

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
[~]#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.org/submit/
```

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.

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

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: 52:54:00:16:9B:31 (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

2.SORU: FTP'nin açılımı nedir?

FTP'nin açılımı nedir?

Tümü Videolar Görseller Haberler Web Kitaplar Finans

Açılımı **"File Transfer Protocol"** olan FTP, dilimizde Dosya Transfer Protokolü olarak biliniyor. İsminden de anlaşılacağı üzere dosya transfer işlemi için kullanılan bir protokoldür. İnternete bağlı iki bilgisayar arasında dosya transferini sağlayan bir protokoldür.

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

```
File Address: 172.20.3.160 (QEMU Virtual NIC)
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 may be abbreviated.  Commands are:

!          dir          mdelete    qc          site
$          disconnect   mdir       sendport    size
account    exit             mget       put         status
append     form            mkdir      pwd         struct
ascii      get             mls        quit        system
bell       glob            mode       quote       sunique
binary     hash            modtime    recv        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            open       restart     verbose
cr        lcd             prompt     rmdir       ?
delete    ls              passive    runique
debug     macdef          proxy      send
ftp>
```

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

get komutunu kullanabiliriz.

```
?Invalid command
ftp> ls
530 Please login with USER and PASS.
ftp> get userlist
local: userlist remote: userlist
530 Please login with USER and PASS.
ftp> help get
get          receive file
ftp>
```

6.SORU: Dosyada hangi kullanıcıların bilgileri vardır?

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

3-Secure Command:

1.SORU: Hangi port(lar) açık?,

Nmap taraması yaptım.

```
(kali@kali)-[~]
$
(kali@kali)-[~]
$ nmap 172.20.5.174
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 11:50 EDT
Nmap scan report for 172.20.5.174
Host is up (0.078s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 17.50 seconds
(kali@kali)-[~]
$
```

2.SORU: Çalışan hizmet adı nedir?

Nmap -sV ile arama yapıyorum.

```
Çalışan hizmet
Gönder
2 Puan
Gönder
2 Puan

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 17.50 seconds
(kali@kali)-[~]
$ nmap -sV 172.20.5.174
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 11:56 EDT
Nmap scan report for 172.20.5.174
Host is up (0.077s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2 (protocol 2.0)
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 15.18 seconds
(kali@kali)-[~]
$
```

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

W3lc0m3 t0 h4ck1ng w0rld

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?

```
Çalışan C — 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

Gönder (kali@kali)-[~]
$ nmap 172.20.4.178
Starting Nmap 7.94SVN ( 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

Gönder (kali@kali)-[~]
```

2.SORU: Çalışan servisin adı nedir?

```
(kali@kali)-[~]
$ nmap -sV 172.20.4.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 12:32 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 172.20.4.178
Host is up (0.078s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp   open  mysql    MySQL 8.0.34

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.47 seconds

EVI (kali@kali)-[~]
```

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?

-u

```
ERROR 2002 (HY000): Can't connect to local server through socket '/run/mysqld/mysqld.sock' (2)

(kali@kali)-[~]
$ mysql -u root -h 172.20.4.178
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
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)]>
```

5.SORU: Bağlandığınız MySQL sunucusunda kaç veritabanı var?

```
MySQL [(none)]> show databases
→ SHOW DATABASES;
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 'SHOW DATABASES' at line 2
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.089 sec)

MySQL [(none)]>
```

6 ve 7.SORU: Hangi komutla bir veritabanı seçebiliriz? Detective_inspector veritabanındaki tablonun adı nedir?

```
(kali㉿kali)-[~]
$ mysql -u root -h 172.20.4.101
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)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.091 sec)

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
```

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 -A

Database changed
MySQL [detective_inspector]> SELECT * from hacker_list;
+----+-----+-----+-----+-----+
| id | firstName | lastName | nickname | type |
+----+-----+-----+-----+-----+
| 1001 | Jed | Meadows | sp1d3r | gray-hat |
| 1002 | Melissa | Gamble | c0c0net | gray-hat |
| 1003 | Frank | Netsi | v3nus | gray-hat |
| 1004 | Nancy | Melton | s1t0rm109 | black-hat |
| 1005 | Jack | Dunn | psyod3d | black-hat |
| 1006 | Arron | Eden | r4nd0myfff | black-hat |
| 1007 | Lea | Wells | pumq7eggy7 | black-hat |
| 1008 | Hackviser | Hackviser | h4ckv1s3r | white-hat |
| 1009 | Xavier | Klein | oricy4l33 | black-hat |
+----+-----+-----+-----+-----+
9 rows in set (0.083 sec)

MySQL [detective_inspector]>
```

Isınmalar 1 bitti.

