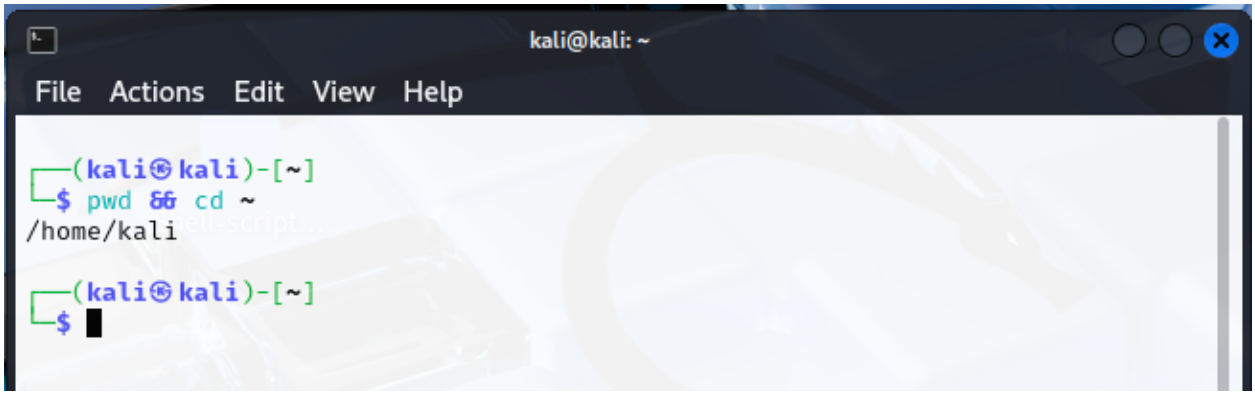
Alend Nezar Mustafa Ismail

🐧 En rundtur i Linux

🐧 Øvelser - Linux commands

📂 1) Filsystem

1. Find din nuværende sti og gå til din hjemmemappe.



2. Opret ~/kali-ovelser/fs med data og tmp som undermapper.

```
(kali㉿kali)-[~]
$ mkdir -p ~/kali-ovelser/fs/{data,tmp}
```

3. Lav filen notes.txt i data med teksten hej kali.

```
(kali㉿kali)-[~]
$ echo "hej kali" > ~/kali-ovelser/fs/data/notes.txt
```

4. Flyt notes.txt til tmp og omdøb den til .hidden_notes.

```
(kali㉿kali)-[~]
$ mv ~/kali-ovelser/fs/data/notes.txt ~/kali-ovelser/fs/tmp/.hidden_notes
```

```
(kali㉿kali)-[~/kali-ovelser/fs/tmp]
$ cat < .hidden_notes
hej kali
```

👤 2) Brugere og grupper

1. Vis dit brugernavn og hvilke grupper du er i.

```
┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),
25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(ne
tdev),117(bluetooth),121(wireshark),127(scanner),134(kaboxer)
```

2. Slå din bruger op i /etc/passwd.

```
┌──(kali㉿kali)-[~]
└─$ grep "^kali:" /etc/passwd
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh
```

3. (Hvis muligt) Opret gruppen lab og tilføj din bruger til den.

```
┌──(kali㉿kali)-[~]
└─$ sudo groupadd lab 2>/dev/null || true && sudo usermod -aG lab kali
[sudo] password for kali:
```

```
┌──(kali㉿kali)-[~]
└─$ groups
kali adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluet
ooth wireshark scanner kaboxer lab

┌──(kali㉿kali)-[~]
```

⚙️ 3) Processer

1. Vis processer for din bruger.

```
┌──(kali㉿kali)-[~]
└─$ ps -u kali
    PID TTY          TIME CMD
    866 ?        00:00:00 systemd
    868 ?        00:00:00 (sd-pam)
    888 ?        00:00:00 dbus-daemon
    889 ?        00:00:00 pipewire
    890 ?        00:00:00 pipewire
    892 ?        00:00:00 gnome-keyring-d
    893 ?        00:00:00 mpris-proxy
    894 ?        00:00:00 wireplumber
    895 ?        00:00:00 pipewire-pulse
    985 ?        00:00:00 at-spi-bus-laun
    992 ?        00:00:00 dbus-daemon
   1027 ?        00:00:00 gvfsd
   1033 ?        00:00:00 gvfsd-fuse
   1058 ?        00:00:00 dconf-service
   1205 ?        00:00:00 applet.py
   1217 ?        00:00:00 agent
   1279 ?        00:00:00 gvfs-udisks2-vo
   1323 ?        00:00:00 gvfs-goa-volume
   1328 ?        00:00:00 gvfs-gphoto2-vo
   1343 ?        00:00:00 gvfs-mtp-volume
   1351 ?        00:00:00 gvfs-afc-volume
   1365 ?        00:00:00 gvfsd-metadata
```

