PEAS Report

Basic information

```
OS: Linux version 5.19.0-46-generic (buildd@lcy02-amd64-025) (x86_64-linux-gnu-gcc
(Ubuntu 11.3.0-1ubuntu1~22.04.1) 11.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38)
#47~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 21 15:35:31 UTC 2
User & Groups: uid=1000(prasad) gid=1000(prasad) groups=1000(prasad),4(adm),24(cdrom)
,27(sudo),30(dip),46(plugdev),122(lpadmin),135(lxd),136(sambashare)
Hostname: prasad-Aspire-A315-23
Writable folder: /dev/shm
[+] /usr/bin/ping is available for network discovery (linpeas can discover hosts,
learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port
forwarding (linpeas can discover hosts, scan ports, and forward ports. Learn more
with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (linpeas can
discover hosts and scan ports, learn more with -h)
Caching directories DONE
```

Container

Container related tools present (if any):

```
/usr/local/bin/docker
/usr/bin/runc
```

Container details

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

Cloud

```
Google Cloud Platform? ............... 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? ............................ No
Azure APP? ........................... No
```

Processes, Crons, Timers, Services and Sockets

Cleaned processes

Check weird & unexpected proceses run by root:
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes

```
root 1 0.0 0.2 166748 12132 ? Ss Jul30 0:03 /sbin/init splash
root 307 0.0 0.5 81500 33060 ? S<s Jul30 0:04 /lib/systemd/systemd-journald
root 360 0.0 0.1 26868 7036 ? Ss Jul30 0:00 /lib/systemd/systemd-udevd
systemd+ 546 0.0 0.1 14824 6224 ? Ss Jul30 0:05 /lib/systemd/systemd-oomd
(Caps) 0x0000000000000022=cap_dac_override,cap_kill
systemd+ 547 0.0 0.2 27112 14948 ? Ss Jul30 0:01 /lib/systemd/systemd-resolved
(Caps) 0x0000000000002000=cap_net_raw
systemd+ 548 0.0 0.1 89376 6692 ? Ssl Jul30 0:00 /lib/systemd/systemd-timesyncd
(Caps) 0x0000000002000000=cap_sys_time
root 625 0.0 0.1 248656 7904 ? Ssl Jul30 0:00 /usr/libexec/accounts-daemon
root 626 0.0 0.0 2812 1140 ? Ss Jul30 0:00 /usr/sbin/acpid
avahi 706 0.0 0.0 7440 332 ? S Jul30 0:00 _ avahi-daemon: chroot helper
root 630 0.0 0.0 10592 5312 ? Ss Jul30 0:00 /usr/lib/bluetooth/bluetoothd
root 632 0.0 0.0 18148 3012 ? Ss Jul30 0:00 /usr/sbin/cron -f -P
message+ 634 0.0 0.1 11104 6520 ? Ss Jul30 0:02 @dbus-daemon --system
--address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
(Caps) 0x0000000020000000=cap_audit_write
root 635 0.0 0.3 270112 19044 ? Ssl Jul30 0:01 /usr/sbin/NetworkManager --no-daemon
root 641 0.0 0.0 82832 3892 ? Ssl Jul30 0:00 /usr/sbin/irqbalance --foreground
root 644 0.0 0.3 49740 20900 ? Ss Jul30 0:00 /usr/bin/python3
/usr/bin/networkd-dispatcher --run-startup-triggers
root 645 0.0 0.1 251588 11124 ? Ssl Jul30 0:02 /usr/libexec/polkitd --no-debug
root 648 0.0 0.1 248740 6788 ? Ssl Jul30 0:00 /usr/libexec/power-profiles-daemon
syslog 653 0.0 0.0 222400 5772 ? Ssl Jul30 0:00 /usr/sbin/rsyslogd -n -iNONE
root 668 0.0 0.6 1466228 37504 ? Ssl Jul30 0:02 /usr/lib/snapd/snapd
root 670 0.0 0.1 245112 6768 ? Ssl Jul30 0:00 /usr/libexec/switcheroo-control
root 674 0.0 0.1 48224 8184 ? Ss Jul30 0:00 /lib/systemd/systemd-logind
root 681 0.0 0.2 393320 13400 ? Ssl Jul30 0:00 /usr/libexec/udisks2/udisksd
root 685 0.0 0.1 17688 10352 ? Ss Jul30 0:00 /sbin/wpa_supplicant -u -s -O
/run/wpa_supplicant
root 719 0.0 0.2 318048 12376 ? Ssl Jul30 0:00 /usr/sbin/ModemManager
root 739 0.0 0.2 81636 12440 ? Ss Jul30 0:00 /usr/sbin/cupsd -l
root 747 0.0 0.7 1653128 42292 ? Ssl Jul30 0:05 /usr/bin/containerd
root 796 0.0 0.1 249888 9140 ? Ssl Jul30 0:00 /usr/sbin/gdm3
prasad 1884 0.0 0.1 171040 6316 tty2 Ssl+ 12:42 0:00 _
/usr/libexec/gdm-wayland-session env GNOME_SHELL_SESSION_MODE=ubuntu
/usr/bin/gnome-session --session=ubuntu
prasad 1889 0.0 0.2 231688 13732 tty2 Sl+ 12:42 0:00 _
/usr/libexec/gnome-session-binary --session=ubuntu
root 820 0.0 0.3 126700 21876 ? Ssl Jul30 0:00 /usr/bin/python3
/usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
rtkit 923 0.0 0.0 154000 1540 ? SNsl Jul30 0:00 /usr/libexec/rtkit-daemon
(Caps) 0x0000000000800004=cap_dac_read_search,cap_sys_nice
root 1069 0.0 0.1 251128 8476 ? Ssl Jul30 0:00 /usr/libexec/upowerd
root 1183 0.0 0.2 306844 16796 ? Ssl Jul30 0:00 /usr/libexec/packagekitd
colord 1338 0.0 0.2 254112 12284 ? Ssl Jul30 0:00 /usr/libexec/colord
root 1425 0.0 0.1 172612 11344 ? Ssl Jul30 0:00 /usr/sbin/cups-browsed
root 1426 0.0 1.2 1762584 73032 ? Ssl Jul30 0:00 /usr/bin/dockerd -H fd://
--containerd=/run/containerd/containerd.sock
kernoops 1429 0.0 0.0 13084 400 ? Ss Jul30 0:00 /usr/sbin/kerneloops --test
kernoops 1433 0.0 0.0 13084 452 ? Ss Jul30 0:00 /usr/sbin/kerneloops
prasad 1790 0.2 0.1 18024 10908 ? Ss 12:42 0:05 /lib/systemd/systemd --user
prasad 1791 0.0 0.0 170160 3692 ? S 12:42 0:00 _ (sd-pam)
prasad 1797 0.0 0.0 48512 4936 ? S<sl 12:42 0:00 _ /usr/bin/pipewire
prasad 1798 0.0 0.0 32256 4372 ? Ssl 12:42 0:00 _ /usr/bin/pipewire-media-session
prasad 1799 0.1 0.4 2030816 24516 ? S<sl 12:42 0:02 _ /usr/bin/pulseaudio
--daemonize=no --log-target=journal
prasad 1811 0.1 0.1 10004 6044 ? Ss 12:42 0:02 _ /usr/bin/dbus-daemon --session
--address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
prasad 1823 0.0 0.1 249380 7832 ? Ssl 12:42 0:00 _ /usr/libexec/gvfsd
prasad 2074 0.0 0.1 397636 8696 ? Sl 12:42 0:00 | _ /usr/libexec/gvfsd-trash
--spawner :1.2 /org/gtk/gvfs/exec_spaw/0
prasad 18132 0.0 0.1 397384 8176 ? Sl 12:58 0:00 | _ /usr/libexec/gvfsd-network
--spawner :1.2 /org/gtk/gvfs/exec_spaw/1
prasad 18171 0.0 0.1 325476 8260 ? Sl 12:58 0:00 | _ /usr/libexec/gvfsd-dnssd
--spawner :1.2 /org/gtk/gvfs/exec_spaw/3
prasad 1834 0.0 0.1 380888 6488 ? Sl 12:42 0:00 _ /usr/libexec/gvfsd-fuse
/run/user/1000/gvfs -f
prasad 1841 0.0 0.1 546592 7020 ? Ssl 12:42 0:00 _ /usr/libexec/xdg-document-portal
root 1855 0.0 0.0 2792 976 ? Ss 12:42 0:00 | _ fusermount3 -o
rw,nosuid,nodev,fsname=portal,auto_unmount,subtype=portal -- /run/user/1000/doc
prasad 1849 0.0 0.0 244800 5448 ? Ssl 12:42 0:00 _
/usr/libexec/xdg-permission-store
prasad 1868 0.1 0.4 715824 24692 ? SNsl 12:42 0:02 _
/usr/libexec/tracker-miner-fs-3
prasad 1883 0.0 0.1 398440 9400 ? Ssl 12:42 0:00 _
/usr/libexec/gvfs-udisks2-volume-monitor
prasad 1916 0.0 0.1 323852 8000 ? Ssl 12:42 0:00 _
/usr/libexec/gvfs-afc-volume-monitor
```

```
prasad 1921 0.0 0.1 245284 6220 ? Ssl 12:42 0:00 _
/usr/libexec/gvfs-goa-volume-monitor
prasad 1925 0.0 0.4 573180 24104 ? Sl 12:42 0:00 _ /usr/libexec/goa-daemon
prasad 1939 0.0 0.0 100560 5172 ? Ssl 12:42 0:00 _ /usr/libexec/gnome-session-ctl
--monitor
prasad 1949 0.0 0.2 347052 13728 ? Sl 12:42 0:00 _
/usr/libexec/goa-identity-service
prasad 1957 0.0 0.1 246196 6580 ? Ssl 12:42 0:00 _
/usr/libexec/gvfs-gphoto2-volume-monitor
prasad 1959 0.0 0.2 601556 15988 ? Ssl 12:42 0:00 _
/usr/libexec/gnome-session-binary --systemd-service --session=ubuntu
prasad 1986 0.0 0.1 309624 7628 ? Sl 12:42 0:00 | _
/usr/libexec/at-spi-bus-launcher --launch-immediately
prasad 2000 0.0 0.0 8560 4212 ? S 12:42 0:00 | | _ /usr/bin/dbus-daemon
--config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork
--print-address 11 --address=unix:path=/run/user/1000/at-spi/bus
prasad 2133 0.0 0.1 232264 6740 ? Sl 12:42 0:00 | _
/usr/libexec/gsd-disk-utility-notify
prasad 2177 0.0 0.7 813732 47912 ? Sl 12:42 0:00 | _
/usr/libexec/evolution-data-server/evolution-alarm-notify
prasad 3494 0.0 0.4 502664 29816 ? Sl 12:43 0:00 | _ update-notifier
prasad 1968 0.0 0.1 245108 6400 ? Ssl 12:42 0:00 _
/usr/libexec/gvfs-mtp-volume-monitor
prasad 1990 10.1 5.5 5829216 335160 ? RLsl 12:42 3:55 _ /usr/bin/gnome-shell
prasad 2409 0.5 1.1 3216472 71224 ? Sl 12:42 0:13 | _ gjs
/usr/share/gnome-shell/extensions/ding@rastersoft.com/ding.js -E -P
/usr/share/gnome-shell/extensions/ding@rastersoft.com -M 0 -D
0:0:1920:1080:1:27:0:74:0:0
prasad 6564 2.5 2.1 917664 131104 ? Sl 12:46 0:53 | _ /usr/bin/Xwayland :0
-rootless -noreset -accessx -core -auth /run/user/1000/.mutter-Xwaylandauth.USD881
-listen 4 -listen 5 -displayfd 6 -initfd 7
prasad 8768 24.1 5.4 34211244 327392 ? SLl 12:48 7:52 | _ /opt/google/chrome/chrome
prasad 8784 0.0 0.0 17164 1008 ? S 12:48 0:00 | | _ cat
prasad 8785 0.0 0.0 17164 1012 ? S 12:48 0:00 | | _ cat
prasad 8807 0.0 0.9 33863796 59016 ? S 12:48 0:00 | | _ /opt/google/chrome/chrome
--type=zygote --no-zygote-sandbox --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable
prasad 8837 6.1 3.9 34258936 237544 ? Sl 12:48 1:59 | | | _
/opt/google/chrome/chrome --type=gpu-process --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --gpu-preferences=WA
AAAAAAAAAgAAAEAAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAABAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --shared-files
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 8808 0.0 1.0 33863788 60124 ? S 12:48 0:00 | | _ /opt/google/chrome/chrome
--type=zygote --crashpad-handler-pid=8799 --enable-crash-reporter=,
--change-stack-guard-on-fork=enable
prasad 8809 0.0 0.0 33567788 4888 ? S 12:48 0:00 | | | _
/opt/google/chrome/nacl_helper
(Caps) 0x0000000000200000=cap_sys_admin
prasad 8812 0.0 0.2 33863816 16208 ? S 12:48 0:00 | | | _ /opt/google/chrome/chrome
--type=zygote --crashpad-handler-pid=8799 --enable-crash-reporter=,
--change-stack-guard-on-fork=enable
(Caps) 0x0000000000200000=cap_sys_admin
prasad 8850 0.0 0.8 33915248 53296 ? Sl 12:48 0:00 | | | _
/opt/google/chrome/chrome --type=utility
--utility-sub-type=storage.mojom.StorageService --lang=en-GB
--service-sandbox-type=utility --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable
--shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 9183 0.5 2.5 1187976288 155416 ? Sl 12:49 0:11 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=13 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=1622049128 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 9322 0.6 2.3 1185842880 141156 ? Sl 12:49 0:12 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=17 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=1629638480 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 10739 0.2 2.5 1185842220 153184 ? Sl 12:50 0:04 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
```

```
--renderer-client-id=32 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=1708225515 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 10986 0.5 2.4 1185849424 145504 ? Sl 12:50 0:09 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=34 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=1720279303 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 22654 0.5 2.2 1185875316 135460 ? Sl 13:02 0:06 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=45 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=2437072030 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 23215 2.4 3.0 1185864640 180548 ? Sl 13:03 0:27 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=47 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=2470974864 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 23413 0.3 2.2 1185850764 134668 ? Sl 13:03 0:03 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=48 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=2481088737 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 29406 41.5 3.3 1188010372 199540 ? Sl 13:08 5:11 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=54 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=2816888007 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 31666 1.2 2.6 1185864592 158000 ? Sl 13:10 0:07 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=61 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=2940565930 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 33818 0.7 2.4 1185843936 148988 ? Sl 13:13 0:03 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=64 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=3063072536 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 33973 1.1 3.1 1185865760 189124 ? Sl 13:13 0:05 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=67 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=3073195803 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 79321 18.6 3.3 1185881028 202948 ? Sl 13:18 0:36 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=116 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=3370772761 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 79885 0.0 1.0 1185796736 61056 ? Sl 13:18 0:00 | | | _
/opt/google/chrome/chrome --type=renderer --crashpad-handler-pid=8799
--enable-crash-reporter=, --change-stack-guard-on-fork=enable --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation
--renderer-client-id=118 --time-ticks-at-unix-epoch=-1690786318821035
--launch-time-ticks=3407525756 --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 8838 2.5 2.0 33942132 122276 ? Sl 12:48 0:50 | | _ /opt/google/chrome/chrome
--type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB
--service-sandbox-type=none --crashpad-handler-pid=8799 --enable-crash-reporter=,
--change-stack-guard-on-fork=enable --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 11065 0.0 1.3 34171760 78080 ? Sl 12:50 0:00 | | _ /opt/google/chrome/chrome
```

```
--type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-GB
--service-sandbox-type=none --crashpad-handler-pid=8799 --enable-crash-reporter=,
--change-stack-guard-on-fork=enable --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,13517092735361423202,8021070193610336525,262144
prasad 27319 3.6 2.8 1176805044 170436 ? SLl 13:07 0:31 | _ /usr/share/code/code
--unity-launch
prasad 27322 0.0 0.7 33776624 46280 ? S 13:07 0:00 | _ /usr/share/code/code
--type=zygote --no-zygote-sandbox
prasad 27351 6.7 2.9 34154308 178820 ? Sl 13:07 0:58 | | _ /usr/share/code/code
--type=gpu-process
--enable-crash-reporter=63ef143a-6604-46c5-b777-43930b5e61b3,no_channel
--user-data-dir=/home/prasad/.config/Code --gpu-preferences=WAAAAAAAAAAgAAAIAAAAAA
AAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAAAAAAAIAAAAAA
AAABAAAAAAAAAAgAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --shared-files
--field-trial-handle=0,i,11034451736267362069,3467079015507541823,131072
--disable-features=CalculateNativeWinOcclusion,SpareRendererForSitePerProcess
prasad 27323 0.0 0.7 33776616 46576 ? S 13:07 0:00 | _ /usr/share/code/code
--type=zygote
prasad 27325 0.0 0.1 33776640 11368 ? S 13:07 0:00 | | _ /usr/share/code/code
--type=zygote
(Caps) 0x0000000000200000=cap_sys_admin
prasad 27392 14.6 3.9 1185838632 238544 ? Rl 13:07 2:05 | | _ /usr/share/code/code
--type=renderer
--enable-crash-reporter=63ef143a-6604-46c5-b777-43930b5e61b3,no_channel
--user-data-dir=/home/prasad/.config/Code
--standard-schemes=vscode-webview,vscode-file --enable-sandbox
--secure-schemes=vscode-webview,vscode-file --bypasscsp-schemes
--cors-schemes=vscode-webview,vscode-file
--fetch-schemes=vscode-webview,vscode-file --service-worker-schemes=vscode-webview
--streaming-schemes --app-path=/usr/share/code/resources/app --enable-sandbox
--enable-blink-features=HighlightAPI --first-renderer-process --lang=en-GB
--num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=4
--time-ticks-at-unix-epoch=-1690786318821034 --launch-time-ticks=2707608811
--shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,11034451736267362069,3467079015507541823,131072
--disable-features=CalculateNativeWinOcclusion,SpareRendererForSitePerProcess
--vscode-window-config=vscode:d8539449-4b74-4501-a90e-cf7f34812ea2
prasad 27377 0.1 1.1 33842420 67748 ? Sl 13:07 0:01 | _ /usr/share/code/code
--type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB
--service-sandbox-type=none
--enable-crash-reporter=63ef143a-6604-46c5-b777-43930b5e61b3,no_channel
--user-data-dir=/home/prasad/.config/Code
--standard-schemes=vscode-webview,vscode-file --enable-sandbox
--secure-schemes=vscode-webview,vscode-file --bypasscsp-schemes
--cors-schemes=vscode-webview,vscode-file
--fetch-schemes=vscode-webview,vscode-file --service-worker-schemes=vscode-webview
--streaming-schemes --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,11034451736267362069,3467079015507541823,131072
--disable-features=CalculateNativeWinOcclusion,SpareRendererForSitePerProcess
prasad 27459 1.1 1.5 1176315664 91492 ? Sl 13:07 0:09 | _ /usr/share/code/code
--type=utility --utility-sub-type=node.mojom.NodeService --lang=en-GB
--service-sandbox-type=none
--enable-crash-reporter=63ef143a-6604-46c5-b777-43930b5e61b3,no_channel
--user-data-dir=/home/prasad/.config/Code
--standard-schemes=vscode-webview,vscode-file --enable-sandbox
--secure-schemes=vscode-webview,vscode-file --bypasscsp-schemes
--cors-schemes=vscode-webview,vscode-file
--fetch-schemes=vscode-webview,vscode-file --service-worker-schemes=vscode-webview
--streaming-schemes --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,11034451736267362069,3467079015507541823,131072
--disable-features=CalculateNativeWinOcclusion,SpareRendererForSitePerProcess
prasad 33173 0.0 0.0 20080 4380 pts/1 Ss+ 13:12 0:00 | | _ /usr/bin/bash
--init-file /usr/share/code/resources/app/out/vs/workbench/contrib/terminal/browse
r/media/shellIntegration-bash.sh
prasad 34311 0.0 0.0 20080 5240 pts/2 Ss 13:13 0:00 | | _ /usr/bin/bash --init-file
/usr/share/code/resources/app/out/vs/workbench/contrib/terminal/browser/media/shel
lIntegration-bash.sh
prasad 81609 0.2 0.0 3924 2868 pts/2 S+ 13:20 0:00 | | _ /bin/sh ./linpeas.sh -s
prasad 84153 0.0 0.0 3924 1152 pts/2 S+ 13:21 0:00 | | _ /bin/sh ./linpeas.sh -s
prasad 84156 0.0 0.0 21748 3900 pts/2 R+ 13:21 0:00 | | | _ ps fauxwww
prasad 84157 0.0 0.0 3924 1152 pts/2 S+ 13:21 0:00 | | _ /bin/sh ./linpeas.sh -s
prasad 27460 1.6 1.9 1176306932 116704 ? Sl 13:07 0:13 | _ /usr/share/code/code
--type=utility --utility-sub-type=node.mojom.NodeService --lang=en-GB
--service-sandbox-type=none
--enable-crash-reporter=63ef143a-6604-46c5-b777-43930b5e61b3,no_channel
--user-data-dir=/home/prasad/.config/Code
--standard-schemes=vscode-webview,vscode-file --enable-sandbox
--secure-schemes=vscode-webview,vscode-file --bypasscsp-schemes
--cors-schemes=vscode-webview,vscode-file
```

```
--fetch-schemes=vscode-webview,vscode-file --service-worker-schemes=vscode-webview
--streaming-schemes --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,11034451736267362069,3467079015507541823,131072
--disable-features=CalculateNativeWinOcclusion,SpareRendererForSitePerProcess
prasad 29236 0.1 1.3 1176323852 81400 ? Sl 13:08 0:00 | _ /usr/share/code/code
--type=utility --utility-sub-type=node.mojom.NodeService --lang=en-GB
--service-sandbox-type=none
--enable-crash-reporter=63ef143a-6604-46c5-b777-43930b5e61b3,no_channel
--user-data-dir=/home/prasad/.config/Code
--standard-schemes=vscode-webview,vscode-file --enable-sandbox
--secure-schemes=vscode-webview,vscode-file --bypasscsp-schemes
--cors-schemes=vscode-webview,vscode-file
--fetch-schemes=vscode-webview,vscode-file --service-worker-schemes=vscode-webview
--streaming-schemes --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,11034451736267362069,3467079015507541823,131072
--disable-features=CalculateNativeWinOcclusion,SpareRendererForSitePerProcess
prasad 29249 0.3 1.8 1176307428 112248 ? Sl 13:08 0:03 | _ /usr/share/code/code
--type=utility --utility-sub-type=node.mojom.NodeService --lang=en-GB
--service-sandbox-type=none --inspect-port=0
--enable-crash-reporter=63ef143a-6604-46c5-b777-43930b5e61b3,no_channel
--user-data-dir=/home/prasad/.config/Code
--standard-schemes=vscode-webview,vscode-file --enable-sandbox
--secure-schemes=vscode-webview,vscode-file --bypasscsp-schemes
--cors-schemes=vscode-webview,vscode-file
--fetch-schemes=vscode-webview,vscode-file --service-worker-schemes=vscode-webview
--streaming-schemes --shared-files=v8_context_snapshot_data:100
--field-trial-handle=0,i,11034451736267362069,3467079015507541823,131072
--disable-features=CalculateNativeWinOcclusion,SpareRendererForSitePerProcess
prasad 2029 0.0 0.2 582660 14556 ? Sl 12:42 0:00 _
/usr/libexec/gnome-shell-calendar-server
prasad 2035 0.0 0.3 400820 21552 ? Ssl 12:42 0:00 _
/usr/libexec/evolution-source-registry
prasad 2043 0.0 0.4 849108 26304 ? Ssl 12:42 0:00 _
/usr/libexec/evolution-calendar-factory
prasad 2052 0.0 0.1 157096 6216 ? Ssl 12:42 0:00 _ /usr/libexec/dconf-service
prasad 2058 0.0 0.3 680880 22256 ? Ssl 12:42 0:00 _
/usr/libexec/evolution-addressbook-factory
prasad 2087 0.0 0.4 2882716 24976 ? Sl 12:42 0:00 _ /usr/bin/gjs
/usr/share/gnome-shell/org.gnome.Shell.Notifications
prasad 2089 0.0 0.1 162680 7316 ? Sl 12:42 0:00 _ /usr/libexec/at-spi2-registryd
--use-gnome-session
prasad 2107 0.0 0.2 323944 12184 ? Sl 12:42 0:01 | _ /usr/bin/ibus-daemon --panel
disable
prasad 2219 0.0 0.1 172132 7408 ? Sl 12:42 0:00 | _ /usr/libexec/ibus-memconf
prasad 2226 0.0 0.4 356492 28292 ? Sl 12:42 0:01 | _
/usr/libexec/ibus-extension-gtk3
prasad 2346 0.0 0.1 172132 7428 ? Sl 12:42 0:00 | _ /usr/libexec/ibus-engine-simple
prasad 2105 0.0 0.1 319080 6664 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-a11y-settings
prasad 2109 0.0 0.4 545036 24656 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-color
prasad 2111 0.0 0.2 384116 14428 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-datetime
prasad 2114 0.0 0.1 320584 7372 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-housekeeping
prasad 2116 0.0 0.3 349248 21344 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-keyboard
prasad 2119 0.0 0.4 651636 24056 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-media-keys
prasad 2122 0.0 0.3 532936 23948 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-power
prasad 2124 0.0 0.1 258504 11608 ? Ssl 12:42 0:00 _
/usr/libexec/gsd-print-notifications
prasad 2125 0.0 0.1 466508 6476 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-rfkill
prasad 2129 0.0 0.1 244940 6540 ? Ssl 12:42 0:00 _
/usr/libexec/gsd-screensaver-proxy
prasad 2130 0.0 0.1 474604 9628 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-sharing
prasad 2131 0.0 0.1 401304 10956 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-smartcard
prasad 2132 0.0 0.1 327996 9272 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-sound
prasad 2136 0.0 0.3 349824 21732 ? Ssl 12:42 0:00 _ /usr/libexec/gsd-wacom
prasad 2235 0.0 0.1 245908 7624 ? Sl 12:42 0:00 _ /usr/libexec/ibus-portal
prasad 2311 0.0 0.2 351008 13912 ? Sl 12:42 0:00 _ /usr/libexec/gsd-printer
prasad 2364 0.0 0.1 697980 10988 ? Ssl 12:42 0:00 _ /usr/libexec/xdg-desktop-portal
prasad 2370 0.0 0.4 671552 27112 ? Ssl 12:42 0:00 _
/usr/libexec/xdg-desktop-portal-gnome
prasad 2391 0.0 0.4 2939928 24256 ? Sl 12:42 0:00 _ /usr/bin/gjs
/usr/share/gnome-shell/org.gnome.ScreenSaver
prasad 2430 0.0 0.4 353108 24836 ? Ssl 12:42 0:00 _
/usr/libexec/xdg-desktop-portal-gtk
prasad 2479 0.0 0.1 171716 6600 ? Ssl 12:42 0:00 _ /usr/libexec/gvfsd-metadata
prasad 6079 0.0 0.7 887412 43624 ? Sl 12:46 0:00 _ /usr/bin/gnome-calendar
--gapplication-service
prasad 6083 0.0 0.6 409124 40224 ? SLl 12:46 0:00 _ /usr/bin/seahorse
--gapplication-service
prasad 6179 0.0 0.0 92640 3440 ? SLs 12:46 0:00 _ /usr/bin/gpg-agent --supervised
prasad 6577 0.0 1.3 833100 82820 ? Ssl 12:46 0:00 _ /usr/libexec/gsd-xsettings
```

```
prasad 6606 0.0 0.4 202804 25020 ? Sl 12:46 0:00 _ /usr/libexec/ibus-x11
prasad 8799 0.0 0.0 33576964 3316 ? Sl 12:48 0:00 _
/opt/google/chrome/chrome_crashpad_handler --monitor-self
--monitor-self-annotation=ptype=crashpad-handler
--database=/home/prasad/.config/google-chrome/Crash Reports
--metrics-dir=/home/prasad/.config/google-chrome
--url=https://clients2.google.com/cr/report --annotation=channel=
--annotation=lsb-release=Ubuntu 22.04.2 LTS --annotation=plat=Linux
--annotation=prod=Chrome_Linux --annotation=ver=114.0.5735.198
--initial-client-fd=5 --shared-client-connection
prasad 8801 0.0 0.0 33567728 3212 ? Sl 12:48 0:00 _
/opt/google/chrome/chrome_crashpad_handler --no-periodic-tasks
--monitor-self-annotation=ptype=crashpad-handler
--database=/home/prasad/.config/google-chrome/Crash Reports
--url=https://clients2.google.com/cr/report --annotation=channel=
--annotation=lsb-release=Ubuntu 22.04.2 LTS --annotation=plat=Linux
--annotation=prod=Chrome_Linux --annotation=ver=114.0.5735.198
--initial-client-fd=4 --shared-client-connection
prasad 13530 1.4 1.2 821176 75172 ? Sl 12:53 0:23 _ /usr/bin/nautilus
--gapplication-service
prasad 30939 0.1 0.7 562088 47316 ? Ssl 13:10 0:01 _
/usr/libexec/gnome-terminal-server
prasad 30992 0.0 0.0 20056 4328 pts/0 Ss+ 13:10 0:00 _ bash
prasad 1813 0.0 0.1 323396 7340 ? Sl 12:42 0:00 /usr/bin/gnome-keyring-daemon
--daemonize --login
prasad 47511 0.0 0.0 7968 4604 ? S 13:15 0:00 _ /usr/bin/ssh-agent -D -a
/run/user/1000/keyring/.ssh
root 8198 0.0 0.1 179096 8576 ? Sl 12:48 0:00
/usr/lib/NetworkManager/nm-openvpn-service --bus-name
org.freedesktop.NetworkManager.openvpn.Connection_4
nm-open+ 8210 1.3 0.1 13588 8160 ? S 12:48 0:26 _ /usr/sbin/openvpn --remote
190.2.132.198 80 udp --explicit-exit-notify --remote 190.2.132.198 51820 udp
--explicit-exit-notify --remote 190.2.132.198 4569 udp --explicit-exit-notify
--remote 190.2.132.198 1194 udp --explicit-exit-notify --remote 190.2.132.198 5060
udp --explicit-exit-notify --remote-random --comp-lzo no --connect-timeout 20
--nobind --dev proton0 --dev-type tun --cipher AES-256-CBC --auth SHA512
--auth-nocache --tls-auth
/home/prasad/.cert/nm-openvpn/ProtonVPN-wbsx05pj-tls-auth.pem 1 --verify-x509-name
node-nl-22.protonvpn.net name --remote-cert-tls server --reneg-sec 0 --verb 1
--syslog nm-openvpn --tun-mtu 1500 --mssfix 1450 --script-security 2 --up
/usr/lib/NetworkManager/nm-openvpn-service-openvpn-helper --debug 0 8198 --bus-name
org.freedesktop.NetworkManager.openvpn.Connection_4 --tun -- --up-restart
--persist-key --persist-tun --management
/var/run/NetworkManager/nm-openvpn-adacfc47-f908-4ac6-b2f0-7c10320b44a7 unix
--management-client-user root --management-client-group root
--management-query-passwords --auth-retry interact --route-noexec --ifconfig-noexec
--client --auth-user-pass --ca
/home/prasad/.cert/nm-openvpn/ProtonVPN-wbsx05pj-ca.pem --user nm-openvpn --group
nm-openvpn --chroot /var/lib/openvpn/chroot
root 28540 0.0 0.0 17988 2444 ? Ss 13:08 0:00 /sbin/mount.ntfs /dev/nvme0n1p4
/media/prasad/New Volume -o
rw,nodev,nosuid,uid=1000,gid=1000,windows_names,uhelper=udisks2
root 28656 0.1 0.0 18296 2624 ? Ss 13:08 0:01 /sbin/mount.ntfs /dev/nvme0n1p6
/media/prasad/New Volume1 -o
rw,nodev,nosuid,uid=1000,gid=1000,windows_names,uhelper=udisks2
```

