### Hackviser Isınmalar

### 1.Isınmalar:

## 1-ARROW:

**1.SORU:** Hangi port açık?

nmap taraması yaptım.

```
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

[root@hackerbox] -[-]

#nmap 172.20.3.58

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 08:27 CDT

Nmap scan report for 172.20.3.58

Host is up (0.00029s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

23/tcp open telnet

MAC Address: 52:54:00:8F:05:A7 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

2.SORU: Çalışan servis adı?

nmap taramasında çıkmıştı ama diğer bir yöntemi daha göstermek için nmap ..... -sV yi kullandım.

```
#nmap 172.20.3.58 -sV

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 08:31 CDT

Nmap scan report for 172.20.3.58

Host is up (0.00031s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE VERSION
23/tcp open telnet Linux telnetd

MAC Address: 52:54:00:8F:05:A7 (QEMU virtual NIC)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
```

3.SORU: Hostname nedir?

Hostname makine ismini verir yani arrow

4.SORU: Telnet'e bağlanmak için kullandığınız username:password nedir?

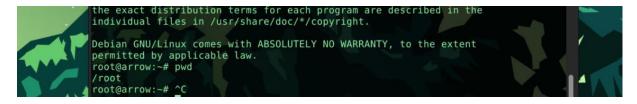
```
#telnet 172.20.3.58
Trying 172.20.3.58...
Connected to 172.20.3.58.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
root@arrow:-#
```

**5.SORU:** Telnet'e bağlandığınızda çalışma dizini konumunuz nedir? pwd komutu ile buluruz.



## 2-File Hunter:

1.SORU: Hangi port(lar) açık?

Nmap araması yaptım yine.

```
Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds

| root@hackerbox | - |
| #nmap 172.20.3.160

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 08:58 CDT

Nmap scan report for 172.20.3.160

Host is up (0.00034s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE
21/tcp open ftp

MAC Address: 52:54:00:16:98:31 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

### 2.SORU: FTP'nin açılımı nedir?



### **3.SORU:** FTP'ye hangi kullanıcı adı ile bağlandınız?

```
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

[root@hackerbox] [~]

#ftp 172.20.3.160
Connected to 172.20.3.160.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.3.160:root): root
530 This FTP server is anonymous only.
Login failed.
ftp>
```

**4.SORU:** Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

ftp dizinine girdiğimde help komutuyla.

```
ftp> ^C
ftp> ftp help
?Invalid command
ftp> help
                                Commands are:
Commands may be abbreviated.
                                   mdelete
                 dir
                                                                      site
                 disconnect
                                   mdir
                                                    sendport
                                                                      size
account
                 exit
                                                    put
                                                                      status
                                   mget
append
                 form
                                   mkdir
                                                    pwd
                                                                      struct
ascii
                 get
                                   mls
                                                    quit
                                                                      system
bell
                 glob
                                   mode
                                                    quote
                                                                      sunique
binary
                 hash
                                                    recv
                                   modtime
                                                                      tenex
bye
                 help
                                   mput
                                                    reget
                                                                      tick
case
                 idle
                                   newer
                                                     rstatus
                                                                      trace
cd
                 image
                                   nmap
                                                    rhelp
                                                                      type
cdup
                 ipany
                                   nlist
                                                    rename
                                                                      user
chmod
                 ipv4
                                   ntrans
                                                    reset
                                                                      umask
close
                 ipv6
                                                     restart
                                                                      verbose
                                   open
                 lcd
                                                     rmdir
cr
                                   prompt
delete
                 ls
                                   passive
                                                     runique
debug
                 macdef
                                   proxy
                                                     send
ftp>
```

**5.SORU:** Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

get komutunu kullanabiliriz.



**6.SORU:** Dosyada hangi kullanıcıların bilgileri vardır?

```
root@hackerbox:~# cat userlist
jack:hackviser
root:root
```

# **3-Secure Command:**

1.SORU: Hangi port(lar) açık?,

Nmap taraması yaptım.

2.SORU: Çalışan hizmet adı nedir?

