

Day 4 - Training

Scenario

Task 9 [Day 4] Training



Deploy

With the entire incident, McElferson has been *very* stressed.

We need all hands on deck now

To help resolve things faster, she has asked you to help the new intern(mcsysadmin) get familiar with Linux.
Access the machine via SSH on port 22 using the command

```
ssh mcsysadmin@[your-machines-ip]
```

username: mcsysadmin

password: bestelf1234

Check out the supporting material [here](#)

now let's login into msysadmin ssh account with the credential provided

```
(nobodyatall@0xDEADBEEF)-[~/Desktop/research]
$ ssh mcsysadmin@10.10.26.238
The authenticity of host '10.10.26.238 (10.10.26.238)' can't be established.
ECDSA key fingerprint is SHA256:IYNPmKurskzl/7GcTFinzOmOKtpQWPkd4wxR3P3pvvI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.26.238' (ECDSA) to the list of known hosts.
mcsysadmin@10.10.26.238'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-10-10-26-238 ~]$
```

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

```
https://aws.amazon.com/amazon-linux-2/
[mcsysadmin@ip-10-10-26-238 ~]$ ls
file1  file2  file3  file4  file5  file6  file7  file8
[mcsysadmin@ip-10-10-26-238 ~]$
```

-8

Question: What is the content of file5?

```
[mcsysadmin@ip-10-10-26-238 ~]$ cat file5
recipes
[mcsysadmin@ip-10-10-26-238 ~]$
```

-recipes

Question: Which file contains the string 'password'?

-grep -H = with filename

```
[mcsysadmin@ip-10-10-26-238 ~]$ find . -type f -exec grep -H 'password' {} \;
./file6:passwordHpKRQfdxzZocwg500RsiyLSVQon72CjFmsV4ZLGjxI8tXYo1NhLsEpLy
[mcsysadmin@ip-10-10-26-238 ~]$
```

-file6

Question: What is the IP address in a file in the home folder?

-grep -Eo = using Extended regex + only matches

```
[mcsysadmin@ip-10-10-26-238 ~]$ find . -type f -exec grep -H -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}
\.[0-9]{1,3}' {} \;
./file2:10.0.0.05
[mcsysadmin@ip-10-10-26-238 ~]$
```

-10.0.0.05

Question: How many users can log into the machine?

-we can check the /etc/passwd to check users that have a shell(bash, sh, zsh,etc) when login
-by removing the sync user, we'll have 3 users that can log into the machine

```
[mcsysadmin@ip-10-10-26-238 ~]$ grep -v '/sbin/' /etc/passwd
root:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
ec2-user:x:1000:1000:EC2 Default User:/home/ec2-user:/bin/bash
mcsysadmin:x:1001:1001::/home/mcsysadmin:/bin/bash
[mcsysadmin@ip-10-10-26-238 ~]$
```

-3

Question: What is the sha1 hash of file8?

```
[mcsysadmin@ip-10-10-26-238 ~]$ sha1sum file8
fa67ee594358d83becdd2cb6c466b25320fd2835  file8
[mcsysadmin@ip-10-10-26-238 ~]$
```

-fa67ee594358d83becdd2cb6c466b25320fd2835

Question: What is mcsysadmin's password hash?

if we find any shadow files that we can read, it seems that there's a shadow.bak we've found in the /var directory

```
[mcsysadmin@ip-10-10-26-238 ~]$ find / -name shadow* -type f 2>/dev/null
/etc/shadow
/etc/shadow-
/var/shadow.bak
```

the content of shadow.bak & it seems like this was the shadow backup file!

```
[mcsysadmin@ip-10-10-26-238 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:::::::::
```

mcsysadmin password hash

```
mcsysadmin:$6$jbosYsU/$qOYToX/hnKGjT0EscuUIiIqF8GHgokHdy/Rg/DaB.RgkrbeBXPdzpHdMLI6cQJLdFIS4gkBMzilD
BYcQvu2ro/:18234:0:99999:7:::
```

-\$6\$jbosYsU/\$qOYToX/hnKGjT0EscuUIiIqF8GHgokHdy/Rg/
DaB.RgkrbeBXPdzpHdMLI6cQJLdFIS4gkBMzilDBYcQvu2ro/