2. Find PID for din nuværende shell.

```
┌──(kali㉿kali)-[~]
└─$ echo $$
19741
```

3. Start sleep 60 i baggrunden og vis at den kører.

```
┌──(kali㉿kali)-[~]
└─$ sleep 60 & jobs
[1] 21025
[1]  + running    sleep 60
```

💻 4) Resurser (CPU, RAM, disk)

1. Vis et snapshot af CPU og RAM.

```
└─$ top -b -n1 | head -n 10
top - 19:36:39 up 35 min,  2 users,  load average: 0.32, 0.46, 0.27
Tasks: 173 total,   1 running, 171 sleeping,   0 stopped,   1 zombie
%Cpu(s):  2.2 us,  0.0 sy,  0.0 ni, 97.8 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
st
MiB Mem :   3910.8 total,   2305.5 free,    742.7 used,   1055.2 buff/cache

MiB Swap:    976.0 total,    976.0 free,      0.0 used.   3168.1 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAN
D
  22404 kali      20   0   10600   4484   2564 R   8.3   0.1   0:00.02 top
      1 root      20   0   24692  14196   9980 S   0.0   0.4   0:01.13 system
d
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthrea
dd
```

2. Vis brug af monterede filerystemer.

```
┌──(kali㉿kali)-[~]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           392M  1.3M  390M   1% /run
/dev/vda2        62G   19G   40G  32% /
tmpfs           2.0G  8.0K  2.0G   1% /dev/shm
efivarfs        256K   25K  231K  10% /sys/firmware/efi/efivars
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.servi
ce
tmpfs           2.0G  8.0K  2.0G   1% /tmp
/dev/vda1       512M  168K  512M   1% /boot/efi
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/serial-getty@ttyAMA0.s
ervice
tmpfs           392M  4.1M  388M   2% /run/user/1000
```

3. Mål hvor lang tid ls / tager.

```
┌──(kali㉿kali)-[~]
└─$ time ls />/dev/null

real    0.00s
user    0.00s
sys     0.00s
cpu     84%
```

🌐 5) Netværk

1. Vis dine netværksinterfaces og IP-adresser.

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether aa:6d:ae:a7:c8:9e brd ff:ff:ff:ff:ff:ff
    inet 192.168.65.3/24 brd 192.168.65.255 scope global dynamic noprefixrout
e eth0
       valid_lft 3067sec preferred_lft 3067sec
    inet6 fd62:4f6b:9390:6570:9e41:c090:1ec6:1b9a/64 scope global temporary d
ynamic
       valid_lft 602467sec preferred_lft 83542sec
    inet6 fd62:4f6b:9390:6570:a86d:aeff:fea7:c89e/64 scope global dynamic mng
tmpaddr noprefixroute
       valid_lft 2591928sec preferred_lft 604728sec
    inet6 fe80::a86d:aeff:fea7:c89e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

2. Ping kali.org med 3 pakker.

```
┌──(kali㉿kali)-[~]
└─$ ping -c 3 kali.org
PING kali.org (104.18.5.159) 56(84) bytes of data.
64 bytes from 104.18.5.159: icmp_seq=1 ttl=58 time=16.5 ms
64 bytes from 104.18.5.159: icmp_seq=2 ttl=58 time=19.2 ms
64 bytes from 104.18.5.159: icmp_seq=3 ttl=58 time=21.4 ms

── kali.org ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 16.516/19.035/21.361/1.982 ms
```

3. Se hvilke processer der lytter på lokale porte.

```
┌──(kali㉿kali)-[~]
└─$ sudo ss -tulnp
Netid  State   Recv-Q   Send-Q     Local Address:Port     Peer Address:Port
Process
tcp    LISTEN  0        128              0.0.0.0:22            0.0.0.0:*
 users:(("sshd",pid=25583,fd=6))
tcp    LISTEN  0        128                 [::]:22               [::]:*
 users:(("sshd",pid=25583,fd=7))

┌──(kali㉿kali)-[~]
└─$
```

