AlienVault

Technical Documentation

ModSecurity Plugin

Documentation for the ModSecurity Data Source Connector

Alexander Goller

Documentation for the ModSecurity Data Source Connector

Alexander Goller

Table of Contents

1. Introduction

This documentation is intended for users of AlienVault USM and OSSIM that want to direct one or many Apache ModSecurity installations to their AlienVault USM sensors.

ModSecurity is an Apache module that works as a Web Application Firewall (WAF). The WAF will inspect each HTTP request entering the web server and, similar like a IDS on the network level, analyze the incoming request based on rules in the system.

Upon execution of those rules a request will either be validated as a successful request or will be blocked by the WAF in order to keep unwanted access to the system out and block well known threats.

2. How it works

Recent versions of Modsecurity include a custom log forwarder called `mlogc`. `mlogc` will forward the ModSecurity audit log to a specified server running a modsecurity log collector.

The data source connector for ModSecurity implements a modsecurity log collector and creates a log file with all forwarded entries on the AlienVault sensor.

The AlienVault sensor will pick up those logs through a data source connector, parse and normalize those logs as usual.

The advantages of running the collector are the following:

- One to many WAF instances can log to the sensor
- Mlogc buffers all audit logs when the sensor or collector is unavailable. No audit log will be lost.
- No syslog configuration needed.
- Encrypted transport from WAF to sensor.

Chapter 2. Requirements

1. Sensor/SIEM

The installation of this data source connector requires additional modules on the AlienVault USM sensor.

- Mojo - a simple web framework.
- The IO::Socket::SSL library for perl.

2. WAF hosts

On the WAF machine, be sure to have the ModSecurity mlogc command installed.

The WAF and mlogc need to be configured properly.

Chapter 3. Installation

This chapter will describe all the needed steps to install the data source connector on Sensor or SIEM and the WAF server itself.

1. WAF/ModSecurity host

ModSecurity Settings

```
LoadModule security2_module libexec/apache22/mod_security2.so

<IfModule security2_module>
    ### Include paths for modsecurity
    Include etc/apache22/Includes/mod_security2/*.conf
    Include etc/apache22/Includes/mod_security2/base_rules/*.conf


    SecRuleEngine On
    SecDataDir /var/log/modsecurity/data
    SecDebugLog /var/log/modsecurity/debug.log
    SecDebugLogLevel 0

    ### this is important for the audit logs
    SecAuditEngine On
    SecAuditLogRelevantStatus "^.*"
    SecAuditLogType Concurrent
    SecAuditLogParts ABCDEFGHZ
    SecAuditLogStorageDir /var/log/modsecurity/audit/
    SecAuditLog /var/log/modsecurity/audit/index

    ### this is the way logs are forwarded via mlogc
    SecAuditLog "|/usr/local/bin/mlogc /usr/local/etc/mlogc.conf"
</IfModule>
```

mlogc configuration

```
CollectorRoot       "/var/log/mlogc"
ConsoleURI          "https://sensor-ip-address:8765/rpc/auditLogReceiver"
SensorUsername      "mlogc"
SensorPassword      "collector"
LogStorageDir       "/var/log/modsecurity/audit"
TransactionLog      "mlogc-transaction.log"
QueuePath           "mlogc-queue.log"
ErrorLog            "mlogc-error.log"
LockFile            "mlogc.lck"
KeepEntries         0
```

After configuring both components be sure that the apache error log and the mlogc error log both contain no errors. At this point you will see mlogc trying to connect to the specified host with no success as the receiver is not set up yet.

2. Sensor

Installing Mojo

Install Mojo from the following URL to the system. https://github.com/jamadam/mojo-legacy.

After unpacking the zip archive, go to the directory and use the command `perl Makefile.PL`.

Type `make install` for building and installing Mojo.

Install IO::Socket::SSL

Install *IO::Socket::SSL* using the CPAN shell. This may require installing a compiler and compile time environment. We will look into how this can be fixed for future releases.

Install the collector

Install the package `modsec_collector.tgz` using the following commands.

```
cd /usr/share/ossim
tar xzvf modseccollector.tgz
```

Copy the plugin file `/usr/share/ossim/modseccollector/modsecurity.cfg` to `/etc/ossim/agent/plugins/modsecurity.cfg` .

Activate the *modsecurity plugin* by using `alienvault-setup`.

Check if the collector process is running by looking at the files `/var/log/modsecurity.log` for modsecurity events and `/var/log/modsec_collector.log` for collector daemon messages.

Copy the *logrotate* file `/usr/share/ossim/modseccollector/modseccollector.logrotate` to `/etc/logrotate.d/modseccollector` to be sure the generated logs on the sensor get rotated by *logrotate*.

Chapter 4. Troubleshooting

If things go wrong, this chapter gives you some hints where to look for information.

1. Be sure that your Apache/ModSecurity installation has started `mlogc`
2. If `mlogc` is started, please ensure that traffic is going to the sensor and collector by issuing `tcpdump host <sensor> and port 8765`.

   If you see traffic flowing in that direction the ModSecurity end seems to be working fine.

   If you don't see traffic at all, please look into the relevant Apache error logs and the mlogc error log in `/var/log`.
3. If you ensured that traffic is coming from mlogc, please check if `modsec_collector` is running on the sensor and the firewall is opened for port TCP/8765.

   If it is not started, please issue `/usr/share/modsec_collector/start.sh` and check if the process is running by looking into `/var/log/modsec_collector.log`.
4. If `modsec_collector` is running (you will see several instances), please check if `/var/log/modsecurity.log` is growing and has current logs in the file.
5. Check if the agent picks up the logs by looking in `/var/log/ossim/agent.log`.
6. If the agent gets the events, please check the corresponding AlienVault server log by looking in `/var/log/ossim/server.log`.