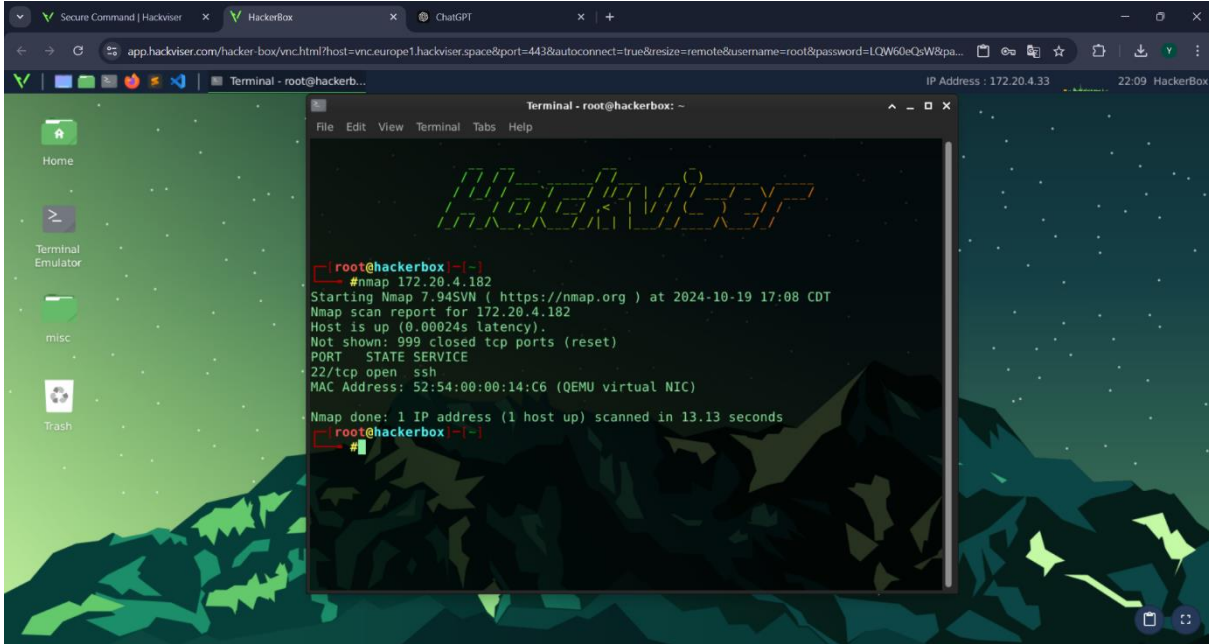


Hackviser Warmup: Secure Command

Soru:Hangi port(lar) açık?

Bu soruyu çözmek için öncelikle nmap aracılığıyla makinemizi tarayalım.



```
root@hackerbox:~# nmap 172.20.4.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 17:08 CDT
Nmap scan report for 172.20.4.182
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 52:54:00:08:14:C6 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
root@hackerbox:~#
```

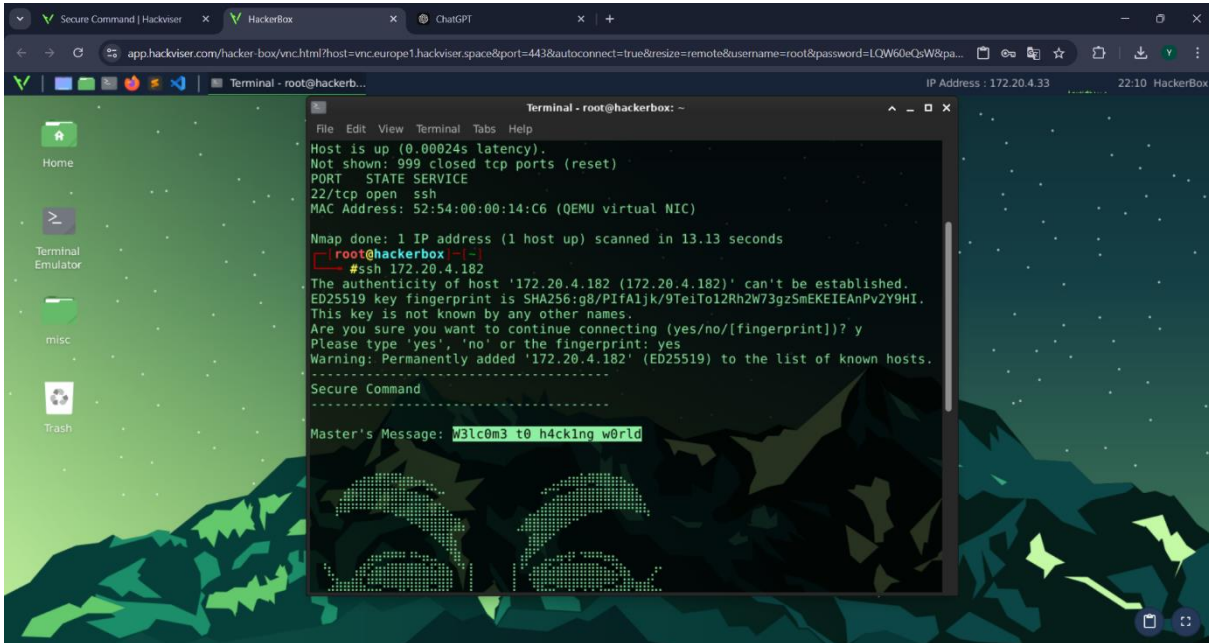
Burada “22” portunun açık olduğunu gördük ilk sorumuzun cevabını bulduk.

