SECURE COMMAND WRİTE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Secure Command adlı Warmup'ın çözümünü anlatacağım.

SORU 1: Hangi port(lar) açık?

Nmap taraması atıp sonuca bakıyoruz.

```
└─# nmap -A -Pn 172.20.4.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 14:03 +03
Nmap scan report for 172.20.4.13
Host is up (0.075s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 3f:1b:07:c7:23:c1:1f:6f:55:45:be:28:90:31:1b:d9 (ECDSA)
|_  256 6e:4b:ac:4b:03:7e:af:06:fb:74:32:26:1a:f1:4d:01 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/6%OT=22%CT=1%CU=37312%PV=Y%DS=2%DC=T%G=Y%TM=6702
OS:6EBF%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%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)
```

22 (SSH) portunun açık olduğunu görüyoruz.

SORU 2: Çalışan hizmet adı nedir?

Bu sorunun cevabını da yine yukarıda verdik. 22 portu SSH'a aittir. Bu yüzden çalışan hizmet **SSH** hizmetidir.

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

Bu sorunun cevabını bulmak için ssh bağlantısı yapmaya çalışacağım.

hackviser: hackviser bilgileri ile giriş yapmam gerektiğini bize soruda vermişti ve bununla giriş yaptım. Master's Message kısmı da şeklin üstünde yer alıyor.

Cevap: ***W3lc0m3 t0 h4ck1ng w0rld***

SORU 4: Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

Linux'ta kullanıcı değiştirmek için **SU** komutunu kullanıyoruz.

SORU 5: Root kullanıcısının parolası nedir?

Burada su root komutu ile root olmak istedim. Benden parola istedi. Hackviser'da verilen ipucu(4 haneli) düşünüldüğünde basit düşünerek şifrenin de root olduğunu varsayarak giriş yapmayı denedim. Giriş başarılı oldu şifremiz: **root**.

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

SORU 6: ls komutunun gizli dosyaları gösteren parametresi nedir?

Ls komutu ile gizli dosyaları görmek istediğimizde **–a** komutunu kullanırız.

SORU 7: Master'in tavsiyesi nedir?

Bu sorunun cevabını bulmak için bağlantı kurduğum terminalde biraz dolandım. Root yetkisi aldıktan sonra root dizinine gittim. Burada ls –a komutunu çalıştırınca şu sonucu aldım:

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

Burada advice_of_the_master dosyasını gördüm ve cat ile okumak istedim.

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

Ve cevabımıza ulaştık: st4y cur10us