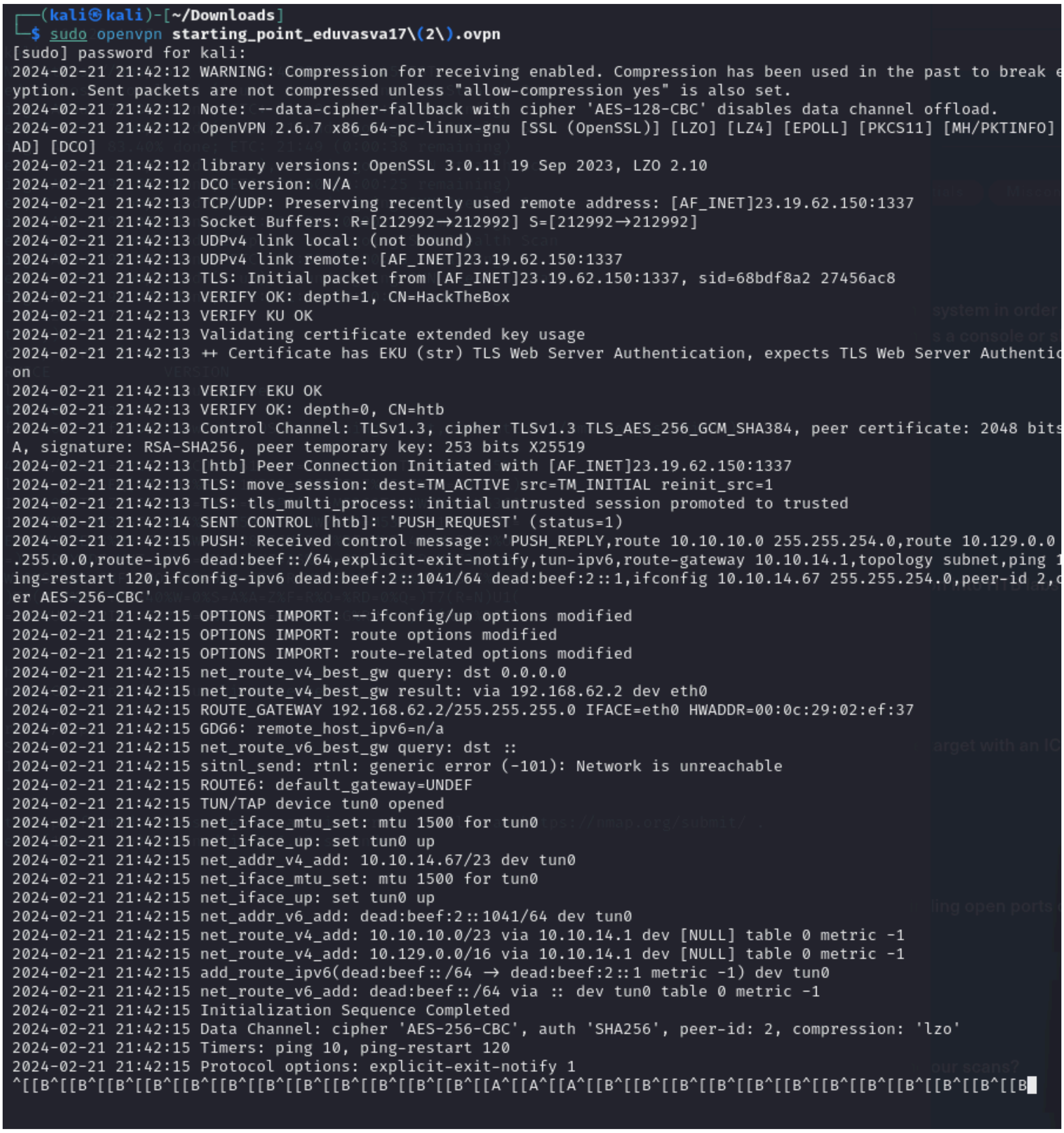
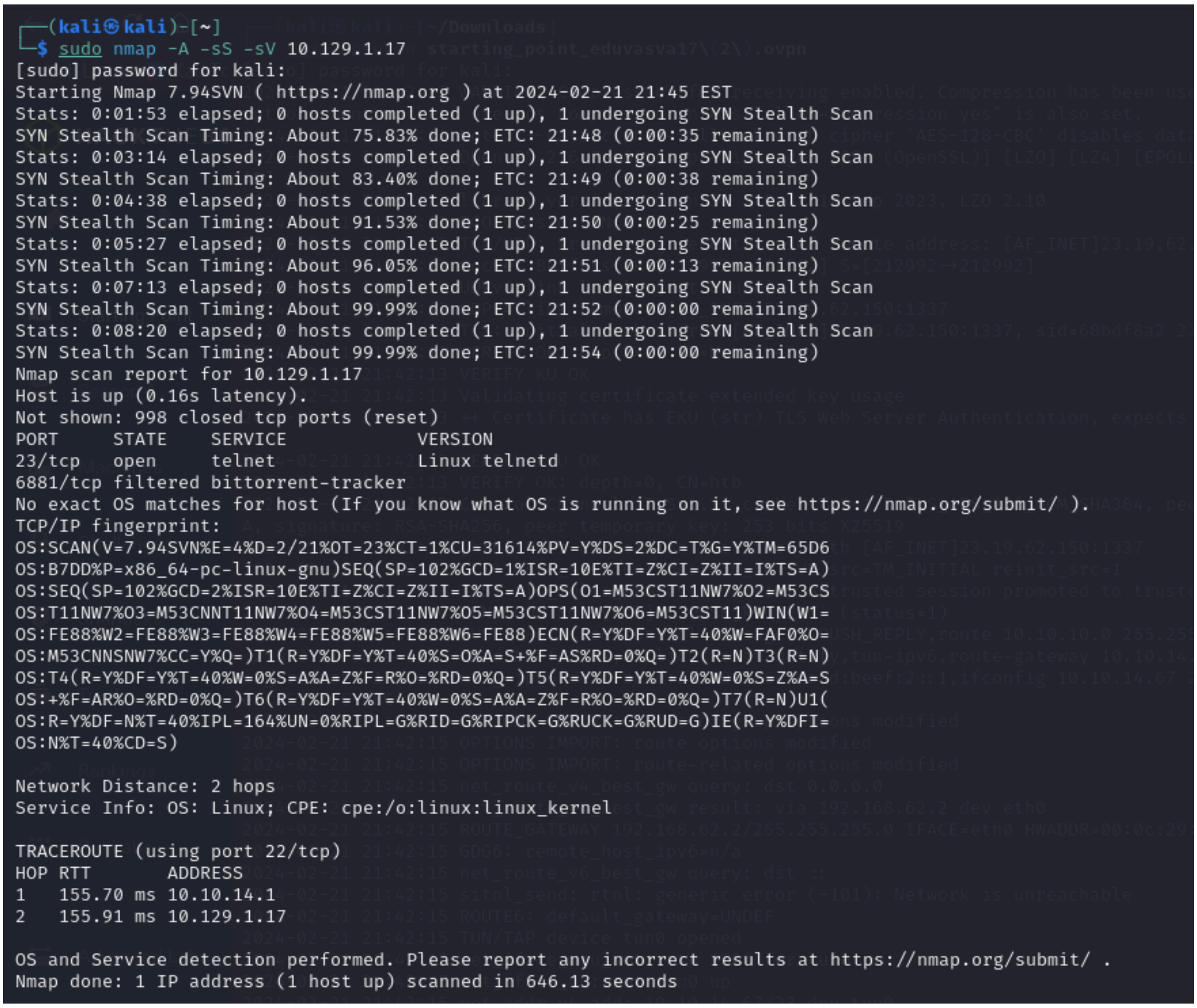
Descargamos y agregamos el open vpn para las máquinas del starting point



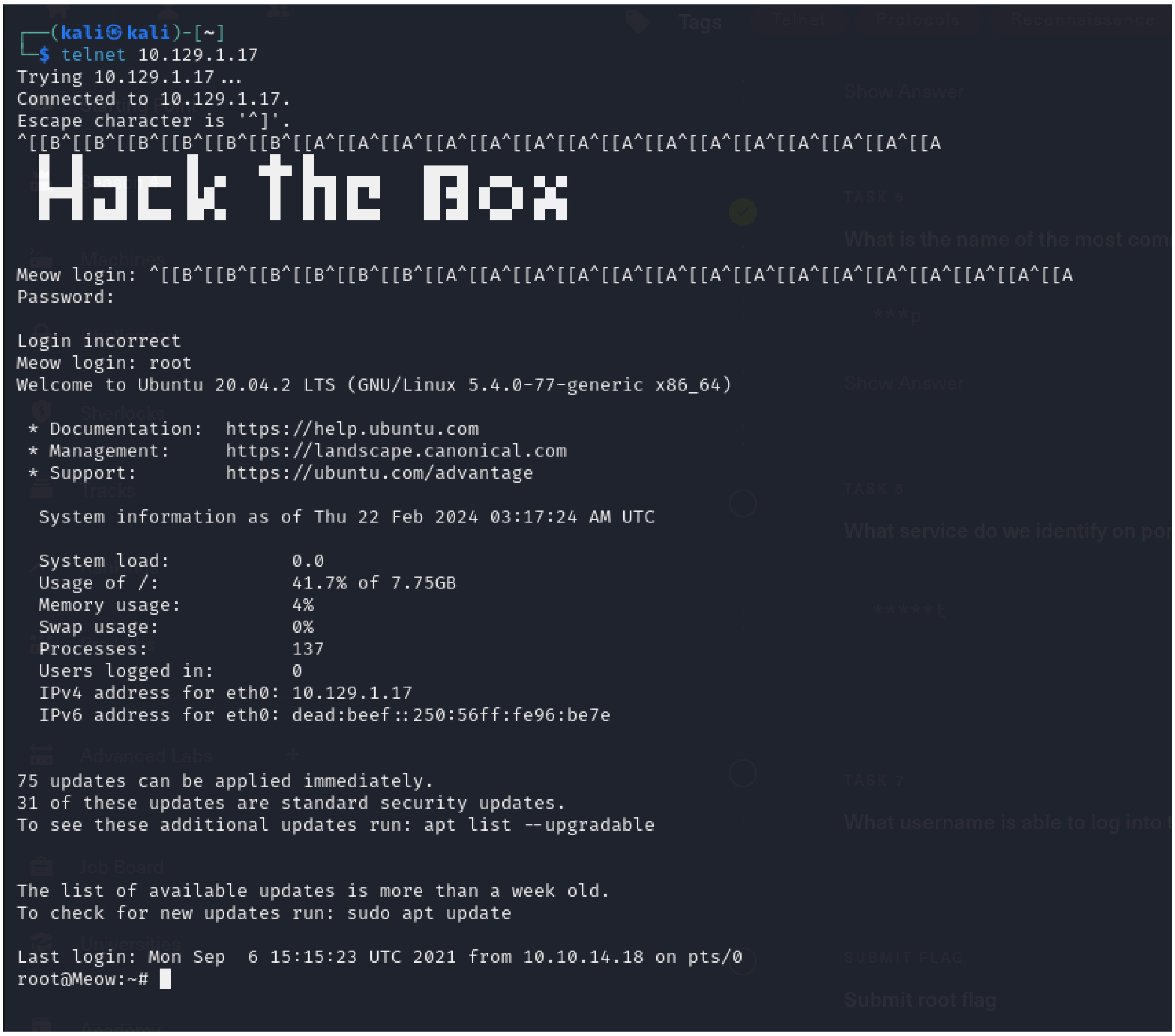
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn starting_point_eduvasva17\(2\).ovpn
[sudo] password for kali:
2024-02-21 21:42:12 WARNING: Compression for receiving enabled. Compression has been used in the past to break e
yption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-02-21 21:42:12 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-02-21 21:42:12 OpenVPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
AD] [DCO]
2024-02-21 21:42:12 library versions: OpenSSL 3.0.11 19 Sep 2023, LZO 2.10
2024-02-21 21:42:12 DCO version: N/A
2024-02-21 21:42:13 TCP/UDP: Preserving recently used remote address: [AF_INET]23.19.62.150:1337
2024-02-21 21:42:13 Socket Buffers: R=[212992→212992] S=[212992→212992]
2024-02-21 21:42:13 UDPv4 link local: (not bound)
2024-02-21 21:42:13 UDPv4 link remote: [AF_INET]23.19.62.150:1337
2024-02-21 21:42:13 TLS: Initial packet from [AF_INET]23.19.62.150:1337, sid=68bdf8a2 27456ac8
2024-02-21 21:42:13 VERIFY OK: depth=1, CN=HackTheBox
2024-02-21 21:42:13 VERIFY KU OK
2024-02-21 21:42:13 Validating certificate extended key usage
2024-02-21 21:42:13 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentic
on
2024-02-21 21:42:13 VERIFY EKU OK
2024-02-21 21:42:13 VERIFY OK: depth=0, CN=htb
2024-02-21 21:42:13 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits
A, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2024-02-21 21:42:13 [htb] Peer Connection Initiated with [AF_INET]23.19.62.150:1337
