

Now that we have some footholds onto the network we need to begin to setup a command and control server to gain persistence as well as escalate privileges.



## Command and Control Server Overview

A command and control server is used as an interface to upload and control various post-exploitation tools without interacting with the target itself. Consider C2 as a means for mass-management of exploited targets for further usage - be it lateral movement, information gathering, or otherwise.

### Installing Starkiller

- 1.) `cd /opt`
- 2.) Download an up to date version of starkiller from the BC-Security Github repo - <https://github.com/BC-SECURITY/Starkiller/releases>
- 3.) `chmod +x starkiller-1.3.2.AppImage`
- 4.) `sudo ./starkiller-1.3.2.AppImage --no-sandbox`

### Installing Empire

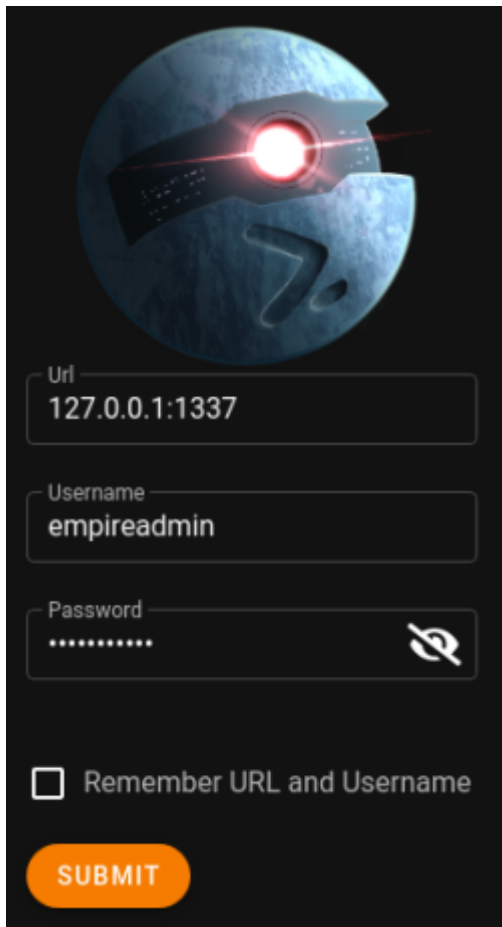
- 1.) `cd /opt`
- 2.) `git clone https://github.com/BC-SECURITY/Empire.git`
- 3.) `cd Empire`
- 4.) `sudo ./setup/install.sh`

## Setting Up Starkiller

- 1.) `cd /opt`
- 2.) `cd Empire`
- 3.) `sudo ./empire --rest`
- 4.) `cd ..`
- 5.) `sudo ./starkiller-1.3.2.ApplImage --no-sandbox`
- 6.) Login to Starkiller

### Default Credentials:

uri: 127.0.0.1:1337  
user: empireadmin  
pass: password123

The image shows the Starkiller login page. At the top is a circular logo featuring a blue planet with a black orbital ring and a red laser beam. Below the logo are three input fields: 'Url' with the value '127.0.0.1:1337', 'Username' with the value 'empireadmin', and 'Password' with masked characters and a toggle icon. Below these fields is a checkbox labeled 'Remember URL and Username' which is unchecked. At the bottom is an orange 'SUBMIT' button.

Url  
127.0.0.1:1337

Username  
empireadmin

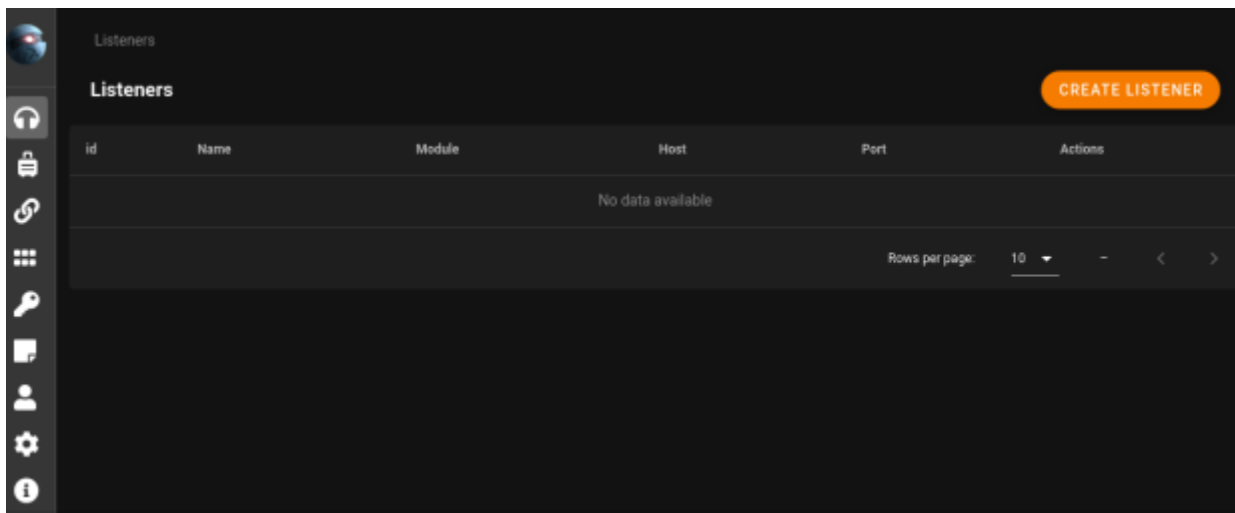
Password  
.....

☐ Remember URL and Username

SUBMIT

### *Starkiller Login Page*

If you properly setup Starkiller and Empire you will be met with a listeners panel after logging in.



*Starkiller Landing Page*

Answer the questions below

Read the above text and install Starkiller

Question Done