Block wp-login.php Brute Force Attacks With Mod_Security

This how-to goes through the needed steps to enable Mod_Security rules that will rate limit access to wp-login.php files server wide. When a user logs into a WordPress site successfully, a 302 redirect is called by WordPress and they are redirected to the admin page. When a failed login happens on wp-login.php a 200 response is generated and the login page refreshes. These Mod_Security rules watch for 10 or more 200 responses in 3 minutes and it will block with a 401 response for 5 minutes once that threshold has been tripped.

Step-by-step guide

1. Check to make sure Mod_Security is compiled into Apache: `/usr/sbin/httpd -M | grep security`
    a. Run EasyApache and enable if it is not enabled. Inform customer that this has to happen to enable Mod_Security.
2. Check the current modsec2.conf for SecDataDir, SecTmpDir, and SecUploadDir directives in `/usr/local/apache/conf/modsec2.conf`
    a. Add them with this if they are not present:
    ```
    sed -i '/^<IfModule/a SecDataDir \/tmp' /usr/local/apache/conf/modsec2.conf
    sed -i '/^<IfModule/a SecTmpDir \/tmp' /usr/local/apache/conf/modsec2.conf
    sed -i '/^<IfModule/a SecUploadDir \/tmp' /usr/local/apache/conf/modsec2.conf
    ```
3. Add these rules to `/usr/local/apache/conf/modsec2.user.conf`

WP Brute Force

```
SecAction
phase:1,nolog,pass,initcol:ip=%{REMOTE_ADDR},initcol:user=%{REMOTE_ADDR},id:5000134
<Files "wp-login.php">
# Setup brute force detection.
# React if block flag has been set.
SecRule user:bf_block "@gt 0" "deny,status:401,log,id:5000135,msg:'ip address
blocked for 5 minutes, more than 10 login attempts in 3 minutes.'"
# Setup Tracking. On a successful login, a 302 redirect is performed, a 200
indicates login failed.
SecRule RESPONSE_STATUS "^302"
"phase:5,t:none,nolog,pass,setvar:ip.bf_counter=0,id:5000136"
SecRule RESPONSE_STATUS "^200"
"phase:5,chain,t:none,nolog,pass,setvar:ip.bf_counter=+1,deprecatevar:ip.bf_counter=1/180,id:5000137"
SecRule ip:bf_counter "@gt 10"
"t:none,setvar:user.bf_block=1,expirevar:user.bf_block=300,setvar:ip.bf_counter=0"
</Files>
```

4. Check to make sure this is all valid syntax:
    ```
    /usr/local/apache/bin/apachectl -t
    ```
5. Restart httpd: `/etc/init.d/httpd restart`
6. Test the new rule sets by trying to login more than 10 times in 3 minutes on one of their WordPress sites.

Enable CSF to Block IP on Firewall on Mod_Security Failure
You can also enable CSF to block IPs on the firewall after a set amount of Mod_Security failures. Verify with the client if they want to turn this feature on.

```
sed -i 's/LF_MODSEC =.*/LF_MODSEC = "20"/g' /etc/csf/csf.conf
sed -i 's/LF_MODSEC_PERM =.*/LF_MODSEC_PERM = "1"/g' /etc/csf/csf.conf
csf -r && service lfd restart
```

This Mod_Security rule set should work with LiteSpeed WebServer too!

Related articles

- Block Access to xmlrpc.php Server Wide
- Search for WordPress Brute Force Attacks
- WordPress Optimization
- Block wp-login.php Brute Force Attacks With Mod_Security