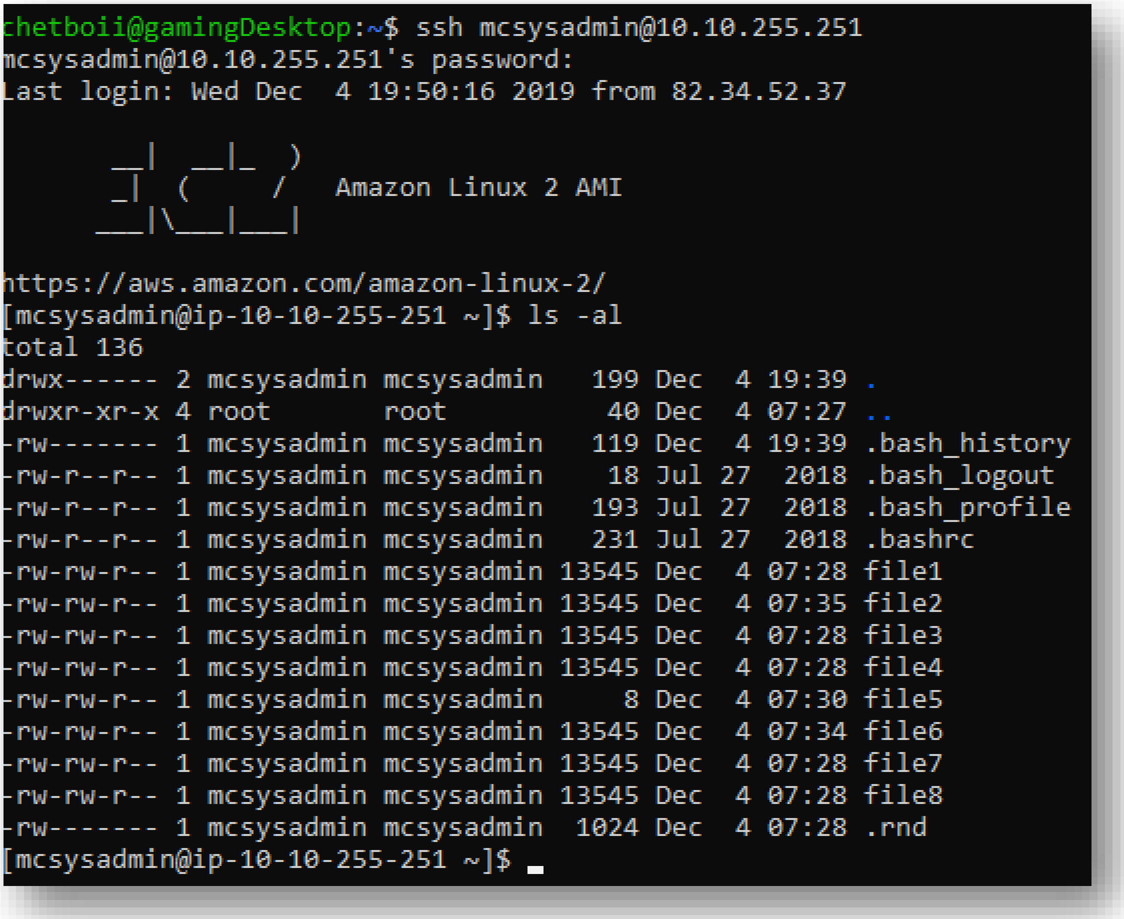
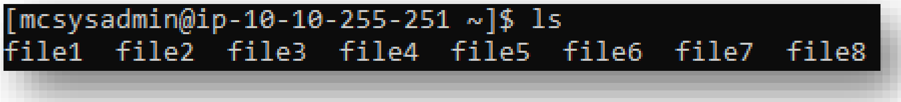
https://docs.google.com/document/d/1CpwM_MdHgRqlPSe4eCC_-rVgi8F1xh88PKOySTRSkxU/edit