🛠️ 6) Systeminfo & environment

1. Vis kernel-version og maskine-arkitektur.

```
┌──(kali㉿kali)-[~]
└─$ uname -r && uname -m
6.12.38+kali-arm64
aarch64
```

2. Vis miljøvariablen PATH.

```
┌──(kali㉿kali)-[~]
└─$ echo "$PATH"
/home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin
:/bin:/usr/local/games:/usr/games
```

📦 7) Installering & opdatering (APT)

1. Opdater pakkelister.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
Get:1 http://ftp.halifax.rwth-aachen.de/kali kali-rolling InRelease [34.0 kB]
Get:2 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main arm64 Packages
 [20.8 MB]
Get:3 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main arm64 Contents
 (deb) [49.1 MB]
Get:4 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/contrib arm64 Packa
ges [100 kB]
Get:5 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/contrib arm64 Conte
nts (deb) [179 kB]
Get:6 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/non-free arm64 Pack
ages [147 kB]
Get:7 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/non-free arm64 Cont
ents (deb) [850 kB]
Get:8 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/non-free-firmware a
rm64 Packages [10.8 kB]
Get:9 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/non-free-firmware a
rm64 Contents (deb) [27.7 kB]
Fetched 71.2 MB in 8s (8417 kB/s)
1284 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

2. Søg efter pakken jq.

```
┌──(kali㉿kali)-[~]
└─$ apt search jq | head -n 10

WARNING: apt does not have a stable CLI interface. Use with caution in script
s.

Sorting ...
Full Text Search ...
dasel/kali-rolling 2.8.1-1 arm64
  Query, update and convert data structures from the command line (program)

fq/kali-rolling 0.9.0-2 arm64
  jq for binary formats (program)

gojq/kali-rolling 0.12.13-1 arm64
  pure Go implementation of jq (program)
```

3. Installer jq, vis versionen, og fjern den igen.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y jq
The following packages were automatically installed and are no longer require
d:
  firebird3.0-common          libgtksourceviewmm-3.0-0v5
  firebird3.0-common-doc      libgumbo2
  firmware-intel-sound        libibverbs1
  firmware-sof-signed         libicu-dev
  fonts-liberation2           libiniparser1
  freerdp2-x11                libjim0.82t64
  hydra-gtk                   libjsoncpp25
  ibverbs-providers           libmbedcrypto7t64
  icu-devtools                libopenh264-7
  libabsl20230802             libpaper1
  libassuan0                  libperl5.38t64
  libavfilter9                libplacebo338
  libbfio1                    libpostproc57
  libboost-iostreams1.83.0    librados2
  libboost-thread1.83.0       librdmacm1t64
  libcapstone4                libsframe1
  libcephfs2                  libsigsegv2
  libconfig++9v5              libtag1v5
  libconfig9                  libtag1v5-vanilla
  libdirectfb-1.7-7t64        libtagc0
  libegl-dev                  libutempter0
```

```
┌──(kali㉿kali)-[~]
└─$ jq --version
jq-1.8.1
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt remove -y jq
The following packages were automatically installed and are no longer require
d:
  firebird3.0-common          libgtksourceviewmm-3.0-0v5
  firebird3.0-common-doc      libgumbo2
  firmware-intel-sound        libibverbs1
  firmware-sof-signed         libicu-dev
  fonts-liberation2           libiniparser1
  freerdp2-x11                libjim0.82t64
  hydra-gtk                   libjsoncpp25
  ibverbs-providers           libmbedcrypto7t64
  icu-devtools                libopenh264-7
  libabsl20230802             libpaper1
  libassuan0                  libperl5.38t64
  libavfilter9                libplacebo338
  libbfio1                    libpostproc57
  libboost-iostreams1.83.0    librados2
  libboost-thread1.83.0       librdmacm1t64
  libcapstone4                libsframe1
  libcephfs2                  libsigsegv2
  libconfig++9v5              libtag1v5
  libconfig9                  libtag1v5-vanilla
```

📜 8) Logging (basic)

1. Se de sidste 20 linjer i systemjournalen.

