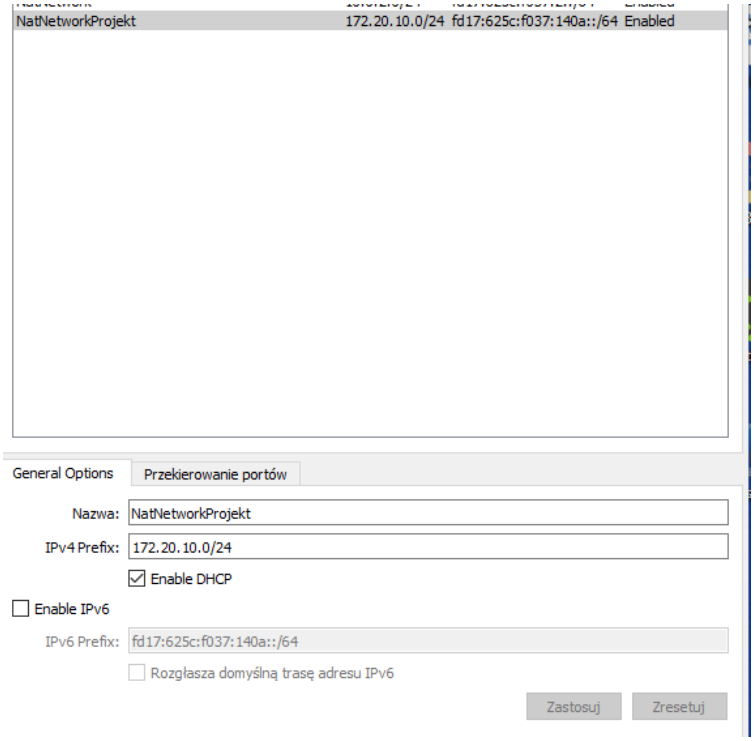
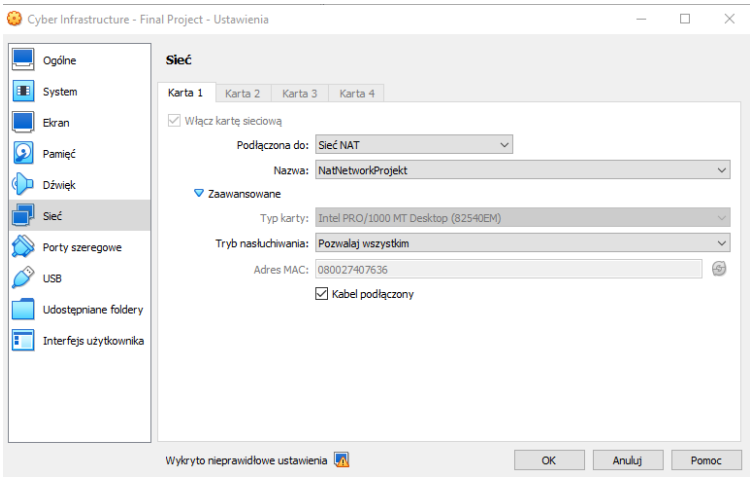
Project III
Bypassing the perimeter

Frejer Witold

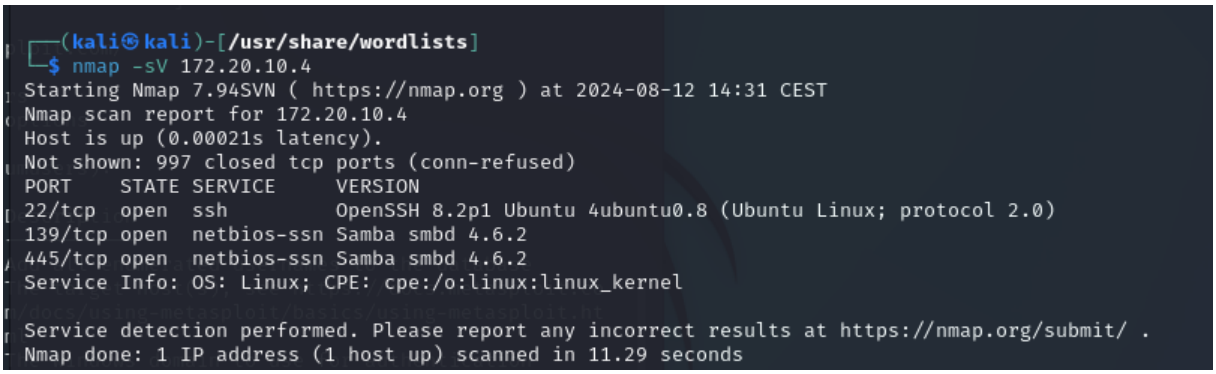
Note: Remember to set up the imported machine and your Kali machine to use the NAT Network interface (172.20.10.0/24)





