

HTB Write-up: Meow (Easy)

GOAL: flag capture

Tools used : nmap,tcp

ENVIRONMENT SETUP

VPN:

client

dev tun

proto udp

remote edge-eu-starting-point-2-dhcp.hackthebox.eu 1337

resolv-retry infinite

nobind

persist-key

persist-tun

remote-cert-tls server

comp-lzo

verb 3

data-ciphers-fallback AES-128-CBC

data-ciphers

AES-256-CBC:AES-256-CFB:AES-256-CFB1:AES-256-CFB8:AES-256-OFB:AES-256-GCM

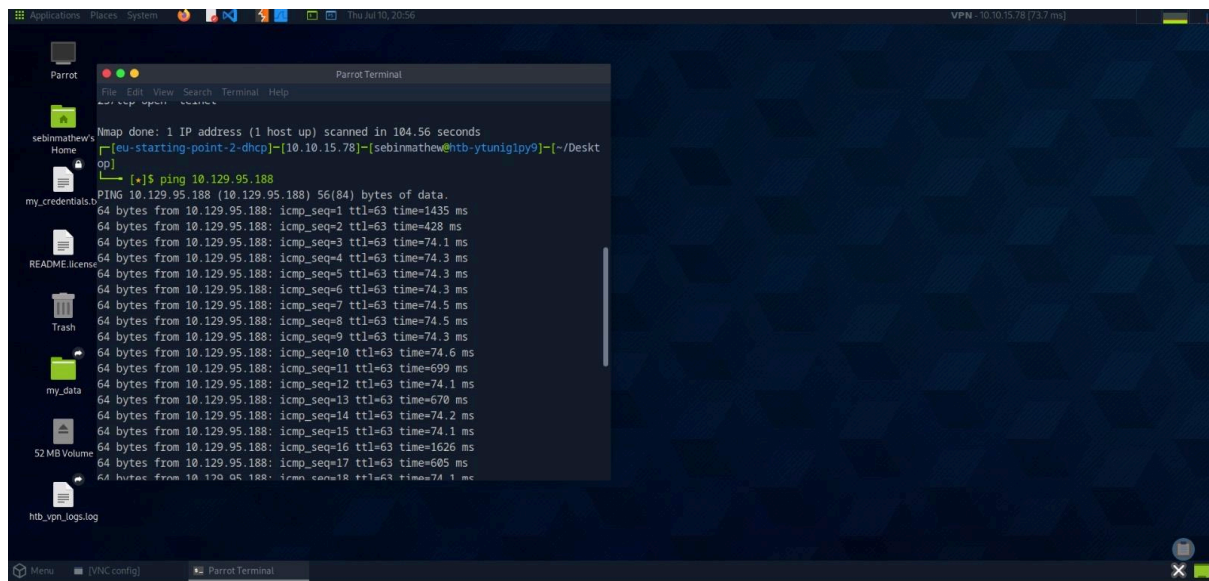
tls-cipher "DEFAULT:@SECLEVEL=0"