2024-02-21 21:42:13 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-02-21 21:42:13 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-02-21 21:42:14 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2024-02-21 21:42:15 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0
.255.0.0,route-ipv6 dead:beef::/64,explicit-exit-notify,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 1
ing-restart 120,ifconfig-ipv6 dead:beef:2::1041/64 dead:beef:2::1,ifconfig 10.10.14.67 255.255.254.0,peer-id 2,c
er AES-256-CBC'
2024-02-21 21:42:15 OPTIONS IMPORT: --ifconfig/up options modified
2024-02-21 21:42:15 OPTIONS IMPORT: route options modified
2024-02-21 21:42:15 OPTIONS IMPORT: route-related options modified
2024-02-21 21:42:15 net_route_v4_best_gw query: dst 0.0.0.0
2024-02-21 21:42:15 net_route_v4_best_gw result: via 192.168.62.2 dev eth0
2024-02-21 21:42:15 ROUTE_GATEWAY 192.168.62.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:02:ef:37
2024-02-21 21:42:15 GDG6: remote_host_ipv6=n/a
2024-02-21 21:42:15 net_route_v6_best_gw query: dst ::
2024-02-21 21:42:15 sitnl_send: rtnl: generic error (-101): Network is unreachable
2024-02-21 21:42:15 ROUTE6: default_gateway=UNDEF
2024-02-21 21:42:15 TUN/TAP device tun0 opened
2024-02-21 21:42:15 net_iface_mtu_set: mtu 1500 for tun0
2024-02-21 21:42:15 net_iface_up: set tun0 up
2024-02-21 21:42:15 net_addr_v4_add: 10.10.14.67/23 dev tun0
2024-02-21 21:42:15 net_iface_mtu_set: mtu 1500 for tun0
2024-02-21 21:42:15 net_iface_up: set tun0 up
2024-02-21 21:42:15 net_addr_v6_add: dead:beef:2::1041/64 dev tun0