Soru:Çalışan hizmet adı nedir?

Bu sorunun cevabı da “nmap” sonucunda gözüküyor “ssh” hizmetidir sorumuzun cevabı.

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

Bunu çözmek için önce “ssh hackviser @[makine ip adresi]” komutunu çalıştırıyoruz.



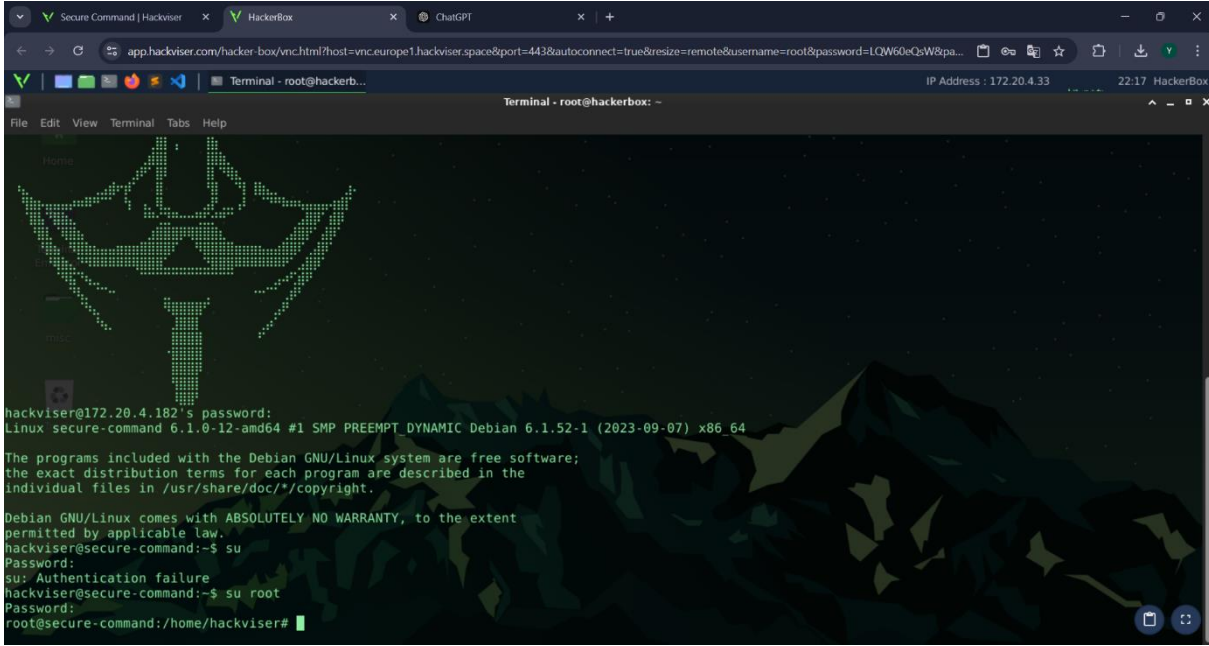
```
root@hackerbox:~# ssh 172.20.4.182
The authenticity of host '172.20.4.182 (172.20.4.182)' can't be established.
ED25519 key fingerprint is SHA256:g8/PIfAljk/9TeiTo12Rh2W73gzSmEKEIEAnPv2Y9HI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.4.182' (ED25519) to the list of known hosts.
Secure Command
-----
Master's Message: w3lc0m3 t0 h4cking w0rld
```

Burada Master's Message'ı görüyoruz.

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

Temel linux komut bilgisine sahip herkesin bilmesi gereken “switch user” anlamına gelen “su” komutudur. Bu komutu kullanarak root olmaya çalışalım.