Task 8 – Day 4



```
chetboii@gamingDesktop:~$ ssh mcsysadmin@10.10.255.251
mcsysadmin@10.10.255.251's password:
Last login: Wed Dec  4 19:50:16 2019 from 82.34.52.37

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[mcsysadmin@ip-10-10-255-251 ~]$ ls -al
total 136
drwx------ 2 mcsysadmin mcsysadmin   199 Dec  4 19:39 .
drwxr-xr-x 4 root       root          40 Dec  4 07:27 ..
-rw------- 1 mcsysadmin mcsysadmin   119 Dec  4 19:39 .bash_history
-rw-r--r-- 1 mcsysadmin mcsysadmin    18 Jul 27  2018 .bash_logout
-rw-r--r-- 1 mcsysadmin mcsysadmin   193 Jul 27  2018 .bash_profile
-rw-r--r-- 1 mcsysadmin mcsysadmin   231 Jul 27  2018 .bashrc
-rw-rw-r-- 1 mcsysadmin mcsysadmin 13545 Dec  4 07:28 file1
-rw-rw-r-- 1 mcsysadmin mcsysadmin 13545 Dec  4 07:35 file2
-rw-rw-r-- 1 mcsysadmin mcsysadmin 13545 Dec  4 07:28 file3
-rw-rw-r-- 1 mcsysadmin mcsysadmin 13545 Dec  4 07:28 file4
-rw-rw-r-- 1 mcsysadmin mcsysadmin     8 Dec  4 07:30 file5
-rw-rw-r-- 1 mcsysadmin mcsysadmin 13545 Dec  4 07:34 file6
-rw-rw-r-- 1 mcsysadmin mcsysadmin 13545 Dec  4 07:28 file7
-rw-rw-r-- 1 mcsysadmin mcsysadmin 13545 Dec  4 07:28 file8
-rw------- 1 mcsysadmin mcsysadmin  1024 Dec  4 07:28 .rnd
[mcsysadmin@ip-10-10-255-251 ~]$ _
```

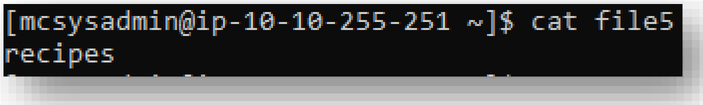
1. **How many visible files are there in the home directory(excluding ./ and ../)?**



```
[mcsysadmin@ip-10-10-255-251 ~]$ ls
file1   file2   file3   file4   file5   file6   file7   file8
```

- There are 8 visible files

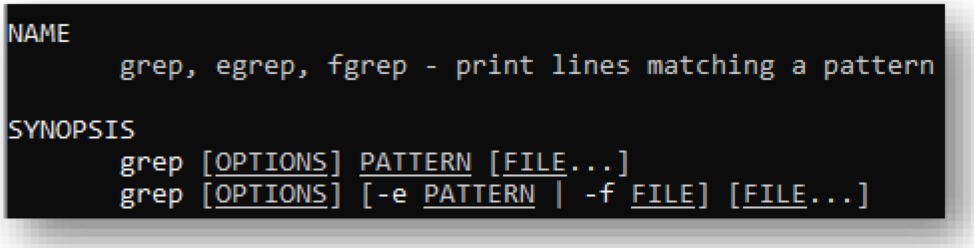
2. **What is the content of file5?**



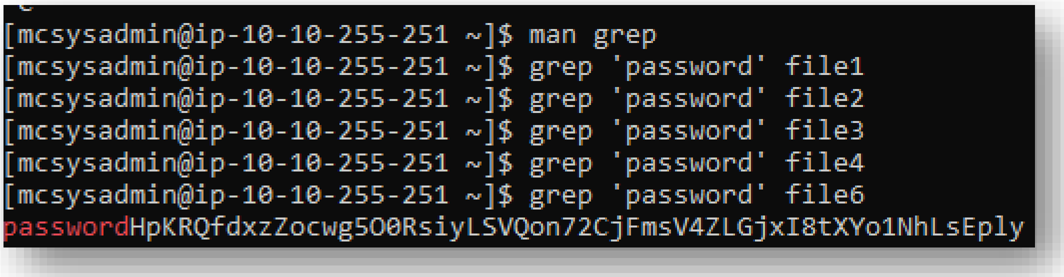
```
[mcsysadmin@ip-10-10-255-251 ~]$ cat file5
recipes
```

