Red Blood

Contents

Introduction:

Red blood is a Command-and-Control framework which will help you for red team operations.

Installations:

Requirement:

1- Node.js

2- Install npm packages

Setup:

```
$ git clone https://github.com/kira2040k/RedbloodC2/
$ cd RedbloodC2
$ npm install
```

Check:

```
$ node server.js
```

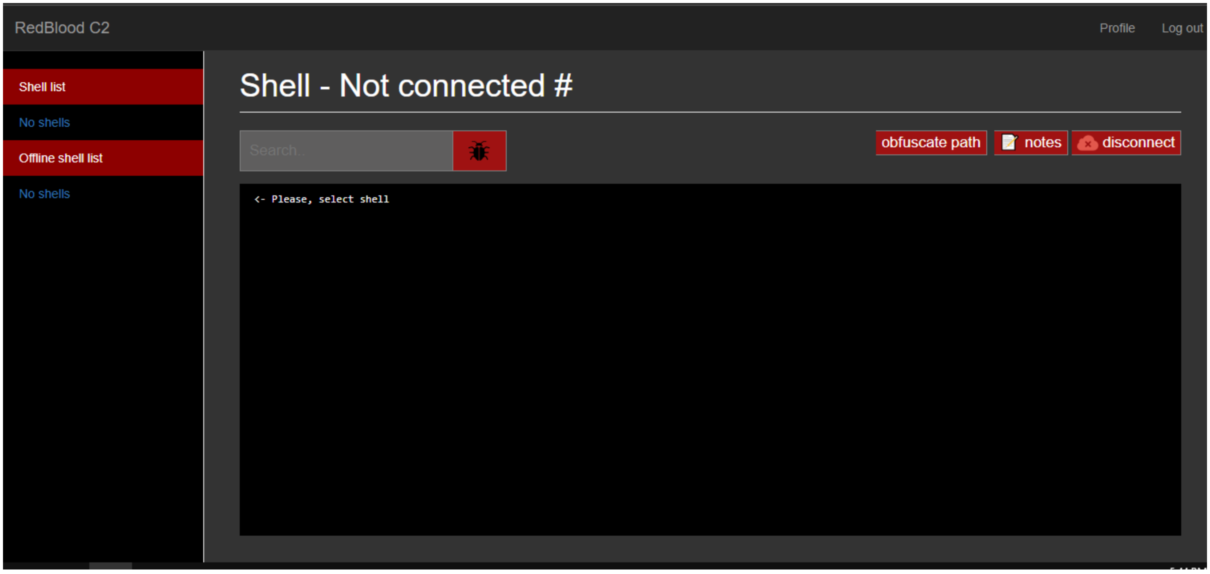
Output:

```
app listening on port 80!
http://localhost:80

username:admin
password:admin
```

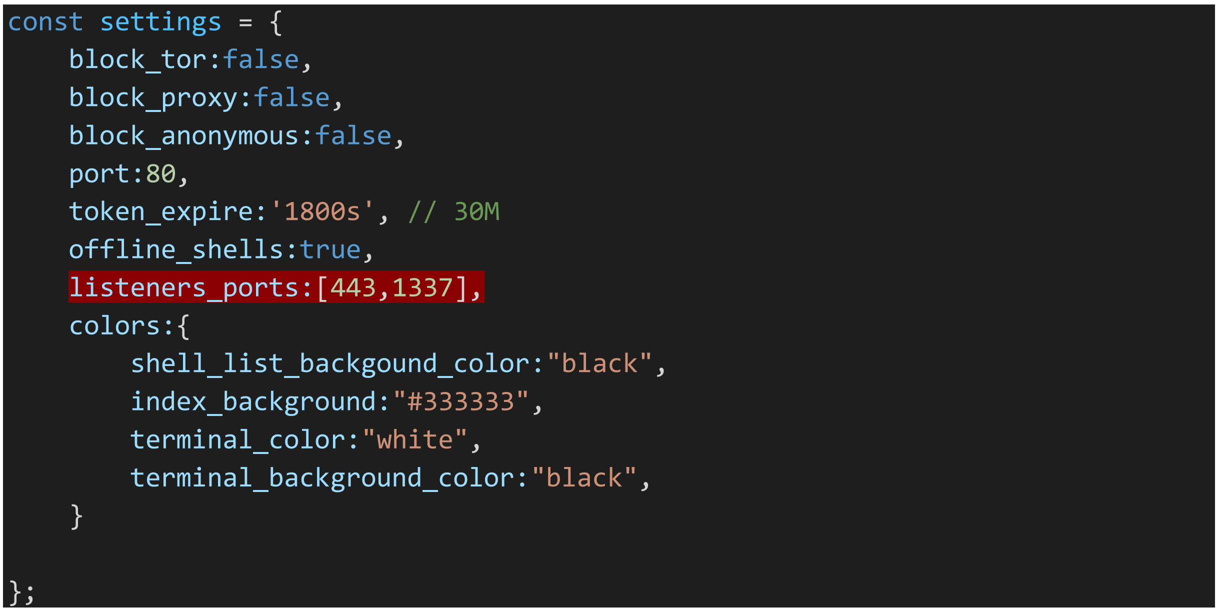
Overview:

After we logged we can see the index page.



```
<- Please, select shell
```

In config.js file we can control and customize the C2.



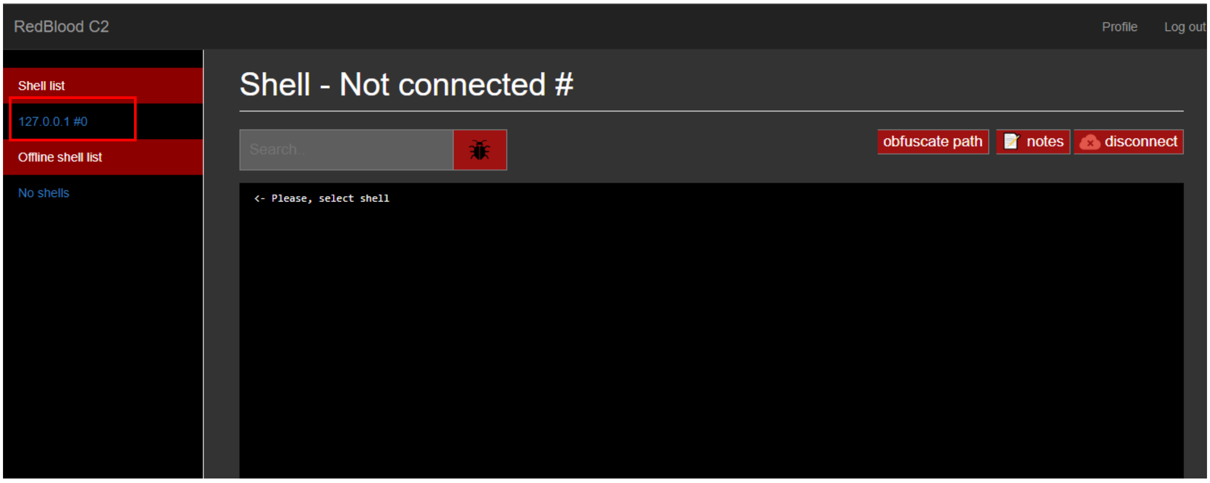
```
const settings = {
    block_tor:false,
    block_proxy:false,
    block_anonymous:false,
    port:80,
    token_expire:'1800s', // 30M
    offline_shells:true,
    listeners_ports:[443,1337],
    colors:{
        shell_list_backgound_color:"black",
        index_background:"#333333",
        terminal_color:"white",
        terminal_background_color:"black",
    }

};
```

The C2 will be listen on two ports by default 443 and 1337

Simple reverse shell:

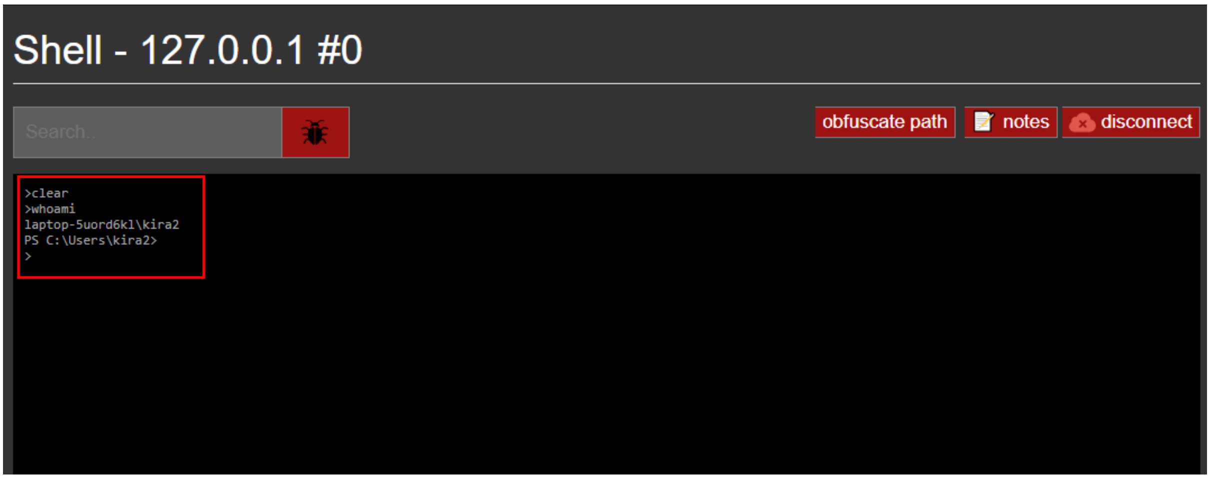
We have executed simple powershell reverse shell we have 1 session



Shell - Not connected #

```
<- Please, select shell
```

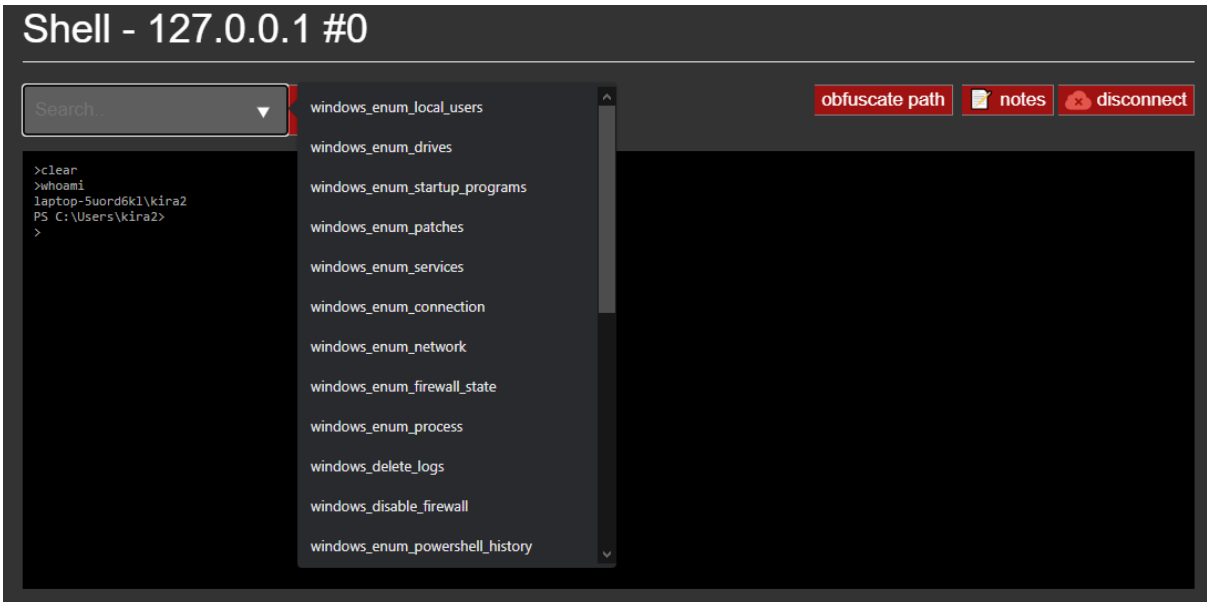
If we navigate to It and execute ‘whoami’ command



```
>clear
>whoami
laptop-5uord6kl\kira2
PS C:\Users\kira2>
>
```

