Secure Command:Isınma

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nmap -sS -sV -O -T4 172.20.4.153

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 18:43 EDT
Nmap scan report for 172.20.4.153
Host is up (0.12s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/sub
mit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/9%OT=22%CT=1%CU=32815%PV=Y%DS=2%DC=I%G=Y%TM=6707
OS:0733%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)
OS:OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509
OS:ST11NW7%O6=M509ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
OS:ECN(R=Y%DF=Y%T=40%W=FAF0%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.65 seconds
```

Nmap ile açık portları tarama işlemi gerçekleştirdim.22/tcp portunun açık olduğunu gördüm.

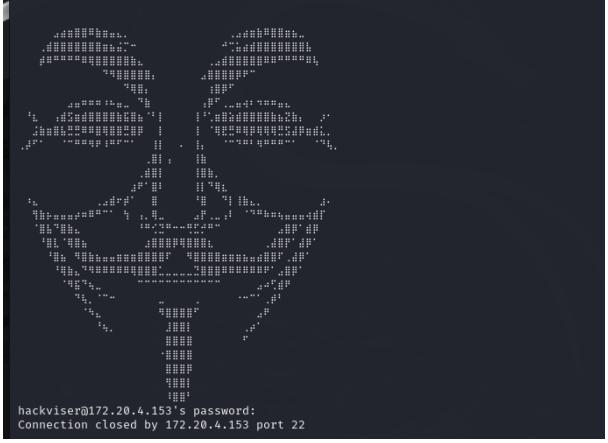
2)Çalışan hizmet adı nedir?

Ssh

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

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ssh hackviser@172.20.4.153
The authenticity of host '172.20.4.153 (172.20.4.153)' can't be established.
ED25519 key fingerprint is SHA256:g8/PIfA1jk/9TeiTo12Rh2W73gzSmEKEIEAnPv2Y9HI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.4.153' (ED25519) to the list of known hosts.
──────────────────────────────
Secure Command
──────────────────────────────

Master's Message: W3lc0m3 t0 h4ck1ng w0rld



hackviser@172.20.4.153's password:
Connection closed by 172.20.4.153 port 22
```

Mesaj: W3lc0m3 t0 h4ck1ng w0rld

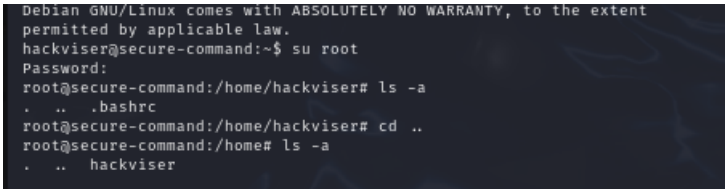
4)Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

Su

5)root kullanıcısının parolası nedir?

Ssh a hackviser ile bağlandıktan sonra bizden parola istedi bizde hackviser denendik bu şekilde sisteme giriş yaptık.

Root kullanıcısının porolasını bulmak için su root komudu ile yetkimizi yükseltik.



Root parolasını girdik ve sisteme root yetkisibde bağlanabildik.

6)ls komutunun gizli dosyaları gösteren parametresi nedir?

ls -a

7) Master'in tavsiyesi nedir?

ssh da root olduktantan sonra ls -a komuduyla gizli dosyalar baktık.Bulduğumuz dizinden alt dizinlere inerek burada da bulunan gizli dosyalra baktık. ".advice_of_the_master" dosyasının içeriğini okuduk ve master tavsiyesine ulaştık.