- **Recipes**

3. **Which file contains the string ‘password’?**



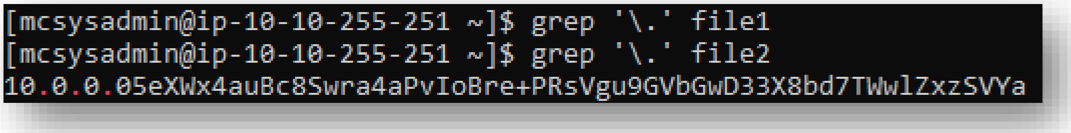
```
NAME
       grep, egrep, fgrep - print lines matching a pattern

SYNOPSIS
       grep [OPTIONS] PATTERN [FILE...]
       grep [OPTIONS] [-e PATTERN | -f FILE] [FILE...]
```



```
[mcsysadmin@ip-10-10-255-251 ~]$ man grep
[mcsysadmin@ip-10-10-255-251 ~]$ grep 'password' file1
[mcsysadmin@ip-10-10-255-251 ~]$ grep 'password' file2
[mcsysadmin@ip-10-10-255-251 ~]$ grep 'password' file3
[mcsysadmin@ip-10-10-255-251 ~]$ grep 'password' file4
[mcsysadmin@ip-10-10-255-251 ~]$ grep 'password' file6
passwordHpKRQfdxzZocwg5O0RsiyLSVQon72CjFmsV4ZLGjxI8tXYo1NhLsEply
```

- Use the grep command for each file, get a result with **file 6**

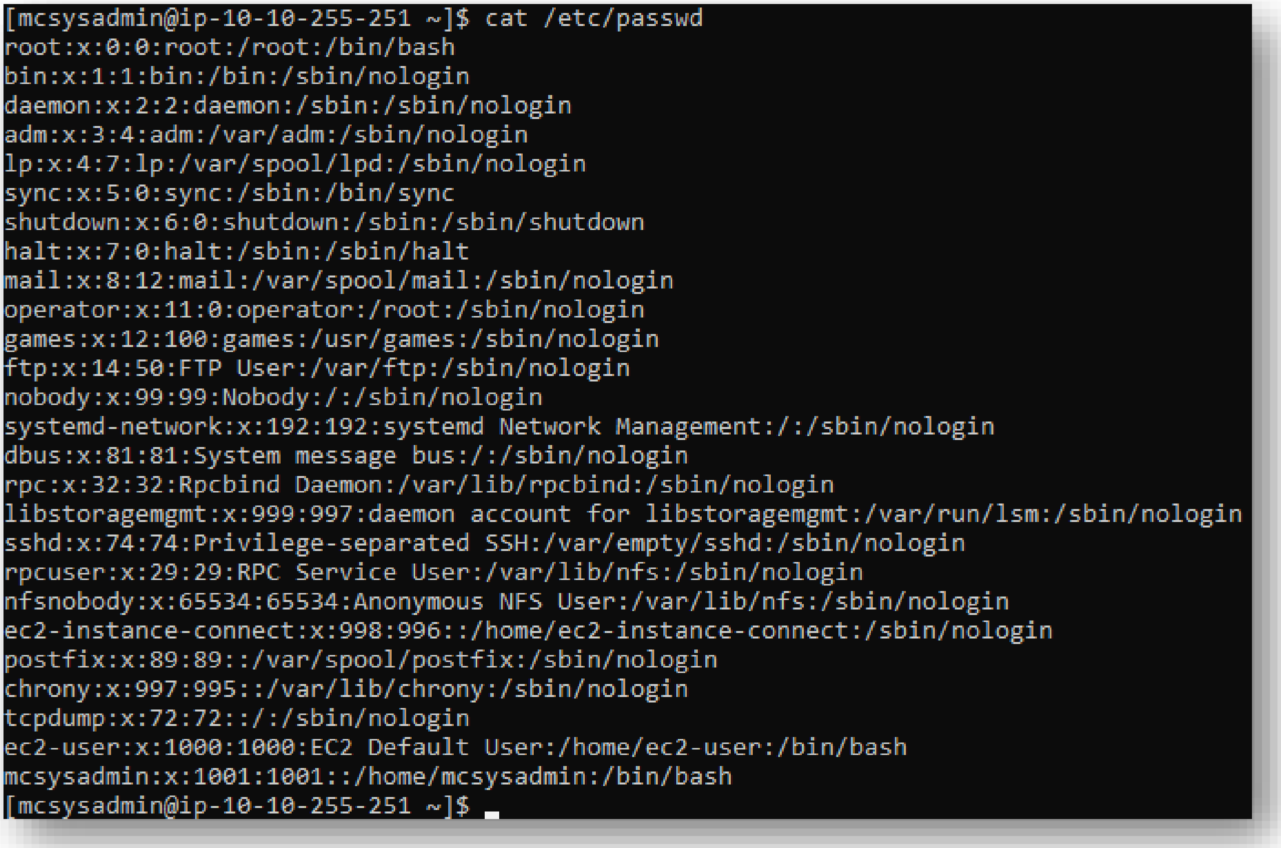
4. **What is the IP address in a file in the home folder?**



```
[mcsysadmin@ip-10-10-255-251 ~]$ grep '\.' file1
[mcsysadmin@ip-10-10-255-251 ~]$ grep '\.' file2
10.0.0.05eXWx4auBc8Swra4aPvIoBre+PRsVgu9GVbGwD33X8bd7TWwlZxzSVYa
```

