

# warmups 1-Secure Command

Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan Warmup 1 / Secure Command makinesinin çözümünü anlatacağım keyifli okumalar.

Öncelikle sitenin bize verdiği ip adresi ile basit bi nmap taraması yapıyorum.

```
(kali@kali)-[~]  
$ nmap -sV 172.20.2.201  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 19:44 EDT  
Nmap scan report for 172.20.2.201  
Host is up (0.064s 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 2.68 seconds
```

Burada açık port olarak "22" portu ve çalışan servisin "ssh" gözüküyor.

Ardından ssh'a bağlanmak için "ssh username@ip" komutunu kullanıyorum



```

hackviser@172.20.2.201'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.
Last login: Tue Sep 10 19:48:27 2024 from 10.8.7.231
hackviser@secure-command:~$
::1          ff02::2          ip6-allrouters ip6-loopback   secure-command
ff02::1      ip6-allnodes ip6-localhost  localhost
hackviser@secure-command:~$

```

Ancak hackviser kullanıcısı ile işlem yapmayı denediğimizde işlemlerimiz kısıtlanıyor. Bizde yetki yükseltme kısmına yöneliyoruz.

```

hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser# ls -la
total 12
drwx----- 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#

```

"su root" komutu ile giriş yapmaya çalışıyoruz ve root kullanıcısı olduğu için şifre giriş kısmına geliyoruz. Burada da "root" şifresini kullandığımız zaman başarılı bir şekilde root kullanıcısının hesabına giriş yapmış olduk.

Ardından sistemde yüklü olan dosyaları görüntülemek istiyoruz

```

root@secure-command:/home# ls -la
total 12
drwxr-xr-x  3 root      root      4096 Sep 12  2023 .
drwxr-xr-x 18 root      root      4096 Sep 12  2023 ..
drwx----- 2 hackviser hackviser 4096 Nov 18  2023 hackviser
root@secure-command:/home# cd ..

```

Ancak dikkat çekecek herhangi birşey ile karşılaşmıyoruz.

Bizde bi üst dizine bakalım diyoruz.

```
root@secure-command:/# ls -la
total 68
drwxr-xr-x 18 root root 4096 Sep 12 2023 .
drwxr-xr-x 18 root root 4096 Sep 12 2023 ..
lrwxrwxrwx 1 root root 7 Sep 12 2023 bin -> usr/bin
drwxr-xr-x 3 root root 4096 Sep 12 2023 boot
drwxr-xr-x 18 root root 3320 Sep 10 19:43 dev
drwxr-xr-x 67 root root 4096 Sep 10 19:43 etc
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 139 root root 0 Sep 10 19:43 proc
drwx----- 4 root root 4096 Sep 10 19:51 root
drwxr-xr-x 16 root root 520 Sep 10 19:51 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 Sep 10 19:43 sys
drwxrwxrwt 8 root root 4096 Sep 10 19:43 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
```

Ve tekrar işe yarar birşey bulamıyoruz.

Ve tekrar bir üst dizine çıkıyoruz.

```
root@secure-command:/# cd
root@secure-command:~# ls -la
total 24
drwx----- 4 root root 4096 Sep 10 19:51 .
drwxr-xr-x 18 root root 4096 Sep 12 2023 ..
-rw-r--r-- 1 root root 13 Nov 18 2023 .advice_of_the_master
-rw-r--r-- 1 root root 697 Nov 18 2023 .bashrc
drwxr-xr-x 3 root root 4096 Nov 18 2023 .local
drwx----- 2 root root 4096 Sep 10 19:43 .ssh
```

Burada işe yarar birşeyler bulduk gibi

Sistemde gizlenmiş olan .advice\_of\_the\_master dosyasını yazdırıyoruz.

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

Ve makineyi başarıyla çözmüş olduk.

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...