NoPUppies4U: Final Presentation

Jason, Andrew, Kaden, Bryan, Harrison

Introduction:

- NoPUppies4U is a light-weight Linux red/blue team tool that will scan your filesystem for common misconfigurations, vulnerabilities, and exploits.
- This project is very modular which each feature is implemented with function/s.

Importance of our project

Computer security is essential for safeguarding confidential data and ensuring the integrity and availability of system resources. By conducting systematic vulnerability assessments and applying remediation, organizations can effectively reduce the attack surface and mitigate potential exploitation vectors.

Functionality:

- Our program runs as a command line utility that can take in flags and parameters and process different functions accordingly. Some functions output to the console, while others create log files /var/log/NoPuppies4U/ directory.
- It can be built in the source directory, or be installed as a system program, via an install.sh file.
- It has manual pages accessible via the “man” command once installed.

What we did - Functions()

Jason Dong

check_sources_list()

check_sudo()

check_sys_updated()

check_ufw()

ncat_backdoor()

Andrew Sagraves

systebd_unit_audit()

suid_package_audit()

suid_binary_audit()

world_writable_ssh_keys()

passwordless_sudo_access()

get_path_vulnerabilities()

get_paths()

Bryan Mullins

check_directory_for_changes()

get_all_files_recursively()

load_previous_date_modified()

parse_log_file()

parse_system_logs()

parse_kernel_logs()

parse_authentication_logs()

parse_application_logs()

parse_all_logs()

Kaden Bissonnette

check_cron_jobs()

check_sudoers()

sanitize_token()

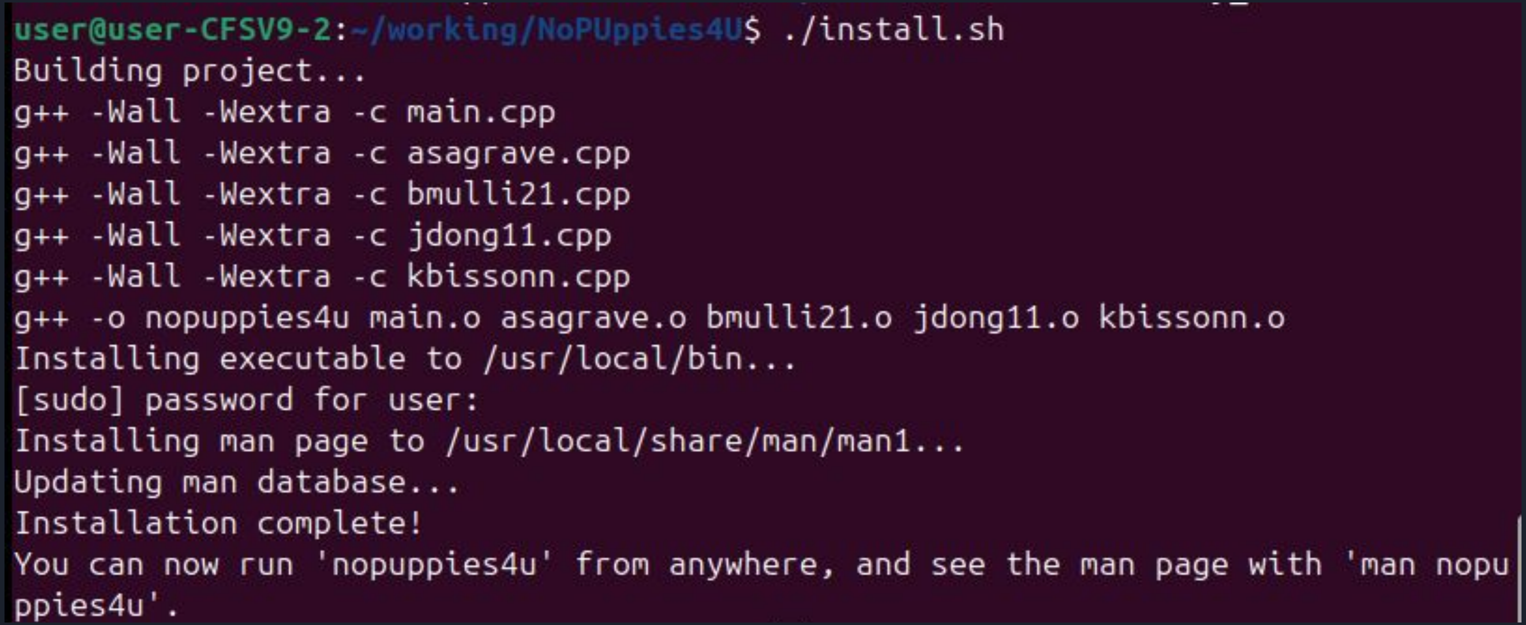
check_sudoers_permissions()