Soru:”root” kullanıcısının parolası nedir?



```
hackviser@172.20.4.182's password:
Linux secure-command 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) x86_64

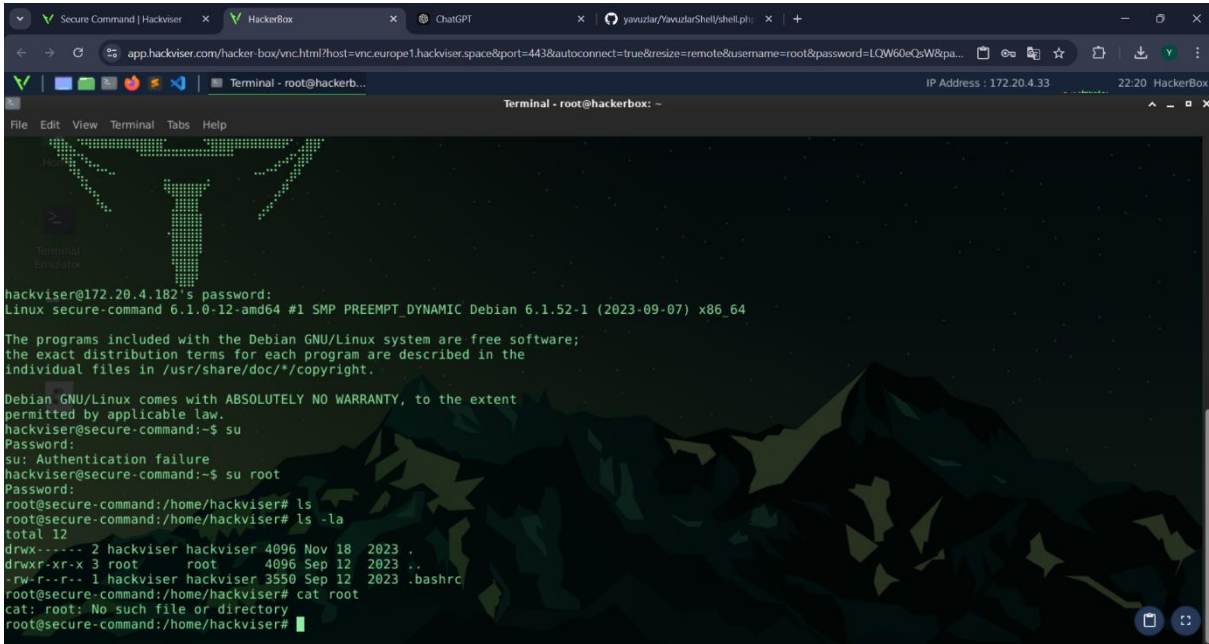
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
hackviser@secure-command:~$ su
Password:
su: Authentication failure
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser#
```

“su root” yazarak root kullanıcısına girmeye çalışıyoruz. Şifre olarak “root” deniyoruz ve oluyor.

Soru:”ls” komutunun gizli dosyaları gösteren parametresi nedir?

Bu sorunun cevabı da temel linux komutlarına bakarak bulabilirsiniz -a olacak doğru cevap.



```
hackviser@172.20.4.182's password:
Linux secure-command 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) x86_64

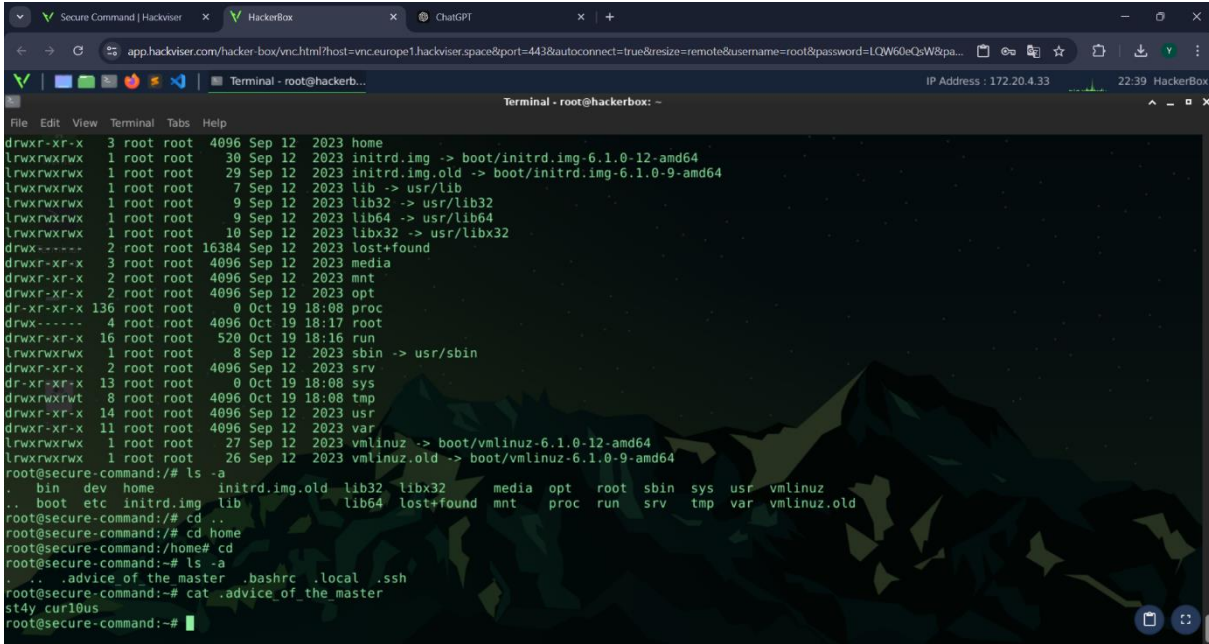
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
hackviser@secure-command:~$ su
Password:
su: Authentication failure
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser# ls
root@secure-command:/home/hackviser# ls -la
total 12
drwxr-xr-x 2 hackviser hackviser 4096 Nov 18 2023 .
drwxr-xr-x 3 root      root      4096 Sep 12 2023 ..
-rw-r--r-- 1 hackviser hackviser 3550 Sep 12 2023 .bashrc
root@secure-command:/home/hackviser# cat root
cat: root: No such file or directory
root@secure-command:/home/hackviser#
```

