Firewalls and Intrusion Detection

Comp 232

Lab 4

Karan Tank

Contents

[Introduction: 3](#_Toc22597453)

[Step 1 3](#_Toc22597454)

[Step 2- Download Latest OWASP Modsecurity Rules 4](#_Toc22597455)

[Setup Reverse Proxy 5](#_Toc22597456)

[Starting Up 6](#_Toc22597457)

# Introduction:

Mod-security is a toolkit for Realtime web application, monitoring, logging and access control. It can prevent SQL injections and many other types of web-based attacks in order to protect your website. In this lab, we will be using MOD-Security to block the sql injection attacks.

# Step 1

* We will be using linux operating system.
* For this, we will install the mod security modules using the command **apt-get install libapache2-mod-security2**

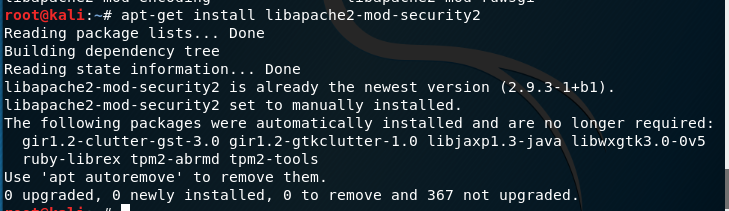


Figure 1

* After installing the mod security modules, you will ned to configure the modsecurity.conf file which is located at /etc/modsecurity/modsecurity.conf
* Change the SecRuleEngine **DetectionOnly** to **ON**



Figure 2

* Now you will need to restart the apache server
* Use the command **systeemctl restart apache2**



Figure 3

# Step 2- Download Latest OWASP Modsecurity Rules

* You can download the new OWSASP Modsecurity rules from git with the command

**”gir clone** [**http://github.com/spiderlabs/owasp-modsecurity-crs.git**](http://github.com/spiderlabs/owasp-modsecurity-crs.git)**”**

* It will create a new directory in the /usr/share/modsecurity-crs
* You need to rename crs-setup.conf.example to crs-setup.conf
* Go to the /etc/apache2/mods-enabled/security2.conf, open the config file and add the following lines

IncludeOptional /etc/modsecurity/\*.conf

IncludeOptional /etc/modsecurity-crs/\*.conf

IncludeOptional /etc/modsecurity-crs/rules/\*.conf

* This will enable the mod security rules to get it working in the apache 2

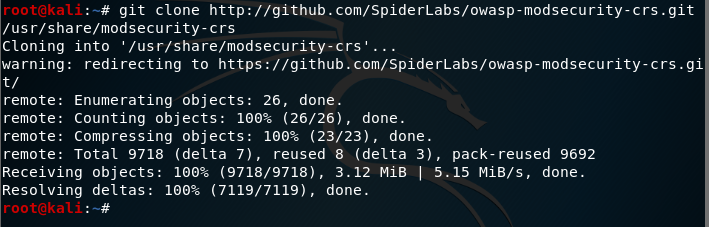


Figure 4



Figure 5

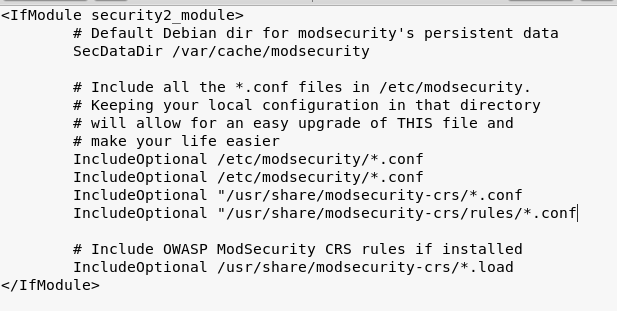


Figure 6

# Setup Reverse Proxy

* Now we will have to setup the reverse proxy.
* If the client makes a request, the reverse proxy will send and return that request. We are setting this at 000-default.conf which is in apache2 directory.
* We will need to configure the proxypass and proxyreverse, proxypass will create a reverse proxy and proxyreverse is used to change the headers sent to apache from proxy app server before apache send it to browser.