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

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

```
Proc 546 with ppid 1 is run by user systemd-oom but the ppid user is root
Proc 547 with ppid 1 is run by user systemd-resolve but the ppid user is root
Proc 548 with ppid 1 is run by user systemd-timesync but the ppid user is root
Proc 628 with ppid 1 is run by user avahi but the ppid user is root
Proc 634 with ppid 1 is run by user messagebus but the ppid user is root
Proc 653 with ppid 1 is run by user syslog but the ppid user is root
Proc 923 with ppid 1 is run by user rtkit but the ppid user is root
Proc 1338 with ppid 1 is run by user colord but the ppid user is root
Proc 1429 with ppid 1 is run by user kernoops but the ppid user is root
Proc 1433 with ppid 1 is run by user kernoops but the ppid user is root
Proc 1790 with ppid 1 is run by user prasad but the ppid user is root
Proc 1813 with ppid 1 is run by user prasad but the ppid user is root
Proc 1884 with ppid 1778 is run by user prasad but the ppid user is root
Proc 8210 with ppid 8198 is run by user nm-openvpn but the ppid user is root
```

Processes with credentials in memory (root req)

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#credentials-from-process-memory

```
gdm-password process found (dump creds from memory as root)
gnome-keyring-daemon process found (dump creds from memory as root)
lightdm Not Found
vsftpd Not Found
apache2 Not Found
sshd Not Found
```

Cron jobs

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#scheduled-cron-jobs

```
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root 1136 Mar 23 2022 /etc/crontab
/etc/cron.d:
total 28
drwxr-xr-x 2 root root 4096 Jul 17 03:22 .
drwxr-xr-x 139 root root 12288 Jul 31 13:06 ..
-rw-r--r-- 1 root root 219 Oct 9 2021 anacron
-rw-r--r-- 1 root root 201 Jan 9 2022 e2scrub_all
-rw-r--r-- 1 root root 102 Mar 23 2022 .placeholder
/etc/cron.daily:
total 52
drwxr-xr-x 2 root root 4096 Jul 17 10:06 .
drwxr-xr-x 139 root root 12288 Jul 31 13:06 ..
-rwxr-xr-x 1 root root 311 Oct 9 2021 0anacron
-rwxr-xr-x 1 root root 376 Nov 12 2019 apport
-rwxr-xr-x 1 root root 1478 Apr 8 2022 apt-compat
-rwxr-xr-x 1 root root 314 Feb 14 2021 aptitude
-rwxr-xr-x 1 root root 384 Nov 19 2019 cracklib-runtime
-rwxr-xr-x 1 root root 123 Dec 6 2021 dpkg
lrwxrwxrwx 1 root root 37 Jun 24 07:53 google-chrome ->
/opt/google/chrome/cron/google-chrome
-rwxr-xr-x 1 root root 377 Jan 24 2022 logrotate
-rwxr-xr-x 1 root root 1330 Mar 18 2022 man-db
-rw-r--r-- 1 root root 102 Mar 23 2022 .placeholder
/etc/cron.hourly:
total 20
drwxr-xr-x 2 root root 4096 Feb 23 09:27 .
drwxr-xr-x 139 root root 12288 Jul 31 13:06 ..
-rw-r--r-- 1 root root 102 Mar 23 2022 .placeholder
/etc/cron.monthly:
total 24
drwxr-xr-x 2 root root 4096 Feb 23 09:29 .
drwxr-xr-x 139 root root 12288 Jul 31 13:06 ..
-rwxr-xr-x 1 root root 313 Oct 9 2021 0anacron
-rw-r--r-- 1 root root 102 Mar 23 2022 .placeholder
/etc/cron.weekly:
total 28
drwxr-xr-x 2 root root 4096 Feb 23 09:29 .
drwxr-xr-x 139 root root 12288 Jul 31 13:06 ..
-rwxr-xr-x 1 root root 312 Oct 9 2021 0anacron
-rwxr-xr-x 1 root root 1020 Mar 18 2022 man-db
-rw-r--r-- 1 root root 102 Mar 23 2022 .placeholder
/var/spool/anacron:
total 20
drwxr-xr-x 2 root root 4096 Jul 17 12:51 .
drwxr-xr-x 7 root root 4096 Feb 23 09:28 ..
-rw------- 1 root root 9 Jul 20 19:01 cron.daily
-rw------- 1 root root 9 Jul 17 14:00 cron.monthly
-rw------- 1 root root 9 Jul 17 13:55 cron.weekly
SHELL=/bin/sh
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 )
SHELL=/bin/sh
HOME=/root
LOGNAME=root
1 5 cron.daily run-parts --report /etc/cron.daily
7 10 cron.weekly run-parts --report /etc/cron.weekly
@monthly 15 cron.monthly run-parts --report /etc/cron.monthly
```

Analyzing .service files

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services

```
/etc/systemd/system/multi-user.target.wants/grub-common.service could be executing
some relative path
/etc/systemd/system/sleep.target.wants/grub-common.service could be executing some
relative path
You can't write on systemd PATH
```

System timers

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers

```
NEXT LEFT LAST PASSED UNIT ACTIVATES
Mon 2023-07-31 13:33:50 IST 11min left Mon 2023-07-31 12:48:17 IST 33min ago
anacron.timer anacron.service
Mon 2023-07-31 17:33:01 IST 4h 10min left Thu 2023-07-20 12:51:29 IST 1 week 4 days
ago man-db.timer man-db.service
Mon 2023-07-31 18:14:28 IST 4h 52min left Mon 2023-07-17 08:53:48 IST 2 weeks 0
days ago fwupd-refresh.timer fwupd-refresh.service
Mon 2023-07-31 20:08:09 IST 6h left Tue 2023-07-18 11:06:24 IST 1 week 6 days ago
apt-daily.timer apt-daily.service
Tue 2023-08-01 00:00:00 IST 10h left n/a n/a dpkg-db-backup.timer
dpkg-db-backup.service
Tue 2023-08-01 00:00:00 IST 10h left Mon 2023-07-31 01:17:31 IST 12h ago
logrotate.timer logrotate.service
Tue 2023-08-01 06:45:27 IST 17h left Mon 2023-07-31 13:20:28 IST 1min 42s ago
apt-daily-upgrade.timer apt-daily-upgrade.service
Tue 2023-08-01 09:42:04 IST 20h left Mon 2023-07-31 13:05:36 IST 16min ago
motd-news.timer motd-news.service
Tue 2023-08-01 12:27:03 IST 23h left Mon 2023-07-31 01:22:29 IST 11h ago
update-notifier-download.timer update-notifier-download.service
Tue 2023-08-01 12:37:03 IST 23h left Mon 2023-07-31 01:32:29 IST 11h ago
systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service
Tue 2023-08-01 22:08:15 IST 1 day 8h left Mon 2023-07-17 08:53:58 IST 2 weeks 0
days ago update-notifier-motd.timer update-notifier-motd.service
Sun 2023-08-06 03:10:31 IST 5 days left Sun 2023-07-30 23:55:11 IST 13h ago
e2scrub_all.timer e2scrub_all.service
Mon 2023-08-07 01:05:01 IST 6 days left Mon 2023-07-31 12:48:17 IST 33min ago
fstrim.timer fstrim.service
n/a n/a n/a n/a apport-autoreport.timer apport-autoreport.service
n/a n/a n/a n/a snapd.snap-repair.timer snapd.snap-repair.service
n/a n/a n/a n/a ua-timer.timer ua-timer.service
```

Analyzing .socket files

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets

```
/etc/systemd/system/sockets.target.wants/avahi-daemon.socket is calling this
writable listener: /run/avahi-daemon/socket
/etc/systemd/system/sockets.target.wants/uuidd.socket is calling this writable
listener: /run/uuidd/request
/snap/core20/1822/usr/lib/systemd/system/dbus.socket is calling this writable
listener: /var/run/dbus/system_bus_socket
```

```
/snap/core20/1822/usr/lib/systemd/system/sockets.target.wants/dbus.socket is
calling this writable listener: /var/run/dbus/system_bus_socket
/snap/core20/1822/usr/lib/systemd/system/sockets.target.wants/systemd-journald-dev
-log.socket is calling this writable listener: /run/systemd/journal/dev-log
/snap/core20/1822/usr/lib/systemd/system/sockets.target.wants/systemd-journald.soc
ket is calling this writable listener: /run/systemd/journal/stdout
/snap/core20/1822/usr/lib/systemd/system/sockets.target.wants/systemd-journald.soc
ket is calling this writable listener: /run/systemd/journal/socket
/snap/core20/1822/usr/lib/systemd/system/syslog.socket is calling this writable
listener: /run/systemd/journal/syslog
/snap/core20/1822/usr/lib/systemd/system/systemd-journald-dev-log.socket is calling
this writable listener: /run/systemd/journal/dev-log
/snap/core20/1822/usr/lib/systemd/system/systemd-journald.socket is calling this
writable listener: /run/systemd/journal/stdout
/snap/core20/1822/usr/lib/systemd/system/systemd-journald.socket is calling this
writable listener: /run/systemd/journal/socket
/snap/core20/1822/usr/lib/systemd/system/systemd-rfkill.socket is calling this
writable listener: /dev/rfkill
/snap/core20/1974/usr/lib/systemd/system/dbus.socket is calling this writable
listener: /var/run/dbus/system_bus_socket
/snap/core20/1974/usr/lib/systemd/system/sockets.target.wants/dbus.socket is
calling this writable listener: /var/run/dbus/system_bus_socket
/snap/core20/1974/usr/lib/systemd/system/sockets.target.wants/systemd-journald-dev
-log.socket is calling this writable listener: /run/systemd/journal/dev-log
/snap/core20/1974/usr/lib/systemd/system/sockets.target.wants/systemd-journald.soc
ket is calling this writable listener: /run/systemd/journal/stdout
/snap/core20/1974/usr/lib/systemd/system/sockets.target.wants/systemd-journald.soc
ket is calling this writable listener: /run/systemd/journal/socket
/snap/core20/1974/usr/lib/systemd/system/syslog.socket is calling this writable
listener: /run/systemd/journal/syslog
/snap/core20/1974/usr/lib/systemd/system/systemd-journald-dev-log.socket is calling
this writable listener: /run/systemd/journal/dev-log
/snap/core20/1974/usr/lib/systemd/system/systemd-journald.socket is calling this
writable listener: /run/systemd/journal/stdout
/snap/core20/1974/usr/lib/systemd/system/systemd-journald.socket is calling this
writable listener: /run/systemd/journal/socket
/snap/core20/1974/usr/lib/systemd/system/systemd-rfkill.socket is calling this
writable listener: /dev/rfkill
```

Unix Sockets Listening

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets

```
/home/prasad/.cache/ibus/dbus-V3mDtGqh
@/home/prasad/.cache/ibus/dbus-V3mDtGqh
/run/acpid.socket
(Read Write)
/run/avahi-daemon/socket
(Read Write)
/run/containerd/containerd.sock
/run/containerd/containerd.sock.ttrpc
/run/cups/cups.sock
(Read Write)
/run/dbus/system_bus_socket
(Read Write)
/run/docker.sock
/run/irqbalance/irqbalance641.sock
(Read )
/run/NetworkManager/nm-openvpn-adacfc47-f908-4ac6-b2f0-7c10320b44a7
(Read Write)
/run/snapd-snap.socket
(Read Write)
/run/snapd.socket
(Read Write)
/run/systemd/fsck.progress
/run/systemd/inaccessible/sock
/run/systemd/io.system.ManagedOOM
(Read Write)
/run/systemd/journal/dev-log
(Read Write)
/run/systemd/journal/io.systemd.journal
/run/systemd/journal/socket
(Read Write)
/run/systemd/journal/stdout
```

```
(Read Write)
/run/systemd/journal/syslog
(Read Write)
/run/systemd/notify
(Read Write)
/run/systemd/private
(Read Write)
/run/systemd/resolve/io.systemd.Resolve
(Read Write)
/run/systemd/userdb/io.systemd.DynamicUser
(Read Write)
/run/udev/control
/run/user/1000/at-spi/bus
(Read Write)
/run/user/1000/bus
(Read Write)
/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/gvfsd/socket-bqmeJmwn
/run/user/1000/gvfsd/socket-c0IX6IhD
/run/user/1000/gvfsd/socket-FYzuSIUO
/run/user/1000/gvfsd/socket-g82Nl5mJ
/run/user/1000/gvfsd/socket-leB5g6TH
/run/user/1000/gvfsd/socket-MSY9BxOG
/run/user/1000/gvfsd/socket-osbiSzpx
/run/user/1000/gvfsd/socket-sK3tlAMV
/run/user/1000/gvfsd/socket-wlJ5I71k
/run/user/1000/gvfsd/socket-Y3xtDji3
/run/user/1000/gvfsd/socket-ZdKhUGst
/run/user/1000/keyring/control
(Read Write)
/run/user/1000/keyring/pkcs11
(Read Write)
/run/user/1000/keyring/.ssh
(Read Write)
/run/user/1000/keyring/ssh
(Read Write)
/run/user/1000/pipewire-0
(Read Write)
/run/user/1000/pk-debconf-socket
(Read Write)
/run/user/1000/pulse/native
(Read Write)
/run/user/1000/snapd-session-agent.socket
(Read Write)
/run/user/1000/speech-dispatcher/speechd.sock
(Read Write)
/run/user/1000/systemd/inaccessible/sock
/run/user/1000/systemd/notify
(Read Write)
/run/user/1000/systemd/private
(Read Write)
/run/user/1000/vscode-128722b6-1.80-main.sock
(Read Write)
/run/user/1000/vscode-git-e27bcaa9d1.sock
(Read Write)
/run/user/1000/wayland-0
(Read Write)
/run/uuidd/request
(Read Write)
/tmp/.com.google.Chrome.9SUn3m/SingletonSocket
(Read Write)
/tmp/dbus-lI7dSTMN
/tmp/dbus-PTJ6Iw2O
/tmp/.ICE-unix/1959
(Read Write)
@/tmp/.ICE-unix/1959
/tmp/.ICE-unix/938
(Read Write)
/tmp/.X11-unix/X0
```

```
(Read Write)
@/tmp/.X11-unix/X0
/tmp/.X11-unix/X1
(Read Write)
@/tmp/.X11-unix/X1
/tmp/.X11-unix/X1024
(Read )
/tmp/.X11-unix/X1025
(Read )
/var/run/docker/libnetwork/a1649895c337.sock
/var/run/docker/metrics.sock
/var/run/NetworkManager/nm-openvpn-adacfc47-f908-4ac6-b2f0-7c10320b44a7
(Read Write)
```

D-Bus config files

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus

```
Possible weak user policy found on /etc/dbus-1/system.d/avahi-dbus.conf ( <policy
user="avahi">)
Possible weak user policy found on /etc/dbus-1/system.d/avahi-dbus.conf ( <policy
group="netdev">)
Possible weak user policy found on /etc/dbus-1/system.d/bluetooth.conf ( <policy
group="bluetooth">)
Possible weak user policy found on /etc/dbus-1/system.d/dnsmasq.conf ( <policy
user="dnsmasq">)
Possible weak user policy found on /etc/dbus-1/system.d/gdm.conf ( <policy
user="gdm">)
Possible weak user policy found on /etc/dbus-1/system.d/kerneloops.conf ( <policy
user="kernoops">)
Possible weak user policy found on /etc/dbus-1/system.d/net.hadess.SensorProxy.conf
( <policy user="geoclue">)
Possible weak user policy found on
/etc/dbus-1/system.d/org.freedesktop.GeoClue2.Agent.conf ( <policy user="geoclue">)
Possible weak user policy found on
/etc/dbus-1/system.d/org.freedesktop.GeoClue2.conf ( <policy user="geoclue">)
Possible weak user policy found on
/etc/dbus-1/system.d/org.freedesktop.thermald.conf ( <policy group="power">)
Possible weak user policy found on
/etc/dbus-1/system.d/org.opensuse.CupsPkHelper.Mechanism.conf ( <policy
user="cups-pk-helper">)
Possible weak user policy found on /etc/dbus-1/system.d/pulseaudio-system.conf (
<policy user="pulse">)
Possible weak user policy found on /etc/dbus-1/system.d/wpa_supplicant.conf (
<policy group="netdev">)
```