- Grep for a period, need to use the escape character or else grep’ing for a period will return everything in that file
- **10.0.0.05**

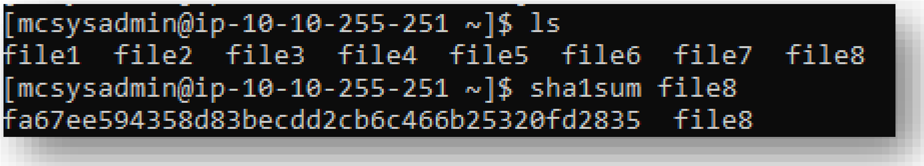
5. **How many users can log into the machine?**



```
[mcsysadmin@ip-10-10-255-251 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
libstoragemgmt:x:999:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
ec2-instance-connect:x:998:996::/home/ec2-instance-connect:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
ec2-user:x:1000:1000:EC2 Default User:/home/ec2-user:/bin/bash
mcsysadmin:x:1001:1001::/home/mcsysadmin:/bin/bash
[mcsysadmin@ip-10-10-255-251 ~]$ _
```

- To view information about users, check out the /etc/passwd file
- Out of all the listed users, only **three** do not have /nologin appended to their shell location

6. **What is the sha1 hash of file8?**

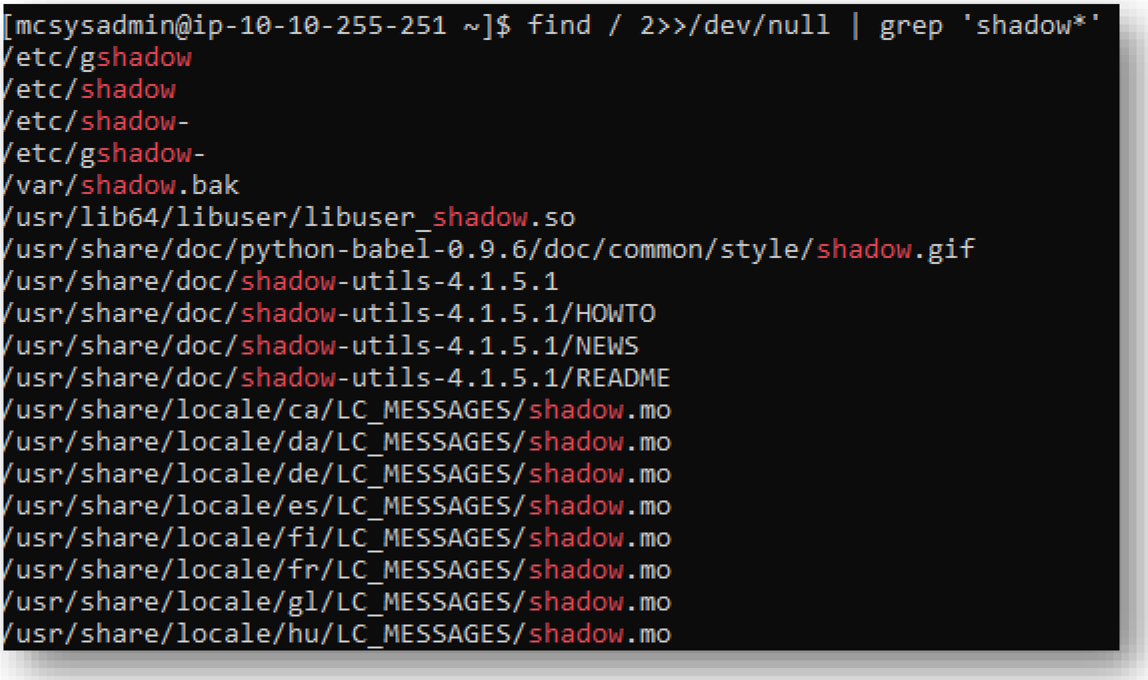


```
[mcsysadmin@ip-10-10-255-251 ~]$ ls
file1  file2  file3  file4  file5  file6  file7  file8
[mcsysadmin@ip-10-10-255-251 ~]$ sha1sum file8
fa67ee594358d83becdd2cb6c466b25320fd2835  file8
```

- Use the sha1sum command to generate the sha1 hash of file8
- **fa67ee594358d83becdd2cb6c466b25320fd2835**

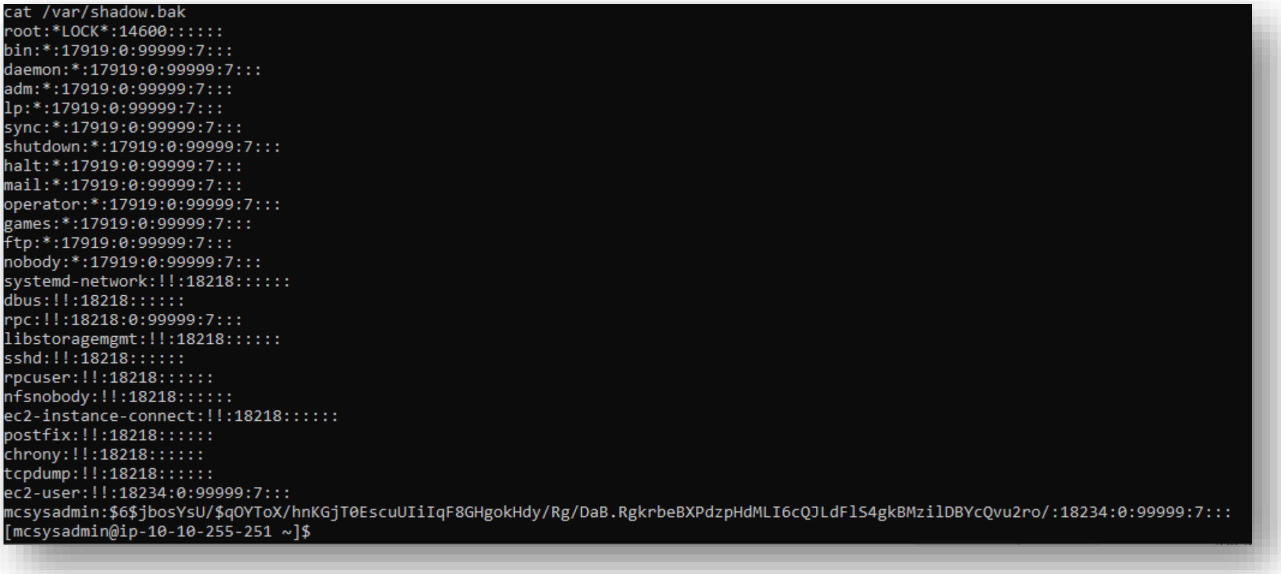
7. **What is mcsysadmin's password hash?**
   - Can find user's password hashes in /etc/shadow
   - But we do not have root access, and cannot give ourselves root access