Project Demonstration

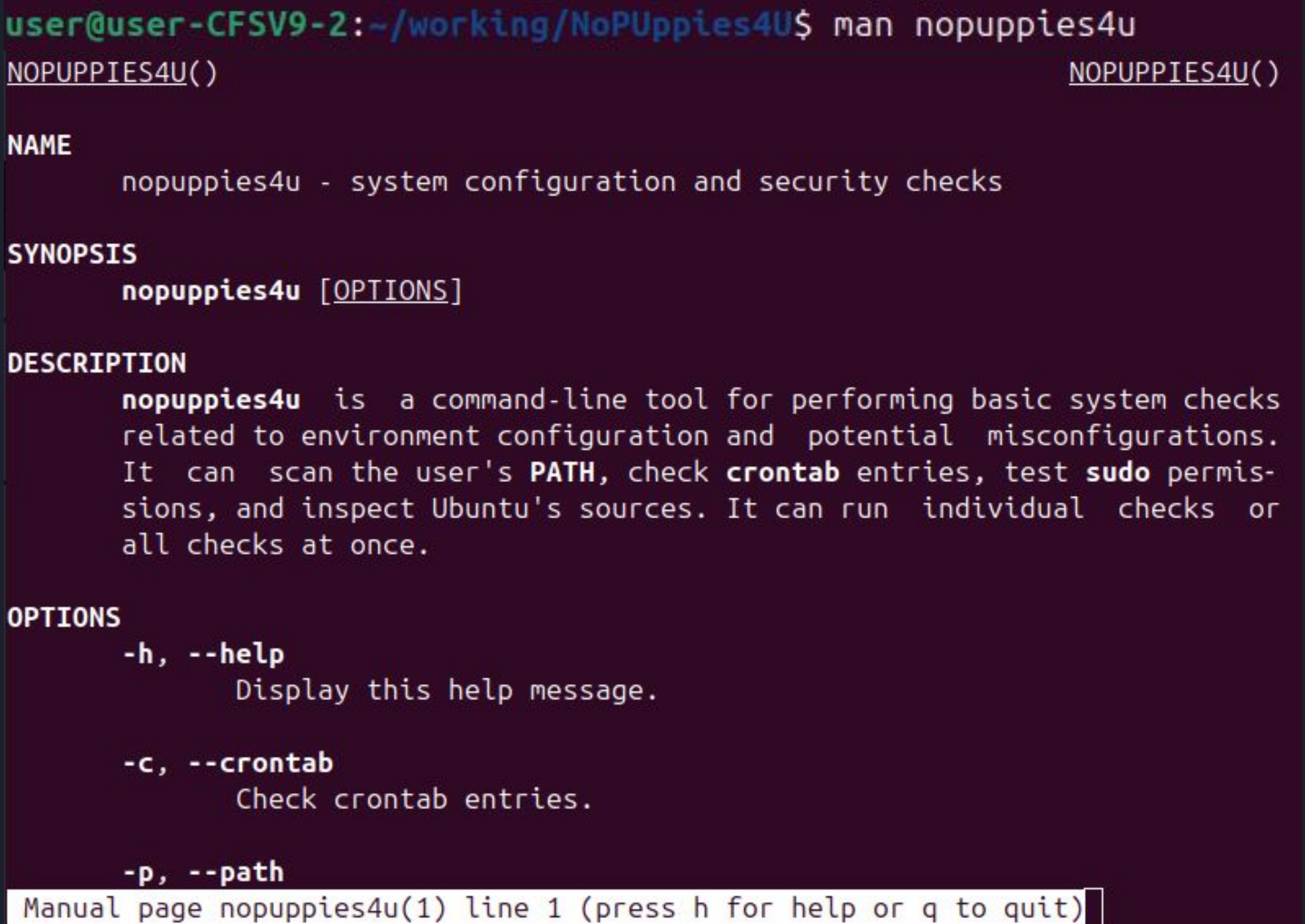
Thank You

GitHub: https://github.com/Andrew-Sagraves/NoPUppies4U

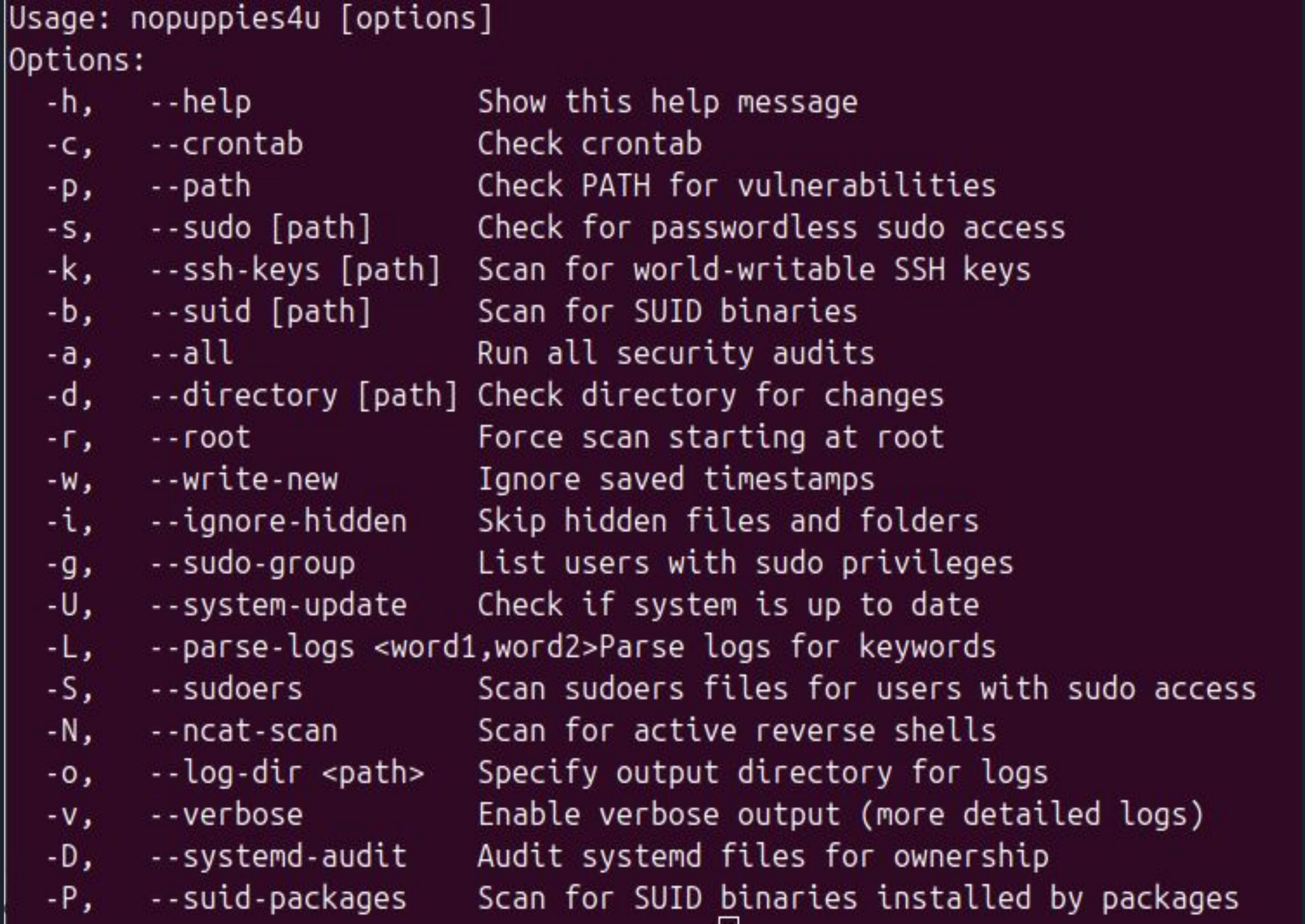
Backup Slides



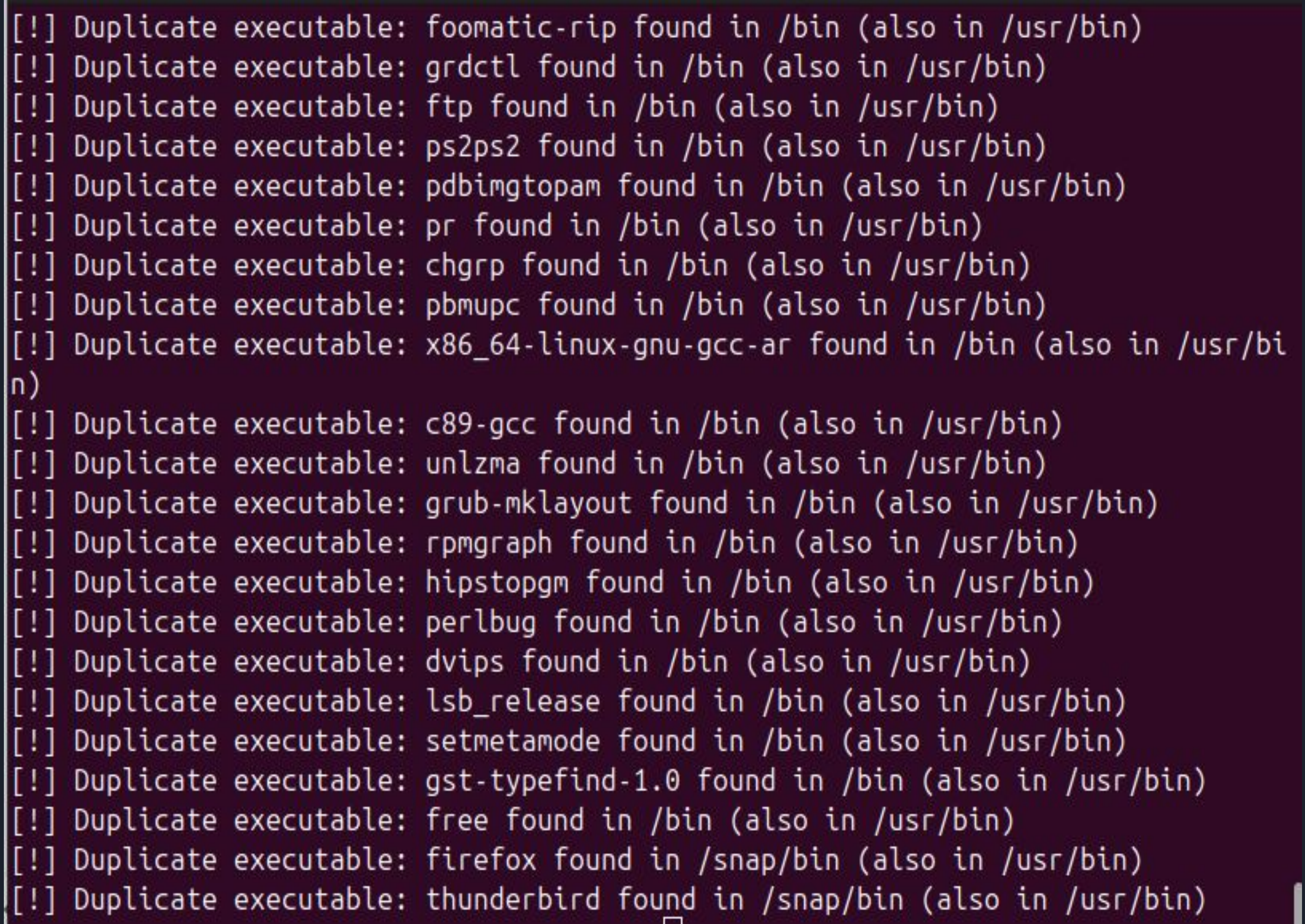
```
user@user-CFSV9-2:~/working/NoPUppies4U$ ./install.sh
Building project...
g++ -Wall -Wextra -c main.cpp
g++ -Wall -Wextra -c asagrave.cpp
g++ -Wall -Wextra -c bmulli21.cpp
g++ -Wall -Wextra -c jdong11.cpp
g++ -Wall -Wextra -c kbissonn.cpp
g++ -o nopuppies4u main.o asagrave.o bmulli21.o jdong11.o kbissonn.o
Installing executable to /usr/local/bin...
[sudo] password for user:
Installing man page to /usr/local/share/man/man1...
Updating man database...
Installation complete!
You can now run 'nopuppies4u' from anywhere, and see the man page with 'man nopu
ppies4u'.
```



