

Arrow Write-up

Giriş

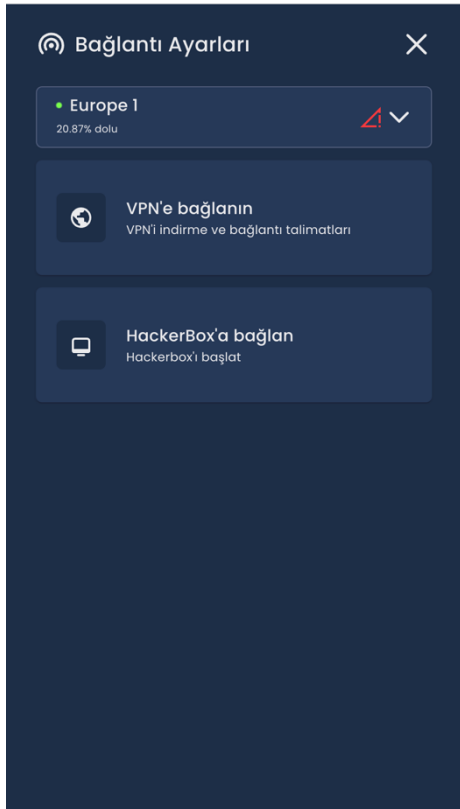
Arrow ısınma makinesi, siber güvenlik dünyasına yeni adım atanlar için kolay ve eğlenceli bir başlangıç noktası sunuyor. Telnet servisi üzerinden zayıf kimlik doğrulama bilgilerini kullanarak bir makineye nasıl sızılabilir? Bu sorunun cevabını ararken, bu makinenin hem teknik zorluklarını hem de siber güvenlikteki temel kavramları öğreneceksiniz.

Yeni başlayanlar için bu tür bir makineyle çalışmak, sadece teknik becerileri değil, aynı zamanda problem çözme yeteneklerini de geliştirir. Bu yazı, siber güvenlikte kritik öneme sahip olan pratik deneyim kazanmanın yanı sıra, teorik bilginin uygulamalı olarak pekiştirilmesine de yardımcı olacaktır.

Hazırlık

Hackviser içerisindeki senaryoları, laboratuvarları, ısınma makinelerini vb. çözebilmek için kullanabileceğiniz 2 yöntem vardır; VPN ve HackerBox.

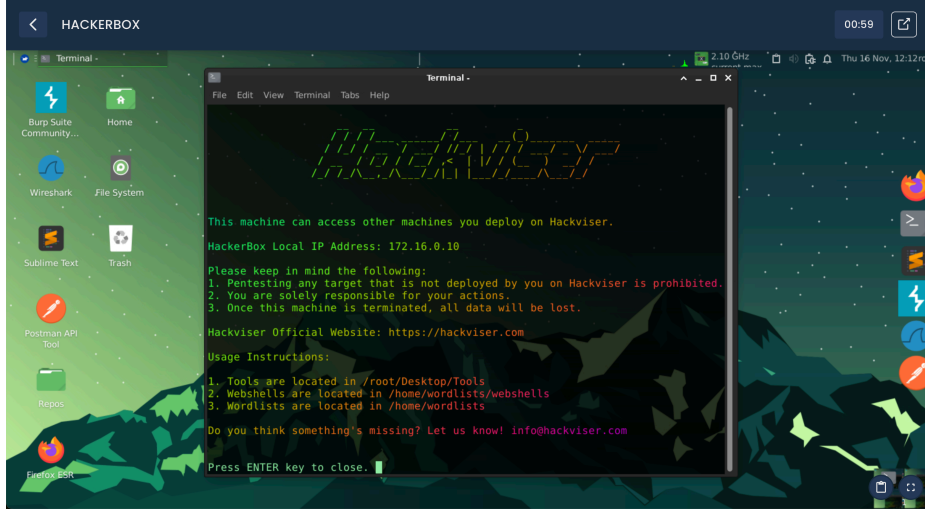
AppBar'da bulunan **Bağlan** butonuna tıkladığımızda karşımıza **VPN** ve **HackerBox** seçenekleri çıkar.



HackerBox (Tavsiye Edilen)

AppBar'da bulunan **Bağlan** butonuna tıkladıktan sonra açılan pencereden **HackerBox'a Bağlan** butonuna tıklayarak bir HackerBox başlatabilirsiniz.

HackerBox başlatıldıktan sonra **HackerBox'a git** butonuna tıklayarak HackerBox'a erişebilirsiniz.



OpenVPN

VPN'e bağlandığınızda kendi bilgisayarınızı kullanarak siber güvenlik faaliyetlerinizi gerçekleştirebilirsiniz. VPN'e bağlanabilmek için AppBar'da bulunan **Bağlan** butonuna tıkladıktan sonra açılan pencereden **VPN'e Bağlan** butonuna tıklayınız.



Açılan pencereden VPN bağlantı talimatlarını takip ederek öncelikle OpenVPN client yazılımını bilgisayarınıza indirmeniz gerekmektedir.

OpenVPN client yazılımını yükledikten sonra **VPN Konfigürasyonunu İndir** butonuna tıklayarak indirdiğiniz VPN konfigürasyon dosyası ile birlikte VPN'e bağlanabilirsiniz.

HackerBox ya da VPN ile Hackviser'a bağlandıysanız senaryoları, ısınma makinelerini, laboratuvarları vb. çözmeye hazırsınız!

Telnet Nedir?