D-Bus Service Objects list

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus

```
NAME PID PROCESS USER CONNECTION UNIT SESSION DESCRIPTION
:1.0 548 systemd-timesyn systemd-timesync :1.0 systemd-timesyncd.service - -
:1.1 546 systemd-oomd systemd-oom :1.1 systemd-oomd.service - -
:1.10 635 NetworkManager root :1.10 NetworkManager.service - -
:1.100 2125 gsd-rfkill prasad :1.100 user@1000.service - -
:1.101 2124 gsd-print-notif prasad :1.101 user@1000.service - -
:1.102 2311 gsd-printer prasad :1.102 user@1000.service - -
:1.103 2109 gsd-color prasad :1.103 user@1000.service - -
:1.104 2119 gsd-media-keys prasad :1.104 user@1000.service - -
:1.105 2116 gsd-keyboard prasad :1.105 user@1000.service - -
:1.106 2122 gsd-power prasad :1.106 user@1000.service - -
:1.109 2370 xdg-desktop-por prasad :1.109 user@1000.service - -
:1.110 2364 xdg-desktop-por prasad :1.110 user@1000.service - -
:1.111 2430 xdg-desktop-por prasad :1.111 user@1000.service - -
:1.112 2409 gjs prasad :1.112 user@1000.service - -
:1.12 648 power-profiles- root :1.12 power-profiles-daemon.service - -
:1.120 6079 gnome-calendar prasad :1.120 user@1000.service - -
:1.122 6083 seahorse prasad :1.122 user@1000.service - -
:1.124 6577 gsd-xsettings prasad :1.124 user@1000.service - -
:1.127 8198 nm-openvpn-serv root :1.127 NetworkManager.service - -
```

```
:1.13 670 switcheroo-cont root :1.13 switcheroo-control.service - -
:1.130 8768 chrome prasad :1.130 user@1000.service - -
:1.131 8768 chrome prasad :1.131 user@1000.service - -
:1.132 8768 chrome prasad :1.132 user@1000.service - -
:1.138 13530 nautilus prasad :1.138 user@1000.service - -
:1.14 739 cupsd root :1.14 cups.service - -
:1.142 18171 gvfsd-dnssd prasad :1.142 user@1000.service - -
:1.146 27319 code prasad :1.146 user@1000.service - -
:1.148 27319 code prasad :1.148 user@1000.service - -
:1.15 719 ModemManager root :1.15 ModemManager.service - -
:1.16 796 gdm3 root :1.16 gdm.service - -
:1.166 92460 busctl prasad :1.166 user@1000.service - -
:1.17 630 bluetoothd root :1.17 bluetooth.service - -
:1.19 674 systemd-logind root :1.19 systemd-logind.service - -
:1.2 547 systemd-resolve systemd-resolve :1.2 systemd-resolved.service - -
:1.23 820 unattended-upgr root :1.23 unattended-upgrades.service - -
:1.25 644 networkd-dispat root :1.25 networkd-dispatcher.service - -
:1.3 645 polkitd root :1.3 polkit.service - -
:1.31 923 rtkit-daemon root :1.31 rtkit-daemon.service - -
:1.4 625 accounts-daemon root :1.4 accounts-daemon.service - -
:1.40 1069 upowerd root :1.40 upower.service - -
:1.41 668 snapd root :1.41 snapd.service - -
:1.44 1183 packagekitd root :1.44 packagekit.service - -
:1.5 1 systemd root :1.5 init.scope - -
:1.57 1338 colord colord :1.57 colord.service - -
:1.6 628 avahi-daemon avahi :1.6 avahi-daemon.service - -
:1.63 1429 kerneloops kernoops :1.63 kerneloops.service - -
:1.64 1433 kerneloops kernoops :1.64 kerneloops.service - -
:1.67 1425 cups-browsed root :1.67 cups-browsed.service - -
:1.68 1425 cups-browsed root :1.68 cups-browsed.service - -
:1.7 681 udisksd root :1.7 udisks2.service - -
:1.72 1778 gdm-session-wor root :1.72 session-2.scope 2 -
:1.76 1790 systemd prasad :1.76 user@1000.service - -
:1.77 1798 pipewire-media- prasad :1.77 user@1000.service - -
:1.78 1797 pipewire prasad :1.78 user@1000.service - -
:1.79 1813 gnome-keyring-d prasad :1.79 session-2.scope 2 -
:1.8 685 wpa_supplicant root :1.8 wpa_supplicant.service - -
:1.81 1799 pulseaudio prasad :1.81 user@1000.service - -
:1.83 1883 gvfs-udisks2-vo prasad :1.83 user@1000.service - -
:1.84 1884 gdm-wayland-ses prasad :1.84 session-2.scope 2 -
:1.85 1925 goa-daemon prasad :1.85 user@1000.service - -
:1.87 1868 tracker-miner-f prasad :1.87 user@1000.service - -
:1.88 1959 gnome-session-b prasad :1.88 user@1000.service - -
:1.90 1990 gnome-shell prasad :1.90 user@1000.service - -
:1.91 2043 evolution-calen prasad :1.91 user@1000.service - -
:1.92 2058 evolution-addre prasad :1.92 user@1000.service - -
:1.95 2133 gsd-disk-utilit prasad :1.95 user@1000.service - -
:1.96 2130 gsd-sharing prasad :1.96 user@1000.service - -
com.canonical.UbuntuAdvantage - - - (activatable) - - -
com.hp.hplip - - - (activatable) - - -
com.redhat.NewPrinterNotification 2311 gsd-printer prasad :1.102 user@1000.service
- -
com.redhat.PrinterDriversInstaller 2311 gsd-printer prasad :1.102 user@1000.service
- -
com.ubuntu.LanguageSelector - - - (activatable) - - -
com.ubuntu.SoftwareProperties - - - (activatable) - - -
com.ubuntu.USBCreator - - - (activatable) - - -
com.ubuntu.WhoopsiePreferences - - - (activatable) - - -
fi.w1.wpa_supplicant1 685 wpa_supplicant root :1.8 wpa_supplicant.service - -
io.netplan.Netplan - - - (activatable) - - -
net.hadess.PowerProfiles 648 power-profiles- root :1.12
power-profiles-daemon.service - -
-- UID=0 EUID=0
net.hadess.SwitcherooControl 670 switcheroo-cont root :1.13
switcheroo-control.service - -
net.reactivated.Fprint - - - (activatable) - - -
org.bluez 630 bluetoothd root :1.17 bluetooth.service - -
org.debian.apt - - - (activatable) - - -
org.freedesktop.Accounts 625 accounts-daemon root :1.4 accounts-daemon.service - -
org.freedesktop.Avahi 628 avahi-daemon avahi :1.6 avahi-daemon.service - -
org.freedesktop.ColorManager 1338 colord colord :1.57 colord.service - -
org.freedesktop.DBus 1 systemd root - init.scope - -
org.freedesktop.GeoClue2 - - - (activatable) - - -
org.freedesktop.ModemManager1 719 ModemManager root :1.15 ModemManager.service - -
org.freedesktop.NetworkManager 635 NetworkManager root :1.10 NetworkManager.service
- -
org.freedesktop.NetworkManager.openvpn.Connection_4 8198 nm-openvpn-serv root
:1.127 NetworkManager.service - -
```

```
org.freedesktop.PackageKit 1183 packagekitd root :1.44 packagekit.service - -
org.freedesktop.PolicyKit1 645 polkitd root :1.3 polkit.service - -
org.freedesktop.RealtimeKit1 923 rtkit-daemon root :1.31 rtkit-daemon.service - -
org.freedesktop.UDisks2 681 udisksd root :1.7 udisks2.service - -
org.freedesktop.UPower 1069 upowerd root :1.40 upower.service - -
org.freedesktop.bolt - - - (activatable) - - -
org.freedesktop.fwupd - - - (activatable) - - -
org.freedesktop.hostname1 - - - (activatable) - - -
org.freedesktop.locale1 - - - (activatable) - - -
org.freedesktop.login1 674 systemd-logind root :1.19 systemd-logind.service - -
org.freedesktop.network1 - - - (activatable) - - -
org.freedesktop.nm_dispatcher - - - (activatable) - - -
org.freedesktop.nm_priv_helper - - - (activatable) - - -
org.freedesktop.oom1 546 systemd-oomd systemd-oom :1.1 systemd-oomd.service - -
-- UID=108 EUID=108
org.freedesktop.resolve1 547 systemd-resolve systemd-resolve :1.2
systemd-resolved.service - -
org.freedesktop.systemd1 1 systemd root :1.5 init.scope - -
org.freedesktop.thermald - - - (activatable) - - -
org.freedesktop.timedate1 - - - (activatable) - - -
org.freedesktop.timesync1 548 systemd-timesyn systemd-timesync :1.0
systemd-timesyncd.service - -
org.gnome.DisplayManager 796 gdm3 root :1.16 gdm.service - -
org.opensuse.CupsPkHelper.Mechanism - - - (activatable) - - -
```

Network Information

Hostname, hosts and DNS

```
prasad-Aspire-A315-23
127.0.0.1 localhost
127.0.1.1 prasad-Aspire-A315-23
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1 kubernetes.docker.internal
nameserver 127.0.0.53
```

Interfaces

```
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN
group default qlen 1000
link/ether b4:a9:fc:e4:d5:4d brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
default qlen 1000
link/ether 94:08:53:6f:eb:3b brd ff:ff:ff:ff:ff:ff
inet 192.168.43.132/24 brd 192.168.43.255 scope global dynamic noprefixroute wlp2s0
valid_lft 3211sec preferred_lft 3211sec
inet6 2409:408d:e81:2c81:361c:2d6f:4102:a21b/64 scope global temporary dynamic
valid_lft 2884sec preferred_lft 2884sec
inet6 2409:408d:e81:2c81:697e:4f99:a8a1:894/64 scope global dynamic mngtmpaddr
noprefixroute
valid_lft 2884sec preferred_lft 2884sec
inet6 fe80::d2e5:b3f8:91ba:a3fc/64 scope link noprefixroute
```

```
valid_lft forever preferred_lft forever
4: ipv6leakintrf0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state
UNKNOWN group default qlen 1000
link/ether fa:b5:30:db:03:8e brd ff:ff:ff:ff:ff:ff
inet6 fdeb:446c:912d:8da::/64 scope global noprefixroute
valid_lft forever preferred_lft forever
inet6 fe80::d58d:9cb4:ceff:4d7a/64 scope link noprefixroute
valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
group default
link/ether 02:42:3e:83:0c:96 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
6: proton0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UNKNOWN group default qlen 500
link/none
inet 10.18.0.18/16 brd 10.18.255.255 scope global noprefixroute proton0
valid_lft forever preferred_lft forever
inet6 fe80::72ca:7b14:e22b:8006/64 scope link stable-privacy
valid_lft forever preferred_lft forever
```

Active Ports

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports

```
tcp LISTEN 0 128 127.0.0.1:631 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:*
tcp LISTEN 0 128 [::1]:631 [::]:*
```

Can I sniff with tcpdump?

```
No
```

Users Information

Do I have PGP keys?

```
/usr/bin/gpg
/home/prasad/.gnupg/pubring.kbx
------------------------------
pub ed25519 2018-11-30 [SC]
248097092B458509C508DAC0350585C4E9518F26
uid [ unknown] proton@srp.modulus
sub cv25519 2018-11-30 [E]
netpgpkeys Not Found
netpgp Not Found
```

Clipboard or highlighted text?

```
Clipboard: /linpeas.sh > -s output.txt
Highlighted text: /linpeas.sh > -s output.txt
```

Checking Pkexec policy

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2

```
[Configuration]
AdminIdentities=unix-user:0
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:admin
```

Users with console

```
prasad:x:1000:1000:Prasad Senapathy,,,:/home/prasad:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

All users & groups

```
uid=0(root) gid=0(root) groups=0(root)
uid=1000(prasad) gid=1000(prasad) groups=1000(prasad),4(adm),24(cdrom),27(sudo),30
(dip),46(plugdev),122(lpadmin),135(lxd),136(sambashare)
uid=100(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(messagebus) gid=105(messagebus) groups=105(messagebus)
uid=103(systemd-timesync) gid=106(systemd-timesync) groups=106(systemd-timesync)
uid=104(syslog) gid=111(syslog) groups=111(syslog),4(adm)
uid=105(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=106(tss) gid=112(tss) groups=112(tss)
uid=107(uuidd) gid=115(uuidd) groups=115(uuidd)
uid=108(systemd-oom) gid=116(systemd-oom) groups=116(systemd-oom)
uid=109(tcpdump) gid=117(tcpdump) groups=117(tcpdump)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=110(avahi-autoipd) gid=119(avahi-autoipd) groups=119(avahi-autoipd)
uid=111(usbmux) gid=46(plugdev) groups=46(plugdev)
uid=112(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=113(kernoops) gid=65534(nogroup) groups=65534(nogroup)
uid=114(avahi) gid=121(avahi) groups=121(avahi)
uid=115(cups-pk-helper) gid=122(lpadmin) groups=122(lpadmin)
uid=116(rtkit) gid=123(rtkit) groups=123(rtkit)
uid=117(whoopsie) gid=124(whoopsie) groups=124(whoopsie)
uid=118(sssd) gid=125(sssd) groups=125(sssd)
uid=119(speech-dispatcher) gid=29(audio) groups=29(audio)
uid=120(fwupd-refresh) gid=126(fwupd-refresh) groups=126(fwupd-refresh)
uid=121(nm-openvpn) gid=127(nm-openvpn) groups=127(nm-openvpn)
uid=122(saned) gid=129(saned) groups=129(saned),128(scanner)
uid=123(colord) gid=130(colord) groups=130(colord)
uid=124(geoclue) gid=131(geoclue) groups=131(geoclue)
uid=125(pulse) gid=132(pulse) groups=132(pulse),29(audio)
uid=126(gnome-initial-setup) gid=65534(nogroup) groups=65534(nogroup)
uid=127(hplip) gid=7(lp) groups=7(lp)
uid=128(gdm) gid=134(gdm) groups=134(gdm)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
```

Login now

```
13:22:18 up 17:34, 1 user, load average: 2.13, 1.99, 1.61
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
prasad tty2 tty2 18:12 12:04m 0.05s 0.04s /usr/libexec/gnome-session-binary
--session=ubuntu
```

Last logons

```
prasad tty2 Mon Jul 17 09:16:11 2023 - down (00:24) 0.0.0.0
reboot system boot Mon Jul 17 09:15:58 2023 - Mon Jul 17 09:40:18 2023 (00:24)
0.0.0.0
prasad tty2 Mon Jul 17 12:51:48 2023 - down (-5:24) 0.0.0.0
reboot system boot Mon Jul 17 12:51:36 2023 - Mon Jul 17 07:26:56 2023 (-5:24)
0.0.0.0
prasad tty2 Sun Jul 16 22:03:46 2023 - down (00:15) 0.0.0.0
reboot system boot Sun Jul 16 22:03:32 2023 - Sun Jul 16 22:18:54 2023 (00:15)
0.0.0.0
prasad tty2 Mon Jul 17 08:54:23 2023 - down (-10:53) 0.0.0.0
reboot system boot Mon Jul 17 08:53:33 2023 - Sun Jul 16 22:01:09 2023 (-10:52)
0.0.0.0
wtmp begins Mon Jul 17 08:53:33 2023
```

Last time logon each user

```
Username Port From Latest
prasad Mon Jul 17 15:51:12 +0530 2023
```

Software Information

Useful software

```
/usr/bin/base64
/usr/bin/ctr
/usr/bin/curl
/usr/local/bin/docker
/usr/bin/gdb
/usr/bin/nc
/usr/bin/netcat
/usr/bin/perl
/usr/bin/ping
/usr/bin/python3
/usr/bin/runc
/usr/bin/sudo
/usr/bin/wget
```

Analyzing Rsync Files (limit 70)

```
-rw-r--r-- 1 root root 1044 Oct 12 2022 /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 Jul 31 2023 /etc/NetworkManager/system-connections
drwxr-xr-x 2 root root 4096 Jul 31 2023 /etc/NetworkManager/system-connections
-rw------- 1 root root 280 Jul 31 2023 /etc/NetworkManager/system-connections/redmi
9A.nmconnection
-rw------- 1 root root 251 Jul 20 13:16
/etc/NetworkManager/system-connections/JioNet@SriKrishnaCollege.nmconnection
-rw------- 1 root root 312 Jul 17 08:59
/etc/NetworkManager/system-connections/OnePlus Nord CE 2 Lite.nmconnection
-rw------- 1 root root 302 Jul 20 11:48
/etc/NetworkManager/system-connections/OnePlus Nord 2T 5G.nmconnection
-rw------- 1 root root 337 Jul 17 17:03
/etc/NetworkManager/system-connections/pvpn-ipv6leak-protection.nmconnection
-rw------- 1 root root 351 Jul 20 13:15
/etc/NetworkManager/system-connections/.nmconnection
-rw------- 1 root root 821 Jul 17 17:03
/etc/NetworkManager/system-connections/Proton VPN NL-FREE#103004.nmconnection
-rw------- 1 root root 285 Jul 17 14:54
/etc/NetworkManager/system-connections/SKCET_WiFi.nmconnection
-rw------- 1 root root 287 Jul 17 16:29
/etc/NetworkManager/system-connections/Xiaomi 11i.nmconnection
```

Analyzing Ldap Files (limit 70)

```
The password hash is from the {SSHA} to 'structural'
drwxr-xr-x 2 root root 4096 Jul 17 10:05 /etc/ldap
drwxr-xr-x 2 root root 32 Oct 19 2022 /snap/snap-store/638/etc/ldap
drwxr-xr-x 2 root root 32 May 29 17:46 /snap/whatsapp-for-linux/57/etc/ldap
```

Searching ssl/ssh files

Some certificates were found (out limited):

```
/etc/pki/fwupd/LVFS-CA.pem
/etc/pki/fwupd-metadata/LVFS-CA.pem
/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/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068_2.pem
/etc/ssl/certs/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.pem
```

```
/etc/ssl/certs/Baltimore_CyberTrust_Root.pem
/etc/ssl/certs/Buypass_Class_2_Root_CA.pem
81609PSTORAGE_CERTSBIN
```

Writable ssh and gpg agents

```
/etc/systemd/user/sockets.target.wants/gpg-agent-extra.socket
/etc/systemd/user/sockets.target.wants/gpg-agent-ssh.socket
/etc/systemd/user/sockets.target.wants/gpg-agent.socket
/etc/systemd/user/sockets.target.wants/gpg-agent-browser.socket
```

/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_*
HashKnownHosts yes
GSSAPIAuthentication yes
```

Analyzing FreeIPA Files (limit 70)

```
drwxr-xr-x 2 root root 4096 Feb 23 09:28
/usr/src/linux-hwe-5.19-headers-5.19.0-32/drivers/net/ipa
drwxr-xr-x 2 root root 4096 Jul 17 10:05
/usr/src/linux-hwe-5.19-headers-5.19.0-46/drivers/net/ipa
```

Analyzing Cloud Init Files (limit 70)

```
-rw-r--r-- 1 root root 3786 Dec 8 2022 /snap/core20/1822/etc/cloud/cloud.cfg
lock_passwd: True
-rw-r--r-- 1 root root 3787 May 19 23:27 /snap/core20/1974/etc/cloud/cloud.cfg
lock_passwd: True
-rw-r--r-- 1 root root 3787 Apr 21 07:07 /snap/core22/817/etc/cloud/cloud.cfg
lock_passwd: True
```

Analyzing Keyring Files (limit 70)

```
drwxr-xr-x 2 root root 4096 Jul 20 15:29 /etc/apt/keyrings
drwx------ 2 prasad prasad 4096 Jul 31 13:07 /home/prasad/.local/share/keyrings
drwxr-xr-x 2 root root 200 Jan 26 2023 /snap/core20/1822/usr/share/keyrings
drwxr-xr-x 2 root root 200 Jun 22 18:16 /snap/core20/1974/usr/share/keyrings
drwxr-xr-x 2 root root 200 Jul 3 19:16 /snap/core22/817/usr/share/keyrings
drwxr-xr-x 2 root root 4096 Jul 18 10:40 /usr/share/keyrings
-rw------- 1 prasad prasad 3518 Jul 31 13:07
/home/prasad/.local/share/keyrings/login.keyring
-rw------- 1 prasad prasad 207 Jul 17 08:54
/home/prasad/.local/share/keyrings/user.keystore
```

Searching uncommon passwd files (splunk)

```
passwd file: /etc/pam.d/passwd
passwd file: /etc/passwd
passwd file: /snap/core20/1822/etc/pam.d/passwd
passwd file: /snap/core20/1822/etc/passwd
passwd file: /snap/core20/1822/usr/share/bash-completion/completions/passwd
passwd file: /snap/core20/1822/usr/share/lintian/overrides/passwd
passwd file: /snap/core20/1822/var/lib/extrausers/passwd
passwd file: /snap/core20/1974/etc/pam.d/passwd
passwd file: /snap/core20/1974/etc/passwd
passwd file: /snap/core20/1974/usr/share/bash-completion/completions/passwd
passwd file: /snap/core20/1974/usr/share/lintian/overrides/passwd
passwd file: /snap/core20/1974/var/lib/extrausers/passwd
passwd file: /snap/core22/817/etc/pam.d/passwd
passwd file: /snap/core22/817/etc/passwd
passwd file: /snap/core22/817/usr/share/bash-completion/completions/passwd
passwd file: /snap/core22/817/usr/share/lintian/overrides/passwd
passwd file: /snap/core22/817/var/lib/extrausers/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /usr/share/lintian/overrides/passwd
```

Analyzing Github Files (limit 70)

```
drwxrwxrwx 1 prasad prasad 4096 Jul 12 19:50 /media/prasad/New Volume1/kavach/.git
drwxrwxrwx 1 prasad prasad 4096 Jul 12 19:51 /media/prasad/New
Volume1/kavach/hoobank-landingpage/.git
```