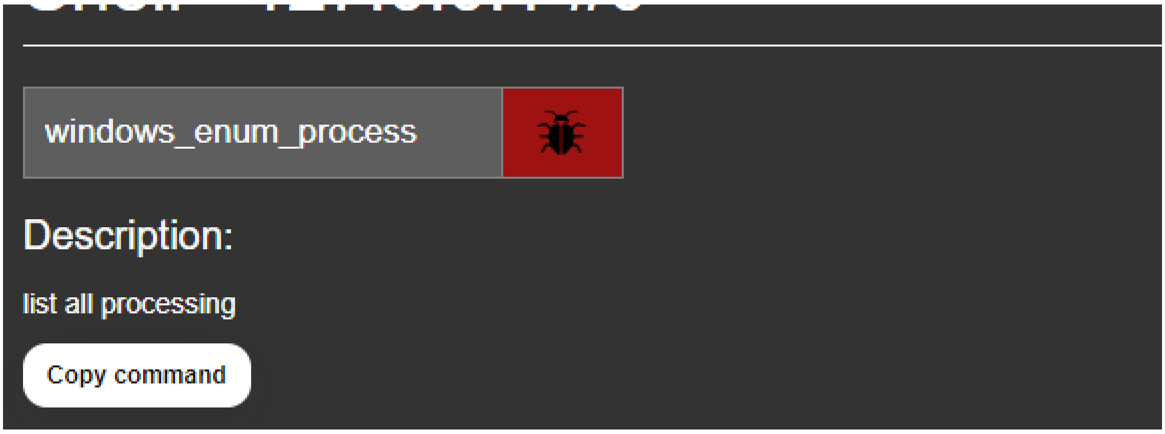
We can see our result let’s execute module

Modules:



```
>clear
>whoami
laptop-5uord6kl\kira2
PS C:\Users\kira2>
>
```

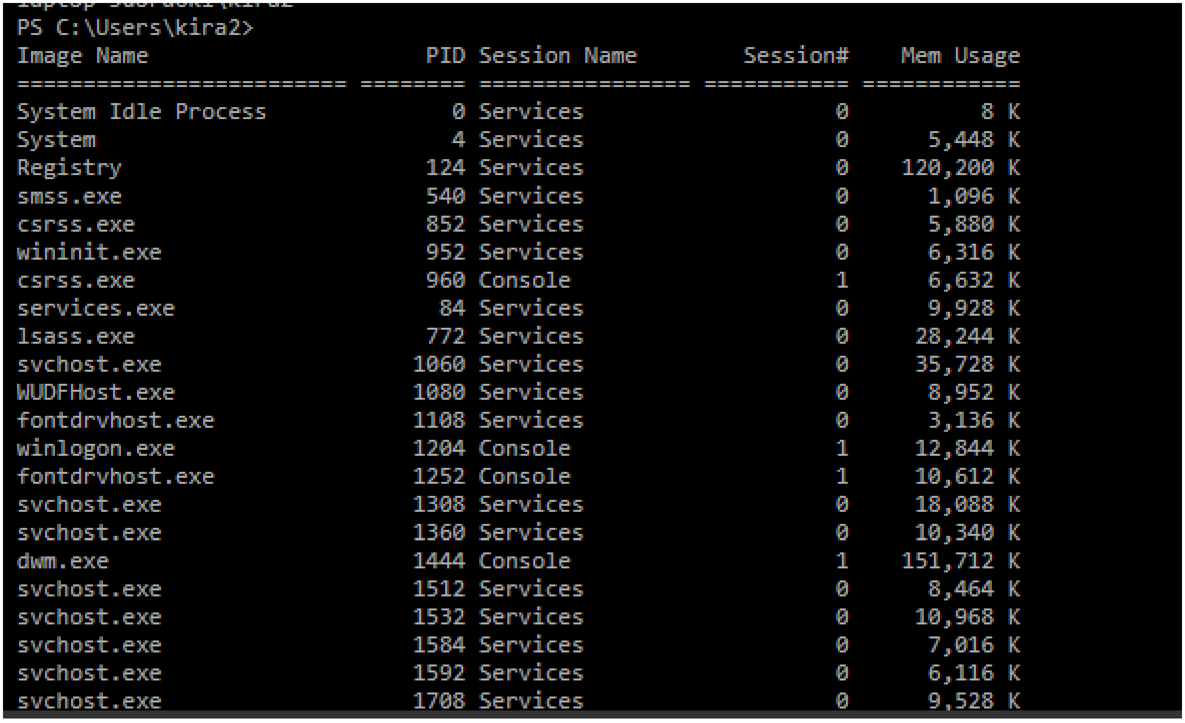
Here all modules we have now. I will select windows_enum_process module


windows_enum_process

Description:

list all processing

As you can see we can see the description and copy command also if we click on the bug the module will be execute.



