NGINX

We can use Fail2ban to

1. Block too many HTTP Authentication attempts
2. Prevent clients from searching for scripts
3. Stop malicious requests from bots
4. Ban clients trying to use NGINX as an open proxy

1. Block too many HTTP Authentication attempts

Create the file `/etc/fail2ban/jail.d/nginx-http.local`. Add the following content:

```
[nginx-http-auth]

enabled  = true
filter   = nginx-http-auth
port     = http,https
logpath  = /var/log/nginx/error.log
```

Keep in mind, that you change the error log, for every site you use. E.G., you only want to monitor failed authentication attempts for your custom log path, `error-bookstack.log`.

2. Prevent clients from searching for scripts

> Only use this function, if you have no scripts and no PHP on your Website!

Create the file `/etc/fail2ban/jail.d/nginx-noscript.local`. Add the following content:

```
[nginx-noscript]

enabled  = true
port     = http,https
filter   = nginx-noscript
logpath  = /var/log/nginx/access.log
maxretry = 6
```

Again, you might want to/have to change the log path.

3. Stop malicious requests from Bots

Create the file `/etc/fail2ban/jail.d/nginx-nobots.local`. Add the following content:

```
[nginx-badbots]

enabled  = true
port     = http,https
filter   = nginx-badbots
logpath  = /var/log/nginx/access.log
maxretry = 2
```

Again, you might want to/have to change the log path.

4.Ban clients trying to use NGINX as open proxy

Create the file `/etc/fail2ban/jail.d/nginx-noproxy.local`. Add the following content:

```
[nginx-noproxy]

enabled  = true
port     = http,https
filter   = nginx-noproxy
logpath  = /var/log/nginx/access.log
maxretry = 2
```

In this case, you should actually leave it at the global access logfile.

Start and reload SSHD, and then add your jail

```
sudo fail2ban-client start
sudo fail2ban-client reload
sudo fail2ban-client add <yournginxjail>
```

Created 2024-11-24 18:13:48 UTC by Nicolas
Updated 2024-12-16 11:42:28 UTC by Nicolas