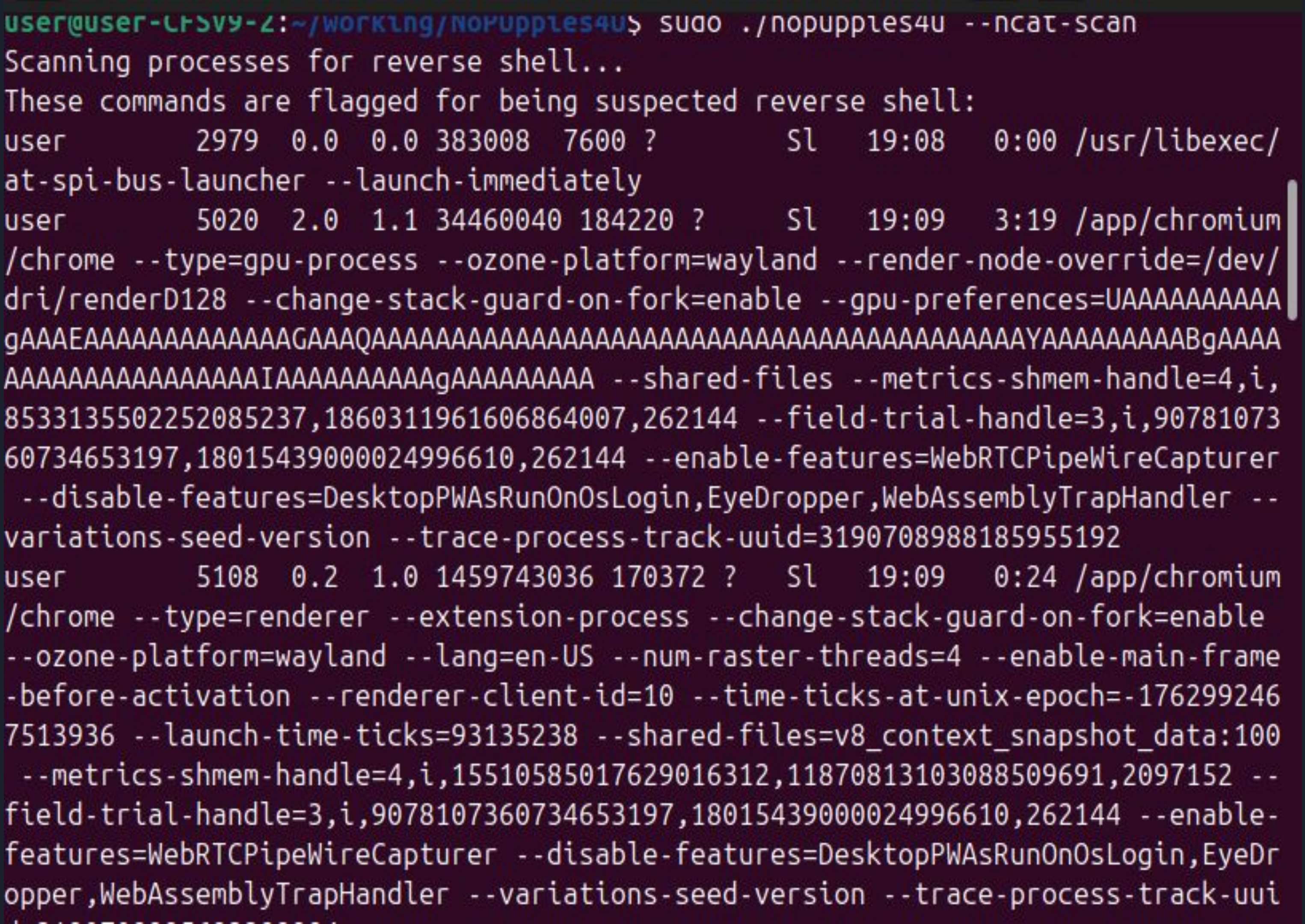
```
user@user-CFSV9-2:~/working/NoPUppies4U$ man nopuppies4u
NOPUPPIES4U()                                                      NOPUPPIES4U()

NAME
       nopuppies4u - system configuration and security checks

SYNOPSIS
       nopuppies4u [OPTIONS]

DESCRIPTION
       nopuppies4u  is  a command-line tool for performing basic system checks
       related to environment configuration and  potential  misconfigurations.
       It  can  scan the user's PATH, check crontab entries, test sudo permis-
       sions, and inspect Ubuntu's sources. It can run  individual  checks  or
       all checks at once.

OPTIONS
       -h, --help
              Display this help message.

       -c, --crontab
              Check crontab entries.

       -p, --path
 Manual page nopuppies4u(1) line 1 (press h for help or q to quit)
```