Scan a given network and find a vulnerable machine with open ports.

1 Use a scanning tool (Nmap) to enumerate the vulnerable machine.



The first step involved scanning the network to identify machines with open ports. We used Nmap to determine which ports were accessible on machines within the 172.20.10.4 network.

Command Executed:

bash
nmap –sV 172.20.10.4

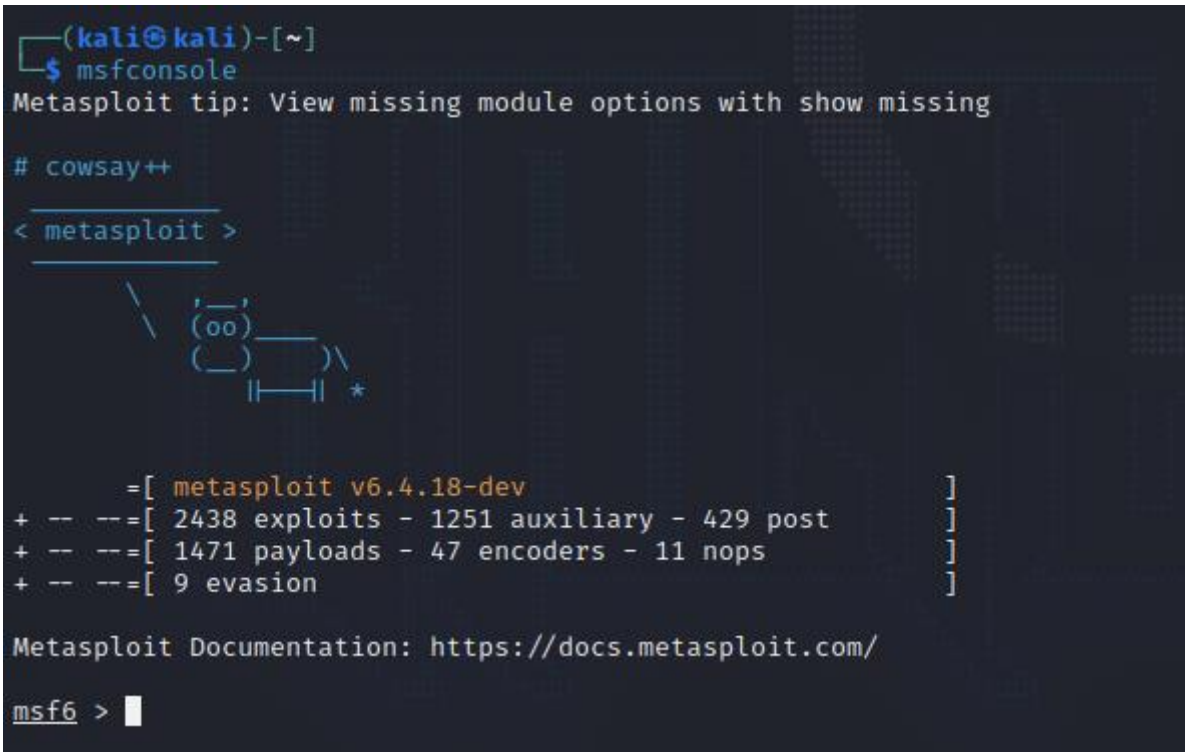
Results:

172.20.10.4: Ports 139 and 445 open (Samba smbd 4.6.2)

