

Hackviser Isınmalar

1. ARROW MAKİNESİ

Soru 1 : Hangi Portlar Açık ?

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

Answer : 23

```
servet@Hegir:~/İndirilenler$ 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?

Çözüm : Nmap'de -sV parametresi ile versiyon ismi ve versiyon numarası öğrenebiliriz ama ben tek taramada karşıma çıktı.

Answer : Telnet

```
STATE SERVICE
23/tcp 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?

Çözüm : Linuxda bulunduğumuz dizini pwd ile görüntüleyebiliriz.

Answer : /root

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

ARROW MAKİNESİ BİTMİŞTİR!

2. FILE-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

ftp açılımı nedir

Tümü Videolar Görseller Haberler

Açılımı "File Transfer Protocol"

Soru 3 : FTP'ye hangi kullanıcı adı ile bağlandınız?

Çözüm : anonymous olarak bağlanabileceğimizi söylüyor

Answer : anonymous

```
[3]+  Stopped                  ftp 172.20.6.136
servet@Hegir:~/İndirilenler$ 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:

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

Soru 5 : FTP sunucusundaki dosyanın adı nedir?

Çözüm : ls 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

```
ftp> get userlist
local: userlist remote: userlist
229 Entering Extended Passive Mode (|||7426|)
150 Opening BINARY mode data connection for userlist (25 bytes).
100% |*****| 25      19.36 KiB/s   00:00 ETA
226 Transfer complete.
WARNING! 2 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
25 bytes received in 00:00 (0.36 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||49989|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp      25 Sep 08  2023 userlist
226 Directory send OK.
```

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 MAKİNESİ 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

Soru

```
Open 172.20.5.63:22
^C
servet@Hegir:~/İndirilenler$ 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:~/İndirilenler$
```

2 :

Çalışan hizmet adı nedir?

Çözüm: nmap ip adresi & 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 çalıştığım da 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 kullanıcısının şifresine root dedim 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#
```

Soru 3 : ls

dosyaları

parametresi nedir?

Answer : ls -a

komutunun gizli
gösteren

```
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 ipadresini &

Answer : 3306

```
PORT      STATE SERVICE
3306/tcp  open  mysql
```

Soru 2 : Çalışan servisin adı nedir?

Çözüm: nmap -sV ipadresini

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:~/Indirilenler$ mysql -u root -h 172.20.5.73
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

```
mysql> show databases;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0,08 sec)

mysql> █
```

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

```
mysql> SHOW TABLES;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list                    |
+-----+
1 row in set (0,10 sec)

mysql> 
```

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 ediyorum daha sonra bunu hangi tabloadn getireceğini söylemek için from ifadesi kullanıp , ; ile sorgumu bitiriyorum.

Answer : h4ckv1s3r

```
mysql> 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 | h4ckv1s3r | white-hat |
| 1009  | Xavier    | Klein   | oricy4l33 | black-hat |
+-----+-----+-----+-----+-----+
9 rows in set (0,08 sec)

mysql> 
```

Query Gate MAKİNESİ BİTMİŞTİR!

ISINMALAR 1 BİTMİŞTİR.