2024-02-21 21:42:15 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-02-21 21:42:15 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-02-21 21:42:15 add_route_ipv6(dead:beef::/64 → dead:beef:2::1 metric -1) dev tun0
2024-02-21 21:42:15 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2024-02-21 21:42:15 Initialization Sequence Completed
2024-02-21 21:42:15 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-id: 2, compression: 'lzo'
2024-02-21 21:42:15 Timers: ping 10, ping-restart 120
2024-02-21 21:42:15 Protocol options: explicit-exit-notify 1
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B
```

Realizamos el nmap en la maquina meow



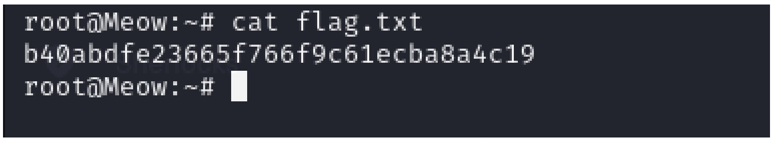
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -sS -sV 10.129.1.17
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 21:45 EST
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.83% done; ETC: 21:48 (0:00:35 remaining)
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.40% done; ETC: 21:49 (0:00:38 remaining)
Stats: 0:04:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.53% done; ETC: 21:50 (0:00:25 remaining)
Stats: 0:05:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.05% done; ETC: 21:51 (0:00:13 remaining)
Stats: 0:07:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 21:52 (0:00:00 remaining)
Stats: 0:08:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 21:54 (0:00:00 remaining)
Nmap scan report for 10.129.1.17
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE    SERVICE            VERSION
23/tcp   open     telnet             Linux telnetd
6881/tcp filtered bittorrent-tracker
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=7.94SVN%E=4%D=2/21%OT=23%CT=1%CU=31614%PV=Y%DS=2%DC=T%G=Y%TM=65D6
OS:B7DD%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=102%GCD=2%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CS
OS:T11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=
OS:FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=
OS:M53CNNSNW7%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)
OS:T4(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=N)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

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

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   155.70 ms 10.10.14.1
2   155.91 ms 10.129.1.17

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 646.13 seconds
```

vemos que el puerto 23 esta abierto con telnet e ingresamos con el usuario por defecto



```
┌──(kali㉿kali)-[~]
└─$ telnet 10.129.1.17
Trying 10.129.1.17...
Connected to 10.129.1.17.
Escape character is '^]'.
^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A
 Hack the Box


Meow login: ^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A
Password:

Login incorrect
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 Thu 22 Feb 2024 03:17:24 AM UTC

  System load:           0.0
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             137
  Users logged in:       0
  IPv4 address for eth0: 10.129.1.17
  IPv6 address for eth0: dead:beef::250:56ff:fe96:be7e


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:~# 
```

Para demostrar que ya tenemos acceso a la maquina buscamos la flag con el comando “cat falg.txt”



```
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~# 
```

Las respuestas en la pagina sobre la maquina son:
Virtual machine
Terminal
Openvpn
Ping
Nmap
Telnet
Root