```
┌──(kali㉿kali)-[~]
└─$ journalctl -n 20 --no-pager
Nov 26 19:46:00 kali sudo[27442]: pam_unix(sudo:session): session opened for
user root(uid=0) by kali(uid=1000)
Nov 26 19:46:00 kali sudo[27442]: pam_unix(sudo:session): session closed for
user root
Nov 26 19:46:00 kali sudo[27446]:     kali : TTY=pts/0 ; PWD=/home/kali ; USE
R=root ; COMMAND=/usr/bin/apt remove -y jq
Nov 26 19:46:00 kali sudo[27446]: pam_unix(sudo:session): session opened for
user root(uid=0) by kali(uid=1000)
Nov 26 19:46:01 kali sudo[27446]: pam_unix(sudo:session): session closed for
user root
Nov 26 19:47:08 kali sudo[28025]:     kali : TTY=pts/0 ; PWD=/home/kali ; USE
R=root ; COMMAND=/usr/bin/apt install -y jq
Nov 26 19:47:08 kali sudo[28025]: pam_unix(sudo:session): session opened for
user root(uid=0) by kali(uid=1000)
Nov 26 19:47:14 kali sudo[28025]: pam_unix(sudo:session): session closed for
user root
Nov 26 19:47:54 kali sudo[28520]:     kali : TTY=pts/0 ; PWD=/home/kali ; USE
R=root ; COMMAND=/usr/bin/apt install -y jq
Nov 26 19:47:54 kali sudo[28520]: pam_unix(sudo:session): session opened for
user root(uid=0) by kali(uid=1000)
Nov 26 19:47:55 kali sudo[28520]: pam_unix(sudo:session): session closed for
user root
Nov 26 19:48:10 kali sudo[28724]:     kali : TTY=pts/0 ; PWD=/home/kali ; USE
```

2. Se de sidste 20 linjer for ssh-servicen.

```
┌──(kali㉿kali)-[~]
└─$ journalctl -u sshd.service -n 20 --no-pager
-- No entries --
```

3. Se de seneste APT-hændelser (pakkehistorik).

```
┌──(kali㉿kali)-[~]
└─$ grep -E '^(Start-Date|Commandline):' /var/log/apt/history.log | tail -n 2
0
Start-Date: 2025-11-26  19:46:01
Commandline: apt remove -y jq
Start-Date: 2025-11-26  19:47:10
Commandline: apt install -y jq
Start-Date: 2025-11-26  19:47:55
Commandline: apt install -y jq
Start-Date: 2025-11-26  19:48:11
Commandline: apt remove -y jq
Start-Date: 2025-11-26  19:48:18
Commandline: apt install -y jq
Start-Date: 2025-11-26  19:49:01
Commandline: apt remove -y jq
```

4. Følg i realtid en logfil i ~10 sekunder og stop med Ctrl+C.

```
┌──(kali㉿kali)-[/var/log]
└─$ sudo tail -f /var/log/dpkg.log.1
2025-08-29 11:27:28 status installed tex-common:all 6.19
2025-08-29 11:27:28 trigproc libgdk-pixbuf-2.0-0:arm64 2.42.12+dfsg-5 <none>
2025-08-29 11:27:28 status half-configured libgdk-pixbuf-2.0-0:arm64 2.42.12+
dfsg-5
2025-08-29 11:27:28 status installed libgdk-pixbuf-2.0-0:arm64 2.42.12+dfsg-5
2025-08-29 11:27:28 trigproc dbus:arm64 1.16.2-2 <none>
2025-08-29 11:27:28 status half-configured dbus:arm64 1.16.2-2
2025-08-29 11:27:28 status installed dbus:arm64 1.16.2-2
2025-08-29 11:27:28 trigproc ca-certificates-java:all 20240118 <none>
2025-08-29 11:27:28 status half-configured ca-certificates-java:all 20240118
2025-08-29 11:27:28 status installed ca-certificates-java:all 20240118
```

5. List de 5 største filer i /var/log (overblik).

```
┌──(kali㉿kali)-[/var/log]
└─$ sudo ls -lhS /var/log | head -n 5
total 1.9M
-rw-r--r--  1 root             root            1.4M Aug 29 11:27 dpkg.log.1
-rw-r--r--  1 root             root            135K Oct 22  2024 dpkg.log.2.
gz
-rw-r--r--  1 root             root             66K Aug 29 11:24 alternative
s.log.1
-rw-r--r--  1 root             root             30K Nov 26 19:32 Xorg.0.log.
old
```

🔧 9) Processer & services

1. Kør ping -c 10 8.8.8.8 og stop den med Ctrl+C.