Burda “.” olarak gözüken dosyalar linux’da gizli dosya olarak kabul edilir. Bunları inceliyoruz.

Soru: Master'ın tavsiyesi nedir?

Bu sorunun cevabını da incelememiz sonucunda buluyoruz.



```
drwxr-xr-x 3 root root 4096 Sep 12 2023 home
lrwxrwxrwx 1 root root 30 Sep 12 2023 initrd.img -> boot/initrd.img-6.1.0-12-amd64
lrwxrwxrwx 1 root root 29 Sep 12 2023 initrd.img.old -> boot/initrd.img-6.1.0-9-amd64
lrwxrwxrwx 1 root root 7 Sep 12 2023 lib -> usr/lib
lrwxrwxrwx 1 root root 9 Sep 12 2023 lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 Sep 12 2023 lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 Sep 12 2023 libx32 -> usr/libx32
drwx----- 2 root root 16384 Sep 12 2023 lost+found
drwxr-xr-x 3 root root 4096 Sep 12 2023 media
drwxr-xr-x 2 root root 4096 Sep 12 2023 mnt
drwxr-xr-x 2 root root 4096 Sep 12 2023 opt
dr-xr-xr-x 136 root root 0 Oct 19 18:08 proc
drwx----- 4 root root 4096 Oct 19 18:17 root
drwxr-xr-x 16 root root 520 Oct 19 18:16 run
lrwxrwxrwx 1 root root 8 Sep 12 2023/sbin -> usr/sbin
drwxr-xr-x 2 root root 4096 Sep 12 2023/srv
dr-xr-xr-x 13 root root 0 Oct 19 18:08 sys
drwxrwxrwt 8 root root 4096 Oct 19 18:08 tmp
drwxr-xr-x 14 root root 4096 Sep 12 2023/usr
drwxr-xr-x 11 root root 4096 Sep 12 2023/var
lrwxrwxrwx 1 root root 27 Sep 12 2023/vmlinuz -> boot/vmlinuz-6.1.0-12-amd64
lrwxrwxrwx 1 root root 26 Sep 12 2023/vmlinuz.old -> boot/vmlinuz-6.1.0-9-amd64
root@secure-command:/# ls -la
.. bin dev home initrd.img.old lib32 libx32 media opt root/sbin sys usr/vmlinuz
.. boot etc initrd.img lib lib64 lost+found mnt proc run/srv tmp var/vmlinuz.old
root@secure-command:/# cd home
root@secure-command:/home# cd
root@secure-command:/# ls -la
.. .advice_of_the_master .bashrc .local .ssh
root@secure-command:/# cat .advice_of_the_master
st4y curl0us
root@secure-command:/#
```

Dizinler arasında gezerek “home” dizininde “.advice_of_the_master” adında dosyayı bulduk ve “cat” komutu ile bunu açtık ve tavsiyeyi bulduk.

Bu son sorumuzu da tamamladık ve “Secure Command” ısınması burada bitmiştir. Okuduğunuz için teşekkür ederim.