sAAEbnCVwAAAAH "-" /20071026/20071026-1752/20071026-175228-eG72FdrsK0sAAEbnCVwAAAAH 0 1282 md5:23776c01b2680eccc120209a4b7e2300

/var/log/httpd/data/20071026/20071026-1752/20071026-175228-eG72FdrsK0sAAEbnCVwAAAAH

console 로그 조회



console 의 부하가 높을 경우?

-. SecAuditEngine On ➔ RelevantOnly

-. SecAuditLogRelevantStatus "^[45]“ ➔ "^(?:5|4₩d[^4])"

-. modsecurity-auditlog-collector ➔ mlogc

-. modsecurity-console 스크립트에

-INSTALL4J_ADD_VM_PARAMS="-Xms128M -Xmx512M

사용가능한 메모리를 시작시 128M, 최대 512M로 제한

오탐에 대한 대응방법

-. 어떤 application이든 오탐은 있을 수 있다.

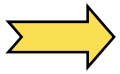
-. 초기에는 DetectionOnly 모드로 사용해야 한다.

-. 특정 룰에 오탐이 있다고 룰 자체를 삭제하면 또 다른 오탐(false negative)
의 원인이 될 수 있으므로 상황에 맞는 커스터마이징이 필요하다.

-. 로그(log)에 원인과 해결방법이 있다.
(만약 특정한 로그만 자세히 보고자 할 경우)➔ 특정 조건만 상세로그를 볼 수 있음
SecRule REMOTE_ADDR "^192₩.168₩.10₩.69$“ phase:1,log,pass,ctl:**debugLogLevel=9**
SecRule REQUEST_URI "^/path/to/script.pl$" phase:1,log,pass,ctl:**debugLogLevel=9**

-. Whitelist에 대해서는 10번과 20번 룰 사이에 생성(예:modsecurity_crs_10_white.conf)
blacklist(negative)에 대해서는 제일 마지막(예: modsecurity_crs_60_black.conf)

-.상세한 로그설정은 performance impact 유발 가능
예)-. snort등의 룰(rule)설정➔ X
-. 정규식을 이용 룰 최소화
SecRule REQUEST_URI “file1₩.cgi”
SecRule REQUEST_URI “file2₩.cgi”



SecRule REQUEST_URI “(file1|file2)\.cgi”

부가 기능 활용

```
#Specify the local directory for collection storage
SecDataDir /path/to/apache/logs/state

# Initiate a collection based on the source IP address
SecAction initcol:ip=%{REMOTE_ADDR},nolog,pass

# Increase the IP collection score based on filter hits
SecRule REQUEST_FILENAME “/cgi-bin/phf" pass,setvar:ip.score=+10
SecRule REQUEST_FILENAME “cmd.exe” pass,setvar:ip.score=+10
SecRule REQUEST_METHOD “TRACE” pass,setvar:ip.score=+5

# Evaluate the overall IP collection score
SecRule IP:SCORE "@ge 30“

SecRule ARGS|REQUEST_BODY|REQUEST_URI "Subject\:" chain
SecRule ARGS|REQUEST_BODY|REQUEST_URI "\s*bcc\:"
```

Modsecurity 1.x / 2.x 차이

	Modsecurity 1.x	Modsecurity 2.x
Processing phase	Inbound(Request body) / Outbound(Response body) 지원	Request header(phase:1) Request body(phase:2) Response header(phase:3) Response body(phase:4) logging(phase:5)
설정방법	apache 1.x 의 경우 <IfModule mod_security.c> apache 2.x의 경우 <IfModule security_module>	<IfModule security2_module>
Turn on/off Rule engine	**SecFilterEngine**	**SecRuleEngine**
Default rule action	**SecFilterDefaultAction**	**SecDefaultAction**
Rule directive	**SecFilter, SecFilterSelective**	**Secrule**
Accessing reuqest bodies	**SecFilterScanPost**	**SecRequestBodyAccess**
Accessing response bodies	**SecFilterScanOutput**	**SecResponseBodyAccess**

Modsecurity 상용 솔루션 및 작동모드

Modsecurity M1100

-. 브리지(Transparent) 모드로 동작

-. 100Mbps 처리 가능, bypass 제공.

-. 약 1500만원

구현방식	라우팅	브리지	Reverse proxy	Embeded
설치공간	동일네트워크	동일네트워크	관계없음	자체
네트워크 설정변경	변경필요	불필요	불필요	불필요
DNS변경	불필요	불필요	필요함	불필요
서버IP노출	노출됨	노출됨	노출 안됨	노출됨
기타	대부분의 상용장비 방식			modsecurity

결론

-. 불필요한 룰을 삭제하고, custommizing한다면 성능저하 없이 이용가능 함
예) sql injection 차단룰만 설정시 95% 내외

-. 초기에는 오탐에 대비, DetectionOnly로 설정 후 로그를 보며
Customizing하여야 함

-. DoS 공격등에는 iptables 이용이 보다 효과적
2.2 이상 버전에는 국가별 설정이 가능한 geoip 기능 제공

```
SecGeoLookupsDb /usr/local/geo/data/GeoLiteCity.dat
SecRule REMOTE_ADDR "@geoLookup" chain,drop,msg:'Non-KR IP address'
SecRule GEO:COUNTRY_CODE "!@streq KR“

/sbin/iptables -A INPUT -m geoip ! --src-cc KR -j DROP
/sbin/iptables -A INPUT -p tcp --syn --dport 80 -m connlimit
              --connlimit-above 30 -j DROP
```

-. 메일링리스트를 통해 최신 정보 습득 및 정보공유 필요
-. Modsecurity 3.0에서는 apache 1.3.x 도 지원예정

Q & A

질문 : antihong@tt.co.kr