Nmap -sV ile arama yapıyorum.

```
Qalişan hizmet

Qalişan hizmet
```

**3.SORU:** SSH'a hackviser:hackviser oturum bilgileri ile bağlanırken "Master's Message" nedir?

W3lc0m3 t0 h4ck1ng w0rld



4.SORU: Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

#### Su

```
2 Pugn

2 Pugn

(**su Kali, su: user kali, does not exist or the user entry does not contain all the required fields

(**su Kali) - [/home/kali]

(**su kali

(**kali**@ kali) - [~]

Gönder
```

**5.SORU:** root kullanıcısının parolası nedir?

### root

```
onder

Puan

| Su kali | S
```

**6.SORU:** ls komutunun gizli dosyaları gösteren parametresi nedir?

Ls -a komutu tüm dosyaları verir.

### 7.SORU: Master'in tavsiyesi nedir?

Dosyalar arasında biraz dolaştıktan sonra root kullanıcısının home dizininde ".advice\_of\_the\_master" adlı ilginç bir gizli dosya bulduk.

```
root@secure-command:~# cat .advice_of_the_master
st4y cur10us
```

# 4-Query Gate:

1.SORU: Hangi port(lar) açık?

```
Callsan

- 172.20.4.178 ping statistics —
12 packets transmitted, 12 received, 0% packet loss, time 11019ms
rtt min/avg/max/mdev = 77.580/80.395/87.028/2.902 ms

Gönde

- (kali@ kali)-[~]
- $ nmap 172.20.4.178

Starting Nmap 7.945VN ( https://nmap.org ) at 2024-10-17 12:29 EDT

Nmap scan report for 172.20.4.178

Host is up (0.081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
3306/tcp open mysql

Nmap done: 1 IP address (1 host up) scanned in 15.74 seconds

Gönds - (kali@ kali)-[~]
```

2.SORU: Çalışan servisin adı nedir?

**3.SORU**: MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?

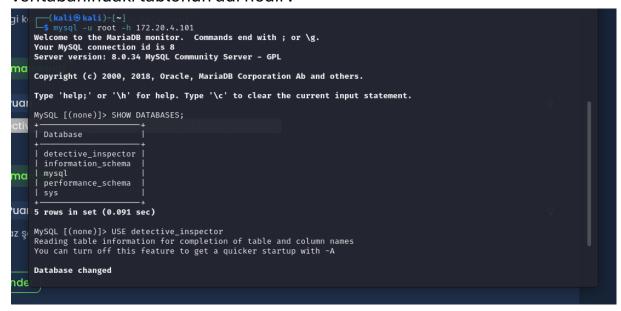
Root

**4.SORU:** Hedef makinede çalışan MySQL'e bağlanmak için komut satırı aracında hostname i belirtmek için hangi parametre kullanılır?

### 5.SORU: Bağlandığınız MySQL sunucusunda kaç veritabanı var?



**6 ve 7.SORU:** Hangi komutla bir veritabanı seçebiliriz? Detective\_inspector veritabanındaki tablonun adı nedir?



8.SORU: Beyaz şapkalı hacker'ın kullanıcı adı nedir?

Beyaz şapkalı hacker'ı tespit edebilmek için tablo içeriklerine bakalım.

```
You can turn off this feature to get a quicker startup with
Database changed
MySQL [detective_inspector]> SELECT * from hacker_list;
        | firstName | lastName | nickname
  1001
                          Meadows
                                        | sp1d3r
                                                          gray-hat
                                                          gray-hat
gray-hat
black-hat
   1002
                          Gamble
                                         c0c0net
   1003
                          Netsi
Melton
                                       | v3nus
| s1torml09
  1004
           Nancy
                                         psyod3d
r4nd0myfff
   1005
            Jack
                                                          black-hat
  1006
1007
                          Eden
Wells
                                                        | black-hat
| black-hat
                          Wells | pumq7eggy7
Hackviser | h4ckv1s3r
Klein | oricy4l33
           Hackviser
                                                       | white-hat
| black-hat
  1009 I
           Xavier
                          Klein
9 rows in set (0.083 sec)
MySQL [detective_inspector]>
```

Isınmalar 1 bitti.