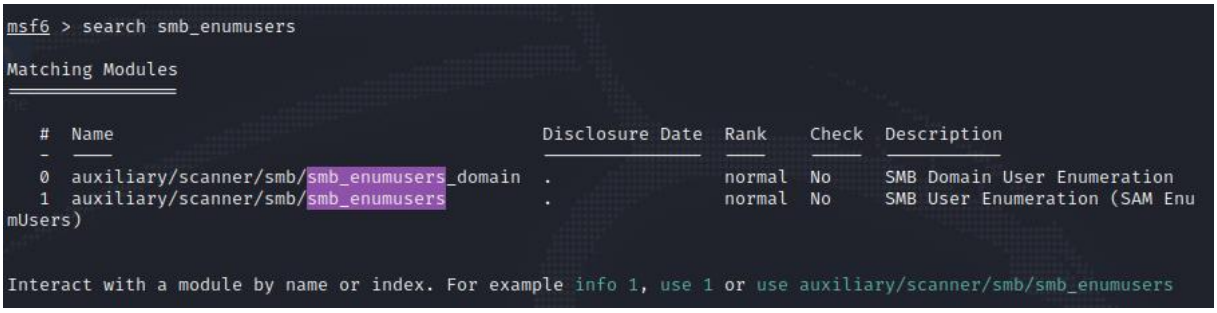
So we can execute metasploit on port 445.

2 Use Metasploit to find an exploit for username enumeration according to the open services you found in the vulnerable machine.

We utilized Metasploit to enumerate users on the SMB server running on port 445.

