

## 1- ARROW

Telnet internet üzerinden sunuculara ulaşmak için kullanılan bir protokoldür. Lakin şifreleme olmadığından oldukça güvensiz bir protokoldür. Bu labımızda telnet e bağlanıp bilgi arayacağız.

Öncelikle NMAP kullanarak ağı tarıyorum ve ilk görevim olan açık portları bulma görevini tamamlıyorum.

```
[root@hackerbox]~# nmap 172.20.4.171
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 15:53 CDT
Nmap scan report for 172.20.4.171
Host is up (0.00035s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 52:54:00:0C:C4:23 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
[root@hackerbox]~#
```

23 portunun açık olduğunu görüyoruz. Genelde de 23 portu default olarak ayarlanmış bir porttur.

```
[root@hackerbox]~# 172.20.4.171 23
bash: 172.20.4.171: command not found
[x]-[root@hackerbox]~# telnet 72.20.4.171 23
Trying 72.20.4.171...
^C
[x]-[root@hackerbox]~# telnet 172.20.4.171
Trying 172.20.4.171...
Connected to 172.20.4.171.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: █
```

Belirtilen şekilde giriş yapıyorum. Hostname girerek hostname ismini bulabiliriz. Son görevimiz olan çalışma dizinimizi öğrenmek için pwd komutunu giriyoruz.

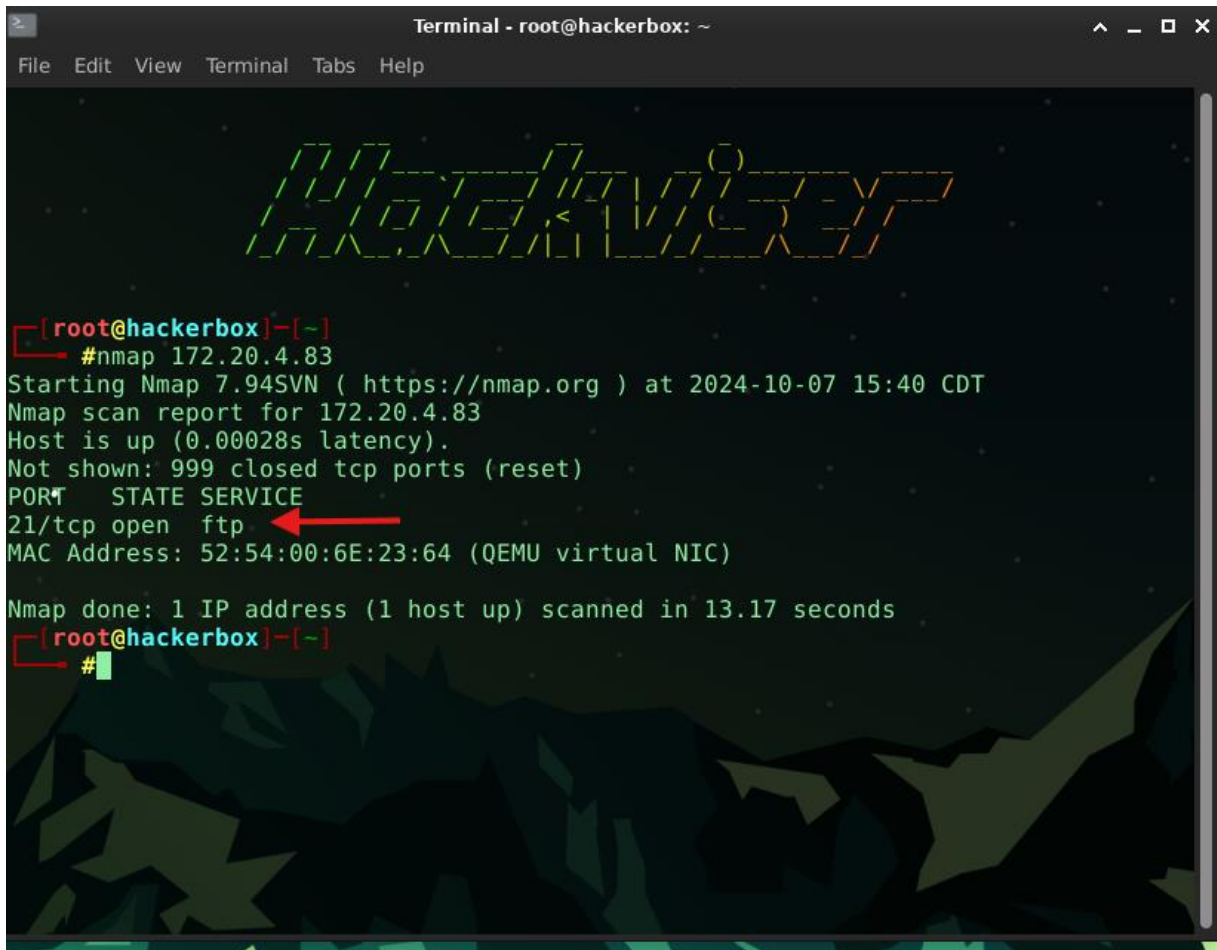
```
root@arrow:~# pwd
/root
root@arrow:~#
```

Görevimizi başarılı bir şekilde tamamladık!

## 2- FILE HUNTER

FTP (file transfer protocol) adından da anlaşılacağı üzere dosya aktarımı yapmak için kullanılan protokoldür.

