ARROW WRİTE-UP

Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan Arrow adlı Warmup' ını yazacağım.

SORU 1: İlk sorumuz ile başlıyoruz*. HANGİ PORTLAR AÇIK?*

Bu soruyu çözmek için nmap taraması atmamız yeterli olacaktır.

```
└─# nmap -A -Pn 172.20.5.43
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 13:30 +03
Nmap scan report for 172.20.5.43
Host is up (0.075s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
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=23%CT=1%CU=38332%PV=Y%DS=2%DC=T%G=Y%TM=6702
OS:66E7%P=x86_64-pc-linux-gnu)SEQ(SP=104%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)
```

Burada **23** portunun olduğunu görüyoruz ve ilk sorumuzu cevaplıyoruz.

SORU 2: *Çalışan servisin adı nedir*?

Yukarıdaki nmap taramasında 23 portunun hemen yanında bize zaten servisin isminin **TELNET** olduğunu söylemiş.

SORU 3: *Hostname nedir?*

Bu soruyu çözmemiz için öncelikle makineye bağlanmamız gerekiyor. 23 (Telnet) portu açık olduğu için biz bu makineye telnet ile bağlantı kurmamız gerekiyor.

```
┌──(root㉿kali)-[/home/kali]
└─# telnet 172.20.5.43
Trying 172.20.5.43 ...
Connected to 172.20.5.43.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login:
```

Burada hostname' in **ARROW** olduğunu görüyoruz. Ve bağlantı kurmamız için root:root gibi basit denemeler yapmamız gerektiğini söylüyor.

Root: root deneyerek içeriye giriş yapmayı deniyoruz.

SORU 4: *Telnet'e bağlanmak için kullandığınız username:password nedir?*

Bize zaten yukarıdaki kısımda basit şeyler deneyerek giriş yapmayı deneyin dediği için **root:root** denemesi yaptım. Ve içeriye başarılı bir şekilde giriş yaptık.

SORU 5: *Telnet'e bağlandığınızda çalışma dizini konumunuz nedir?*

Bu sorunun cevabını bulmak için de pwd komutunun yazılması yeterli olur.
Pwd: İçinde bulunduğumuz dizini bize göstermeye yarayan komuttur.
/root