Analyzing PGP-GPG Files (limit 70)

```
/usr/bin/gpg
/home/prasad/.gnupg/pubring.kbx
------------------------------
pub ed25519 2018-11-30 [SC]
248097092B458509C508DAC0350585C4E9518F26
uid [ unknown] proton@srp.modulus
sub cv25519 2018-11-30 [E]
netpgpkeys Not Found
netpgp Not Found
-rw-r--r-- 1 root root 2760 Jul 17 15:46 /etc/apt/keyrings/docker.gpg
-rw-r--r-- 1 root root 641 Jul 20 15:29 /etc/apt/keyrings/packages.microsoft.gpg
-rw-r--r-- 1 root root 9444 Jul 20 19:01 /etc/apt/trusted.gpg.d/google-chrome.gpg
-rw-r--r-- 1 root root 2794 Mar 27 2021
/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg
-rw-r--r-- 1 root root 1733 Mar 27 2021
/etc/apt/trusted.gpg.d/ubuntu-keyring-2018-archive.gpg
-rw------- 1 prasad prasad 1200 Jul 16 22:18 /home/prasad/.gnupg/trustdb.gpg
-rw-r--r-- 1 root root 7399 Sep 18 2018
/snap/core20/1822/usr/share/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 6713 Oct 27 2016
/snap/core20/1822/usr/share/keyrings/ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 4097 Feb 6 2018
/snap/core20/1822/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg
-rw-r--r-- 1 root root 0 Jan 17 2018
/snap/core20/1822/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg
-rw-r--r-- 1 root root 1227 May 27 2010
/snap/core20/1822/usr/share/keyrings/ubuntu-master-keyring.gpg
-rw-r--r-- 1 root root 7399 Sep 18 2018
/snap/core20/1974/usr/share/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 6713 Oct 27 2016
/snap/core20/1974/usr/share/keyrings/ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 4097 Feb 6 2018
/snap/core20/1974/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg
-rw-r--r-- 1 root root 0 Jan 17 2018
/snap/core20/1974/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg
-rw-r--r-- 1 root root 1227 May 27 2010
/snap/core20/1974/usr/share/keyrings/ubuntu-master-keyring.gpg
-rw-r--r-- 1 root root 7399 Sep 18 2018
/snap/core22/817/usr/share/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 6713 Oct 27 2016
/snap/core22/817/usr/share/keyrings/ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 3023 Mar 27 2021
```

```
/snap/core22/817/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg
-rw-r--r-- 1 root root 0 Jan 17 2018
/snap/core22/817/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg
-rw-r--r-- 1 root root 1227 May 27 2010
/snap/core22/817/usr/share/keyrings/ubuntu-master-keyring.gpg
-rw-r--r-- 1 root root 3267 Jul 4 2022
/snap/snap-store/638/usr/share/gnupg/distsigkey.gpg
-rw-r--r-- 1 root root 2899 Jul 4 2022
/snap/snap-store/959/usr/share/gnupg/distsigkey.gpg
-rw-r--r-- 1 root root 2899 Jul 4 2022 /usr/share/gnupg/distsigkey.gpg
-rw-r--r-- 1 root root 1765 Apr 24 17:30
/usr/share/keyrings/protonvpn-stable-archive-keyring.gpg
-rw-r--r-- 1 root root 2247 May 31 00:12
/usr/share/keyrings/ubuntu-advantage-cc-eal.gpg
-rw-r--r-- 1 root root 2274 May 31 00:12
/usr/share/keyrings/ubuntu-advantage-cis.gpg
-rw-r--r-- 1 root root 2236 May 31 00:12
/usr/share/keyrings/ubuntu-advantage-esm-apps.gpg
-rw-r--r-- 1 root root 2264 May 31 00:12
/usr/share/keyrings/ubuntu-advantage-esm-infra-trusty.gpg
-rw-r--r-- 1 root root 2275 May 31 00:12
/usr/share/keyrings/ubuntu-advantage-fips.gpg
-rw-r--r-- 1 root root 2250 May 31 00:12
/usr/share/keyrings/ubuntu-advantage-realtime-kernel.gpg
-rw-r--r-- 1 root root 2235 May 31 00:12
/usr/share/keyrings/ubuntu-advantage-ros.gpg
-rw-r--r-- 1 root root 7399 Sep 18 2018
/usr/share/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 6713 Oct 27 2016
/usr/share/keyrings/ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 3023 Mar 27 2021
/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg
-rw-r--r-- 1 root root 0 Jan 17 2018
/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg
-rw-r--r-- 1 root root 1227 May 27 2010
/usr/share/keyrings/ubuntu-master-keyring.gpg
-rw-r--r-- 1 root root 2236 Jul 16 22:16 /var/lib/ubuntu-advantage/apt-esm/etc/apt
/trusted.gpg.d/ubuntu-advantage-esm-apps.gpg
drwx------ 3 prasad prasad 4096 Jul 31 13:22 /home/prasad/.gnupg
```

Checking if containerd(ctr) is available

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/containerd-ctr-privilege-escalation

```
ctr was found in /usr/bin/ctr, you may be able to escalate privileges with it
ctr: failed to dial "/run/containerd/containerd.sock": connection error: desc =
"transport: error while dialing: dial unix /run/containerd/containerd.sock:
connect: permission denied"
```

Searching docker files (limit 70)

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation

```
lrwxrwxrwx 1 root root 33 Jul 17 10:34
/etc/systemd/system/sockets.target.wants/docker.socket ->
/lib/systemd/system/docker.socket
total 4
drwxr-xr-x 3 prasad prasad 4096 Jul 31 13:14 contexts
-rw-rw-r-- 1 prasad prasad 11607 Jul 17 15:42 /home/prasad/docker-compose.yml
-rw-r--r-- 1 root root 295 Jul 7 20:20 /usr/lib/systemd/system/docker.socket
-rw-r--r-- 1 root root 0 Jul 17 10:34
/var/lib/systemd/deb-systemd-helper-enabled/sockets.target.wants/docker.socket
```

Analyzing Kubernetes Files (limit 70)

```
drwxr-xr-x 2 prasad prasad 4096 Jul 20 16:06 /home/prasad/.kube
-rw------- 1 prasad prasad 5692 Jul 20 16:06 /home/prasad/.kube/config
apiVersion: v1
clusters:
- cluster:
certificate-authority-data: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMvakNDQWVhZ0
F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VRWURWUVFERXdwcmRXSmwKY201bGRHVnpN
QjRYRFRJek1EY3lNREV3TXpZeU9Wb1hEVE16TURjeE56RXdNell5T1Zvd0ZURVRNQkVHQTFVRQpBeE1LYT
NWaVpYSnVaWFJsY3pDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBS2x5CmQv
UGprS2VDTXBGWEJxV0VNZ24yRm9ramhhd0E3WU9PYXFTL0kwN3JDL1l3NFVVMnVia2c1V2VLOHJEcGhZVn
YKQnkvbTcwNG9pcVNxTlQzdi84YnhyM1NRQ3JxdExuRUV2djVqWGJiMktxUlI3UnJydjFxVUc4VFA5Y3cy
aTlUSgo4cUI2N0dtR2VjcUZiaktKcmdtUnlFRVZ0a0VmaXJKa2c1K1pNejQyNzkyQnFkUy93UnVHY0J4Ml
ltV0JGYVNICjVlUUZ6YWxJQ1V1ZTI3MVdZU01JMzlnK1RjZWxCMmZDREJ0Y2NxalRmMVBJWVE5MWgxQ3Ji
ak4vaUNzZjVhcEwKVk9BSUwyTDd0Unh0NExxQlpXcEZzWGo1emhwOStxdytJT2xudVVSWW1ZSmJta20yYm
gyc21xQm9CRDZtSlNrVwpjblEzbTlBUFJMdTJmTjEwK0VNQ0F3RUFBYU5aTUZjd0RnWURWUjBQQVFIL0JB
UURBZ0trTUE4R0ExVWRFd0VCCi93UUZNQU1CQWY4d0hRWURWUjBPQkJZRUZFdjI1VW9OdjBNa2laVVJuQ0
1kbkhCaFpJdW9NQlVHQTFVZEVRUU8KTUF5Q0NtdDFZbVZ5Ym1WMFpYTXdEUVlKS29aSWh2Y05BUUVMQlFB
RGdnRUJBRU1VSUE4bGZaTzlOYVVUVkI4VworQXU5c0tWdVJmM290akViZmJsVE9CRUwwaDRtenZGMUh3OU
NRcE1nVjQ5eTR1Z2ZuRWZRZDFKMlFCYWt4cVhLCmo5SWpvM3NTSm93dlJ2d1k1UVg0ME1IRGZnakc4R3Na
Tm10eVU1dWozNVN0cWJDZkg1cGtEWThXeitzbmtVSWgKYUg3alRkd0xrdmpTMzZ1WHJ5Qk81TkcxeTBZOW
4wLysxNHY4S3VvbzVGcTMwWHhVaXZ1ejRKNjV1bHBBMVRKZwp5bnlTbHZDREJOQmRWNDRhVEljQ0lZUzJx
aWJYUzJMY0lIOVNwZ0VuMkRwUlczNWFIMlFwS0Y0RFRGcHYrUVhUCjR0MVdTekNhWUVWaWgwa0JSaFdnOU
F2ODdnRVFFcHFFSC90ck9iejBFN3Yvb0VUd1dqYVFVSFI4SWgzRjRScVQKSnNvPQotLS0tLUVORCBDRVJU
SUZJQ0FURS0tLS0tCg==
server: https://kubernetes.docker.internal:6443
name: docker-desktop
contexts:
- context:
cluster: docker-desktop
user: docker-desktop
name: docker-desktop
current-context: docker-desktop
kind: Config
preferences: {}
users:
- name: docker-desktop
user:
client-certificate-data: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURRakNDQWlxZ0F3S
UJBZ0lJRElFUFZjKzBPakF3RFFZSktvWklodmNOQVFFTEJRQXdGVEVUTUJFR0ExVUUKQXhNS2EzVmlaWEp
1WlhSbGN6QWVGdzB5TXpBM01qQXhNRE0yTWpsYUZ3MHlOREEzTVRreE1ETTJNekZhTURZeApGekFWQmdOV
kJBb1REbk41YzNSbGJUcHRZWE4wWlhKek1Sc3dHUVlEVlFRREV4SmtiMk5yWlhJdFptOXlMV1JsCmMydDB
iM0F3Z2dFaU1BMEdDU3FHU0liM0RRRUJBUVVBQTRJQkR3QXdnZ0VLQW9JQkFRRHkxanVJMkpHaWIxeksKN
nRCVnl0Q3VVeEhSZG5PQ2VQZDBQY0c2RWJKRkp1QlpHTkRUZE01ekRraVEyZGs2MzE3ODBTUzhvVzF6bG0
yaAp1b1BNNStDMy9OV1dCYURTbFZEVWpEYXRqUUZnVlh5cEExVkVkclpDTXhhVUZPTzJQQW4zS1pwWW9qV
XFrZC9BCjNwdWtNQkd4VFNzd1RZZzlhTWpSWmpGVmQ3V0djSVJtamx3NDVjbUx6eTV6aHZVcithZ3laeGd
WM0U5SCtPUHUKdDd1NWRxVTl5SXI3Mk1CZVd6OHVQcE1PTUZ6U2NzRFk3OHIwN3ZSeFZjREtPRzlUNVNFO
EdGRUJsSWt4aURtaAplQW1OSG8raE05L1I5NWx1dXF0T0pJN1pmcUJUUzZ6MWR6UU14eCtmdFRMeUpjRWd
iaFRzSVJkUHpja0M3TUpDCkdubFVQTVU1QWdNQkFBR2pkVEJ6TUE0R0ExVWREd0VCL3dRRUF3SUZvREFUQ
mdOVkhTVUVEREFLQmdnckJnRUYKQlFjREFqQU1CZ05WSFJNQkFmOEVBakFBTUI4R0ExVWRJd1FZTUJhQUZ
FdjI1VW9OdjBNa2laVVJuQ01kbkhCaApaSXVvTUIwR0ExVWRFUVFXTUJTQ0VtUnZZMnRsY2kxbWIzSXRaR
1Z6YTNSdmNEQU5CZ2txaGtpRzl3MEJBUXNGCkFBT0NBUUVBT1Rta2NVZlZUG96NWNLenBVZmJFTHR0YVB
GLzhTUFl4bnFGc2ZQc1RxZHhybnoxbzRNMEovVUYKMkw5ck5SK3dFTUE4NGZaNHNscld0ZGhabndYVE9ZV
FJBaXlsZ0hhbUhPemIvOU9KV3R2RVRGeFpsTWpMMFBFUgplcElvckNJYkhqNTNjNEpOQS9kVnBXZlpPVkx
Va1RCYTFoWHUxYllMVDJNN2hDazBtd05VUzdSOTJ2cFFBWVBOCnB3bGRSZStXV2RNKzVJU051cWZZTVZ2T
UtYY2dyVUk2NUNYS0l5QXBkdDVlWGNwNTFWSVR5ZzVYeENMdXFpaW8KYnQ3M2NRTXljcjNxa2RJMFFWdkQ
xR3JJTXhiVGN6M3o3MHRnMmNKQmtPUTE1WlBvYk10WDZOdU1uVjVrdlhZOQpDNmhMNS9yWDh3Vy85VUdMb
WtqVTh1WXlQZnJzS3c9PQotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==
client-key-data: LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcFFJQkFBS0NBUUVBO
HRZN2lOaVJvbTljeXVyUVZjclFybE1SMFhaemduajNkRDNCdWhHeVJTYmdXUmpRCjAzVE9jdzVJa05uWk9
0OWUvTkVrdktGdGM1WnRvYnFEek9mZ3QvelZsZ1dnMHBWUTFJdzJyWTBCWUZWOHFRTlYKUkhhMlFqTVdsQ
lRqdGp3Sjl5bWFXS0kxS3BIZndONmJwREFSc1Uwck1FMklQV2pJMFdZeFZYZTFobkNFWm81YwpPT1hKaTg
4dWM0YjFLL21vTW1jWUZkeFBSL2pqN3JlN3VYYWxQY2lLKzlqQVhscy9MajZURGpCYzBuTEEyTy9LCjlPN
zBjVlhBeWpodlUrVWhQQmhSQVpTSk1ZZzVvWGdKalI2UG9UUGYwZmVaYnJxclRpU08yWDZnVTB1czlYYzA
KRE1jZm43VXk4aVhCSUc0VTdDRVhUODNKQXV6Q1FocDVWRHpGT1FJREFRQUJBb0lCQVFEc092QUxmZktld
kFyZQo4M0xjSXNMQzh0aWdsY1JrcGx6RFhkaDV0QUZpT0NHRFN4ckt1aFNqNUw4KytrM1NjYjJyMzZFSFI
xcDhXVmdwClBwSTg0VTNBYmxzdzZDUzg5cmg5TERGOHYzRVpUOUJIY3BDZVc0V04vTGo0TVNJY0EyZ0dZe
GhkSk43bm5LUzQKc1ZWamNjZWtYVmVvVTZRM2FSb0NhcEdQZlRhL29neEhyaUVoVEtsTFdETXhxRnN5eGI
2bnMzZUFlblJMaWw1RQprTmhNWWJuZUNleFBNOHJZN3krbkNlWHhRM3piQmRPTFh4NTdlVm9zL2swejFqT
3hLZk9qSkh6dnl6SDF3ZTg2CjhLNmZxTFJXcVVsNmVrc3NXTzdQVkoxWElJK041dDFBdStWaXJuY0ZMOWh
HQzB0MEx0MTREaGlRUWdjWjUxc2sKRHN1aHBSbHBBb0dCQVAvSjVrT2YzSlVGRk4rRllEMUw1MmUxeWZEU
VpaK3luWEw0eG53UE9GTWlzZ0RrM0NsSApzSjVwWWhQZG5hRklCOU5UZ2VoME9mWDRjWVYzblVDUjREY3Z
XU2JYanFFV29uZjFRNXlsSmZyNnhIeGJhdmdMCkpYZ2xhMk15NE5TMWpGeS9YQyt2RmlNRGV4cFRKWithb
k9PcXFManNYclp2VWlWdkxqTTdmOTVUQW9HQkFQTUoKbC8ydVBRQjhlWERhYmVKbStGU2ZWTEd1LzFnVVF
CS2tkdm1wdk1ZV3JBSXYyWTh3OTZ4K1AyaTdFMmtrVmFiYQpVQmRCVWUwNGRUeCtvRElnR0I3eDJkR2ZhT
1ZwTU50MHp1YWkvUkhtOE1nRXZxd1RWSFZYSk9DNVVBbXJPcjQrCmI5emFEdGcvZFhxRWtJdEdlZlptM3l
jL1BwR1Z4VHg2M1Y2cFNtVERBb0dCQU4wclcySGZxV0JrKzI1bUtoZjIKT01tUkEyS3BIeVhkMEl4b0ZWK
1IzWGJ0Q2hNQjBHZ1ZKOTloYWIrWm9VR2lRYm4xZTk5ZUYvdlo3WGFsUGFCbQpRZ1FWZWJXL0x3R1V5N2l
EcHdtY051SHowTTlpVUhUWFZuZXppMDVENE9tcmJRbUpJUkhPQjRzUTZIR1RzWFYyCnYrK1BVY0pNQjMwa
```

```
GRsc043bG00T2RFbkFvR0JBTm1IQXJVWjJKdXd6WGxHNkFjMkpwcUhLV1VIdnAvMU1Bdi8KakVXVnVOS0x
4RlVJd3U4NDR0VlBBaTRaRXh5T1d1TkdqMXpoS0JUczdYSEIzRnhCQVpYZzNoYVRXVzNNSXVDcAp3ZTRJZ
i80ZjkrN3U0RUpmNHI1THkwUWdXUlR1WDF1YndyK25wSlhFNXI5TUc1dXM3c2l0OXBuSUw1WmF1UGlTCjk
4UWNQZXZGQW9HQUR1OFU4T3pYVExkVkhKYU9YVVZMV3oxcGd0ck54N01RMzFxREF0dEltblhNWnN6RkdIS
W4KTENZaTk5T0JBUnU0Q0orWWpuYS9uSHVBQ3BIcEFJN3p4Z3Z0TFpwM3FBWnNVT1g3aE5sNVMwQnk4RUV
TQi96dgpHQ3FoNFFQVXFHWDhLNUNOWUJQWkdGY1l0a3N0NFBxK1dmYXc5TVR4V00wVk1tNzdGMS8xMHh3P
QotLS0tLUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=
```

Analyzing Postfix Files (limit 70)

```
-rw-r--r-- 1 root root 813 Feb 2 2020
/snap/core20/1822/usr/share/bash-completion/completions/postfix
-rw-r--r-- 1 root root 813 Feb 2 2020
/snap/core20/1974/usr/share/bash-completion/completions/postfix
-rw-r--r-- 1 root root 761 Nov 16 2021
/snap/core22/817/usr/share/bash-completion/completions/postfix
-rw-r--r-- 1 root root 761 Nov 16 2021
/usr/share/bash-completion/completions/postfix
```

Analyzing DNS Files (limit 70)

```
-rw-r--r-- 1 root root 826 Nov 16 2021 /usr/share/bash-completion/completions/bind
-rw-r--r-- 1 root root 826 Nov 16 2021 /usr/share/bash-completion/completions/bind
```

Analyzing Other Interesting Files (limit 70)

```
-rw-r--r-- 1 root root 3771 Jan 6 2022 /etc/skel/.bashrc
-rw-r--r-- 1 prasad prasad 3771 Jul 17 03:19 /home/prasad/.bashrc
-rw-r--r-- 1 root root 3771 Feb 25 2020 /snap/core20/1822/etc/skel/.bashrc
-rw-r--r-- 1 root root 3771 Feb 25 2020 /snap/core20/1974/etc/skel/.bashrc
-rw-r--r-- 1 root root 3771 Jan 6 2022 /snap/core22/817/etc/skel/.bashrc
-rw-r--r-- 1 root root 807 Jan 6 2022 /etc/skel/.profile
-rw-r--r-- 1 prasad prasad 807 Jul 17 03:19 /home/prasad/.profile
-rw-r--r-- 1 root root 807 Feb 25 2020 /snap/core20/1822/etc/skel/.profile
-rw-r--r-- 1 root root 807 Feb 25 2020 /snap/core20/1974/etc/skel/.profile
-rw-r--r-- 1 root root 807 Jan 6 2022 /snap/core22/817/etc/skel/.profile
-rw-r--r-- 1 prasad prasad 0 Jul 17 09:56 /home/prasad/.sudo_as_admin_successful
```

Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid

```
strings Not Found
-rwsr-xr-x 1 root root 52K Jun 23 08:33 /usr/share/code/chrome-sandbox
-rwsr-xr-x 1 root root 44K Nov 24 2022 /usr/bin/chsh
-rwsr-xr-x 1 root root 72K Nov 24 2022 /usr/bin/chfn ---> SuSE_9.3/10
-rwsr-xr-x 1 root root 31K Feb 26 2022 /usr/bin/pkexec --->
Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 55K Feb 21 2022 /usr/bin/su
-rwsr-xr-x 1 root root 28K Nov 24 2022 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 40K Nov 24 2022 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 root root 35K Mar 23 2022 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 35K Feb 21 2022 /usr/bin/umount ---> BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 59K Nov 24 2022 /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 47K Feb 21 2022 /usr/bin/mount --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 71K Nov 24 2022 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 28K Nov 24 2022 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 227K Apr 3 23:30 /usr/bin/sudo --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-- 1 root messagebus 35K Oct 25 2022
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root root 15K Apr 4 11:50 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 136K May 29 17:38 /usr/lib/snapd/snap-confine --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root root 331K Nov 23 2022 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 19K Feb 26 2022 /usr/libexec/polkit-agent-helper-1
-rwsr-xr-- 1 root dip 415K Feb 24 2022 /usr/sbin/pppd --->
Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root root 214K Jun 24 07:53 /opt/google/chrome/chrome-sandbox
-rwsr-xr-x 1 root root 121K Jan 26 2023
/snap/snapd/18357/usr/lib/snapd/snap-confine --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root root 129K May 27 14:11
/snap/snapd/19457/usr/lib/snapd/snap-confine --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root root 84K Nov 29 2022 /snap/core20/1974/usr/bin/chfn --->
SuSE_9.3/10
-rwsr-xr-x 1 root root 52K Nov 29 2022 /snap/core20/1974/usr/bin/chsh
-rwsr-xr-x 1 root root 87K Nov 29 2022 /snap/core20/1974/usr/bin/gpasswd
-rwsr-xr-x 1 root root 55K May 30 21:12 /snap/core20/1974/usr/bin/mount --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 44K Nov 29 2022 /snap/core20/1974/usr/bin/newgrp --->
HP-UX_10.20
-rwsr-xr-x 1 root root 67K Nov 29 2022 /snap/core20/1974/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 67K May 30 21:12 /snap/core20/1974/usr/bin/su
-rwsr-xr-x 1 root root 163K Apr 4 17:26 /snap/core20/1974/usr/bin/sudo --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 39K May 30 21:12 /snap/core20/1974/usr/bin/umount --->
BSD/Linux(08-1996)
-rwsr-xr-- 1 root systemd-resolve 51K Oct 25 2022
/snap/core20/1974/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 463K Apr 4 04:17
/snap/core20/1974/usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 84K Nov 29 2022 /snap/core20/1822/usr/bin/chfn --->
SuSE_9.3/10
-rwsr-xr-x 1 root root 52K Nov 29 2022 /snap/core20/1822/usr/bin/chsh
-rwsr-xr-x 1 root root 87K Nov 29 2022 /snap/core20/1822/usr/bin/gpasswd
-rwsr-xr-x 1 root root 55K Feb 7 2022 /snap/core20/1822/usr/bin/mount --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 44K Nov 29 2022 /snap/core20/1822/usr/bin/newgrp --->
HP-UX_10.20
-rwsr-xr-x 1 root root 67K Nov 29 2022 /snap/core20/1822/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 67K Feb 7 2022 /snap/core20/1822/usr/bin/su
-rwsr-xr-x 1 root root 163K Jan 16 2023 /snap/core20/1822/usr/bin/sudo --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 39K Feb 7 2022 /snap/core20/1822/usr/bin/umount --->
BSD/Linux(08-1996)
-rwsr-xr-- 1 root systemd-resolve 51K Oct 25 2022
/snap/core20/1822/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 463K Mar 30 2022
/snap/core20/1822/usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 72K Nov 24 2022 /snap/core22/817/usr/bin/chfn --->
SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Nov 24 2022 /snap/core22/817/usr/bin/chsh
-rwsr-xr-x 1 root root 71K Nov 24 2022 /snap/core22/817/usr/bin/gpasswd
-rwsr-xr-x 1 root root 47K Feb 21 2022 /snap/core22/817/usr/bin/mount --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 40K Nov 24 2022 /snap/core22/817/usr/bin/newgrp --->
HP-UX_10.20
-rwsr-xr-x 1 root root 59K Nov 24 2022 /snap/core22/817/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 55K Feb 21 2022 /snap/core22/817/usr/bin/su
-rwsr-xr-x 1 root root 227K Apr 3 23:30 /snap/core22/817/usr/bin/sudo --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 35K Feb 21 2022 /snap/core22/817/usr/bin/umount --->
BSD/Linux(08-1996)
-rwsr-xr-- 1 root systemd-resolve 35K Oct 25 2022
/snap/core22/817/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 331K Nov 23 2022
```

```
/snap/core22/817/usr/lib/openssh/ssh-keysign
```