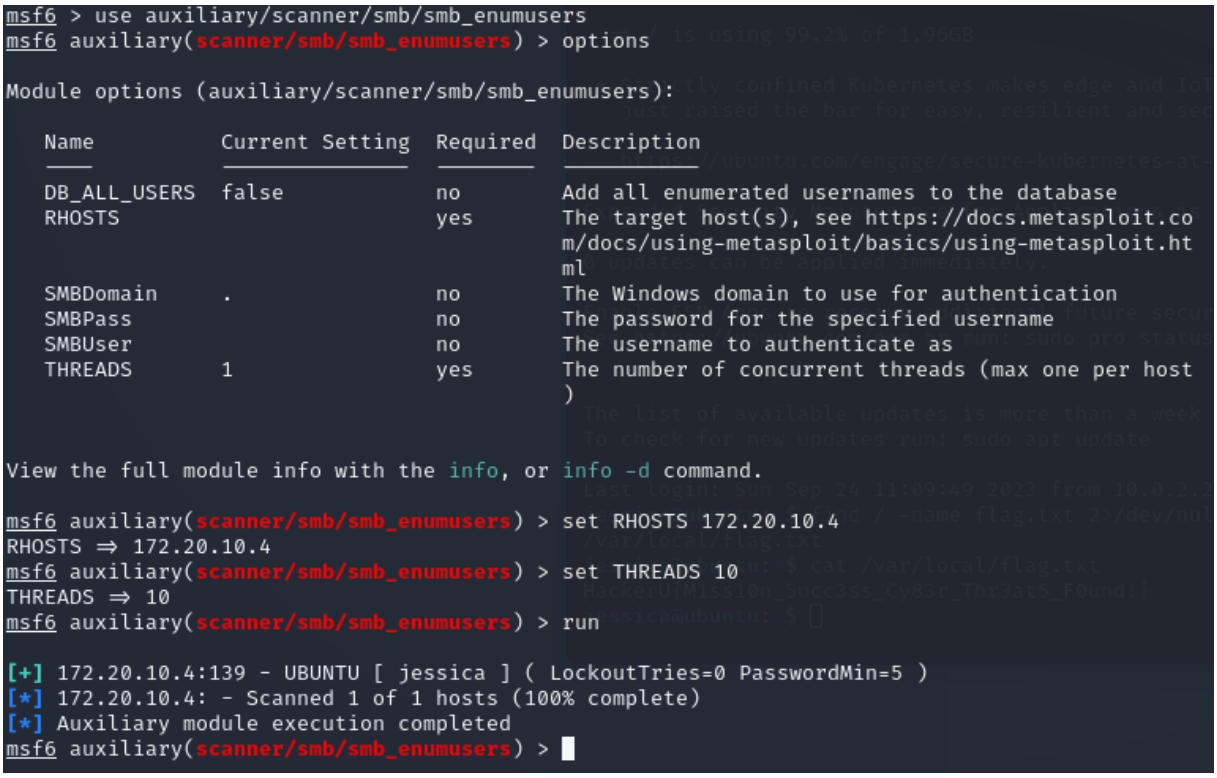


Search for exploit for SMB service on Metasploit.



Use the smb_enumusers exploit to enumerate users working via the SMB service.

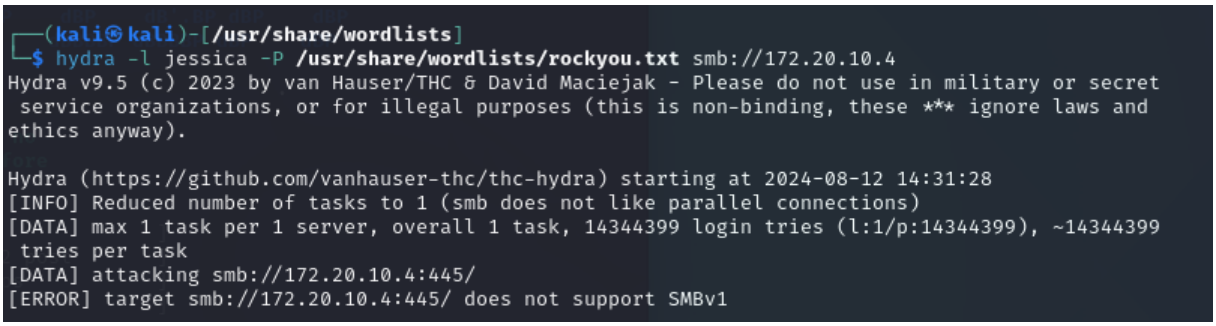
Use the smb_enumusers module to enumerate users:



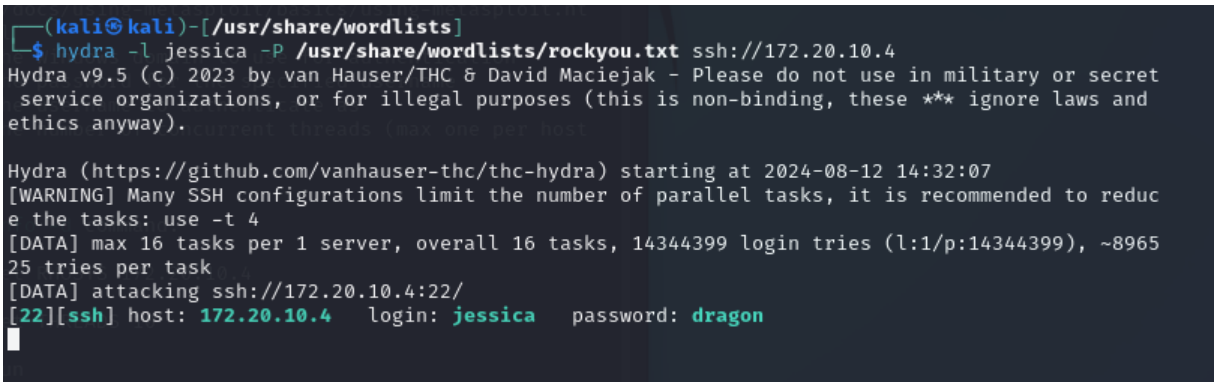
The enumeration process provided a list of usernames from the SMB service.

3 Use Hydra to crack the password using the username you found with rockyou.txt wordlist.

We used Hydra to attempt password cracking against the usernames found through SMB enumeration. The rockyou.txt wordlist was used for brute-force attempts. Login is jessica we get it from metasploit response.