İlk adım olarak yine nmap kullanalım.



```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help

[root@hackerbox]~# nmap 172.20.4.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 15:40 CDT
Nmap scan report for 172.20.4.83
Host is up (0.00028s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 52:54:00:6E:23:64 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
[root@hackerbox]~#
```

21 portunun açık olduğunu görüyoruz. 21 portu tcp için default değerdir.

```
[root@hackerbox]~# nmap 172.20.4.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 15:43 CDT
Nmap scan report for 172.20.4.83
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 52:54:00:6E:23:64 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
[root@hackerbox]~# ftp 172.20.4.83
Connected to 172.20.4.83.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.4.83:root): anonymous
```

İpucu içinde verilen kullanıcı adıyla giriş yapıyorum.

```
[root@hackerbox]~# ftp 172.20.4.83
Connected to 172.20.4.83.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.4.83:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Giriş Başarılı! Dosyaları görüntülemek için ls komutunu kullanıyorum. Amacım kullanıcı bilgilerinin olduğu bir dosya bulmak. User list dosyasını buluyorum (Resimler silinmiş). Cat ile okuyup içeri görebiliriz. (Daha öncesinde get komutu ile indirmeniz gerekmektedir.)

```
ftp> exit
221 Goodbye.
[root@hackerbox]~# cat userlist
jack:hackviser
root:root
[root@hackerbox]~#
```

### 3- SECURE COMMAND

Verilen adresi taradığımızda ssh görüyoruz.

```
[root@hackerbox]~  
#clear 172.20.4.54  
bash: clear172.20.4.54: command not found  
[x]-[root@hackerbox]~  
#nmap 172.20.4.54  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 16:03 CDT  
Nmap scan report for 172.20.4.54  
Host is up (0.00024s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: 52:54:00:ED:71:40 (QEMU virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds  
[root@hackerbox]~  
#
```

22 portunun açık olduğunu görüyoruz. Verilen ipcu sayesinde hackviser ismiyle ssh bağlantısı kuruyorum.

```
destination [command [argument ...]]  
ssh [-Q query_option]  
[x]-[root@hackerbox]~  
#ssh hackviser@172.20.4.54  
-----  
Secure Command  
-----  
Master's Message: W3lc0m3 t0 h4ck1ng w0rld
```

İlk görevim olan mesajı buluyorum.

```
hackviser@secure-command:~$ pwd
/home/hackviser
hackviser@secure-command:~$ sudo root
-bash: sudo: command not found
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser#
```

Yukarıda gördüğünüz gibi pwd komutuyla çalışma dizinimizi öğreniyoruz. Diğer görevimiz olan root yükselmesi var. Her zaman ilk denenmesi gereken root:root şifresini giriyoruz. Su root ile parolamızı doğru girerek yükseliyoruz. Bir sonraki görevimiz gizli dosyaları görüntülemek. Ls -a komutu sayesinde gizli dosyaları görüntüleyebiliriz.

```
root@secure-command:/home/hackviser# ls -a
.  ..  .bashrc
```

```
root@secure-command:~# get .advice_of_the_master
bash: get: command not found
root@secure-command:~# cat .advice_of_the_master
st4y curl0us
root@secure-command:~#
```

Son olarak get ile dosyayı alıp cat ile okuyoruz.

#### 4- QUERY GATE

Bu ısınmada nihayi görevimiz beyaz şapkalı hacker'ı bulmak. Yine verilen adrese nmap yapıyorum.

```
#nmap 172.20.4.208
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 15:54 CDT
Nmap scan report for 172.20.4.208
Host is up (0.00030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: 52:54:00:BF:07:13 (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

3306 portu mysql de default olan porttur.



```
[root@hackerbox]~#mysql -u root -h 172.20.4.208
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.34 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Başarılı girişten sonra database leri görüntülemek için SHOW komutunu kullanalım.

```
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.010 sec)

MySQL [(none)]>
```

Use komutunu kullanarak database'leri kontrol edelim.

```
MySQL [(none)]> USE detective_inspector
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [detective_inspector]> LS
-> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near 'LS' a
t line 1
MySQL [detective_inspector]> SHOW TABLES;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list |
+-----+
1 row in set (0.004 sec)
```

SHOW TABLES ile tabloları görüntülüyorum ve istediğimi bana verebilecek bir tabloyu görüyorum.

```
ySQL [detective_inspector]> SHOW TABLES
-> ;
-----+-----
Tables_in_detective_inspector |
-----+-----
hacker_list                    |
-----+-----
row in set (0.004 sec)

ySQL [detective_inspector]> SELECT * FROM hacker_list
-> ;
-----+-----+-----+-----+-----+
id | firstName | lastName | nickname | type |
-----+-----+-----+-----+-----+
1001 | Jed       | Meadows | spld3r   | gray-hat |
1002 | Melissa  | Gamble  | c0c0net  | gray-hat |
1003 | Frank    | Netsi   | v3nus    | gray-hat |
1004 | Nancy    | Melton  | sltorml09 | black-hat |
1005 | Jack     | Dunn    | psyod3d  | black-hat |
1006 | Arron    | Eden    | r4nd0myfff | black-hat |
1007 | Lea      | Wells   | pumq7eggy7 | black-hat |
1008 | Hackviser | Hackviser | h4ckvls3r | white-hat |
1009 | Xavier   | Klein   | oricy4l33 | black-hat |
-----+-----+-----+-----+-----+
rows in set (0.004 sec)
```

Son olarak `SELECT * FROM hacker_list` yazarak `hacker_list` tablosunu görüntülüyorum. Ve beyaz Şapkalı Hacker'ımı buldum.