SGID

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid

```
-rwxr-sr-x 1 root tty 23K Feb 21 2022 /usr/bin/write.ul (Unknown SGID binary)
-rwxr-sr-x 1 root shadow 23K Nov 24 2022 /usr/bin/expiry
-rwxr-sr-x 1 root crontab 39K Mar 23 2022 /usr/bin/crontab
-rwxr-sr-x 1 root _ssh 287K Nov 23 2022 /usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 23K Feb 21 2022 /usr/bin/wall
-rwxr-sr-x 1 root shadow 71K Nov 24 2022 /usr/bin/chage
-rwsr-sr-x 1 root root 15K Apr 4 11:50 /usr/lib/xorg/Xorg.wrap
-rwxr-sr-x 1 root mail 23K Jul 6 2022 /usr/libexec/camel-lock-helper-1.2
-rwxr-sr-x 1 root shadow 27K Feb 2 14:51 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 23K Feb 2 14:51 /usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 83K Nov 29 2022 /snap/core20/1974/usr/bin/chage
-rwxr-sr-x 1 root shadow 31K Nov 29 2022 /snap/core20/1974/usr/bin/expiry
-rwxr-sr-x 1 root messagebus 343K Apr 4 04:17 /snap/core20/1974/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 35K May 30 21:12 /snap/core20/1974/usr/bin/wall
-rwxr-sr-x 1 root shadow 43K Feb 2 14:52
/snap/core20/1974/usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 43K Feb 2 14:52 /snap/core20/1974/usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 83K Nov 29 2022 /snap/core20/1822/usr/bin/chage
-rwxr-sr-x 1 root shadow 31K Nov 29 2022 /snap/core20/1822/usr/bin/expiry
-rwxr-sr-x 1 root messagebus 343K Mar 30 2022 /snap/core20/1822/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 35K Feb 7 2022 /snap/core20/1822/usr/bin/wall
-rwxr-sr-x 1 root shadow 43K Jan 24 2023
/snap/core20/1822/usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 43K Jan 24 2023 /snap/core20/1822/usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 71K Nov 24 2022 /snap/core22/817/usr/bin/chage
-rwxr-sr-x 1 root shadow 23K Nov 24 2022 /snap/core22/817/usr/bin/expiry
-rwxr-sr-x 1 root _ssh 287K Nov 23 2022 /snap/core22/817/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 23K Feb 21 2022 /snap/core22/817/usr/bin/wall
-rwxr-sr-x 1 root shadow 23K Feb 2 14:51
/snap/core22/817/usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 27K Feb 2 14:51 /snap/core22/817/usr/sbin/unix_chkpwd
```

Checking misconfigurations of ld.so

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#ld.so

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

Capabilities

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities

Current shell capabilities

```
CapInh: 0x0000000000000000=
CapPrm: 0x0000000000000000=
CapEff: 0x0000000000000000=
CapBnd: 0x000001ffffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fo
wner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,c
```

```
ap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap
_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pa
cct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sy
s_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,c
ap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_au
dit_read,cap_perfmon,cap_bpf,cap_checkpoint_restore
CapAmb: 0x0000000000000000=
```

Parent process capabilities

```
CapInh: 0x0000000000000000=
CapPrm: 0x0000000000000000=
CapEff: 0x0000000000000000=
CapBnd: 0x000001ffffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fo
wner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,c
ap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap
_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pa
cct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sy
s_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,c
ap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_au
dit_read,cap_perfmon,cap_bpf,cap_checkpoint_restore
CapAmb: 0x0000000000000000=
Files with capabilities (limited to 50):
/usr/bin/mtr-packet cap_net_raw=ep
/usr/bin/ping cap_net_raw=ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper
cap_net_bind_service,cap_net_admin=ep
/opt/docker-desktop/bin/com.docker.backend
cap_net_bind_service,cap_sys_resource=ep
/snap/core20/1974/usr/bin/ping cap_net_raw=ep
/snap/core20/1822/usr/bin/ping cap_net_raw=ep
/snap/core22/817/usr/bin/ping cap_net_raw=ep
```

AppArmor binary profiles

```
-rw-r--r-- 1 root root 3500 Feb 1 00:37 sbin.dhclient
-rw-r--r-- 1 root root 11233 Dec 7 2022 usr.bin.evince
-rw-r--r-- 1 root root 3448 Mar 18 2022 usr.bin.man
-rw-r--r-- 1 root root 1518 Feb 10 23:44 usr.bin.tcpdump
-rw-r--r-- 1 root root 1519 Oct 27 2022 usr.lib.libreoffice.program.oosplash
-rw-r--r-- 1 root root 1227 Oct 27 2022 usr.lib.libreoffice.program.senddoc
-rw-r--r-- 1 root root 10740 Oct 27 2022 usr.lib.libreoffice.program.soffice.bin
-rw-r--r-- 1 root root 1046 Oct 27 2022 usr.lib.libreoffice.program.xpdfimport
-rw-r--r-- 1 root root 28486 Dec 1 2022 usr.lib.snapd.snap-confine.real
-rw-r--r-- 1 root root 677 Apr 6 2022 usr.sbin.cups-browsed
-rw-r--r-- 1 root root 6141 May 27 2022 usr.sbin.cupsd
-rw-r--r-- 1 root root 1592 Nov 16 2021 usr.sbin.rsyslogd
```

Files (scripts) in /etc/profile.d/

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#profiles-files

```
total 60
drwxr-xr-x 2 root root 4096 Jul 17 10:07 .
drwxr-xr-x 139 root root 12288 Jul 31 13:06 ..
-rw-r--r-- 1 root root 96 Oct 15 2021 01-locale-fix.sh
-rw-r--r-- 1 root root 835 Dec 1 2022 apps-bin-path.sh
-rw-r--r-- 1 root root 726 Nov 16 2021 bash_completion.sh
-rw-r--r-- 1 root root 1003 Aug 13 2019 cedilla-portuguese.sh
-rw------- 1 root root 677 Feb 23 09:29 debuginfod.csh
-rw------- 1 root root 692 Feb 23 09:29 debuginfod.sh
-rw-r--r-- 1 root root 1012 Mar 22 2022 gnome-session_gnomerc.sh
-rw-r--r-- 1 root root 376 Nov 16 2021 im-config_wayland.sh
-rw-r--r-- 1 root root 1908 Mar 28 2022 vte-2.91.sh
-rw-r--r-- 1 root root 967 Mar 28 2022 vte.csh
-rw-r--r-- 1 root root 954 Mar 22 2022 xdg_dirs_desktop_session.sh
```

Permissions in init, init.d, systemd, and rc.d

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d

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

Searching root files in home dirs (limit 30)

```
/home/
/root/
```

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

```
-rw-r----- 1 root dip 1093 Feb 23 09:29 /etc/ppp/peers/provider
-rw-r----- 1 root dip 656 Feb 23 09:29 /etc/chatscripts/provider
-rw-r----- 1 root adm 23476 Jul 22 04:02 /var/log/dmesg.3.gz
-rw-r----- 1 root adm 2636 Jul 18 12:39 /var/log/apport.log
-rw-r----- 1 root adm 23377 Jul 30 00:57 /var/log/dmesg.1.gz
-rw-r----- 1 root adm 29425 Jul 31 2023 /var/log/cups/access_log
-rw-r----- 1 root adm 144195 Jul 31 13:06 /var/log/apt/term.log
-rw-r----- 1 root adm 96717 Jul 31 01:17 /var/log/dmesg
-rw-r----- 1 root adm 23529 Jul 20 22:05 /var/log/dmesg.4.gz
-rw-r----- 1 root adm 23259 Jul 28 19:13 /var/log/dmesg.2.gz
-rw-r----- 1 root adm 2542 Jul 17 03:05 /var/log/installer/casper.log
-rw-r----- 1 root adm 52 Jul 17 03:12 /var/log/installer/casper-md5check.json
-rw-r----- 1 root adm 11432 Jul 17 03:21 /var/log/installer/debug
-rw-r----- 1 root adm 18 Jul 17 03:06 /var/log/installer/version
-rw-r----- 1 root adm 512212 Jul 17 03:11 /var/log/installer/partman
-rw-r----- 1 root adm 98530 Jul 30 23:54 /var/log/dmesg.0
```

Interesting writable files owned by me or writable by everyone (not in Home) (max 500)

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files

```
/dev/mqueue
/dev/shm
/home/prasad
/media/prasad/New Volume
/media/prasad/New Volume/$RECYCLE.BIN
/media/prasad/New
Volume/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001
/media/prasad/New
Volume/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001/desktop.ini
/media/prasad/New Volume1
/media/prasad/New Volume1/$RECYCLE.BIN
/media/prasad/New
Volume1/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001
/media/prasad/New
Volume1/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001/desktop.ini
```

```
/media/prasad/New Volume1/c++ challenge yourself
/media/prasad/New Volume1/C++ classwork
/media/prasad/New Volume1/c++ homework
/media/prasad/New Volume1/DBMS
/media/prasad/New Volume1/DumpStack.log.tmp
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/ideathon/ideathon.pptx
/media/prasad/New Volume1/Java I
/media/prasad/New Volume1/Java I/Challenge yourself
/media/prasad/New Volume1/Java I/Classwork
/media/prasad/New Volume1/Java I/Homework
/media/prasad/New Volume1/kavach
/media/prasad/New Volume1/kavach/afterlogin.html
/media/prasad/New Volume1/kavach/example.html
/media/prasad/New Volume1/kavach/.git
/media/prasad/New Volume1/kavach/.git/config
/media/prasad/New Volume1/kavach/.git/description
/media/prasad/New Volume1/kavach/.git/HEAD
/media/prasad/New Volume1/kavach/.git/hooks
/media/prasad/New Volume1/kavach/.git/hooks/applypatch-msg.sample
/media/prasad/New Volume1/kavach/.git/hooks/commit-msg.sample
/media/prasad/New Volume1/kavach/.git/hooks/fsmonitor-watchman.sample
/media/prasad/New Volume1/kavach/.git/hooks/post-update.sample
/media/prasad/New Volume1/kavach/.git/hooks/pre-applypatch.sample
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/.git/info
/media/prasad/New Volume1/kavach/.git/info/exclude
/media/prasad/New Volume1/kavach/.git/objects
/media/prasad/New Volume1/kavach/.git/objects/info
/media/prasad/New Volume1/kavach/.git/objects/pack
/media/prasad/New Volume1/kavach/.git/refs
/media/prasad/New Volume1/kavach/.git/refs/heads
/media/prasad/New Volume1/kavach/.git/refs/tags
/media/prasad/New Volume1/kavach/hoobank-landingpage
/media/prasad/New Volume1/kavach/hoobank-landingpage/dashboard.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/dashboard_style.css
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/config
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/description
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/hooks
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/hooks/applypatch-msg.sample
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/hooks/commit-msg.sample
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/hooks/fsmonitor-watchman.sample
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/hooks/post-update.sample
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/hooks/pre-applypatch.sample
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/.gitignore
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/index
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/info
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/info/exclude
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/heads
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/heads/main
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/remotes
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/remotes/origin
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/logs/refs/remotes/origin/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/info
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack/pack-d67dc8
4098fc621712e96dbe34fd42580b1ce648.idx
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack/pack-d67dc8
4098fc621712e96dbe34fd42580b1ce648.pack
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack/pack-d67dc8
4098fc621712e96dbe34fd42580b1ce648.rev
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/packed-refs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/heads
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/heads/main
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/remotes
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/remotes/origin
```

```
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/remotes/origin/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/tags
/media/prasad/New Volume1/kavach/hoobank-landingpage/index.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/package.json
/media/prasad/New Volume1/kavach/hoobank-landingpage/postcss.config.cjs
/media/prasad/New Volume1/kavach/hoobank-landingpage/public
/media/prasad/New Volume1/kavach/hoobank-landingpage/README.md
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/App.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/assets
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/assets/index.js
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Billing.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Business.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Button.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/CardDeal.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Clients.jsx
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/constants
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/constants/index.js
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/dashboard
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/dashboard.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/dashboard_style.css
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/ex.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/graph.html
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/tailwind.config.cjs
/media/prasad/New Volume1/kavach/hoobank-landingpage/vite.config.js
/media/prasad/New Volume1/kavach/hoobank-landingpage/yarn.lock
/media/prasad/New Volume1/kavach/index.html
/media/prasad/New Volume1/kavach/linpeas
/media/prasad/New Volume1/kavach/linpeas/linpeas.sh
/media/prasad/New Volume1/kavach/linpeas/output.txt
/media/prasad/New Volume1/kavach/linpeas/peas2json.py
/media/prasad/New Volume1/kavach/loginpag.css
/media/prasad/New Volume1/kavach/loginpage.html
/media/prasad/New Volume1/kavach/otpgenerate.js
/media/prasad/New Volume1/kavach/otpstyle.css
/media/prasad/New Volume1/kavach/otpverify.html
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/zap/fetch.html
/media/prasad/New Volume1/kavach/zap/fetch.py
/media/prasad/New Volume1/kavach/zap/networkscanning.py
/media/prasad/New Volume1/kavach/zap/portscanning.py
/media/prasad/New Volume1/kavach/zap/zap.py
/media/prasad/New Volume1/MATLAB first year answers
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(1)
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(2)
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(3)
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(4)
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(5)
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/MATLAB full project with questions
/media/prasad/New Volume1/Program Files
/media/prasad/New Volume1/Program Files/ModifiableWindowsApps
/media/prasad/New Volume1/screen-capture (1).webm
/media/prasad/New Volume1/skillathon bot
/media/prasad/New Volume1/skillathon bot/botmaking2.MP4
/media/prasad/New Volume1/skillathon bot/Untitled1.approj
/media/prasad/New Volume1/skillathon bot/Untitled1_files
/media/prasad/New Volume1/System Volume Information
/media/prasad/New Volume1/System Volume Information/EDP
/media/prasad/New Volume1/System Volume Information/EDP/Recovery
/media/prasad/New Volume1/System Volume Information/EfaSIDat
/media/prasad/New Volume1/System Volume Information/EfaSIDat/SYMEFA.DB
/media/prasad/New Volume1/System Volume Information/IndexerVolumeGuid
/media/prasad/New Volume1/System Volume Information/LightningSand.CFD
/media/prasad/New Volume1/System Volume Information/tracking.log
/media/prasad/New Volume1/System Volume Information/Wcifs.md
/media/prasad/New Volume1/System Volume Information/WPAppSettings.dat
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/Videos
/media/prasad/New Volume1/Videos/Adade Sundara (2022) Tamil HDRip.mkv
/media/prasad/New Volume1/Videos/Annabelle.Comes.Home.2019.
MultiAud.HDRip.950MB.x264.mkv
/media/prasad/New Volume1/Videos/Annabelle Creation (2017) BluRay 720p
Tel.Tam.Hin.Eng.mkv
/media/prasad/New
```

```
Volume1/Videos/_Brahmastra_Part_One_Shiva_2022_Tamil_HQ_HDRip_720p_ESub.mkv
/media/prasad/New Volume1/Videos/[DC] Transformers 3 Dark of the Moon (2011) [720p
- BDRip -.mkv
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/WindowsApps
/media/prasad/New Volume1/WindowsApps/Deleted
/media/prasad/New Volume1/WindowsApps/MutableBackup
/media/prasad/New Volume1/WpSystem
/media/prasad/New Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001
/media/prasad/New
Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001/AppData
/media/prasad/New
Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001/AppData/Local
/media/prasad/New Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001/
AppData/Local/Packages
/media/prasad/New Volume1/WUDownloadCache
/media/prasad/New Volume/System Volume Information
/media/prasad/New Volume/System Volume Information/EDP
/media/prasad/New Volume/System Volume Information/EDP/Recovery
/media/prasad/New Volume/System Volume Information/EfaSIDat
/media/prasad/New Volume/System Volume Information/EfaSIDat/SYMEFA.DB
/media/prasad/New Volume/System Volume Information/IndexerVolumeGuid
/media/prasad/New Volume/System Volume Information/LightningSand.CFD
/media/prasad/New Volume/System Volume Information/tracking.log
/media/prasad/New Volume/System Volume Information/WPSettings.dat
/run/lock
/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.snapd-desktop-integration
/run/user/1000/doc/by-app/snap.snap-store
/run/user/1000/gnome-shell
/run/user/1000/gnome-shell/runtime-state-LE.
/run/user/1000/gnupg
/run/user/1000/gvfs
/run/user/1000/gvfsd
/run/user/1000/ICEauthority
/run/user/1000/keyring
#)You_can_write_even_more_files_inside_last_directory
/run/user/1000/pulse/pid
/run/user/1000/speech-dispatcher
/run/user/1000/systemd
/run/user/1000/systemd/generator.late
/run/user/1000/systemd/generator.late/app-geocluex2ddemox2dagent@autostart.service
/run/user/1000/systemd/generator.late/app-gnomex2dinitialx2dsetupx2dfirstx2dlogin@
autostart.service
/run/user/1000/systemd/generator.late/app-gnomex2dshellx2doverridesx2dmigration@au
tostart.service
/run/user/1000/systemd/generator.late/app-imx2dlaunch@autostart.service
/run/user/1000/systemd/generator.late/app-nmx2dapplet@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/transient
/run/user/1000/systemd/transient/app-gnome-atx2dspix2ddbusx2dbus-1986.scope
/run/user/1000/systemd/transient/app-gnome-code-27319.scope
/run/user/1000/systemd/transient/app-gnome-googlex2dchrome-8768.scope
/run/user/1000/systemd/transient/app-gnome-org.gnome.Evolutionx2dalarmx2dnotify-21
77.scope
/run/user/1000/systemd/transient/app-gnome-org.gnome.SettingsDaemon.DiskUtilityNot
ify-2133.scope
#)You_can_write_even_more_files_inside_last_directory
/run/user/1000/systemd/units
/run/user/1000/update-notifier.pid
/run/user/1000/wayland-0.lock
/snap/core20/1822/run/lock
/snap/core20/1822/tmp
/snap/core20/1822/var/tmp
/snap/core20/1974/run/lock
/snap/core20/1974/tmp
/snap/core20/1974/var/tmp
/snap/core22/817/run/lock
/snap/core22/817/tmp
```

```
/snap/core22/817/var/tmp
/tmp
/tmp/.com.google.Chrome.9SUn3m
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/tracker-extract-3-files.1000
#)You_can_write_even_more_files_inside_last_directory
/var/crash
/var/crash/_opt_docker-desktop_Docker Desktop.1000.crash
/var/crash/_opt_docker-desktop_Docker Desktop.1000.upload
/var/crash/_usr_bin_update-notifier.1000.crash
/var/crash/_usr_bin_update-notifier.1000.upload
/var/lib/BrlAPI
/var/metrics
/var/tmp
```

Interesting GROUP writable files (not in Home) (max 500)

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files

```
Group prasad:
/run/user/1000/wayland-0.lock
/run/user/1000/pipewire-0.lock
/media/prasad/New Volume1
/media/prasad/New Volume1/$RECYCLE.BIN
/media/prasad/New
Volume1/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001
/media/prasad/New
Volume1/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001/desktop.ini
/media/prasad/New Volume1/c++ challenge yourself
/media/prasad/New Volume1/C++ classwork
/media/prasad/New Volume1/c++ homework
/media/prasad/New Volume1/DBMS
/media/prasad/New Volume1/DumpStack.log.tmp
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/ideathon/ideathon.pptx
/media/prasad/New Volume1/Java I
/media/prasad/New Volume1/Java I/Challenge yourself
/media/prasad/New Volume1/Java I/Classwork
/media/prasad/New Volume1/Java I/Homework
/media/prasad/New Volume1/kavach
/media/prasad/New Volume1/kavach/.git
/media/prasad/New Volume1/kavach/.git/config
/media/prasad/New Volume1/kavach/.git/description
/media/prasad/New Volume1/kavach/.git/HEAD
/media/prasad/New Volume1/kavach/.git/hooks
/media/prasad/New Volume1/kavach/.git/hooks/applypatch-msg.sample
/media/prasad/New Volume1/kavach/.git/hooks/commit-msg.sample
/media/prasad/New Volume1/kavach/.git/hooks/fsmonitor-watchman.sample
/media/prasad/New Volume1/kavach/.git/hooks/post-update.sample
/media/prasad/New Volume1/kavach/.git/hooks/pre-applypatch.sample
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/.git/info
/media/prasad/New Volume1/kavach/.git/info/exclude
/media/prasad/New Volume1/kavach/.git/objects
/media/prasad/New Volume1/kavach/.git/objects/info
/media/prasad/New Volume1/kavach/.git/objects/pack
/media/prasad/New Volume1/kavach/.git/refs
/media/prasad/New Volume1/kavach/.git/refs/heads
/media/prasad/New Volume1/kavach/.git/refs/tags
/media/prasad/New Volume1/kavach/afterlogin.html
/media/prasad/New Volume1/kavach/example.html
/media/prasad/New Volume1/kavach/hoobank-landingpage
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/config
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/description
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/hooks
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/hooks/applypatch-msg.sample
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/hooks/commit-msg.sample
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/hooks/fsmonitor-watchman.sample
```

```
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/hooks/post-update.sample
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/hooks/pre-applypatch.sample
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/index
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/info
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/info/exclude
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/heads
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/heads/main
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/remotes
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/logs/refs/remotes/origin
/media/prasad/New
Volume1/kavach/hoobank-landingpage/.git/logs/refs/remotes/origin/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/info
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack/pack-d67dc8
4098fc621712e96dbe34fd42580b1ce648.idx
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack/pack-d67dc8
4098fc621712e96dbe34fd42580b1ce648.pack
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/objects/pack/pack-d67dc8
4098fc621712e96dbe34fd42580b1ce648.rev
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/packed-refs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/heads
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/heads/main
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/remotes
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/remotes/origin
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/remotes/origin/HEAD
/media/prasad/New Volume1/kavach/hoobank-landingpage/.git/refs/tags
/media/prasad/New Volume1/kavach/hoobank-landingpage/.gitignore
/media/prasad/New Volume1/kavach/hoobank-landingpage/dashboard.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/dashboard_style.css
/media/prasad/New Volume1/kavach/hoobank-landingpage/index.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/package.json
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/App.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/assets
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/assets/index.js
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Billing.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Business.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Button.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/CardDeal.jsx
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/components/Clients.jsx
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/constants
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/constants/index.js
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/dashboard
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/dashboard.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/dashboard_style.css
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/ex.html
/media/prasad/New Volume1/kavach/hoobank-landingpage/src/graph.html
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/hoobank-landingpage/tailwind.config.cjs
/media/prasad/New Volume1/kavach/hoobank-landingpage/vite.config.js
/media/prasad/New Volume1/kavach/hoobank-landingpage/yarn.lock
/media/prasad/New Volume1/kavach/index.html
/media/prasad/New Volume1/kavach/linpeas
/media/prasad/New Volume1/kavach/linpeas/linpeas.sh
/media/prasad/New Volume1/kavach/linpeas/output.txt
/media/prasad/New Volume1/kavach/linpeas/peas2json.py
/media/prasad/New Volume1/kavach/loginpag.css
/media/prasad/New Volume1/kavach/loginpage.html
/media/prasad/New Volume1/kavach/otpgenerate.js
/media/prasad/New Volume1/kavach/otpstyle.css
/media/prasad/New Volume1/kavach/otpverify.html
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/kavach/zap/fetch.html
/media/prasad/New Volume1/kavach/zap/fetch.py
/media/prasad/New Volume1/kavach/zap/networkscanning.py
/media/prasad/New Volume1/kavach/zap/portscanning.py
/media/prasad/New Volume1/kavach/zap/zap.py
/media/prasad/New Volume1/MATLAB first year answers
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3 example
```

```
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(1)
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(2)
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(3)
/media/prasad/New Volume1/MATLAB first year answers/lab experiment3(4)
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/MATLAB full project with questions
/media/prasad/New Volume1/Program Files
/media/prasad/New Volume1/Program Files/ModifiableWindowsApps
/media/prasad/New Volume1/screen-capture (1).webm
/media/prasad/New Volume1/skillathon bot
/media/prasad/New Volume1/skillathon bot/botmaking2.MP4
/media/prasad/New Volume1/skillathon bot/Untitled1.approj
/media/prasad/New Volume1/skillathon bot/Untitled1_files
/media/prasad/New Volume1/System Volume Information
/media/prasad/New Volume1/System Volume Information/EDP
/media/prasad/New Volume1/System Volume Information/EDP/Recovery
/media/prasad/New Volume1/System Volume Information/EfaSIDat
/media/prasad/New Volume1/System Volume Information/EfaSIDat/SYMEFA.DB
/media/prasad/New Volume1/System Volume Information/IndexerVolumeGuid
/media/prasad/New Volume1/System Volume Information/LightningSand.CFD
/media/prasad/New Volume1/System Volume Information/tracking.log
/media/prasad/New Volume1/System Volume Information/Wcifs.md
/media/prasad/New Volume1/System Volume Information/WPAppSettings.dat
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/Videos
/media/prasad/New Volume1/Videos/Ice_Age_4_Continental_Drift_Tamil_+_Telugu_+_Hind
i_+_English_720P.mkv
/media/prasad/New
Volume1/Videos/Sita.Ramam.2022.Tam.1080p.10bit.AMZN.6CH.Esub-ALB.mkv
/media/prasad/New Volume1/Videos/@HEVC_Moviesz 7 Aum Arivu (2011) Tamil 1080p
WEB-DL HEVC.mkv
/media/prasad/New Volume1/Videos/@luxmv_Linkz - RRR (2022) Tamil HDRip 1080p - HEVC
- AAC].mkv
/media/prasad/New Volume1/Videos/@Srilinks4k_Thunivu_2023_Tamil_1080p_Proper_TRUE_
HD_AVC_UNTOUCHED.mkv
#)You_can_write_even_more_files_inside_last_directory
/media/prasad/New Volume1/WindowsApps
/media/prasad/New Volume1/WindowsApps/Deleted
/media/prasad/New Volume1/WindowsApps/MutableBackup
/media/prasad/New Volume1/WpSystem
/media/prasad/New Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001
/media/prasad/New
Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001/AppData
/media/prasad/New
Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001/AppData/Local
/media/prasad/New Volume1/WpSystem/S-1-5-21-2599125077-3711717779-1984677719-1001/
AppData/Local/Packages
/media/prasad/New Volume1/WUDownloadCache
/media/prasad/New Volume
/media/prasad/New Volume/$RECYCLE.BIN
/media/prasad/New
Volume/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001
/media/prasad/New
Volume/$RECYCLE.BIN/S-1-5-21-2599125077-3711717779-1984677719-1001/desktop.ini
/media/prasad/New Volume/System Volume Information
/media/prasad/New Volume/System Volume Information/EDP
/media/prasad/New Volume/System Volume Information/EDP/Recovery
/media/prasad/New Volume/System Volume Information/EfaSIDat
/media/prasad/New Volume/System Volume Information/EfaSIDat/SYMEFA.DB
/media/prasad/New Volume/System Volume Information/IndexerVolumeGuid
/media/prasad/New Volume/System Volume Information/LightningSand.CFD
/media/prasad/New Volume/System Volume Information/tracking.log
/media/prasad/New Volume/System Volume Information/WPSettings.dat
Group lpadmin:
/usr/share/ppd/custom
```