```
┌──(kali㉿kali)-[/var/log]
└─$ ping -c 10 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=36.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=27.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=31.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=30.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=34.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=26.5 ms
^C
── 8.8.8.8 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5013ms
rtt min/avg/max/mdev = 26.454/31.146/36.291/3.414 ms
```

2. Start sleep 120 i baggrunden og stop den igen.

```
┌──(kali㉿kali)-[/var/log]
└─$ sleep 120 & kill %1
[1] 36450
[1]  + terminated  sleep 120
```

3. Tjek status for ssh-service.

```
┌──(kali㉿kali)-[/var/log]
└─$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: >
     Active: active (running) since Wed 2025-11-26 19:42:43 CET; 19min ago
 Invocation: 508a004bc6df41e9865fd6f8471cd672
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 25581 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUC>
   Main PID: 25583 (sshd)
      Tasks: 1 (limit: 4490)
     Memory: 2.1M (peak: 2.9M)
        CPU: 32ms
     CGroup: /system.slice/ssh.service
             └─25583 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup>

Nov 26 19:42:43 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell>
Nov 26 19:42:43 kali sshd[25583]: Server listening on 0.0.0.0 port 22.
Nov 26 19:42:43 kali sshd[25583]: Server listening on :: port 22.
Nov 26 19:42:43 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell >
lines 1-18/18 (END)
```

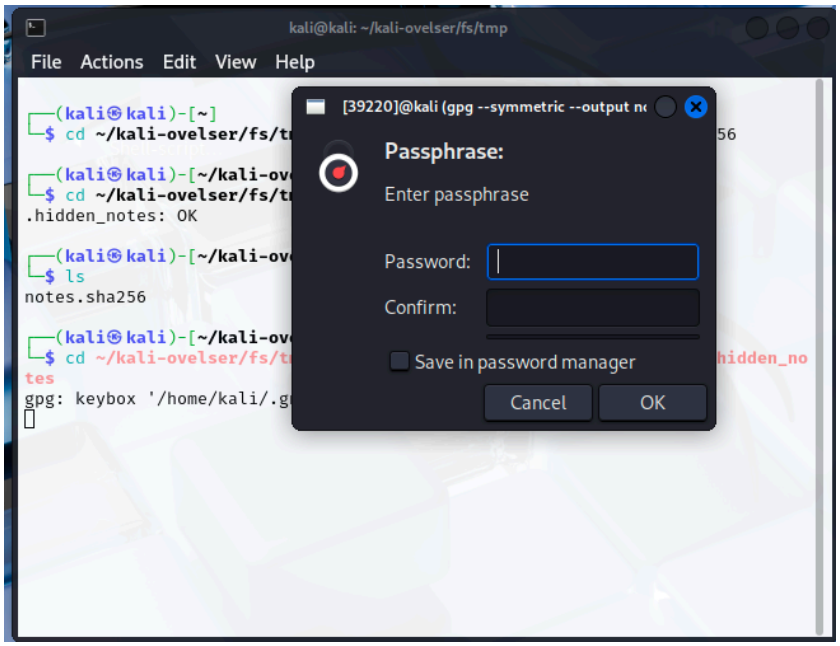
🔐 10) Kryptografi (basic): hash, kryptering, signatur

1. Lav en SHA-256 hash af .hidden_notes og gem den.

```
┌──(kali㉿kali)-[~]
└─$ cd ~/kali-ovelser/fs/tmp && sha256sum .hidden_notes > notes.sha256

┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ cd ~/kali-ovelser/fs/tmp && sha256sum -c notes.sha256
.hidden_notes: OK
```

