### Hackviser Isınmalar

#### 1. ARROW MAKINESI

**Soru 1:** Hangi Portlar Açık?

Çözüm: port taraması yapmak için rustscan veya nmap ile | nmap ip | adresi şeklinde

öğrenebiliriz. Answer: 23

servet@Hegir:~/indirilenler\$ nmap 172.20.5.122
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-21 21:03 +03
Nmap scan report for 172.20.5.122
Host is up (0.065s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
23/tcp open telnet
Nmap done: 1 IP address (1 host up) scanned in 14.15 seconds

Soru 2: Hangi Servis Çalışıyor?

Cözüm: Nmap'de -sV parametresi ile versiyon ismi ve versiyon numarası öğrenebiliriz ama

ben tek taramada karşıma çıktı.

**Answer:** Telnet

STATE SERVICE o open telnet

**Soru 3:** Hostname Bilgisi Nedir?

Çözüm: Linuxda hostname komutu makine adını verir.

**Answer: Arrow** 

root@arrow:~# hostname arrow

Soru 4: Çalışılan dizin nedir?

Cözüm: Linuxda bulunduğumuz dizini pwd ile görüntüleyebiliriz.

**Answer:/root** 

root@arrow:~# pwd /root

ARROW MAKİNESİ BİTMİŞTİR!

## 2. FİLE-HUNTER MAKİNESİ

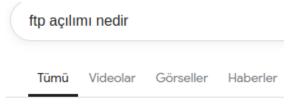
Soru 1: Hangi Portlar Açık?

Çözüm: rustscan ile tarama yaptım

Answer: 21

PORT STATE SERVICE REASON 21/tcp open ftp syn-ack

Soru 2: FTP'nin açılımı nedir? Answer: File Transfer Protocol



Açılımı "File Transfer Protocol"

Soru 3: FTP'ye hangi kullanıcı adı ile bağlandınız? Çözüm: anonymous olarak bağlanabilecğeimizi söylüyor

**Answer:** anonymous

```
[3]+ Stopped ftp 172.20.6.136
servet@Hegir:~/indirilenler$ ftp 172.20.6.136
Connected to 172.20.6.136.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.6.136:servet): anonymous
230 Login successful.
Remote system type is UNIX.
ftp> ■
```

Soru 4 : Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

**Answer:** help

ftp> help Commands may	be abbreviated.	Commands are:							
! \$ account append ascii bell binary bye case cd cdup ftp>	chmod close cr debug delete dir disconnect edit epsv epsv4 epsv6	exit features fget form ftp gate get glob hash help	image lcd less lpage lpwd ls macdef mdelete mdir mget mkdir	mls mlsd mlsd mlst mode modime more mput mreget msend newer nlist	nmap ntrans open page passive pdir pls pmlsd preserve progress prompt	proxy put pwd quit quote rate rcvbuf recv reget remopts rename	reset restart rhelp rmdir rstatus runique send sendport set site size	sndbuf status struct sunique system tenex throttle trace type umask unset	usage user verbose xferbuf ?

Soru 5 : FTP sunucusundaki dosyanın adı nedir? Çözüm : İs yaparal bulunduğum dizini listeliyorum

**Answer**: userlist

```
ftp> ls

229 Entering Extended Passive Mode (|||14313|)

150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 25 Sep 08 2023 userlist

226 Directory send OK.
ftp> |
```

Soru 6:Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

**Answer: get** 

Soru 7: Dosyada hangi kullanıcıların bilgileri vardır?

**Answer:** jack:hackviser | root:root

```
servet@Hegir:~/İndirilenler$ cat userlist
jack:hackviser
root:root
servet@Hegir:~/İndirilenler$
```

FILE-HUNTER MAKINESI BİTMİŞTİR!

#### 3. Secure Command Makinesi

Soru 1: Hangi portlar açık?

Çözüm: İlk önce hızlıca hangi portların açık olduğunu öğrenmek için rustscan ile taradım ve

23 ü gördüm, daha sonra nmap ile sadece 22 portuna yönelik tarama yaptım.