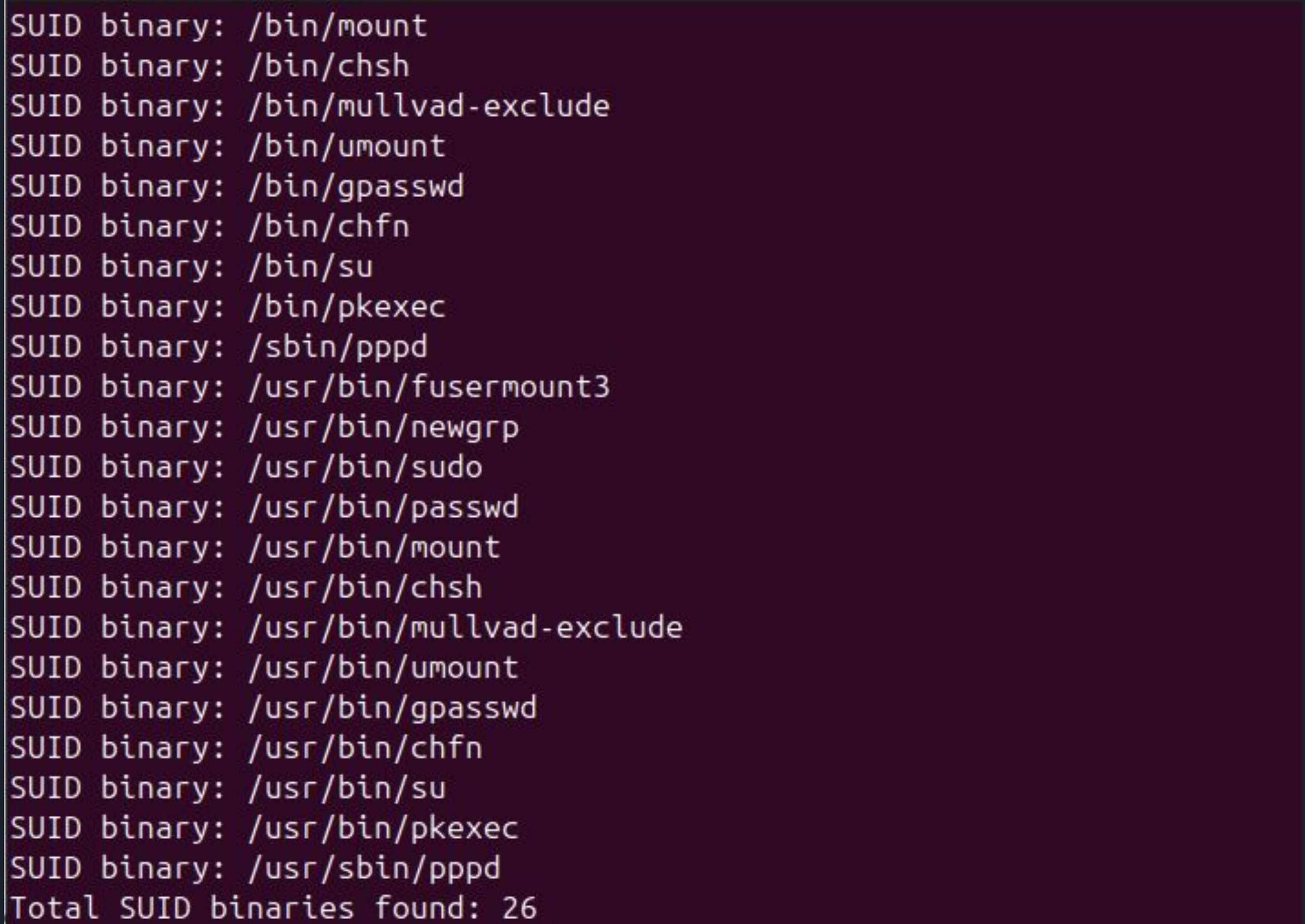
```
Usage: nopuppies4u [options]
Options:
  -h,   --help               Show this help message
  -c,   --crontab            Check crontab
  -p,   --path               Check PATH for vulnerabilities
  -s,   --sudo [path]        Check for passwordless sudo access
  -k,   --ssh-keys [path]    Scan for world-writable SSH keys
  -b,   --suid [path]        Scan for SUID binaries
  -a,   --all                Run all security audits
  -d,   --directory [path] Check directory for changes
  -r,   --root               Force scan starting at root
  -w,   --write-new          Ignore saved timestamps
  -i,   --ignore-hidden      Skip hidden files and folders
  -g,   --sudo-group         List users with sudo privileges
  -U,   --system-update      Check if system is up to date
  -L,   --parse-logs <word1,word2>Parse logs for keywords
  -S,   --sudoers            Scan sudoers files for users with sudo access
  -N,   --ncat-scan          Scan for active reverse shells
  -o,   --log-dir <path>     Specify output directory for logs
  -v,   --verbose            Enable verbose output (more detailed logs)
  -D,   --systemd-audit      Audit systemd files for ownership
  -P,   --suid-packages      Scan for SUID binaries installed by packages
```