auth SHA256

key-direction 1

Machine Ip:10.129.95.188

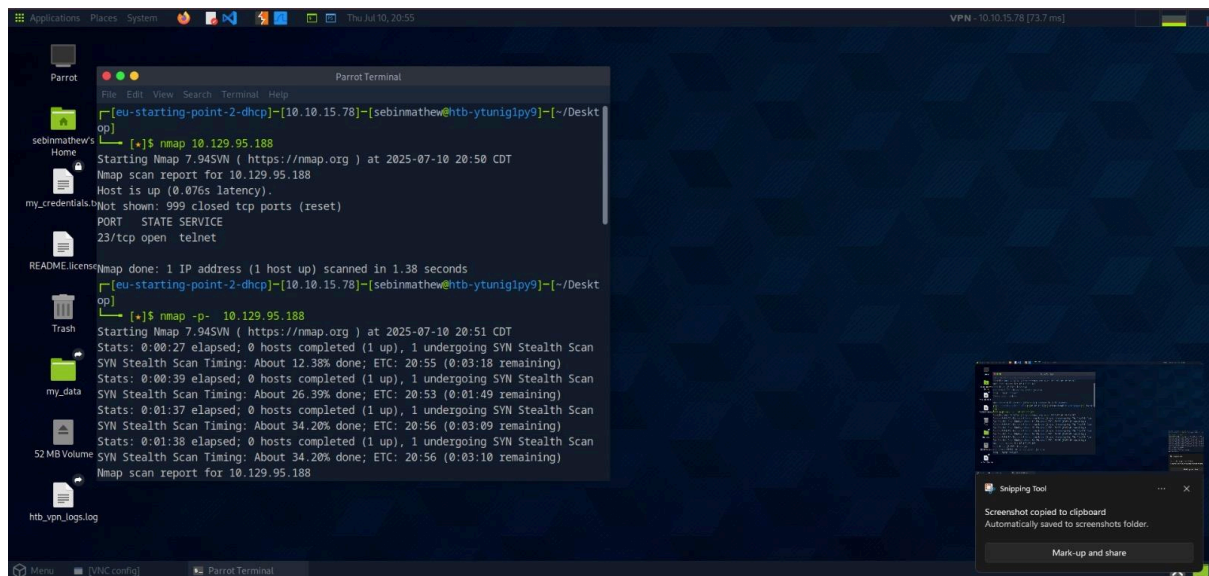
Reconnaissance



Ping command: Ping 10.129.95.188

Ping output

```
64 bytes from 10.129.95.188: icmp_seq=1 ttl=63 time=1435 ms
64 bytes from 10.129.95.188: icmp_seq=2 ttl=63 time=428 ms
. 64 bytes from 10.129.95.188: icmp_seq=3 ttl=63 time=74.1 ms
```



Nmap command : nmap 10.129.95.188

Nmap output

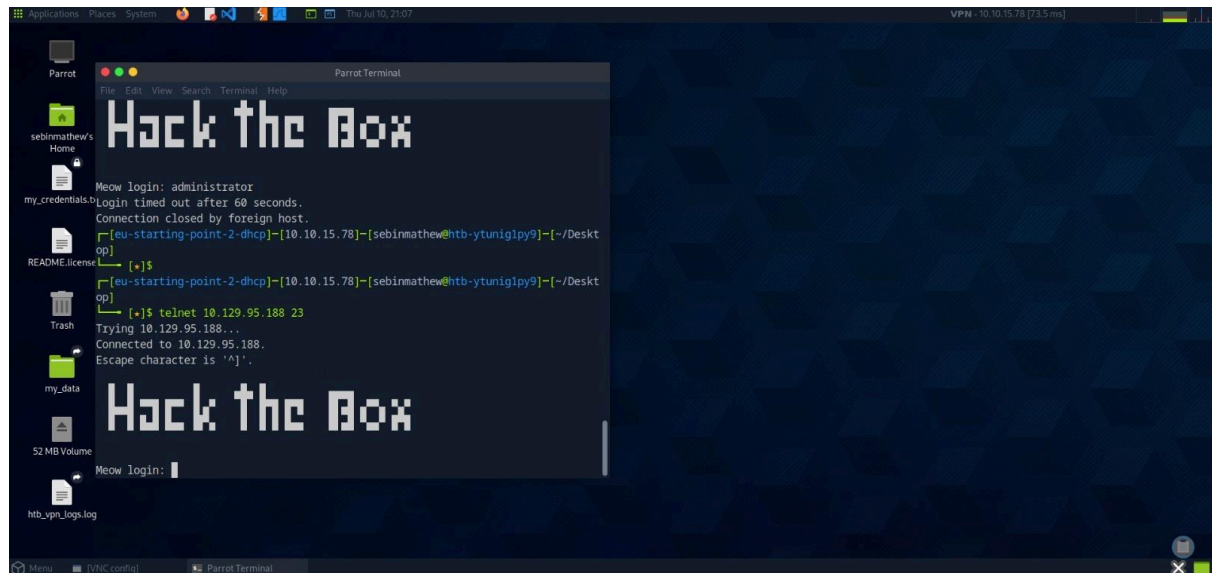
Host is up

Port: 23/tcp

State:open

Service:telnet

Enumeration



TCP Commands: TCP 10.129.95.188

Username: 'administrator'