Other Interesting Files

.sh files in path

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path

```
/usr/bin/dockerd-rootless-setuptool.sh
/usr/bin/gettext.sh
/usr/bin/dockerd-rootless.sh
```

Executable files potentially added by user (limit 70)

```
2023-07-31+13:23:25.7732129880
/home/prasad/.config/Code/User/History/1bdce176/sLny.py
2023-07-18+11:06:25.4007878410
/var/lib/snapd/desktop/applications/whatsapp-for-linux_whatsapp-for-linux.desktop
2023-07-18+10:40:29.6708506290
/var/lib/snapd/desktop/applications/firefox_firefox.desktop
2023-07-17+11:37:56.8628613850
/var/lib/snapd/desktop/applications/snap-store_ubuntu-software.desktop
2023-07-17+11:37:56.8588612960
/var/lib/snapd/desktop/applications/snap-store_ubuntu-software-local-file.desktop
2023-07-17+11:37:56.8548612070
/var/lib/snapd/desktop/applications/snap-store_snap-store.desktop
2023-07-17+08:57:09.0021103700
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/times.json
2023-07-17+08:53:52.0851476920 /var/lib/colord/storage.db
2023-07-17+08:53:52.0851476920 /var/lib/colord/mapping.db
2023-07-17+03:19:29.2808139980 /etc/console-setup/cached_setup_terminal.sh
2023-07-17+03:19:29.2808139980 /etc/console-setup/cached_setup_keyboard.sh
2023-07-17+03:19:29.2808139980 /etc/console-setup/cached_setup_font.sh
2023-07-16+22:14:27.5322472920 /home/prasad/snap/firefox/common/.mozilla/firefox/e
qwqc8u1.default/gmp-gmpopenh264/1.8.1.2/libgmpopenh264.so
2023-07-16+22:14:27.5122472310 /home/prasad/snap/firefox/common/.mozilla/firefox/e
qwqc8u1.default/gmp-gmpopenh264/1.8.1.2/gmpopenh264.info
```

Unexpected in /opt (usually empty)

```
total 20
drwxr-xr-x 5 root root 4096 Jul 17 15:50 .
drwxr-xr-x 20 root root 4096 Jul 17 03:18 ..
drwx--x--x 4 root root 4096 Jul 17 10:34 containerd
drwxr-xr-x 7 root root 4096 Jul 17 15:51 docker-desktop
drwxr-xr-x 3 root root 4096 Jul 17 12:53 google
```

Modified interesting files in the last 5mins (limit 100)

```
/boot/grub/grubenv
/home/prasad/.cache/gstreamer-1.0/registry.x86_64.bin
/home/prasad/.cache/mesa_shader_cache/55/9072054247fdf5185b1578089068b236962af0
/home/prasad/.cache/mesa_shader_cache/e1/457d826655ffad6d0864e9447f5faa815bd17e
/home/prasad/.cache/mesa_shader_cache/ad/4bc299f3e04e260a6b3565315212b8f058fcd4
/home/prasad/.cache/mesa_shader_cache/76/4ca5506a3b0eb5fd9f98b0fae330974c2779fd
/home/prasad/.cache/mesa_shader_cache/1c/a851e5891a461d711a740ea0e6e09f4317d190
/home/prasad/.cache/mesa_shader_cache/index
/home/prasad/.cache/mesa_shader_cache/dc/d9fd97ce123a29817c6f62e2e320d6a0d22c5e
/home/prasad/.cache/mesa_shader_cache/e0/b1ad0f358e028426d0316be06ad519d3506f8b
/home/prasad/.cache/mesa_shader_cache/ee/9219e7a4126b9868e033ce973904478ddbb892
/home/prasad/.cache/mesa_shader_cache/3e/914739146a3acb8d4033109cef2ba5a59d474e
/home/prasad/.cache/mesa_shader_cache/94/5c3f9de5de27ae99933263e8858c7bf1541b86
/home/prasad/.cache/mesa_shader_cache/21/73a9c00ecdef7f173374e444cdb298b9a7eb22
/home/prasad/.cache/mesa_shader_cache/bd/2216319a7c889dcf03fa51a9041c77ee7f9ea0
/home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2
Fv3%2Ftracker%23Audio.db-wal
/home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2
Fv3%2Ftracker%23Video.db-wal
/home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2
Fv3%2Ftracker%23Pictures.db-shm
/home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2
```

```
Fv3%2Ftracker%23Video.db-shm
/home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2
Fv3%2Ftracker%23Pictures.db-wal
/home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2
Fv3%2Ftracker%23Audio.db-shm
/home/prasad/.cache/tracker3/files/.meta.isrunning
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/08c9c93c6f4479dc_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/c5b7c78e1414b402_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/1249cfc2840e890c_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/5a611dc179a2c439_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/b8794d177ebf39fd_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/5196379e43b40b1f_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/b51dd28bb67204cc_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/eebdc382b99cf518_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/f7a64dfd88a72a31_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/47787a3d3afe295b_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/ac25decfc47e2273_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/2c2f8d65546824d8_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/2d73cfc393d9583d_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/9d5848acde921931_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/d8ba50917b0a2714_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/18f007357dbc0550_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/5129ef89b24d1b13_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/d1f2c459564be44d_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/471c6c8d44034fee_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/6a5def04d7ceb0f1_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/1ea21481f1308a27_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/7323b0fd606ab87a_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/611de8a7587f7e01_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/index-dir/the-real-index
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/b6b5899acd061f99_0
/home/prasad/.cache/google-chrome/Profile 1/Code Cache/js/50ad3196b1c88610_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/2e04fef6eefbed17_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/2a2ba7a7e23e683d_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/60b9ba0ce2f8e452_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/8d32c6dc26f7677c_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/51820f85d5df8069_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/59f14c2c5a27b6d6_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/a3a1d15300e3327e_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/15af641257489746_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/e126b795d72bc3e1_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/3d29c661ec69b964_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/f2ba6651fe6e153a_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/ab3bcfa51d06b01e_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/b45fe6ae1ea94f5a_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/b7196e2f7698b2f3_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/1c504ccab6bfe11a_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/c016a6055ed600a8_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/99352d1e45390da5_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/e1c625abd355f7d9_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/86605831425ec4a2_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/3a264cf142c1b3b1_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/5c3865570fe00eae_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/c6b0d6252b982c80_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/62d726c99b4665f8_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/bb68e10d42c79127_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/3e74ece0ada8118f_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/a0cd9e897640c78b_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/31b29288448e7253_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/444bd7e4560a70c7_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/9bb732ca72120cc6_0
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/301b100285b0e8e9_0
/home/prasad/.cache/google-chrome/Profile
1/Cache/Cache_Data/index-dir/the-real-index
/home/prasad/.cache/google-chrome/Profile 1/Cache/Cache_Data/b36108f3739c34a6_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/116d603b819fb7e2_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/d46ab7364b1bc29b_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/3cea953c90e95499_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/cb526b63339bf632_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/b560d43183a520d5_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/a799cfb38573beed_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/642a4119fd009563_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/97e113fab02de06e_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/03c4dde4fa9d78fc_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/37dc0a5c0da50ed2_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/4c813d863b10d6e6_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/f89108faeca2619d_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/b338f71da732fd37_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/79cbe69ff1a04377_0
```

```
/home/prasad/.cache/google-chrome/Default/Code Cache/js/b2bbe4047008639d_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/4e42e17852431cb3_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/87935b83549039aa_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/a9c720db0a97cee7_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/e4d9a3619b01347c_0
/home/prasad/.cache/google-chrome/Default/Code Cache/js/c2487b656b98756b_0
```

Files inside /home/prasad (limit 20)

```
total 136
drwxr-x--- 21 prasad prasad 4096 Jul 31 13:07 .
drwxr-xr-x 3 root root 4096 Jul 17 03:19 ..
-rw------- 1 prasad prasad 7162 Jul 31 13:10 .bash_history
-rw-r--r-- 1 prasad prasad 220 Jul 17 03:19 .bash_logout
-rw-r--r-- 1 prasad prasad 3771 Jul 17 03:19 .bashrc
drwx------ 18 prasad prasad 4096 Jul 18 10:52 .cache
drwxr-xr-x 3 prasad prasad 4096 Jul 17 14:12 .cert
drwx------ 24 prasad prasad 4096 Jul 31 13:07 .config
drwxr-xr-x 2 prasad prasad 4096 Jul 17 08:54 Desktop
drwxr-xr-x 3 prasad prasad 4096 Jul 31 13:14 .docker
-rw-rw-r-- 1 prasad prasad 11607 Jul 17 15:42 docker-compose.yml
-rw-rw-r-- 1 prasad prasad 11607 Jul 20 14:10 docker-compose.yml.1
drwxr-xr-x 2 prasad prasad 4096 Jul 17 08:54 Documents
drwxr-xr-x 2 prasad prasad 4096 Jul 31 13:12 Downloads
drwx------ 3 prasad prasad 4096 Jul 31 13:22 .gnupg
drwxr-xr-x 2 prasad prasad 4096 Jul 20 16:06 .kube
drwx------ 3 prasad prasad 4096 Jul 17 08:54 .local
drwxr-xr-x 2 prasad prasad 4096 Jul 17 08:54 Music
drwxr-xr-x 3 prasad prasad 4096 Jul 18 11:26 Pictures
drwx------ 3 prasad prasad 4096 Jul 17 07:24 .pki
-rw-r--r-- 1 prasad prasad 807 Jul 17 03:19 .profile
drwxr-xr-x 2 prasad prasad 4096 Jul 17 08:54 Public
```

Backup files (limited 100)

```
-rw------- 1 prasad prasad 225 Jul 31 13:07 /home/prasad/.config/Code/Service
Worker/Database/LOG.old
-rw------- 1 prasad prasad 221 Jul 31 13:07 /home/prasad/.config/Code/Local
Storage/leveldb/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/AutofillStrikeDatabase/LOG.old
-rw------- 1 prasad prasad 285 Jul 17 09:45
/home/prasad/.config/google-chrome/Default/Extension Scripts/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Segmentation Platform/SignalDB/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Segmentation
Platform/SignalStorageConfigDB/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Segmentation
Platform/SegmentInfoDB/LOG.old
-rw------- 1 prasad prasad 312 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Site Characteristics Database/LOG.old
-rw------- 1 prasad prasad 281 Jul 17 09:45
/home/prasad/.config/google-chrome/Default/Extension Rules/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/BudgetDatabase/LOG.old
-rw------- 1 prasad prasad 359 Jul 18 11:59 /home/prasad/.config/google-chrome/Def
ault/IndexedDB/https_mail.google.com_0.indexeddb.leveldb/LOG.old
-rw------- 1 prasad prasad 323 Jul 17 14:42 /home/prasad/.config/google-chrome/Def
ault/IndexedDB/https_skcet530.examly.io_0.indexeddb.leveldb/LOG.old
-rw------- 1 prasad prasad 17045 Jul 18 09:56 /home/prasad/.config/google-chrome/D
efault/IndexedDB/https_web.whatsapp.com_0.indexeddb.leveldb/LOG.old
-rw------- 1 prasad prasad 356 Jul 20 14:28 /home/prasad/.config/google-chrome/Def
ault/IndexedDB/https_www.youtube.com_0.indexeddb.leveldb/LOG.old
-rw------- 1 prasad prasad 300 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Service Worker/Database/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023 /home/prasad/.config/google-chrome/Defaul
t/optimization_guide_hint_cache_store/LOG.old
```

```
-rw------- 1 prasad prasad 292 Jul 20 18:59
/home/prasad/.config/google-chrome/Default/File System/Origins/LOG.old
-rw------- 1 prasad prasad 0 Jul 17 09:59
/home/prasad/.config/google-chrome/Default/VideoDecodeStats/LOG.old
-rw------- 1 prasad prasad 294 Jul 31 2023
/home/prasad/.config/google-chrome/Default/GCM Store/Encryption/LOG.old
-rw------- 1 prasad prasad 272 Jul 31 2023
/home/prasad/.config/google-chrome/Default/GCM Store/LOG.old
-rw------- 1 prasad prasad 284 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Extension State/LOG.old
-rw------- 1 prasad prasad 2837 Jul 20 18:59
/home/prasad/.config/google-chrome/Default/Bookmarks.bak
-rw------- 1 prasad prasad 288 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Local Storage/leveldb/LOG.old
-rw------- 1 prasad prasad 298 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Platform Notifications/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/commerce_subscription_db/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/coupon_db/LOG.old
-rw------- 1 prasad prasad 302 Jul 31 2023
/home/prasad/.config/google-chrome/Default/shared_proto_db/metadata/LOG.old
-rw------- 1 prasad prasad 640 Jul 31 2023
/home/prasad/.config/google-chrome/Default/shared_proto_db/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Feature Engagement
Tracker/AvailabilityDB/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Feature Engagement
Tracker/EventDB/LOG.old
-rw------- 1 prasad prasad 288 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Sync Data/LevelDB/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Download Service/EntryDB/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.config/google-chrome/Default/LOG.old
-rw------- 1 prasad prasad 365 Jul 17 07:25
/home/prasad/.config/google-chrome/Default/Local Extension
Settings/ghbmnnjooekpmoecnnnilnnbdlolhkhi/LOG.old
-rw------- 1 prasad prasad 626 Jul 31 2023
/home/prasad/.config/google-chrome/Default/Session Storage/LOG.old
-rw------- 1 prasad prasad 0 Jul 31 2023 /home/prasad/.config/google-chrome/Defaul
t/optimization_guide_model_metadata_store/LOG.old
-rw------- 1 prasad prasad 0 Jul 20 10:12 /home/prasad/.config/Docker Desktop/Local
Storage/leveldb/LOG.old
-rw------- 1 prasad prasad 0 Jul 20 10:12 /home/prasad/.config/Docker
Desktop/Session Storage/LOG.old
-rw-r--r-- 1 root root 12285 Jul 17 10:08 /usr/share/info/dir.old
-rw-r--r-- 1 root root 2543 Sep 14 2022
/usr/share/help-langpack/en_GB/evolution/backup-restore.page
-rw-r--r-- 1 root root 2013 Apr 13 2022
/usr/share/help/C/gnome-help/backup-frequency.page
-rw-r--r-- 1 root root 3330 Apr 13 2022
/usr/share/help/C/gnome-help/backup-thinkabout.page
-rw-r--r-- 1 root root 2505 Apr 13 2022
/usr/share/help/C/gnome-help/backup-what.page
-rw-r--r-- 1 root root 2499 Apr 13 2022
/usr/share/help/C/gnome-help/backup-how.page
-rw-r--r-- 1 root root 1815 Apr 13 2022
/usr/share/help/C/gnome-help/backup-check.page
-rw-r--r-- 1 root root 1262 Apr 13 2022
/usr/share/help/C/gnome-help/backup-why.page
-rw-r--r-- 1 root root 1320 Apr 13 2022
/usr/share/help/C/gnome-help/backup-restore.page
-rw-r--r-- 1 root root 2261 Apr 13 2022
/usr/share/help/C/gnome-help/backup-where.page
-rw-r--r-- 1 root root 1581 Sep 29 2021
/usr/share/help/C/seahorse/misc-key-backup.page
-rw-r--r-- 1 root root 7867 Jul 16 1996 /usr/share/doc/telnet/README.old.gz
-rw-r--r-- 1 root root 416107 Dec 21 2020 /usr/share/doc/manpages/Changes.old.gz
-rwxr-xr-x 1 root root 1513 Jan 24 2020
/usr/share/doc/libipc-system-simple-perl/examples/rsync-backup.pl
-rw-r--r-- 1 root root 4459 Dec 25 2021
/usr/share/doc/duplicity/examples/system-backup
-rw-r--r-- 1 root root 138 Dec 6 2021 /usr/lib/systemd/system/dpkg-db-backup.timer
-rw-r--r-- 1 root root 147 Dec 6 2021
/usr/lib/systemd/system/dpkg-db-backup.service
-rw-r--r-- 1 root root 10849 Jan 30 21:14
```

```
/usr/lib/modules/5.19.0-32-generic/kernel/drivers/power/supply/wm831x_backup.ko
-rw-r--r-- 1 root root 56969 Jan 30 21:14 /usr/lib/modules/5.19.0-32-generic/kerne
l/drivers/net/team/team_mode_activebackup.ko
-rw-r--r-- 1 root root 10849 Jun 21 20:08
/usr/lib/modules/5.19.0-46-generic/kernel/drivers/power/supply/wm831x_backup.ko
-rw-r--r-- 1 root root 56969 Jun 21 20:08 /usr/lib/modules/5.19.0-46-generic/kerne
l/drivers/net/team/team_mode_activebackup.ko
-rwxr-xr-x 1 root root 2196 Apr 1 19:13 /usr/libexec/dpkg/dpkg-db-backup
-rwxr-xr-x 1 root root 1086 Aug 1 2022 /usr/src/linux-hwe-5.19-headers-5.19.0-46/t
ools/testing/selftests/net/tcp_fastopen_backup_key.sh
-rwxr-xr-x 1 root root 1086 Aug 1 2022 /usr/src/linux-hwe-5.19-headers-5.19.0-32/t
ools/testing/selftests/net/tcp_fastopen_backup_key.sh
-rw-r--r-- 1 root root 1219 Feb 23 09:30 /etc/xml/sgml-data.xml.old
-rw-r--r-- 1 root root 10151 Feb 23 09:30 /etc/xml/docbook-xml.xml.old
-rw-r--r-- 1 root root 673 Feb 23 09:29 /etc/xml/xml-core.xml.old
-rw-r--r-- 1 root root 3210 Feb 23 09:30 /etc/xml/catalog.old
-rw-r--r-- 1 root root 0 Feb 23 09:27 /var/lib/systemd/deb-systemd-helper-enabled/
timers.target.wants/dpkg-db-backup.timer
-rw-r--r-- 1 root root 61 Jul 17 10:04
/var/lib/systemd/deb-systemd-helper-enabled/dpkg-db-backup.timer.dsh-also
-rw-r--r-- 1 root root 191 Feb 23 09:30 /var/lib/sgml-base/supercatalog.old
```