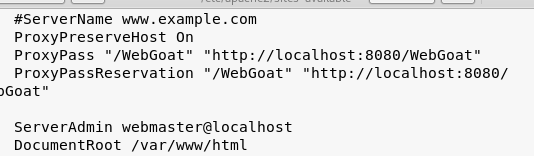


Figure 7

# Starting Up

* We will enable the module proxy using the command sudo a2enmod proxy and sudo a2enmod proxy\_http
* We will use tail -f /var/log/modsec\_audit.log o see the live logs.
* After that we will go to webgoat and try to inject the sql.
* You wont be able to bypass using the sql and you will be able to see logs in the tail -f, it will detect the mod security injection.
* You can also see the traffic in the Wireshark, you should see HTTP forbidden packets

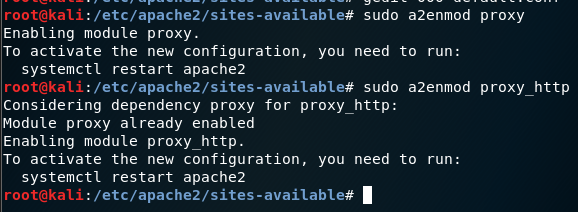


Figure 8



Figure 9

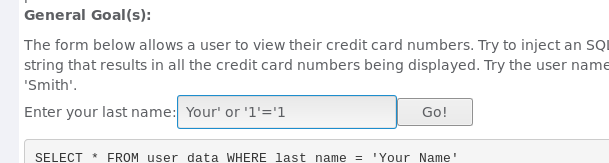


Figure 10

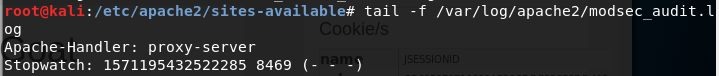


Figure 11

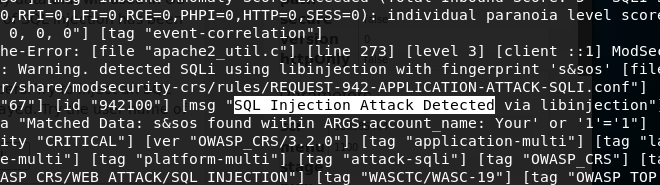


Figure 12

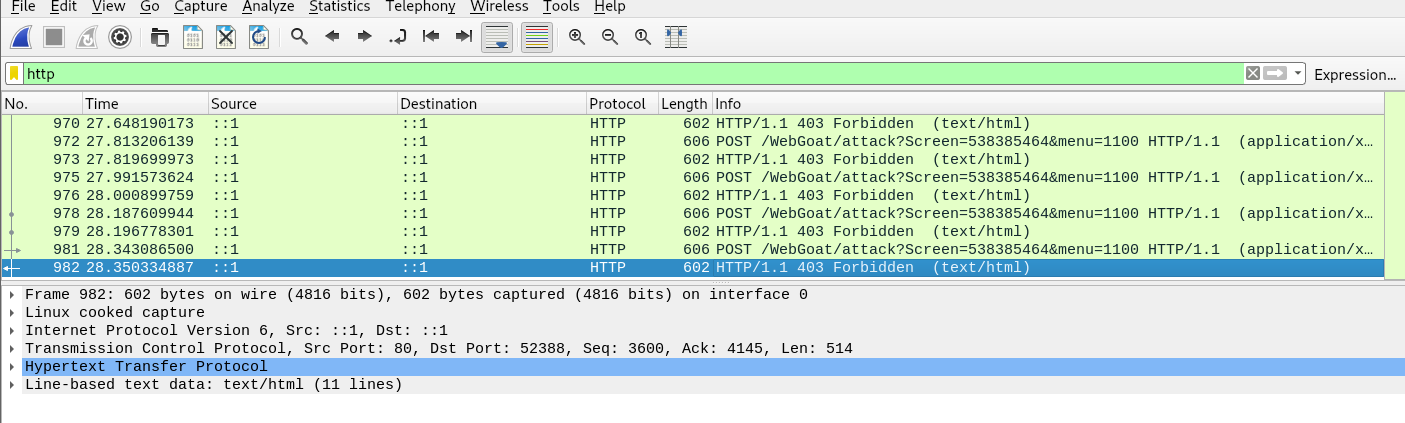


Figure 13