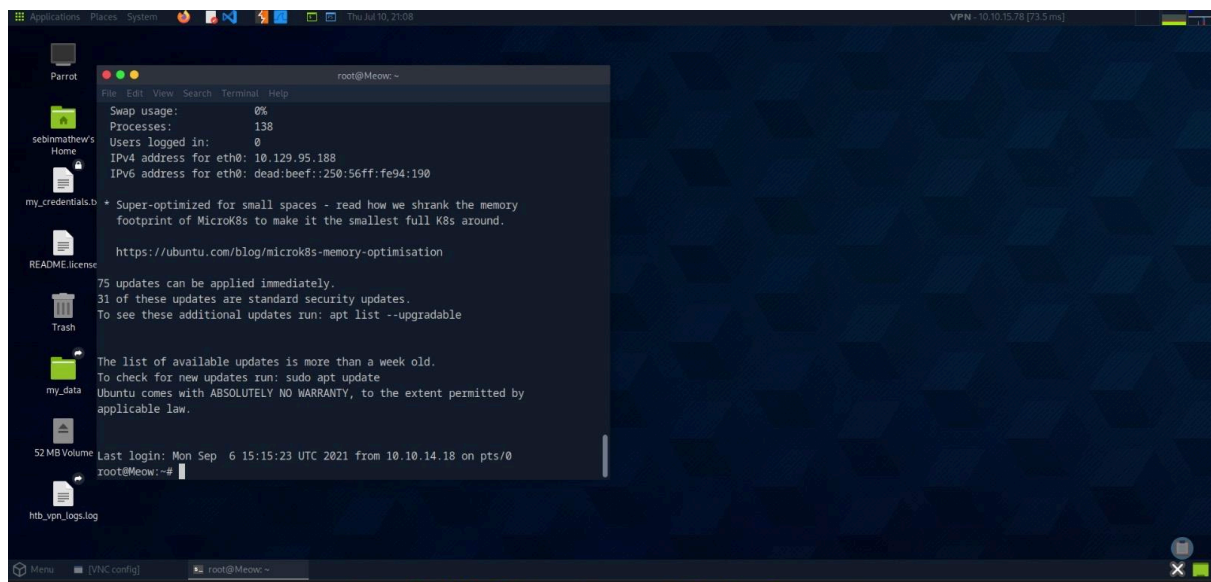
Password: ''

ls

Get flag.txt

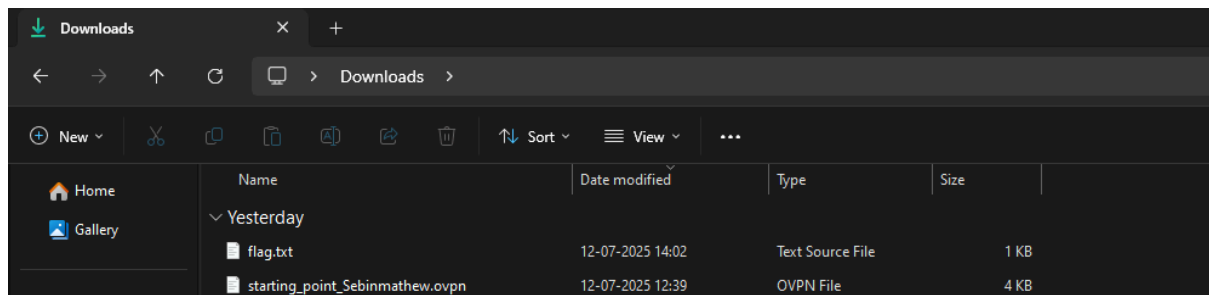
Initial Access

Vulnerability: weak credentials/misconfiguration



Flags:

Root flag.txt: 035db21c881520061c53e0536e44f815



[illegible]