```
┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ ls
notes.sha256
```

2. Krypter .hidden_notes symmetrisk til en ny fil og dekrypter igen.



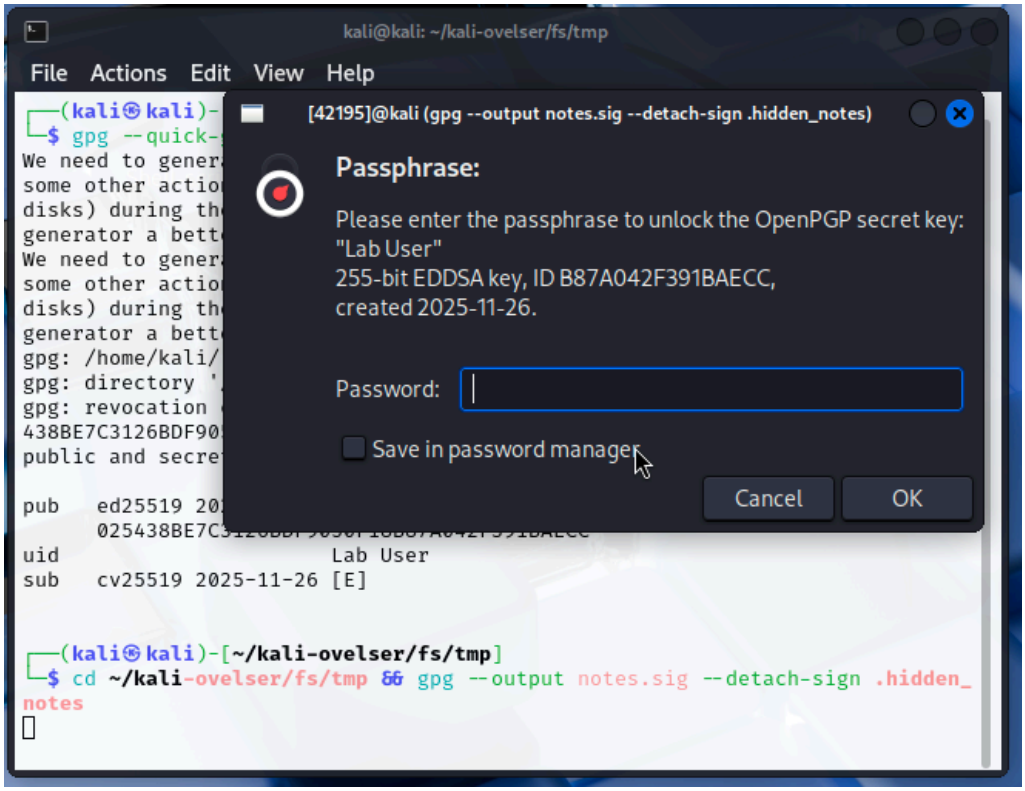

```
┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ cd ~/kali-ovelser/fs/tmp && gpg --symmetric --output notes.gpg .hidden_no
tes
gpg: keybox '/home/kali/.gnupg/pubring.kbx' created
```

```
┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ cd ~/kali-ovelser/fs/tmp && gpg --decrypt --output notes.dec notes.gpg &&
 diff -u .hidden_notes notes.dec || true
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
```

```
┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ cat notes.dec
hej kali

┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ cat notes.gpg
◆
>◆)e◆◆◆◆◆K◆◆◆|◆e◆J◆%◆◆K◆`6\b◆
                              ◆◆0q◆+}◆◆,qeW_Yu6◆◆◆◆f◆)◆0◆◆◆      Z◆◆c␈bщ◆'Ме◆◆

┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ cat notes.sha256
09f062b24fd1c3bb7091b99180a7451e04599b484fe47e3ddb52d53c0333cc98  .hidden_not
es

┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$
```

3. (Med nøgle) Signér .hidden_notes og verificér signaturen.

```
┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ gpg --quick-generate-key "Lab User" default default never
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/kali/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/kali/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/025
438BE7C3126BDF9050F18B87A042F391BAECC.rev'
public and secret key created and signed.

pub   ed25519 2025-11-26 [SC]
      025438BE7C3126BDF9050F18B87A042F391BAECC
uid                      Lab User
sub   cv25519 2025-11-26 [E]
```




```
┌──(kali㉿kali)-[~/kali-ovelser/fs/tmp]
└─$ cd ~/kali-ovelser/fs/tmp && gpg --verify notes.sig .hidden_notes
gpg: Signature made Wed Nov 26 20:12:24 2025 CET
gpg:                using EDDSA key 025438BE7C3126BDF9050F18B87A042F391BAECC
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: Good signature from "Lab User" [ultimate]
```

Alend Nezar Mustafa Ismail

🔐 11) AI i shell

Undersøg applikationen shell-gpt: https://pypi.org/project/shell-gpt/
Det er en command-line AI