Answer: 22

```
Open 172.20.5.63:22

^C
servet@Hegir:~/indirilenler$ nmap 172.20.5.63 -p 22
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-21 21:58 +03
Nmap scan report for 172.20.5.63 (172.20.5.63)
Host is up (0.065s latency).

PORT STATE SERVICE
22/tcp open ssh

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
servet@Hegir:~/indirilenler$
```

Çalışan hizmet adı nedir?

Çözüm: nmap ipadresi & nmap -sV ip adresi

**Answer: SSH** 

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

Çözüm: ben öncelikle direkt root dizine erişmeye çalıştığımda yetkisiz olduğumu belirtti , parolayı öğrenmek için cat ile passwd dosyasını okudum ve shadow dosyasını da okuyacaktım yetkim maalesef yetmedi. Daha sonra sudo -l yaparak hangi komutları şifre istemeden çalıştırabilirim diye baktım onda da bir şey bulamadım, en son yaptığım işlem ise su ile su root deyip root kullanıcısın şifresine root denedim ve girdim

**Answer:** st4y cur10us

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

Soru 2 : Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

**Answer: su** (username)

Soru 3: root kullanıcısının parolası nedir?

**Answer:** root

```
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser#
```

komutunun gizli

gösteren

dosyaları parametresi nedir?

Answer: ls -a

Soru 3: ls

```
root@secure-command:~# ls -a
. .. .advice_of_the_master .bashrc .local .ssh
root@secure-command:~#
```

Soru 4: Master'in tavsiyesi nedir?

**Answer:** st4y cur10us

root@secure-command:~# cat .advice\_of\_the\_master st4y cur10us root@secure-command:~#

# SECURE COMMAND MAKİNESİ BİTMİŞTİR!

### **4.Query Gate**

Soru 1 : Hangi port(lar) açık? Çözüm: nmap ipadresi &

**Answer: 3306** 

PORT STATE SERVICE 3306/tcp open mysql

Soru 2 : Çalışan servisin adı nedir?

Çözüm: nmap -sV ipadresi

**Answer:** mysql

PORT STATE SERVICE 3306/tcp open mysql

Soru 3: MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?

**Answer:** root

```
Servet@Hegir:~/Indiritenter$ mysql -u root -h 1/2.20.5./3
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.34 MySQL Community Server - GPL

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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

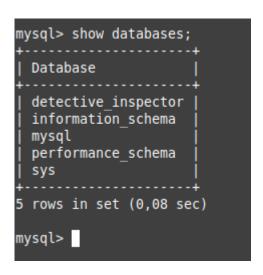
mysql> show databases;
```

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

Answer: -u

Soru 5 : Bağlandığınız MySQL sunucusunda kaç veritabanı var?

Answer: 5



Soru 6: Hangi komutla bir veritabanı seçebiliriz?

**Answer: USE** 

Soru

mysql> 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

7 :detective\_inspector veritabanındaki tablonun adı nedir? Çözüm: SHOW TABLES; ile tabloları görüntüleyebiliriz.

**Answer:** hacker\_list

Soru 8: Beyaz şapkalı hacker'ın kullanıcı adı nedir?

Çözüm: Burada bir tablo var, öncelikle tabloyu okumak için select ile içinden verileri seçiyorum. \* koyarak tüm verileri getirmesini talep ediytorum daha sonra bunu hangi tabloadn getireceğini söylemek için from ifadesi kullanıp,; ile sorgumu bitiriyorum.

Answer: h4ckv1s3r

mysql> S ++   id	ELECT * FROM  firstName	1 hacker_list  lastName	t; +   nickname	++   type
1001     1002     1003     1004     1005     1006     1007     1008     1009	Jed Melissa Frank Nancy Jack Arron Lea Hackviser Xavier	Meadows Gamble Netsi Melton Dunn Eden Wells Hackviser Klein	spld3r   c0c0net   v3nus   s1torml09   psyod3d   r4nd0myfff   pumq7eggy7   h4ckv1s3r   oricy4l33	gray-hat   gray-hat   gray-hat   black-hat   black-hat   black-hat   black-hat   white-hat
9 rows i	n set (0,08	sec)		++

# Query Gate MAKINESI BİTMİŞTİR!

ISINMALAR 1 BİTMİŞTİR.