As you see there is a problem with attack target by SMB version 1. Hydra doesnt support it. So I decide to attack machine with ssh protocole, it was also open as you see in nmap results.

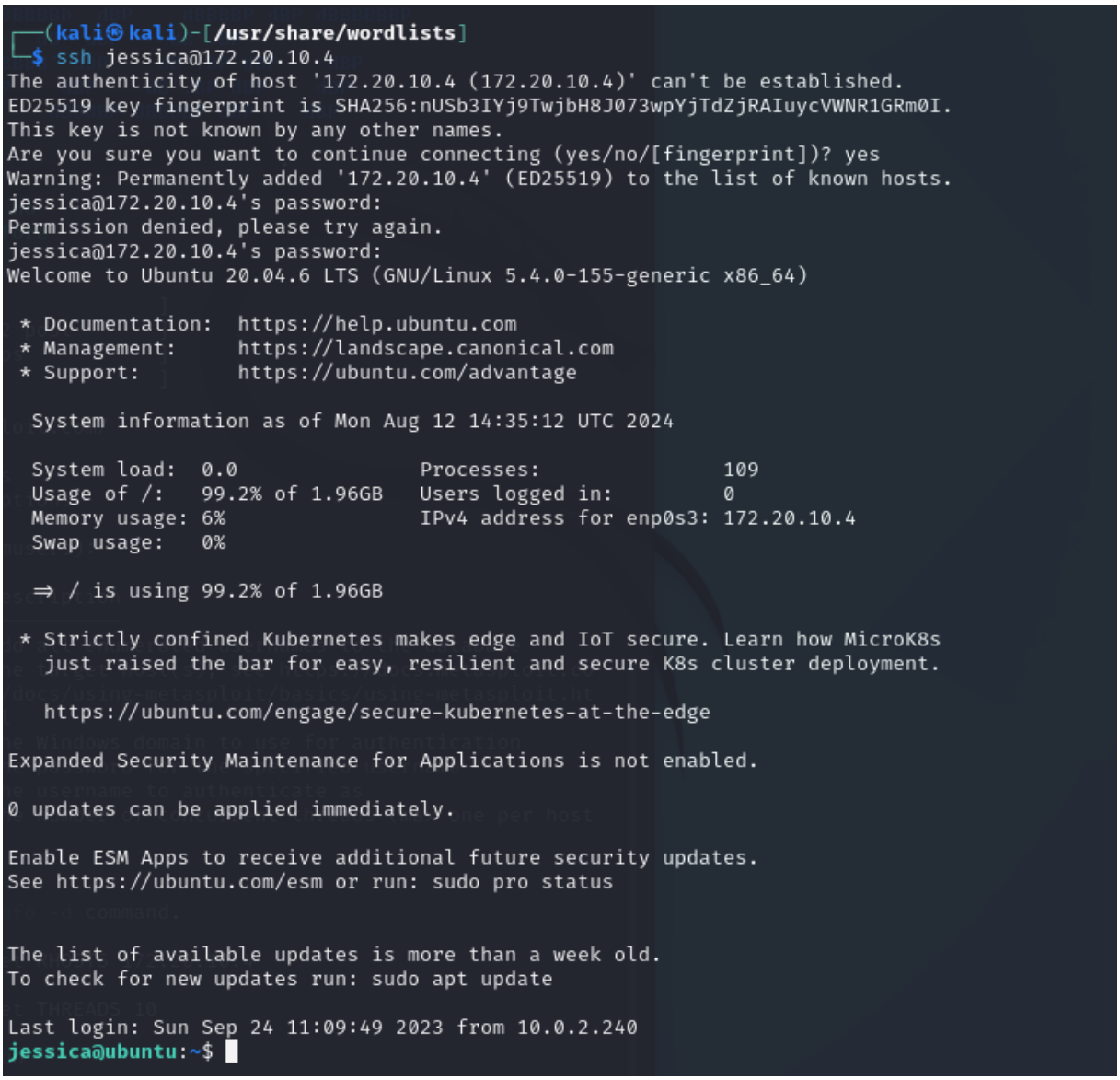


We Get the password.