Searching tables inside readable .db/.sql/.sqlite files (limit 100)

```
Found /home/prasad/.cache/fanal/fanal.db: data
Found /home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fonto
logy%2Fv3%2Ftracker%23Audio.db: SQLite 3.x database, last written using SQLite
version 3037002, writer version 2, read version 2, file counter 2, database pages
316, cookie 0x12a, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fonto
logy%2Fv3%2Ftracker%23Documents.db: SQLite 3.x database, last written using SQLite
version 3037002, writer version 2, read version 2, file counter 4, database pages
320, 1st free page 317, free pages 1, cookie 0x12a, schema 4, UTF-8,
version-valid-for 4
Found /home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fonto
logy%2Fv3%2Ftracker%23FileSystem.db: SQLite 3.x database, last written using SQLite
version 3037002, writer version 2, read version 2, file counter 13, database pages
349, 1st free page 349, free pages 1, cookie 0x12a, schema 4, UTF-8,
version-valid-for 13
Found /home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fonto
logy%2Fv3%2Ftracker%23Pictures.db: SQLite 3.x database, last written using SQLite
version 3037002, writer version 2, read version 2, file counter 2, database pages
316, cookie 0x12a, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fonto
logy%2Fv3%2Ftracker%23Software.db: SQLite 3.x database, last written using SQLite
version 3037002, writer version 2, read version 2, file counter 8, database pages
373, 1st free page 373, free pages 6, cookie 0x12a, schema 4, UTF-8,
version-valid-for 8
Found /home/prasad/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fonto
logy%2Fv3%2Ftracker%23Video.db: SQLite 3.x database, last written using SQLite
version 3037002, writer version 2, read version 2, file counter 2, database pages
316, cookie 0x12a, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/.cache/tracker3/files/meta.db: SQLite 3.x database, user version
26, last written using SQLite version 3037002, page size 8192, writer version 2,
read version 2, file counter 8, database pages 347, cookie 0x12d, schema 4, UTF-8,
version-valid-for 8
Found /home/prasad/.config/Code/databases/Databases.db: SQLite 3.x database, last
written using SQLite version 3039004, file counter 1, database pages 7, cookie 0x4,
schema 4, UTF-8, version-valid-for 1
Found /home/prasad/.config/google-chrome/Default/databases/Databases.db: SQLite 3.x
database, last written using SQLite version 3041002, file counter 1, database pages
7, cookie 0x4, schema 4, UTF-8, version-valid-for 1
Found /home/prasad/.config/google-chrome/Default/heavy_ad_intervention_opt_out.db:
SQLite 3.x database, last written using SQLite version 3041002, file counter 2,
database pages 4, cookie 0x2, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/.config/google-chrome/Profile
1/heavy_ad_intervention_opt_out.db: SQLite 3.x database, last written using SQLite
version 3041002, file counter 2, database pages 4, cookie 0x2, schema 4, UTF-8,
version-valid-for 2
Found /home/prasad/.local/share/evolution/addressbook/system/contacts.db: SQLite
3.x database, last written using SQLite version 3037002, file counter 30, database
pages 21, cookie 0x11, schema 4, UTF-8, version-valid-for 30
```

```
Found /home/prasad/.local/share/nautilus/tags/meta.db: SQLite 3.x database, user
version 26, last written using SQLite version 3037002, page size 8192, writer
version 2, read version 2, file counter 2, database pages 37, cookie 0x22, schema
4, UTF-8, version-valid-for 2
Found /home/prasad/.pki/nssdb/cert9.db: SQLite 3.x database, last written using
SQLite version 3037002, file counter 1, database pages 7, cookie 0x5, schema 4,
UTF-8, version-valid-for 1
Found /home/prasad/.pki/nssdb/key4.db: SQLite 3.x database, last written using
SQLite version 3037002, file counter 2, database pages 9, cookie 0x6, schema 4,
UTF-8, version-valid-for 2
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/cert9.db:
SQLite 3.x database, last written using SQLite version 3038003, page size 32768,
file counter 11, database pages 7, cookie 0x5, schema 4, UTF-8, version-valid-for
11
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/content-p
refs.sqlite: SQLite 3.x database, user version 5, last written using SQLite version
3041002, page size 32768, file counter 2, database pages 7, cookie 0x6, schema 4,
UTF-8, version-valid-for 2
Found
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/cookies.sqlite:
SQLite 3.x database, user version 12, last written using SQLite version 3038003,
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/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/favicons.
sqlite: SQLite 3.x database, last written using SQLite version 3038003, page size
32768, writer version 2, read version 2, file counter 5, database pages 11, cookie
0x6, schema 4, largest root page 8, UTF-8, vacuum mode 1, version-valid-for 5
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/formhisto
ry.sqlite: SQLite 3.x database, user version 5, last written using SQLite version
3038003, page size 32768, file counter 3, database pages 8, cookie 0x7, schema 4,
UTF-8, version-valid-for 3
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/key4.db:
SQLite 3.x database, last written using SQLite version 3038003, page size 32768,
file counter 4, database pages 9, cookie 0x6, schema 4, UTF-8, version-valid-for 4
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/permissio
ns.sqlite: SQLite 3.x database, user version 12, last written using SQLite version
3041002, page size 32768, file counter 12, database pages 3, cookie 0x2, schema 4,
UTF-8, version-valid-for 12
Found
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/places.sqlite:
SQLite 3.x database, user version 74, last written using SQLite version 3041002,
page size 32768, writer version 2, read version 2, file counter 4, database pages
44, cookie 0x2a, schema 4, UTF-8, version-valid-for 4
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/protectio
ns.sqlite: SQLite 3.x database, user version 1, last written using SQLite version
3038003, page size 32768, file counter 3, database pages 2, cookie 0x1, schema 4,
UTF-8, version-valid-for 3
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/d
efault/https+++account.protonvpn.com/ls/data.sqlite: SQLite 3.x database, user
version 80, last written using SQLite version 3038003, page size 1024, file counter
5, database pages 5, cookie 0x2, schema 4, largest root page 5, UTF-8, vacuum mode
1, version-valid-for 5
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/d
efault/https+++protonvpn.com/ls/data.sqlite: SQLite 3.x database, user version 80,
last written using SQLite version 3038003, page size 1024, file counter 4, database
pages 5, cookie 0x2, schema 4, largest root page 5, UTF-8, vacuum mode 1,
version-valid-for 4
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/d
efault/https+++www.google.com/ls/data.sqlite: SQLite 3.x database, user version 80,
last written using SQLite version 3038003, page size 1024, file counter 4, database
pages 30, cookie 0x2, schema 4, largest root page 5, UTF-8, vacuum mode 1,
version-valid-for 4
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/l
s-archive.sqlite: SQLite 3.x database, user version 2, last written using SQLite
version 3038003, page size 32768, file counter 4, database pages 4, cookie 0x3,
schema 4, UTF-8, version-valid-for 4
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/p
ermanent/chrome/idb/1451318868ntouromlalnodry--epcr.sqlite: SQLite 3.x database,
user version 416, last written using SQLite version 3038003, writer version 2, read
version 2, file counter 3, database pages 11, cookie 0xd, schema 4, largest root
page 11, UTF-8, vacuum mode 1, version-valid-for 3
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/p
ermanent/chrome/idb/1657114595AmcateirvtiSty.sqlite: SQLite 3.x database, user
version 416, last written using SQLite version 3038003, writer version 2, read
version 2, file counter 3, database pages 11, cookie 0xd, schema 4, largest root
page 11, UTF-8, vacuum mode 1, version-valid-for 3
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/p
ermanent/chrome/idb/2823318777ntouromlalnodry--naod.sqlite: SQLite 3.x database,
```

```
user version 416, last written using SQLite version 3038003, writer version 2, read
version 2, file counter 3, database pages 11, cookie 0xd, schema 4, largest root
page 11, UTF-8, vacuum mode 1, version-valid-for 3
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/p
ermanent/chrome/idb/2918063365piupsah.sqlite: SQLite 3.x database, user version
416, last written using SQLite version 3038003, writer version 2, read version 2,
file counter 3, database pages 11, cookie 0xd, schema 4, largest root page 11,
UTF-8, vacuum mode 1, version-valid-for 3
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/p
ermanent/chrome/idb/3561288849sdhlie.sqlite: SQLite 3.x database, user version 416,
last written using SQLite version 3038003, writer version 2, read version 2, file
counter 3, database pages 11, cookie 0xd, schema 4, largest root page 11, UTF-8,
vacuum mode 1, version-valid-for 3
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage/p
ermanent/chrome/idb/3870112724rsegmnoittet-es.sqlite: SQLite 3.x database, user
version 416, last written using SQLite version 3038003, writer version 2, read
version 2, file counter 25, database pages 2446, cookie 0xd, schema 4, largest root
page 11, UTF-8, vacuum mode 1, version-valid-for 25
Found
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage.sqlite:
SQLite 3.x database, user version 131075, last written using SQLite version
3041002, page size 512, file counter 12, database pages 8, cookie 0x4, schema 4,
UTF-8, version-valid-for 12
Found /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/webappsst
ore.sqlite: SQLite 3.x database, user version 2, last written using SQLite version
3038003, 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/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/12928FBA479206F56C3B36F6374E59B7327133831C9BE54
50E81174034543B5E/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 3, database pages
215, cookie 0xb, schema 4, UTF-8, version-valid-for 3
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/18BB90C4E7AEF442AB4C72596B96C589D20DB00AB14B073
CFBFCAD7276585A84/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/1A6651E4C0CCBC1D4D82498BBDFF192E0E8639E567A4098
193963661EEC76340/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/3096C503380E7414CE083C8180F4883BB787BC74B5FFCF5
2EF50FB2E68902DDB/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 3, database pages
11837, cookie 0xb, schema 4, UTF-8, version-valid-for 3
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/56902304CAE21DAE24D853AA667A15AACB895459D30747B
89428FF46F57C5035/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/7865B7E6B9D241D744D330EEC3B3A0FE4F9D36AF75D9629
1638504680F805BFD/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/83DEE90ACE06C285F2767CF49004C2CFCF4A22EA8F9D83C
A2889624B8AC2AA8A/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 3, database pages
534, 1st free page 314, free pages 5, cookie 0xb, schema 4, UTF-8,
version-valid-for 3
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/8EEB39BEB7EFF005C3D99B9BD7C643D35CE8E592778D1BB
75C36A44257B8ED13/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/A20C4D737EFFC2C2D3CF27A9999E4B95430B10DAADA9F60
3BAD9CFC4C1C6E6E1/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/AB8F0F16257B3B58FC31ABFB1880173D4FEDB8D4D9EBAD4
E912A19DAE362A590/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
```

```
exeddb/v1/https_web.whatsapp.com_0/C0DAE66D1136CA6CE2F2BAD1D37077AB75D076F50440EC6
64774EBDC8D0C6624/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 3, database pages
20290, 1st free page 2154, free pages 308, cookie 0xb, schema 4, UTF-8,
version-valid-for 3
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/databases/ind
exeddb/v1/https_web.whatsapp.com_0/D9279FBF58EC4B75ACA01DCD7B7B6FCAB53AB832C8F8453
B4247F4A80032C6C8/IndexedDB.sqlite3: SQLite 3.x database, last written using SQLite
version 3031001, writer version 2, read version 2, file counter 2, database pages
18, cookie 0xb, schema 4, UTF-8, version-valid-for 2
Found /home/prasad/snap/whatsapp-for-linux/57/.local/share/webkitgtk/serviceworker
s/ServiceWorkerRegistrations-8.sqlite3: SQLite 3.x database, last written using
SQLite version 3031001, writer version 2, read version 2, file counter 2, database
pages 4, cookie 0x1, schema 4, UTF-8, version-valid-for 2
Found /var/lib/colord/mapping.db: SQLite 3.x database, last written using SQLite
version 3037002, file counter 3, database pages 4, cookie 0x2, schema 4, UTF-8,
version-valid-for 3
Found /var/lib/colord/storage.db: SQLite 3.x database, last written using SQLite
version 3037002, file counter 3, database pages 7, cookie 0x3, schema 4, UTF-8,
version-valid-for 3
Found /var/lib/command-not-found/commands.db: SQLite 3.x database, last written
using SQLite version 3037002, file counter 5, database pages 824, cookie 0x4,
schema 4, UTF-8, version-valid-for 5
Found /var/lib/fwupd/pending.db: SQLite 3.x database, last written using SQLite
version 3037002, file counter 3, database pages 7, cookie 0x5, schema 4, UTF-8,
version-valid-for 3
Found /var/lib/PackageKit/transactions.db: SQLite 3.x database, last written using
SQLite version 3037002, file counter 91, database pages 8, cookie 0x4, schema 4,
UTF-8, version-valid-for 91
-> Extracting tables from /home/prasad/.cache/tracker3/files/meta.db (limit 20)
--> Found interesting column names in nco:Role_nco:hasEmailAddress (output limit
10)
CREATE TABLE "nco:Role_nco:hasEmailAddress" (ID INTEGER NOT NULL,
"nco:hasEmailAddress" INTEGER NOT NULL)
--> Found interesting column names in nco:EmailAddress (output limit 10)
CREATE TABLE "nco:EmailAddress" (ID INTEGER NOT NULL PRIMARY KEY,
"nco:emailAddress" TEXT COLLATE TRACKER UNIQUE)
--> Found interesting column names in nco:VoicePhoneNumber (output limit 10)
CREATE TABLE "nco:VoicePhoneNumber" (ID INTEGER NOT NULL PRIMARY KEY,
"nco:voiceMail" INTEGER)
--> Found interesting column names in nfo:FileDataObject (output limit 10)
CREATE TABLE "nfo:FileDataObject" (ID INTEGER NOT NULL PRIMARY KEY,
"nfo:fileLastAccessed" INTEGER, "nfo:fileCreated" INTEGER, "nfo:fileSize" INTEGER,
"nfo:permissions" TEXT COLLATE TRACKER, "nfo:fileName" TEXT COLLATE TRACKER,
"nfo:hasHash" INTEGER, "nfo:fileOwner" INTEGER, "nfo:fileLastModified" INTEGER,
"tracker:extractorHash" TEXT COLLATE TRACKER)
--> Found interesting column names in nfo:FileHash (output limit 10)
CREATE TABLE "nfo:FileHash" (ID INTEGER NOT NULL PRIMARY KEY, "nfo:hashValue" TEXT
COLLATE TRACKER, "nfo:hashAlgorithm" TEXT COLLATE TRACKER)
--> Found interesting column names in nfo:ArchiveItem (output limit 10)
CREATE TABLE "nfo:ArchiveItem" (ID INTEGER NOT NULL PRIMARY KEY,
"nfo:isPasswordProtected" INTEGER)
--> Found interesting column names in fts5 (output limit 10)
CREATE VIRTUAL TABLE fts5 USING fts5(content="fts_view", "nao:description",
"nao:prefLabel", "nco:department", "nco:role", "nco:title", "nco:fullname",
"nco:nickname", "nco:contactGroupName", "nco:note", "nco:emailAddress", "nco:imID",
"nco:imNickname", "nco:nameAdditional", "nco:nameFamily", "nco:nameGiven",
"nco:phoneNumber", "nco:country", "nco:county", "nco:district",
"nco:extendedAddress", "nco:locality", "nco:pobox", "nco:postalcode", "nco:region",
"nco:streetAddress", "nfo:tableOfContents", "nfo:fileName", "nfo:fontFamily",
"nfo:genre", "nmm:genre", "nie:comment", "nie:description", "nie:plainTextContent",
"nie:subject", "nie:title", "nie:keyword", "nmm:artistName", "nmm:category",
tokenize=TrackerTokenizer)
-> Extracting tables from
/home/prasad/.config/google-chrome/Default/databases/Databases.db (limit 20)
-> Extracting tables from
/home/prasad/.config/google-chrome/Default/heavy_ad_intervention_opt_out.db (limit
20)
-> Extracting tables from
/home/prasad/.local/share/evolution/addressbook/system/contacts.db (limit 20)
--> Found interesting column names in folder_id_email_list (output limit 10)
CREATE TABLE 'folder_id_email_list' (uid TEXT NOT NULL REFERENCES 'folder_id'
(uid), value TEXT)
-> Extracting tables from /home/prasad/.local/share/nautilus/tags/meta.db (limit
20)
-> Extracting tables from /home/prasad/.pki/nssdb/cert9.db (limit 20)
-> Extracting tables from /home/prasad/.pki/nssdb/key4.db (limit 20)
-> Extracting tables from
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/cert9.db (limit
```

```
20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/content-prefs.sqlite (limit 20)
-> Extracting tables from
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/cookies.sqlite
(limit 20)
-> Extracting tables from
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/favicons.sqlite
(limit 20)
--> Found interesting column names in moz_icons (output limit 10)
CREATE TABLE moz_icons ( id INTEGER PRIMARY KEY, icon_url TEXT NOT NULL,
fixed_icon_url_hash INTEGER NOT NULL, width INTEGER NOT NULL DEFAULT 0, root
INTEGER NOT NULL DEFAULT 0, color INTEGER, expire_ms INTEGER NOT NULL DEFAULT 0,
data BLOB )
1, fake-favicon-uri:https://support.mozilla.org/products/firefox, 136573370287311,
32, 0, None, 1690169231834, b'\x89PNG\r\n\x1a\n\x00\x00\x00\rIHDR\x00\x00\x00
\x00\x00\x00 \x08\x06\x00\x00\x00szz\xf4\x00\x00\x07cIDATx\x01\xad\xd5\x03\x94kI\x
d7\xc6\xf1\xff\xae:\'I\xa7\xfb\xa6s9\xb6}\xf1al\xdb\xc6\xf7\xbd\xb6m\xdb\xf6\xd8\x
b6m\xfbr<\xd7\xed8\x07U\xef~\x93\xe6X{\xad\xdf)4\xea\xc9\xae\xb3Vx/\xcb\x97\x0e\xf
e\x8c\x1f:h\xc0\x0f\x1eXT\xbc\x15\xa6=yO\x9c\n\xfcZ\x15\xf1|[\xf1V\x18<\xbck\xa9\x
fb\x0c\xce\xff\x1f\xde\x83Gy]\xbbC\x15o\xc6\xb4\'\xefB#Z\x97$\xfduk\xee\xfd\x18\xe
7O\xd5\xfdu\x15o\xc4\xb4\'\xefB\x9c|\x9b8\x85\xc4\xc1\xc4\x10Eu)\x89+*^\x8fy\xadMn
z\xec\xff\xb8s\xee\xad\x8aQ\x0b*E\xc5\x04\xfd\xe5ui\xc6\xff\xa7!P\xed\xbfM\xdd\xf8
.\xcc\xd4\xf1V\xc5\xeb1\xaf\xda\xbcX\x0fo\xa4\xa7\xbaF<[\xa1 ^\xfb3\xae\xcc\xe3\x8
a\xf1\xf4\xf0]\x15-\x91J\xd2\xb6\xd4\x81\x1b}\x1ff\x92\xfaS\x91\xceu1\x9d3\x15\xe3
\x99\t\x1b\xa7\xcd=\x94\x86\x9cJ\x1dL\x9c\x14\x14f\xe9\x86\xa7R\x96_\xc7\xfd,V\x8c
G=\xdaF1J\x83\xb4\xbb1\x1c\xc2\x8ft\x83\xffk\x94\xaaG\xa4)\x97\xe3\xddL\xc5\x083\x
ba\xf8\xed\x13E"{*\xb1\x85\x86@\xddA\xa9\xf0(\xd4\xb5#\x11\xd9\x8a\xe4\x15\xd7\xfe
\xfe\xcc\xe2\xf5\x7f<\xfb37\xfe\xe9\xdcK\x1f\xfc\xd7\xf7\xfe\xef\xf1\xf3>\xcb\xbc\
xabOb\xf0\xc5\rp%\x07Q2&q\xe0\x00/\xe4B\xf9E\xb5\x9c\xcc\xc7\xb9K\xf1IQ\x81\nZ\x13
\x80\xc4\xfe\x1a\xe3\x8b\x8a\x96\x86\xca\x0f\xce\xa4\xbb\x84\xfe5H\xe7\xcc\x07o\xf
c\xecw\x10\xf9\xb4\x15[\x0c\xc408\xf7\xbf\xf1@\xea\x1d\x8b\xae<\x98\xc2fs\xf9\x9f\
x0f\xfe\x99\xfc\x94>\x10\x03F\xd9\x00h\x87\xe8\xb2\xe9\xb6\xdeIA\xc4\x7f\x1b\xf8\x
ac\xc2~\xe73\x1b\xc2\x0f^.\x02\xe7!\xd0\xc2\xf0\xe8=\x88B\x05)3\xd6\x7fr\xd7\xe5\x
8bw\xccE\xcdU1\xc6b\x11\x8c\x12\x01Tu\xc5d^|hKV\xdd\xecq\xb2\x9d\x15\xf0\x06\x9c\x
f2\nA\x9cd\x01D\xdc\xa6\x90\xfe\x15\\\xa3\xdd\x81\xd8\xfc\x1fbA\xfc8\x0cW\n\xde\x0
11av\x80\x9d\x8f\xfc\x18\xf3\x1e\xfe\x18\xcf?v<\x89\xf3Xe\x9c#\xd3Qg\xc7o\xfd\x10\
x97$TzV\xa5\x10\xf7\x02\x1e\xcc\x08@\x04I=\xde\xb8\xa2\x18\x7f(pZ\x80\xf7\x10\x07\
xbb \x80x\x08Tw\x0c\xd3\x052Ye\x00\xa0\xd6\x84\xba\x86\xc8\xf5\xb3\xf5v?e\xc3Y\xe7
2\xf7\xa1\x8f\xf2\xd2\xd3\x07b\x9d\x83\xb8\xc0\xcd_\xfe\x1e\xb3\xde\xffg\xd6\xdd\x
e9Np\x16\x06=8e\x00;,TN\xc0\xcb.\xed\x00\xa9\x81\xc8\xee\n\x1e\x00\xb2\x0eVkB&\x80
\xd0\xea\xa8t\xce\xb4<\x88\x80\xf3\xca\x91\x9f\xdcd\xeb-\xced\xfe7\x0e#p\x0eI\x04\
xefR\x1e<\xf3X\xa6m\xf0$]\xd3z!\x0f\xf4Y\x00\xb0\xa2\x80\x8c\x07k\x00f*\x02\x92V\x
80"\x02-\x95\x0c,\xec\x82\x8d\x1b`\x1d8\x95*#\x10\x06\x90\x0f!\x13\xb2d\xd9\x7fs\x
cfu\x9f\xa2\xae\xf3 M1xH\x05W\xef\xe4\x91\x0b\xf7c\xe7\xf7\xff\x0b\xa0\xfdw\x95\x1
0,\x10\x08\x14\x12H,\x88m\x07X6k\xcb\x99\xab\xed~/\x08\x80W\xc0\x92N\xe8\xcf\xc2\x
aa\x11l\x98\xc2$\xc7@y\x15n{\xe8\xffX\xb8xOb7\x8d\xc0\x84\x84\xde\x12\x86`\xc5a\x1
d\x88\x01p\xbc8wCh\xc6\x00`\x1cT\xf3`\x05\x02\x03\xd2\x84z\x1e\x8c\x01 PEb\xcbhyQ\
xb4\xbd,\xb0Z\x8d\xfeh2\xbf:\xeb\x074\xc2U\x90\xbcA25\x02\x9b!\xc4\x92\xc1\x90M!\x
f0\x0e\xe3SP\xf5\x95\xdd\xd0\x88\x01\x01\x07T\x0c\x04\x16\xa64!q\xf8\xba\x80(
\xb8;S\x9b{\xc8P\x17aw\x05\x00\xfc\xf8 \xaal\xb8\xf7\xf9\xff\xa6\xbf\xea\xf1\x93*\
xe0<\xe2\x13\x024@\xebi\x89=d]J\x90F\xa0\xbc\xa2\x16\x83\xcb@j\xa0l\xf19A:\xab\xd0
\xf00\x18\x8e\xbe\xdc\xe6\xe4\xe2\xe2\xdeh\xa0\x00Q0\xa69\xce\x0b9\x8a\x85\x95\xd4
\x93*\xf5\xb8L-.\xa92\xd5\xa4\xad6N#\xaa\x11E\rV[\xeb)\x1820hu\x0cp\xe5\x10\neH\x1
2\xa8\n\xbebi\x96\xcc\\E\xd0\xff\x0b\xebV|\xa4x_\xe7\xf4\xbem\xf1\xd0&mN-\xcb\xb3\
xc3\x86\x0fqa\xf7\xfe\xac\xacM\xc7\x9b\x14|\x84I3\xa4\x84\xb8\xd4\xa2K|3\xc5E\tV\x
03l\xb5\xe1\xbd\xd0\x9f\x01\x17\xe2\x1byd\xca@\xeb\xda\xa8[\\\x94\xd1Q\x90@\x9e\x0
30\xa2\x8bF#{[\xad\xb7\x08\xb1\x1d\xee\x82\x9d\xd8\x85\xbb\xa7\xf3\xd9}\xfeJ>\xa8
\xd5\x1a\x94+\xb8r\x89\xa86\xa4\x06i\xea\xd8\xac\x97h6J\xac5\xf5)f\xae\xfa(\xf4f\x
a0/\x83\x04u$[\x85\x9a(p=9\x1d\r\x03}r\x8d\xc2\xe8\x83\'\xc2\xe8\xec\xd2\xcai\x10\
xb7\x0eW\xe3GU\xcd\xb0\xce\xfd\x9eo\xee\xf8\'\xa6O\xeaA\x9a\xcd\xe1 e\x92j\x89\xa4
V&\x8e\xaal6\xf91N\xdc\xe2,X\x99\x85!\x0b\xb6\ti\x0cU\x81\x8a\xe0K\x16\xb7\xb2\x03
_\xb5\xdc0\xdf_\xae\xb0[\xaf\xbb)\x1fX<\xd4\xff\x81\xf2\xb4\xbd%\x955s\xf9&\xe2\x0
1\'\x13\xaf"\xb1\x14W:vY\xe7AVO\xfb\x01(\xda\n\xd3\xec\x00\x9b\xe5^\xe0\xd8\x19\xd
7\xb1W\xf1\x1e\xc2\xc4\x81\xf1\x90M\x86\xff\xd6BjZ\x92\x95\xddP\xcb3X\x97\x8b\xf6\
xbc<:\xed\xaag\x9c\x97\x8eu\x0f\x02\xe0\xf2\x81\xb5\x0e\xd9\xcc\x99\xcb\n\xab\xf6\
xd0\xd5]\xc1\x98\x14\xec\x7f8\x08|{\x9c\xc0\x83q (\xaf\x00;|x\x00\xe4\x04\xb2F\xb5
\xc74\xc9\xd1\xec\x99N\xd0\x11pE\x7f<\x13x\\\x11\x9c\xb1m\x0e\x80C\xee{\xf9\xfa\xf
b\xfa\xd6\xfd\x97_1\xe5}\x1e\xe8*\xd41.A\\\n\xa9\x03+\xca\x8c\x1d\xd2\x1e\xc7\x88\
x123\x16\xa8)\x90mK\xc9P\xd7\xc3m&\xc3\xd2\x9a\xff\xcd\xc9\xf77\x9ef\xb8F;\x00\xf0
\x99\xea\xd4u>X/\\cMs\xf3\xaei%\n\xdd\r\xc4$\xadn\x88\xa4c\x9f\xba}\xe8\xc4\xb9\xf
0\xeao\xd2\x10\x122TV\xce \xc8f\x89rr\xdf\x9a\x0b\xfa\xf6\x03\x06\x19.\x1b\x167a\x
a4\xee\xcb\xd4\xcb\x03\xe2o\xda)\xee\xda=\xa9\x87\xd3kMC&\x0b"\x06\x8f\x01\'\xca \
xadQ\xa5\x16\x9ciKGXH\x94\xce\xab+\nT_\x9a\x81\x89;\x88\xd3`\xee\xf7\x86\xaa\xc7\x
cc\xc9\x84K\x15#\x82\x0fv\xe5\x19W\xee\xef\x0c-\x02\x0e\xffFu\xea%R3\x9b/_\x1c\x92
\xebj0\xa9\x10\x91\xcd\xa4\x88Q\xce!2\xc2\xc3(\x94\xa7V\xcdR\x1b\x98DZ\xeb\xc4\xfa
\x0c\xcd\xd0\xcc\xfdv\xd4\x7f\xf8\x19\xbe\xf6,\xa35\xfe\n^]\xe6\xf8z\xf7F\x9f\xaeM
\xfe\xd2\x14x_*1\xa9\x89\x90 &\x93K\x08\xc2\x94\x8e\x9c\x03q\x08\xbe\x15\xa2\xd1\x
08\x88\x9b\xaa\xd1\x81\xa4!\xd6)\x1f\xb0\xc2\xb8\xdf\xfco\xf1\x85\x9f\x01+\x94{\xa
```

```
b\x01\x00\x8c\xea>cp\x8d\xbdg%\xd9\xcf\xe4\xf0\xdb:\x93\xe0$\xc5\xe3Z\x10\xc0\x0b\
x82`\xbcE\x94i\t(\x89\xbf\xe8\xfc\xdc\xd0o~\xd2\xd5\xf3\xf4\xf8;\x7f\xeb\x01\xc6*\
xa7\xba\xbf\\\x99\xbe\xe1\xbe\xcd\xce\xbd\xa7y\xbbw\x87g[\xc4\xe3\x01\xa1\x1d\xc2a
J\x11\xcc\xed\x91\xf4\x86\xeb\xb2\x95\x1b~:i\xe5|`H%\x8aw\x11`\xb4\x02\x95W\x1d*\x
c7\xab\xcb\xa9H\xd5UM%\xbc\x85\xfa7i\xf2\x03\xc6\xe0M<\x98\x00\x00\x00\x00IEND\xae
B`\x82'
--> Found interesting column names in moz_pages_w_icons (output limit 10)
CREATE TABLE moz_pages_w_icons ( id INTEGER PRIMARY KEY, page_url TEXT NOT NULL,
page_url_hash INTEGER NOT NULL )
1, https://support.mozilla.org/products/firefox, 47358327123126
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/formhistory.sqlite (limit 20)
-> Extracting tables from
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/key4.db (limit
20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/permissions.sqlite (limit 20)
-> Extracting tables from
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/places.sqlite
(limit 20)
--> Found interesting column names in moz_places (output limit 10)
CREATE TABLE moz_places ( id INTEGER PRIMARY KEY, url LONGVARCHAR, title
LONGVARCHAR, rev_host LONGVARCHAR, visit_count INTEGER DEFAULT 0, hidden INTEGER
DEFAULT 0 NOT NULL, typed INTEGER DEFAULT 0 NOT NULL, frecency INTEGER DEFAULT -1
NOT NULL, last_visit_date INTEGER , guid TEXT, foreign_count INTEGER DEFAULT 0 NOT
NULL, url_hash INTEGER DEFAULT 0 NOT NULL , description TEXT, preview_image_url
TEXT, site_name TEXT, origin_id INTEGER REFERENCES moz_origins(id), recalc_frecency
INTEGER NOT NULL DEFAULT 0, alt_frecency INTEGER, recalc_alt_frecency INTEGER NOT
NULL DEFAULT 0)
1, https://support.mozilla.org/products/firefox, None, gro.allizom.troppus., 0, 0,
0, 140, None, i4HGZJx-9DTE, 1, 47358327123126, None, None, None, 1, 0, None, 0
--> Found interesting column names in moz_previews_tombstones (output limit 10)
CREATE TABLE moz_previews_tombstones ( hash TEXT PRIMARY KEY ) WITHOUT ROWID
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/protections.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/default/https+++account.protonvpn.com/ls/data.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/default/https+++protonvpn.com/ls/data.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/default/https+++www.google.com/ls/data.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/ls-archive.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/permanent/chrome/idb/1451318868ntouromlalnodry--epcr.sqlite
(limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/permanent/chrome/idb/2823318777ntouromlalnodry--naod.sqlite
(limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/permanent/chrome/idb/2918063365piupsah.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/permanent/chrome/idb/3561288849sdhlie.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.sqlite (limit 20)
-> Extracting tables from
/home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8u1.default/storage.sqlite
(limit 20)
-> Extracting tables from /home/prasad/snap/firefox/common/.mozilla/firefox/eqwqc8
u1.default/webappsstore.sqlite (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/12928FBA479206F56C3B36F6374
E59B7327133831C9BE5450E81174034543B5E/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/18BB90C4E7AEF442AB4C72596B9
6C589D20DB00AB14B073CFBFCAD7276585A84/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/1A6651E4C0CCBC1D4D82498BBDF
F192E0E8639E567A4098193963661EEC76340/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/3096C503380E7414CE083C8180F
4883BB787BC74B5FFCF52EF50FB2E68902DDB/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/56902304CAE21DAE24D853AA667
A15AACB895459D30747B89428FF46F57C5035/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/7865B7E6B9D241D744D330EEC3B
```

```
3A0FE4F9D36AF75D96291638504680F805BFD/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/83DEE90ACE06C285F2767CF4900
4C2CFCF4A22EA8F9D83CA2889624B8AC2AA8A/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/8EEB39BEB7EFF005C3D99B9BD7C
643D35CE8E592778D1BB75C36A44257B8ED13/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/A20C4D737EFFC2C2D3CF27A9999
E4B95430B10DAADA9F603BAD9CFC4C1C6E6E1/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/AB8F0F16257B3B58FC31ABFB188
0173D4FEDB8D4D9EBAD4E912A19DAE362A590/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/C0DAE66D1136CA6CE2F2BAD1D37
077AB75D076F50440EC664774EBDC8D0C6624/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/databases/indexeddb/v1/https_web.whatsapp.com_0/D9279FBF58EC4B75ACA01DCD7B7
B6FCAB53AB832C8F8453B4247F4A80032C6C8/IndexedDB.sqlite3 (limit 20)
-> Extracting tables from /home/prasad/snap/whatsapp-for-linux/57/.local/share/web
kitgtk/serviceworkers/ServiceWorkerRegistrations-8.sqlite3 (limit 20)
-> Extracting tables from /var/lib/colord/mapping.db (limit 20)
-> Extracting tables from /var/lib/colord/storage.db (limit 20)
-> Extracting tables from /var/lib/command-not-found/commands.db (limit 20)
-> Extracting tables from /var/lib/fwupd/pending.db (limit 20)
-> Extracting tables from /var/lib/PackageKit/transactions.db (limit 20)
```