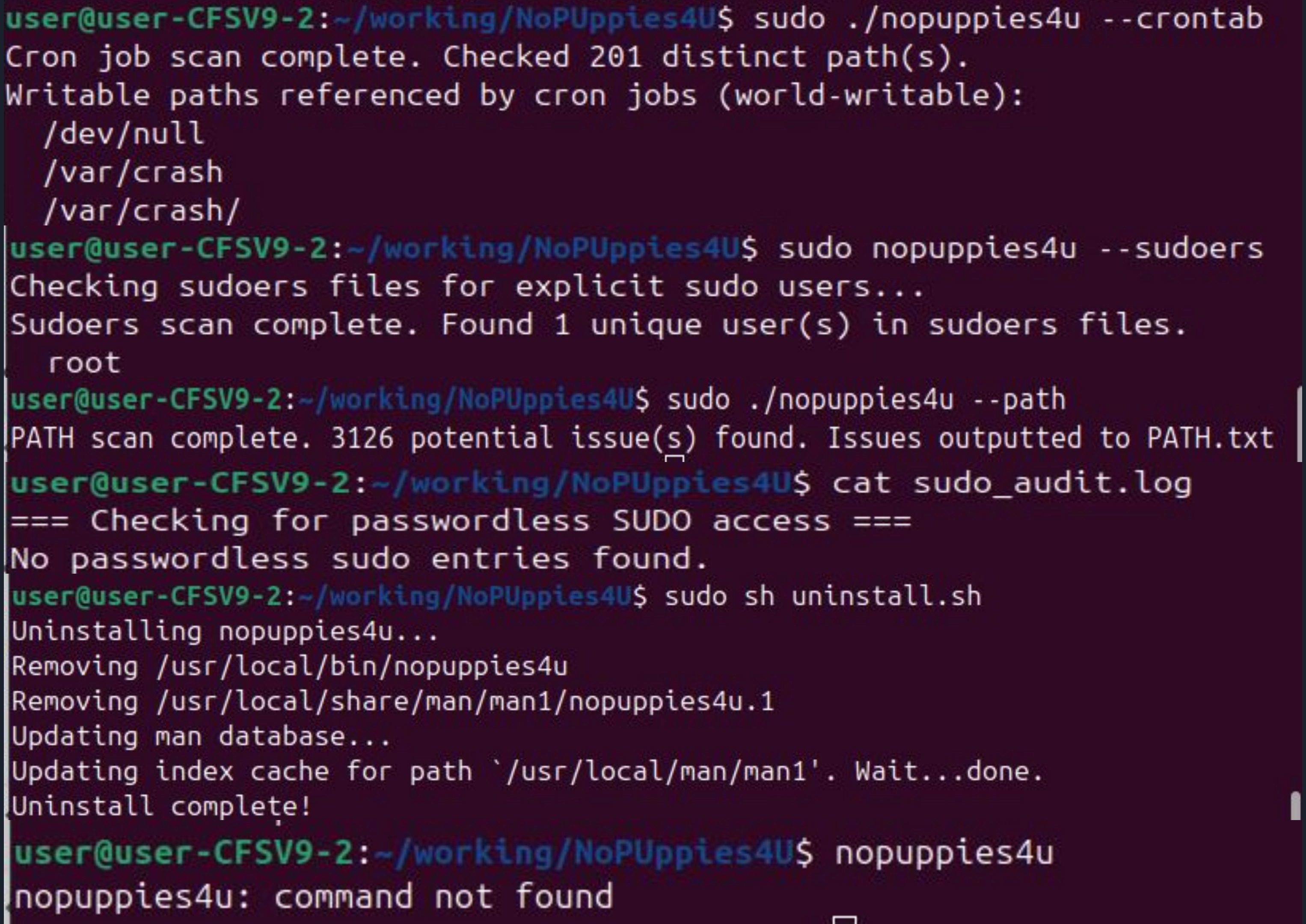
```
[!] Duplicate executable: foomatic-rip found in /bin (also in /usr/bin)
[!] Duplicate executable: grdctl found in /bin (also in /usr/bin)
[!] Duplicate executable: ftp found in /bin (also in /usr/bin)
[!] Duplicate executable: ps2ps2 found in /bin (also in /usr/bin)
[!] Duplicate executable: pdbimgtopam found in /bin (also in /usr/bin)
[!] Duplicate executable: pr found in /bin (also in /usr/bin)
[!] Duplicate executable: chgrp found in /bin (also in /usr/bin)
[!] Duplicate executable: pbmupc found in /bin (also in /usr/bin)
[!] Duplicate executable: x86_64-linux-gnu-gcc-ar found in /bin (also in /usr/bi
n)
[!] Duplicate executable: c89-gcc found in /bin (also in /usr/bin)
[!] Duplicate executable: unlzma found in /bin (also in /usr/bin)
[!] Duplicate executable: grub-mklayout found in /bin (also in /usr/bin)
[!] Duplicate executable: rpmgraph found in /bin (also in /usr/bin)
[!] Duplicate executable: hipstopgm found in /bin (also in /usr/bin)
[!] Duplicate executable: perlbug found in /bin (also in /usr/bin)
[!] Duplicate executable: dvips found in /bin (also in /usr/bin)
[!] Duplicate executable: lsb_release found in /bin (also in /usr/bin)
[!] Duplicate executable: setmetamode found in /bin (also in /usr/bin)
[!] Duplicate executable: gst-typefind-1.0 found in /bin (also in /usr/bin)
[!] Duplicate executable: free found in /bin (also in /usr/bin)
[!] Duplicate executable: firefox found in /snap/bin (also in /usr/bin)
[!] Duplicate executable: thunderbird found in /snap/bin (also in /usr/bin)
```