Login : jessica password: dragon

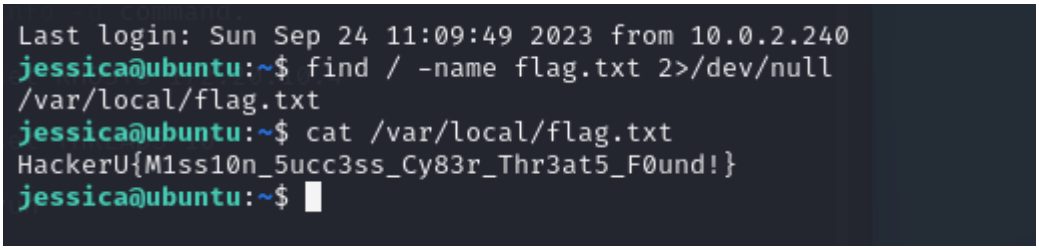
4 Connect remotely via SSH using the username and password you found.

After successfully cracking the password, we used the obtained credentials to connect to the target machine via SSH.



Successfully logged into the target machine.

5 Find the flag.txt file and read the content.

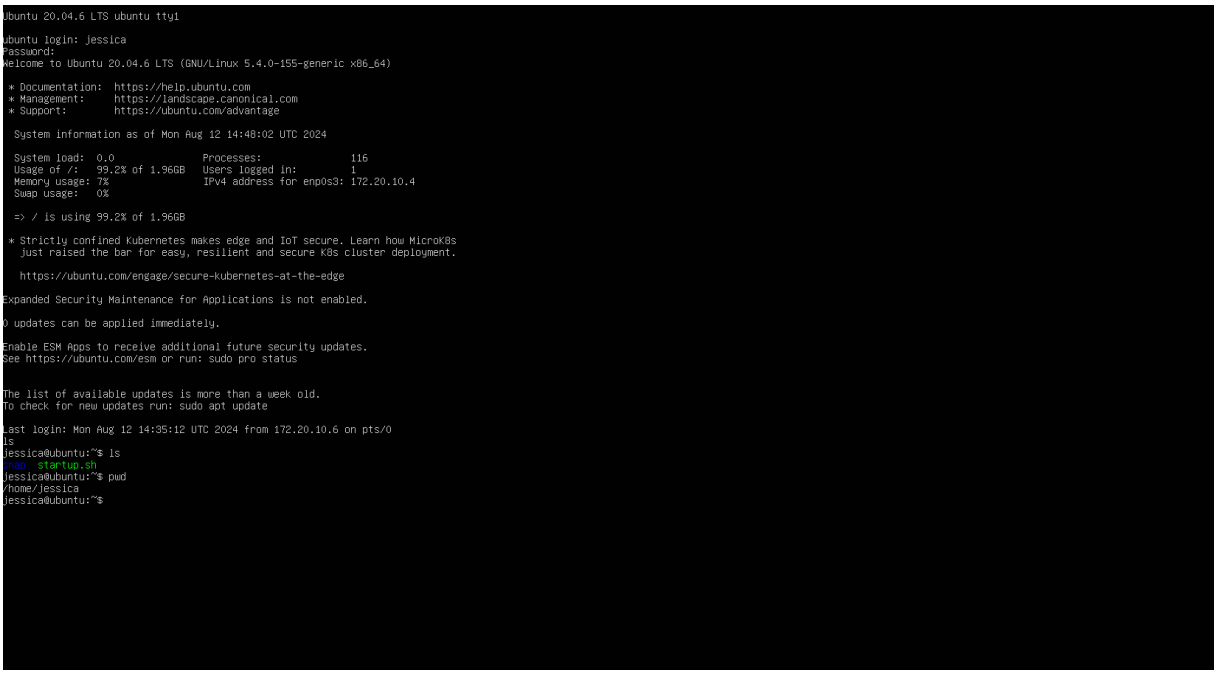


Once connected via SSH, we searched for the flag.txt file and read its contents.

Located and read the content of the flag.txt file.

Flag is Hackeru{…}

Well done.



Proof.