All relevant hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)

```
-rw------- 1 root root 0 Jul 31 01:17 /run/snapd/lock/.lock
-rw------- 1 prasad prasad 130 Jul 31 2023
/run/user/1000/.mutter-Xwaylandauth.USD881
-rw-rw---- 1 prasad prasad 0 Jul 31 2023
/home/prasad/.cache/tracker3/files/.meta.isrunning
-rw------- 1 prasad prasad 24 Jul 17 16:37
/home/prasad/.config/google-chrome/Default/File System/000/t/.usage
-rw-rw---- 1 prasad prasad 0 Jul 31 12:53
/home/prasad/.local/share/nautilus/tags/.meta.isrunning
-rw-r--r-- 1 prasad prasad 220 Jul 17 03:19 /home/prasad/.bash_logout
-rw-rw-r-- 1 prasad prasad 262 Jul 20 15:29 /home/prasad/.wget-hsts
-rw-rw-r-- 1 prasad prasad 30 Jul 18 11:11
/home/prasad/snap/whatsapp-for-linux/57/.last_revision
-rw-rw-r-- 1 prasad prasad 31 Jul 16 22:16
/home/prasad/snap/snap-store/959/.last_revision
-rw-rw-r-- 1 prasad prasad 31 Jul 16 22:16
/home/prasad/snap/snap-store/638/.last_revision
-rw-rw-r-- 1 prasad prasad 32 Jul 17 08:57
/home/prasad/snap/firefox/2356/.last_revision
-rw-rw-r-- 1 prasad prasad 32 Jul 20 14:20
/home/prasad/snap/firefox/2908/.last_revision
-rw-rw-r-- 1 prasad prasad 30 Jul 17 08:54
/home/prasad/snap/snapd-desktop-integration/49/.last_revision
-rw-rw-r-- 1 prasad prasad 30 Jul 17 08:54
/home/prasad/snap/snapd-desktop-integration/83/.last_revision
-r--r--r-- 1 prasad prasad 11 Jul 31 2023 /tmp/.X0-lock
-r--r--r-- 1 gdm gdm 11 Jul 31 01:17 /tmp/.X1024-lock
-r--r--r-- 1 prasad prasad 11 Jul 31 2023 /tmp/.X1-lock
-r--r--r-- 1 gdm gdm 11 Jul 31 01:17 /tmp/.X1025-lock
-rw-r--r-- 1 root root 0 Dec 2 2021
/usr/share/dictionaries-common/site-elisp/.nosearch
-rw------- 1 root root 0 Feb 23 09:27 /etc/.pwd.lock
-rw-r--r-- 1 root root 220 Jan 6 2022 /etc/skel/.bash_logout
-rw-r--r-- 1 root root 0 Nov 15 2018
/snap/gnome-3-38-2004/143/usr/share/dictionaries-common/site-elisp/.nosearch
-rw-r--r-- 1 root root 0 Nov 15 2018
/snap/gnome-3-38-2004/119/usr/share/dictionaries-common/site-elisp/.nosearch
-rw-r--r-- 1 root root 0 Dec 2 2021
/snap/snap-store/959/usr/share/dictionaries-common/site-elisp/.nosearch
-rw-r--r-- 1 root root 0 Nov 15 2018
/snap/snap-store/638/usr/share/dictionaries-common/site-elisp/.nosearch
-rw------- 1 root root 0 Jun 22 10:03 /snap/core20/1974/etc/.pwd.lock
-rw-r--r-- 1 root root 220 Feb 25 2020 /snap/core20/1974/etc/skel/.bash_logout
```

```
-rw------- 1 root root 0 Jan 26 2023 /snap/core20/1822/etc/.pwd.lock
-rw-r--r-- 1 root root 220 Feb 25 2020 /snap/core20/1822/etc/skel/.bash_logout
-rw------- 1 root root 0 Jul 3 10:23 /snap/core22/817/etc/.pwd.lock
-rw-r--r-- 1 root root 220 Jan 6 2022 /snap/core22/817/etc/skel/.bash_logout
```

Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)

```
-r--r--r-- 1 prasad prasad 11 Jul 31 2023 /tmp/.X0-lock
-r--r--r-- 1 gdm gdm 11 Jul 31 01:17 /tmp/.X1024-lock
-r--r--r-- 1 prasad prasad 11 Jul 31 2023 /tmp/.X1-lock
-r--r--r-- 1 gdm gdm 11 Jul 31 01:17 /tmp/.X1025-lock
-rw-r--r-- 1 root root 11 Jul 17 03:18 /var/backups/dpkg.arch.0
-rw-r--r-- 1 root root 61440 Jul 21 00:26 /var/backups/alternatives.tar.0
```

Searching passwords in history files

```
sudo apt-get install -f
sudo dpkg-configure -a
sudo apt-get update
sudo apt-get install aptitude
sudo apt-get -u dist-upgrade
sudo apt-get remove docker-engine docker.io
sudo apt-get update
sudo apt install docker.io
sudo snap install docker
sudo docker run hello-world
sudo apt-get install ./docker-desktop-<23.0.3>-<arch>.deb
sudo apt-get install docker
sudo cp/etc/apt/sources.list/etc/apt/sources.list.original
sudo dpkg configure -a
sudo apt-get insatll openvpn
sudo apt-get install openvpn
sudo openvpn --config /etc/openvpn/client.conf
sudo apt install openvpn -y
sudo nano /etc/openvpn/client.conf
sudo apt install openvpn easy-rsa
sudo chown prasad ~/easy-rsa
sudo cp /home/prasad/easy-rsa/pki/private/server.key /etc/openvpn/server/
sudo sysctl -w vm.max_map_count=262144
sudo apt openvpn
sudo apt-get openvpn
sudo apt install openvpn
sudo apt install openvpn resolvconfig
sudo apt install openvpn resolvconf
sudo openvpn nl-free-138.protonvpn.net.udp.ovpn
sudo sysctl -w vm.max_map_count=262144
sudo apt install openvpn resolvconf
sudo open nl-free-138.protonvpn.net.udp.ovpn
sudo apt install openvpn resolvconf
sudo open nl-free-138.protonvpn.net.udp.ovpn
sudo apt install openvpn resolvcof
sudo openvpn nl-free-138.protonvpn.net.udp.ovpn
sudo apt install openvpn resolvcof
sudo openvpn nl-free-138.protonvpn.net.udp.ovpn
sudo apt install openvpn resolvcof
sudo openvpn nl-free-79.protonvpn.net.udp.ovpn
sudo apt install openvpn resolvconf
sudo openvpn nl-free-79.protonvpn.net.udp.ovpn
sudo apt update
sudo apt upgrade
sudo apt upgrade
sudo dpkg -i protonvpn-stable-release_1.0.3_all.deb
sudo apt update
sudo apt install protonvpn
sudo sysctl -w vm.max_map_count=262144
```

```
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo apt-get update
sudo apt-get install ./docker-desktop-4.21.1-amd64.deb
sudo apt --fix-broken install ./docker-desktop-4.21.1-amd64.deb
sudo sysctl -w vm.max_map_count=262144
sudo apt-get install ./docker-desktop-4.21.1-amd64.deb
sudo sysctl -w vm.max_map_count=262144
sudo apt-get install ./docker-desktop-4.21.1-amd64.deb
sudo apt-get update
sudo apt-get install ca-certificates curl gnupg lsb-release
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
echo "deb [arch=$(dpkg --print-architecture)
signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list >
/dev/null
sudo apt update
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin
sudo apt-get install ./docker-desktop-4.21.1-amd64.deb
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo snap install whatsapp-for-linux
sudo sysctl -w vm.max_map_count=262144
sudo sysctl -w vm.max_map_count=262144
sudo nano resolv.conf
sudo apt install ./<file>.deb
sudo apt-get install wget gpg
sudo install -D -o root -g root -m 644 packages.microsoft.gpg
/etc/apt/keyrings/packages.microsoft.gpg
sudo sh -c 'echo "deb [arch=amd64,arm64,armhf
signed-by=/etc/apt/keyrings/packages.microsoft.gpg]
https://packages.microsoft.com/repos/code stable main" >
/etc/apt/sources.list.d/vscode.list'
sudo apt install apt-transport-https
sudo apt update
sudo dnf install code
sudo apt install code
sudo apt-get clean
sudo apt install ./code_1.80.1-1689183569_amd64.deb -y
```

Searching *password* or *credential* files in home (limit 70)

```
/etc/brlapi.key
/etc/openvpn/server/server.key
/etc/pam.d/common-password
/etc/pam.d/gdm-password
/etc/pam.d/gdm-smartcard-sssd-or-password
/home/prasad/.config/google-chrome/ZxcvbnData/3/passwords.txt
/opt/docker-desktop/bin/docker-credential-pass
```

Searching passwords inside logs (limit 70)

```
2023-02-23 03:57:14 configure base-passwd:amd64 3.5.52build1 3.5.52build1
2023-02-23 03:57:14 install base-passwd:amd64 <none> 3.5.52build1
2023-02-23 03:57:14 status half-configured base-passwd:amd64 3.5.52build1
2023-02-23 03:57:14 status half-installed base-passwd:amd64 3.5.52build1
2023-02-23 03:57:14 status installed base-passwd:amd64 3.5.52build1
2023-02-23 03:57:14 status unpacked base-passwd:amd64 3.5.52build1
2023-02-23 03:57:16 status half-configured base-passwd:amd64 3.5.52build1
2023-02-23 03:57:16 status half-installed base-passwd:amd64 3.5.52build1
```

```
2023-02-23 03:57:16 status unpacked base-passwd:amd64 3.5.52build1
2023-02-23 03:57:16 upgrade base-passwd:amd64 3.5.52build1 3.5.52build1
2023-02-23 03:57:18 configure base-passwd:amd64 3.5.52build1 <none>
2023-02-23 03:57:18 install passwd:amd64 <none> 1:4.8.1-2ubuntu2
2023-02-23 03:57:18 status half-configured base-passwd:amd64 3.5.52build1
2023-02-23 03:57:18 status half-installed passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:18 status installed base-passwd:amd64 3.5.52build1
2023-02-23 03:57:18 status unpacked base-passwd:amd64 3.5.52build1
2023-02-23 03:57:18 status unpacked passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:20 configure passwd:amd64 1:4.8.1-2ubuntu2 <none>
2023-02-23 03:57:20 status half-configured passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:20 status installed passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:20 status unpacked passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:46 configure passwd:amd64 1:4.8.1-2ubuntu2.1 <none>
2023-02-23 03:57:46 status half-configured passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:46 status half-configured passwd:amd64 1:4.8.1-2ubuntu2.1
2023-02-23 03:57:46 status half-installed passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:46 status installed passwd:amd64 1:4.8.1-2ubuntu2.1
2023-02-23 03:57:46 status unpacked passwd:amd64 1:4.8.1-2ubuntu2
2023-02-23 03:57:46 status unpacked passwd:amd64 1:4.8.1-2ubuntu2.1
2023-02-23 03:57:46 upgrade passwd:amd64 1:4.8.1-2ubuntu2 1:4.8.1-2ubuntu2.1
[ 2.362237] systemd[1]: Started Forward Password Requests to Wall Directory Watch.
[ 2.446830] systemd[1]: Started Forward Password Requests to Wall Directory Watch.
base-passwd depends on libc6 (>= 2.34); however:
base-passwd depends on libdebconfclient0 (>= 0.145); however:
dpkg: base-passwd: dependency problems, but configuring anyway as you requested:
Installing new version of config file /etc/pam.d/gdm-smartcard-sssd-or-password ...
Jul 16 21:36:03 ubuntu kernel: [ 21.087512] systemd[1]: Started Forward Password
Requests to Wall Directory Watch.
Jul 16 21:36:03 ubuntu systemd[1]: Condition check resulted in Dispatch Password
Requests to Console Directory Watch being skipped.
Jul 16 21:36:03 ubuntu systemd[1]: Started Forward Password Requests to Plymouth
Directory Watch.
Jul 16 21:49:32 ubuntu ubiquity: BAD PASSWORD: The password is shorter than 8
characters
Jul 16 21:49:32 ubuntu user-setup: Shadow passwords are now on.
Jul 16 22:03:34 prasad-Aspire-A315-23 kernel: [ 2.111339] systemd[1]: Started
Forward Password Requests to Wall Directory Watch.
Jul 16 22:03:34 prasad-Aspire-A315-23 systemd[1]: Condition check resulted in
Dispatch Password Requests to Console Directory Watch being skipped.
Jul 16 22:03:34 prasad-Aspire-A315-23 systemd[1]: Started Forward Password Requests
to Plymouth Directory Watch.
Jul 16 22:03:45 prasad-Aspire-A315-23 gdm-password]: gkr-pam: stashed password to
try later in open session
Jul 16 22:03:45 prasad-Aspire-A315-23 gdm-password]: gkr-pam: unable to locate
daemon control file
Jul 16 22:03:45 prasad-Aspire-A315-23 gdm-password]:
pam_unix(gdm-password:session): session opened for user prasad(uid=1000) by (uid=0)
Jul 16 22:03:46 prasad-Aspire-A315-23 gdm-password]: gkr-pam: gnome-keyring-daemon
started properly and unlocked keyring
Jul 17 08:53:48 prasad-Aspire-A315-23 kernel: [ 2.325411] systemd[1]: Started
Forward Password Requests to Wall Directory Watch.
Jul 17 08:53:48 prasad-Aspire-A315-23 systemd[1]: Condition check resulted in
Dispatch Password Requests to Console Directory Watch being skipped.
Jul 17 08:53:48 prasad-Aspire-A315-23 systemd[1]: Started Forward Password Requests
to Plymouth Directory Watch.
Jul 17 08:54:23 prasad-Aspire-A315-23 gdm-password]: gkr-pam: gnome-keyring-daemon
started properly and unlocked keyring
Jul 17 08:54:23 prasad-Aspire-A315-23 gdm-password]: gkr-pam: stashed password to
try later in open session
Jul 17 08:54:23 prasad-Aspire-A315-23 gdm-password]: gkr-pam: unable to locate
daemon control file
Jul 17 08:54:23 prasad-Aspire-A315-23 gdm-password]:
pam_unix(gdm-password:session): session opened for user prasad(uid=1000) by (uid=0)
Jul 17 09:16:00 prasad-Aspire-A315-23 kernel: [ 2.337654] systemd[1]: Started
Forward Password Requests to Wall Directory Watch.
Jul 17 09:16:00 prasad-Aspire-A315-23 systemd[1]: Condition check resulted in
Dispatch Password Requests to Console Directory Watch being skipped.
Jul 17 09:16:00 prasad-Aspire-A315-23 systemd[1]: Started Forward Password Requests
to Plymouth Directory Watch.
Jul 17 09:16:10 prasad-Aspire-A315-23 gdm-password]: gkr-pam: gnome-keyring-daemon
started properly and unlocked keyring
Jul 17 09:16:10 prasad-Aspire-A315-23 gdm-password]: gkr-pam: stashed password to
try later in open session
Jul 17 09:16:10 prasad-Aspire-A315-23 gdm-password]: gkr-pam: unable to locate
daemon control file
Jul 17 09:16:10 prasad-Aspire-A315-23 gdm-password]:
pam_unix(gdm-password:session): session opened for user prasad(uid=1000) by (uid=0)
```

```
Jul 17 09:41:58 prasad-Aspire-A315-23 kernel: [ 2.338847] systemd[1]: Started
Forward Password Requests to Wall Directory Watch.
Jul 17 09:41:58 prasad-Aspire-A315-23 systemd[1]: Condition check resulted in
Dispatch Password Requests to Console Directory Watch being skipped.
Jul 17 09:41:58 prasad-Aspire-A315-23 systemd[1]: Started Forward Password Requests
to Plymouth Directory Watch.
Jul 17 09:42:27 prasad-Aspire-A315-23 gdm-password]: gkr-pam: gnome-keyring-daemon
started properly and unlocked keyring
Jul 17 09:42:27 prasad-Aspire-A315-23 gdm-password]: gkr-pam: stashed password to
try later in open session
Jul 17 09:42:27 prasad-Aspire-A315-23 gdm-password]: gkr-pam: unable to locate
daemon control file
Jul 17 09:42:27 prasad-Aspire-A315-23 gdm-password]:
pam_unix(gdm-password:session): session opened for user prasad(uid=1000) by (uid=0)
Jul 17 09:56:43 prasad-Aspire-A315-23 sudo: prasad : TTY=pts/0 ; PWD=/home/prasad ;
USER=root ; COMMAND=/usr/bin/apt-get install -f
Jul 17 09:58:10 prasad-Aspire-A315-23 sudo: prasad : TTY=pts/0 ; PWD=/home/prasad ;
USER=root ; COMMAND=/usr/bin/apt-get update
```

API Keys Regex

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