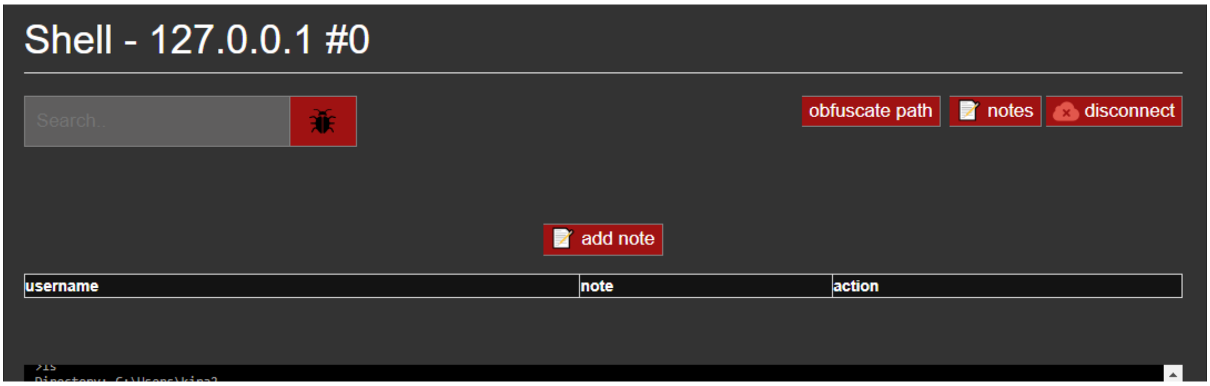
```
PS C:\Users\kira2>
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      5,448 K
Registry                       124 Services                   0    120,200 K
smss.exe                       540 Services                   0      1,096 K
csrss.exe                      852 Services                   0      5,880 K
wininit.exe                    952 Services                   0      6,316 K
csrss.exe                      960 Console                    1      6,632 K
services.exe                    84 Services                   0      9,928 K
lsass.exe                      772 Services                   0     28,244 K
svchost.exe                   1060 Services                   0     35,728 K
WUDFHost.exe                  1080 Services                   0      8,952 K
fontdrvhost.exe               1108 Services                   0      3,136 K
winlogon.exe                  1204 Console                    1     12,844 K
fontdrvhost.exe               1252 Console                    1     10,612 K
svchost.exe                   1308 Services                   0     18,088 K
svchost.exe                   1360 Services                   0     10,340 K
dwm.exe                       1444 Console                    1    151,712 K
svchost.exe                   1512 Services                   0      8,464 K
svchost.exe                   1532 Services                   0     10,968 K
svchost.exe                   1584 Services                   0      7,016 K
svchost.exe                   1592 Services                   0      6,116 K
svchost.exe                   1708 Services                   0      9,528 K
```

Also we can execute it using the terminal with “run” keyword

```
➢ run windows_enum_process
```

this will execute the same thing.

Notes:

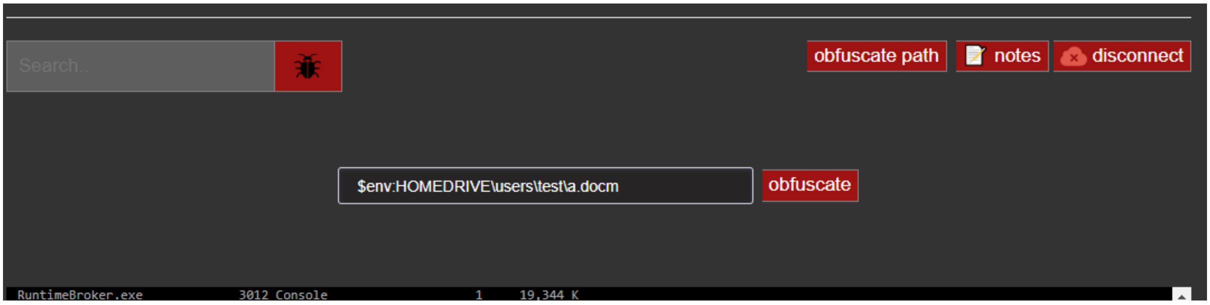


username	note	action

Note for every session we have. We can store creds there.

obfuscate path:

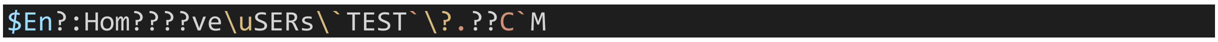
it’s way for obfuscate paths for hide and only work on powershell if we try to obfuscate this path .