- Try to find a copy or older version of that shadow file
- Use the find command to search for a file in linux
- Then can filter the output of that search for ‘shadow’ with grep



```
[mcsysadmin@ip-10-10-255-251 ~]$ find / 2>>/dev/null | grep 'shadow*'
/etc/gshadow
/etc/shadow
/etc/shadow-
/etc/gshadow-
/var/shadow.bak
/usr/lib64/libuser/libuser_shadow.so
/usr/share/doc/python-babel-0.9.6/doc/common/style/shadow.gif
/usr/share/doc/shadow-utils-4.1.5.1
/usr/share/doc/shadow-utils-4.1.5.1/HOWTO
/usr/share/doc/shadow-utils-4.1.5.1/NEWS
/usr/share/doc/shadow-utils-4.1.5.1/README
/usr/share/locale/ca/LC_MESSAGES/shadow.mo
/usr/share/locale/da/LC_MESSAGES/shadow.mo
/usr/share/locale/de/LC_MESSAGES/shadow.mo
/usr/share/locale/es/LC_MESSAGES/shadow.mo
/usr/share/locale/fi/LC_MESSAGES/shadow.mo
/usr/share/locale/fr/LC_MESSAGES/shadow.mo
/usr/share/locale/gl/LC_MESSAGES/shadow.mo
/usr/share/locale/hu/LC_MESSAGES/shadow.mo
```

- There is a version of shadow.bak in /var/



```
cat /var/shadow.bak
root:*LOCK*:14600::::::
bin:*:17919:0:99999:7:::
daemon:*:17919:0:99999:7:::
adm:*:17919:0:99999:7:::
lp:*:17919:0:99999:7:::
sync:*:17919:0:99999:7:::
shutdown:*:17919:0:99999:7:::
halt:*:17919:0:99999:7:::
mail:*:17919:0:99999:7:::
operator:*:17919:0:99999:7:::
games:*:17919:0:99999:7:::
ftp:*:17919:0:99999:7:::
nobody:*:17919:0:99999:7:::
systemd-network:!!:18218::::::
dbus:!!:18218::::::
rpc:!!:18218:0:99999:7:::
libstoragemgmt:!!:18218::::::
sshd:!!:18218::::::
rpcuser:!!:18218::::::
nfsnobody:!!:18218::::::
ec2-instance-connect:!!:18218::::::
postfix:!!:18218::::::
chrony:!!:18218::::::
tcpdump:!!:18218::::::
ec2-user:!!:18234:0:99999:7:::
mcsysadmin:$6$jbosYsU/$qOYToX/hnKGjT0EscuUIiIqF8GHgokHdy/Rg/DaB.RgkrbeBXPdzpHdMLI6cQJLdFlS4gkBMzilDBYcQvu2ro/:18234:0:99999:7:::
[mcsysadmin@ip-10-10-255-251 ~]$
```

- **$6$jbosYsU/$qOYToX/hnKGjT0EscuUIiIqF8GHgokHdy/Rg/DaB.RgkrbeBXPdzpHdMLI6cQJLdFlS4gkBMzilDBYcQvu2ro/:18234:0:99999:7:::**