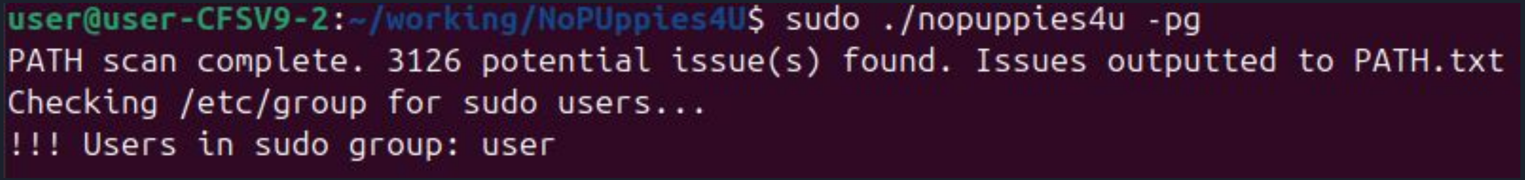
```
user@user-CFSV9-2:~/working/NoPupples4U$ sudo ./nopupples4u --ncat-scan
Scanning processes for reverse shell...
These commands are flagged for being suspected reverse shell:
user        2979  0.0  0.0 383008  7600 ?        Sl   19:08   0:00 /usr/libexec/
at-spi-bus-launcher --launch-immediately
user        5020  2.0  1.1 34460040 184220 ?     Sl   19:09   3:19 /app/chromium
/chrome --type=gpu-process --ozone-platform=wayland --render-node-override=/dev/
dri/renderD128 --change-stack-guard-on-fork=enable --gpu-preferences=UAAAAAAAAAA
gAAAEAAAAAAAAAAAAAGAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYAAAAAAAAABgAAAA
AAAAAAAAAAAAAAAAIAAAAAAAAAAAgAAAAAAAAA --shared-files --metrics-shmem-handle=4,i,
8533135502252085237,1860311961606864007,262144 --field-trial-handle=3,i,90781073
60734653197,1801543900024996610,262144 --enable-features=WebRTCPipeWireCapturer
 --disable-features=DesktopPWAsRunOnOsLogin,EyeDropper,WebAssemblyTrapHandler --
variations-seed-version --trace-process-track-uuid=3190708988185955192
user        5108  0.2  1.0 1459743036 170372 ?   Sl   19:09   0:24 /app/chromium
/chrome --type=renderer --extension-process --change-stack-guard-on-fork=enable
--ozone-platform=wayland --lang=en-US --num-raster-threads=4 --enable-main-frame
-before-activation --renderer-client-id=10 --time-ticks-at-unix-epoch=-176299246
7513936 --launch-time-ticks=93135238 --shared-files=v8_context_snapshot_data:100
 --metrics-shmem-handle=4,i,15510585017629016312,11870813103088509691,2097152 --
field-trial-handle=3,i,9078107360734653197,1801543900024996610,262144 --enable-
features=WebRTCPipeWireCapturer --disable-features=DesktopPWAsRunOnOsLogin,EyeDr
opper,WebAssemblyTrapHandler --variations-seed-version --trace-process-track-uui
```



```
SUID binary: /bin/mount
SUID binary: /bin/chsh
SUID binary: /bin/mullvad-exclude
SUID binary: /bin/umount
SUID binary: /bin/gpasswd
SUID binary: /bin/chfn
SUID binary: /bin/su
SUID binary: /bin/pkexec
SUID binary: /sbin/pppd
SUID binary: /usr/bin/fusermount3
SUID binary: /usr/bin/newgrp
SUID binary: /usr/bin/sudo
SUID binary: /usr/bin/passwd
SUID binary: /usr/bin/mount
SUID binary: /usr/bin/chsh
SUID binary: /usr/bin/mullvad-exclude
SUID binary: /usr/bin/umount
SUID binary: /usr/bin/gpasswd
SUID binary: /usr/bin/chfn
SUID binary: /usr/bin/su
SUID binary: /usr/bin/pkexec
SUID binary: /usr/sbin/pppd
Total SUID binaries found: 26
```



```
user@user-CFSV9-2:~/working/NoPUppies4U$ sudo ./nopuppies4u --crontab
Cron job scan complete. Checked 201 distinct path(s).
Writable paths referenced by cron jobs (world-writable):
  /dev/null
  /var/crash
  /var/crash/
user@user-CFSV9-2:~/working/NoPUppies4U$ sudo nopuppies4u --sudoers
Checking sudoers files for explicit sudo users...
Sudoers scan complete. Found 1 unique user(s) in sudoers files.
  root
user@user-CFSV9-2:~/working/NoPUppies4U$ sudo ./nopuppies4u --path
PATH scan complete. 3126 potential issue(s) found. Issues outputted to PATH.txt
user@user-CFSV9-2:~/working/NoPUppies4U$ cat sudo_audit.log
=== Checking for passwordless SUDO access ===
No passwordless sudo entries found.
user@user-CFSV9-2:~/working/NoPUppies4U$ sudo sh uninstall.sh
Uninstalling nopuppies4u...
Removing /usr/local/bin/nopuppies4u
Removing /usr/local/share/man/man1/nopuppies4u.1
Updating man database...
Updating index cache for path `/usr/local/man/man1'. Wait...done.
Uninstall complete!
user@user-CFSV9-2:~/working/NoPUppies4U$ nopuppies4u
nopuppies4u: command not found
```



```
user@user-CFSV9-2:~/working/NoPUppies4U$ sudo ./nopuppies4u -pg
PATH scan complete. 3126 potential issue(s) found. Issues outputted to PATH.txt
Checking /etc/group for sudo users...
!!! Users in sudo group: user
```