$env:HOMEDRIVE\users\test\a.docm

```
RuntimeBroker.exe            3012 Console                    1     19,344 K
```

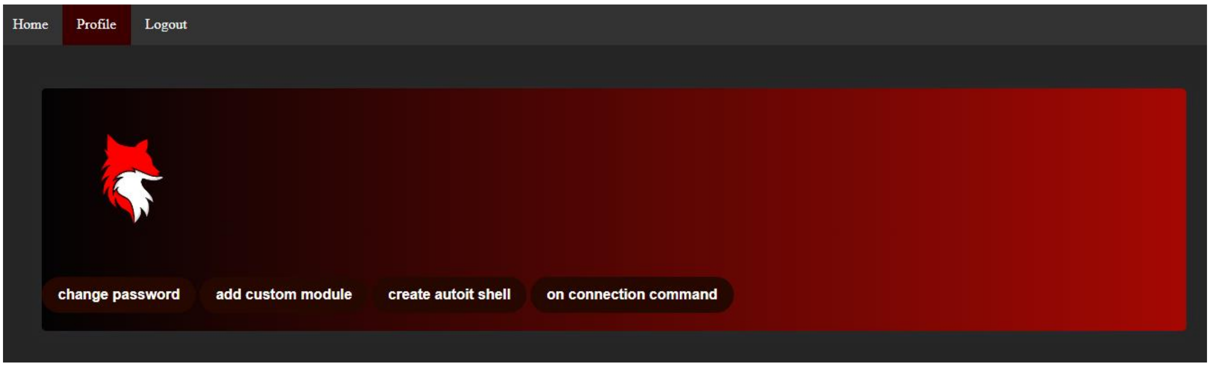
We will get.



```
$En?:Hom????ve\uSERs\`TEST`\?.??C`M
```

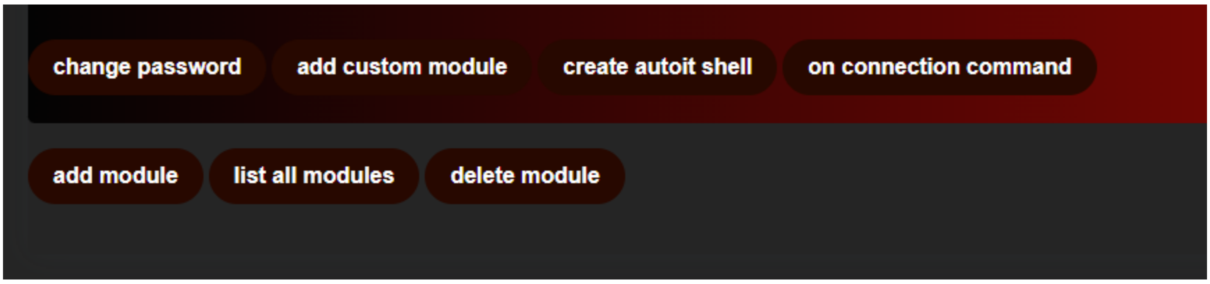
Profile:

