ModSecurityWAF-on-DVWA-from-template

1) Deploy a VM from template "Templ_DVWA_2021" in the netlab
2) From vsphere web client modify:

- Memory: from 1 to 4G
- CPU: from 1 to 2 cores
- Network: connect a WAN VLAN so you can reach the VM directly from your laptop (with VPN)

3) Boot, login (student/student) and immediately type:

```
sudo apt update
sudo apt full-upgrade
```

4) Set a decent password for student by typing:

```
passwd
```

5) Enable SSH connection by typing (for easy copy/paste):

```
sudo apt install openssh-server
```

6) Verify that DVWA is reachable as it should be at http://192.168.<yournetwork>.<yourip>/dvwa

-- if you cannot browse your DVWA site now, it makes no sense to continue below ---

7) ModSecurity can be installed by running the following command in your terminal:

```
sudo apt install libapache2-mod-security2 -y
```

8) After installing ModSecurity, enable the Apache 2 headers module by running the following command:

```
sudo a2enmod headers security2
```

9) After installing ModSecurity and enabling the header module, you need to restart the apache2 service, this can be done by running the following command:

```
sudo systemctl restart apache2
```

10) Verify again that DVWA is (still) reachable as it should be at http://192.168.<yournetwork>.<yourip>/dvwa

11) By default, ModSecurity is only configured to detect and log suspicious activity. We need to go an extra step and configure it to not only detect but also block suspicious activity. Copy, the default ModSecurity configuration file – modsecurity.conf-recommended – to a new file as provided in the command below:

```
sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

12) Using your preferred text editor, open the file

```
sudo nano /etc/modsecurity/modsecurity.conf
```

Locate the line:

```
SecRuleEngine DetectionOnly
```

Set it to:

```
SecRuleEngine On
```

13) To apply the changes in Apache, restart the webserver.

```
sudo systemctl restart apache2
```

14) Verify again that DVWA is (still) reachable as it should be at http://192.168.<yournetwork>.<yourip>/dvwa

15) The next step is to download the latest OWASP ModSecurity Core Rule Set (CRS) from the GitHub page. Clone the OWASP git repository as shown:

```
	cd
	git clone https://github.com/coreruleset/coreruleset.git
```

Navigate into the directory.

```
	cd coreruleset/
```

Be sure to move the crs-setup.conf.example file to the modsecurity directory and rename it as crs-setup.conf.

```
	sudo mv crs-setup.conf.example /etc/modsecurity/crs-setup.conf
```

In addition, move the rules directory to the modsecurity directory as well.

```
	sudo mv rules/ /etc/modsecurity/
```

Next, edit the security2.conf file.

```
	sudo nano /etc/apache2/mods-enabled/security2.conf
```

Ensure that it contains the following line:

```
	IncludeOptional /etc/modsecurity/*.conf
```

REPLACE the line: `IncludeOptional /usr/share/modsecurity-crs/owasp-crs.load`

WITH

```
	Include /etc/modsecurity/rules/*.conf
```

16) There seems to be a compatibility problem with one particular rule file (September 2022) so rename that file with the following oneliner:

```
	sudo mv /etc/modsecurity/rules/REQUEST-922-MULTIPART-ATTACK.conf
/etc/modsecurity/rules/REQUEST-922-MULTIPART-ATTACK.conf.renamed
```

17) To have modsecurity also protect the dvwa default virtualhost you have to modify the default entry as follows:

```
	sudo nano /etc/apache2/sites-available/000-default.conf
```

and add the following rule :

```
	SecRuleEngine On
```

a few lines above the ‘`Virtualhost`’ closing tag.

18) Restart the webserver again by

```
	sudo systemctl restart apache2
```

19) Now browse to your dvwa, set the security to "low" and see that almost all evil actions will be blocked.

20) All evil action is logged into the apache error.log and you can continuously visualise this with:

```
	tail -f /var/log/apache2/error.log
```

(If you like or prefer nice visualisations, you might search the web for free open source dashboards like grafana)

If you want to use this website for dvwa practicing again, so without waf-blocking, you can simply toggle protection on and off with the "`SecRuleEngine`" setting in /etc/apache2/sites-available/000-default.conf and restarting apache as you know by now.

Resource: https://www.tecmint.com/install-modsecurity-with-apache-on-debian-ubuntu/