From profile page we can control and make custom modules



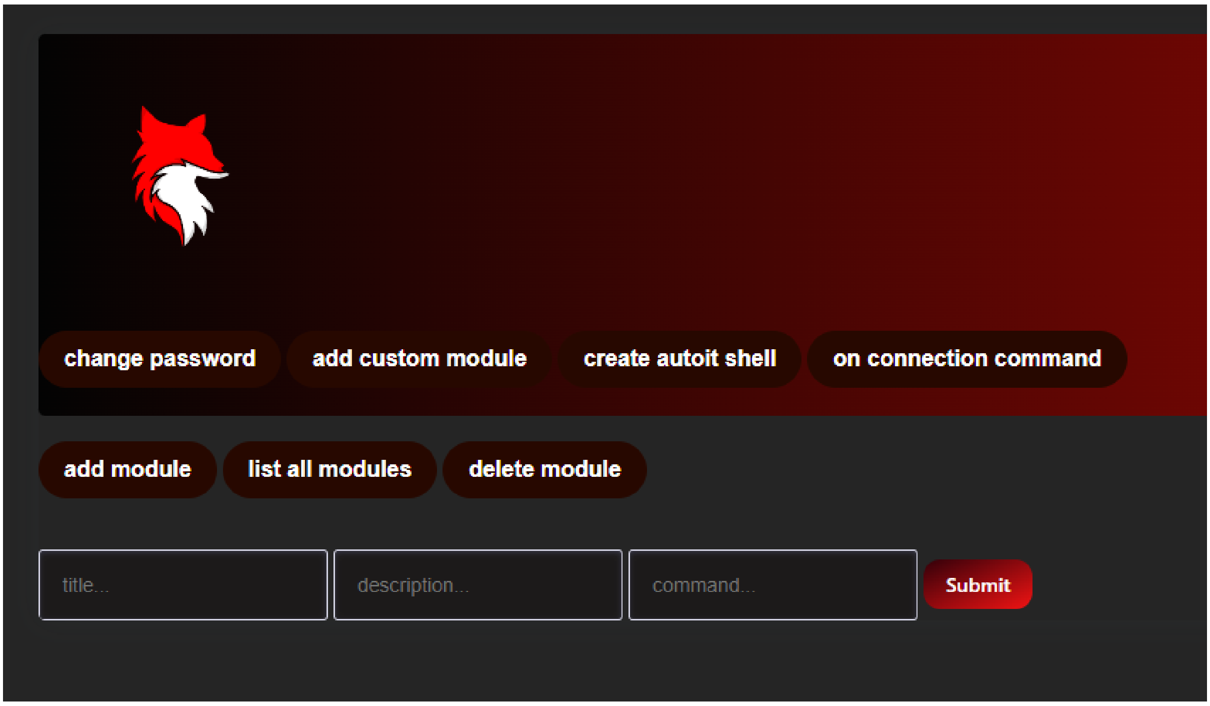
Custom modules:

if we click on custom module we can see



Add module - list modules – delete module

It’s easy to understand but I will explain add module. Because there is good thing there.

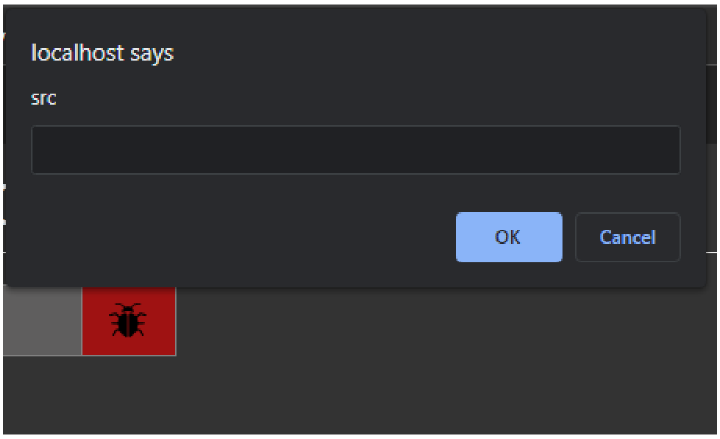


Put the title and description but when put the command we have extra option there. **We can use arguments.**

For example I want to make module for copy file and it will have 2 arguments source file and destination file.
I can put this on command input.

```
copy kiraC1_src_kiraC1 kiraC2_dst_kiraC2
```

Now let's execute this new module



localhost says

src

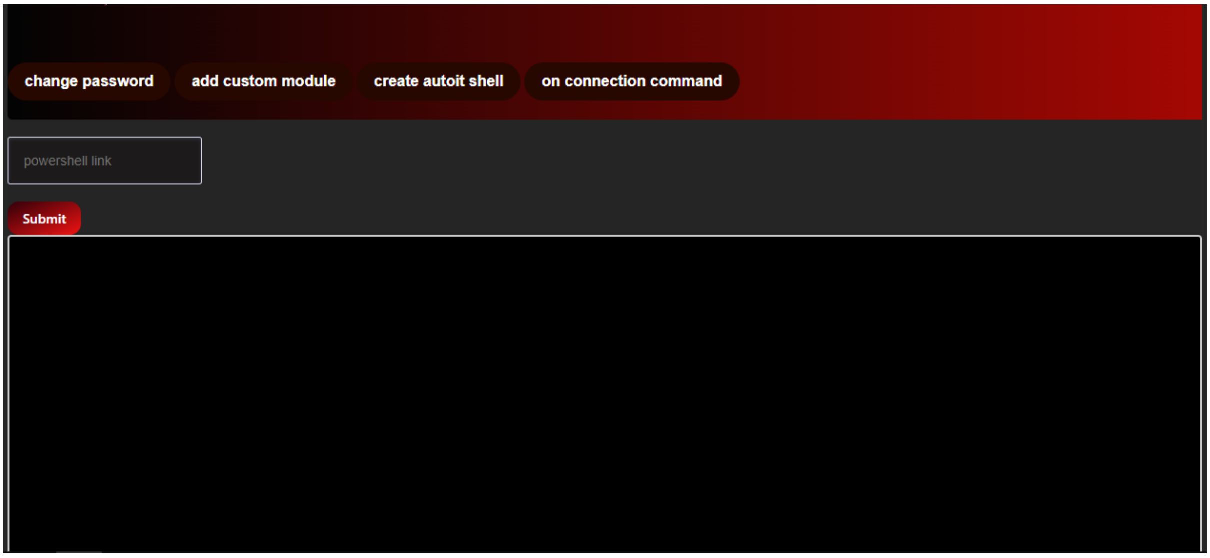
It will ask you for argument from website
If we want to execute it from terminal we can use it like this.

```
>run windows_copy srcfilehere dstfilehere
```

It we have 3 arguments just put C3 and C4….

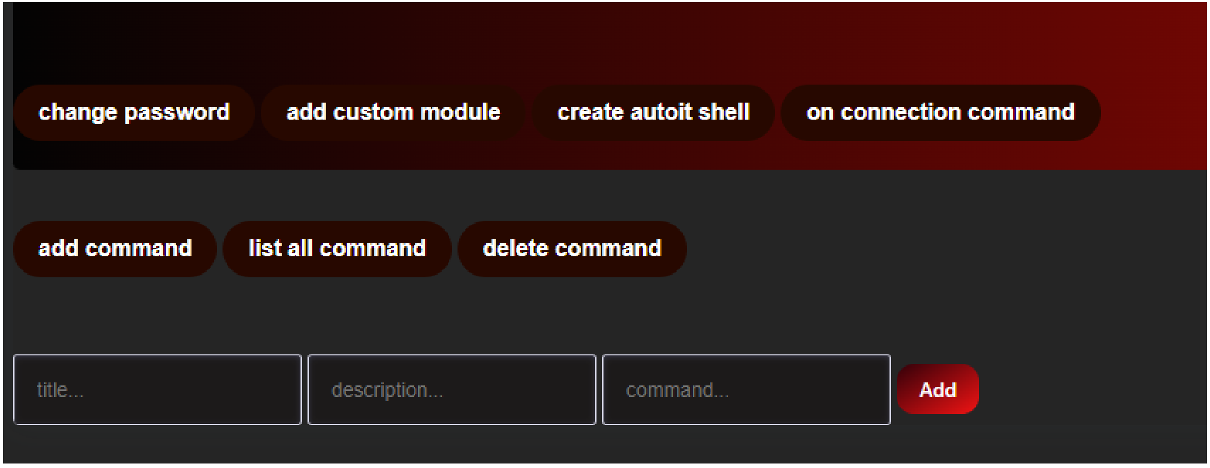
Autoit:

It will generate autoit shell just put link for powershell link that will be executed.



On connection:

The commands you put here will execute automatic when new victims connect it's helpful for persistent. btw we have persistent modules 😊.



Files:

Config.js file:

In config.js file you will find a lot of setting that you can customize your C2 with. Like terminal color or sessions

.env:

There is two values you can changes them
You have to change TOKEN_SECRET value to unique value you can do it with node .

```
crypto.randomBytes(64).toString('hex');
```

Also there are ipdata api key value change it to your key

Block connections:

Because malware analysis use vpns for test malwares we create this feature. After you put your ipdata key change config.js values

```
block_tor:false,
    block_proxy:false,
    block_anonymous:false,
```

as you can see we have 3 options block tor,vpns,proxy just change any one of them to true and will block it using ipdata.