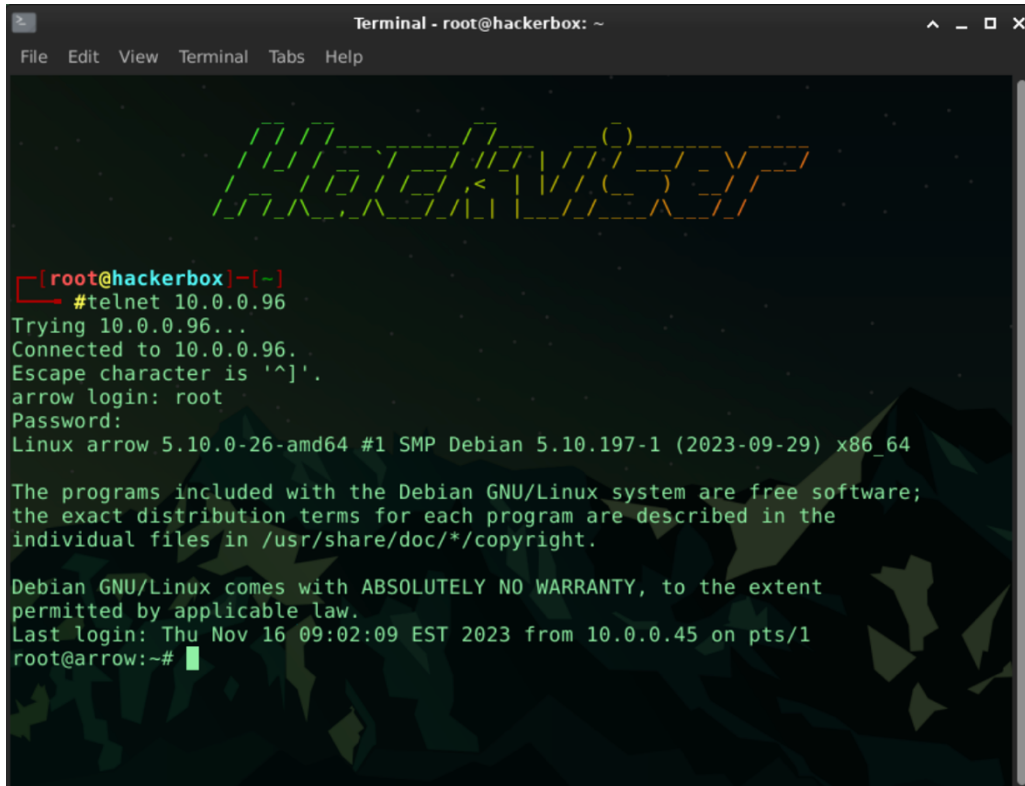
Telnet (**Te**letype **Ne**twork), uzaktan bir bilgisayara bağlanmak için kullanılan, metin tabanlı bir ağ protokolüdür. 1969 yılında geliştirilen ve İnternet'in ilk günlerinde yaygın olarak kullanılan bu protokol, özellikle ağ cihazları, sunucular veya diğer uçbirimlerle etkileşim kurmak için tasarlanmıştır. Kullanıcı adı ve şifre ile giriş yapılabilen bir arayüz sağlar, böylece kullanıcılar, sanki o bilgisayarın yerel terminalindeymiş gibi komutlar çalıştırabilir.

Telnet'in en büyük dezavantajı, veri iletiminin şifrelenmemiş olmasıdır. Bu, iletilen her türlü bilginin, özellikle de kullanıcı adı ve şifrelerin, potansiyel olarak kötü niyetli kişiler tarafından ele geçirilebileceği anlamına gelir. Bu güvenlik zaafiyeti, Telnet'i özellikle hassas verilerin işlendiği modern ağ ortamlarında riskli bir seçenek haline getirir.

Bir sunucuya telnet protokolü ile bağlanmak için aşağıdaki komut dizisi kullanılır.

```
telnet <SERVER-IP-ADDRESS> <PORT-NUMBER>
```

Not: Eğer telnet servisi varsayılan olarak 23 portunu kullanıyorsa bağlanırken port numarası belirtmemize gerek yoktur.



```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help

[root@hackerbox]~# telnet 10.0.0.96
Trying 10.0.0.96...
Connected to 10.0.0.96.
Escape character is '^]'.
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) 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: Thu Nov 16 09:02:09 EST 2023 from 10.0.0.45 on pts/1
root@arrow:~#
```

Yukarıdaki örnekte görüldüğü üzere telnet servisine bağlanırken kullanıcı adı ve parola bilgilerini giriyoruz.

Bu bilgileri doğru bir şekilde girdikten sonra telnet protokolü ile uzaktaki bir bilgisayara bağlanmış oluyoruz.

-

Telnet servisinin güvenlik açısından taşıdığı riskleri ve barındırdığı zafiyetlerin nasıl tespit edilip istismar edilebileceğini **Arrow** ısınma makinesi üzerinden ele alacağız.

Bilgi Toplama

Siber güvenlikte her başarılı saldırının temelinde, hedef sistem hakkında derinlemesine bilgi toplama yatar. Bu anlamda, "Bilgi Toplama" süreci, hedef makineye yönelik saldırıların başarısında kritik bir rol oynar. Bu bölümde, **Telnet** servisini içeren makineye sızma sürecinin ilk ve en önemli aşaması olan bilgi toplama adımlarını ele alacağız.

Bu aşamada doğrudan hedef sisteme yönelik taramalar yaparak detaylı bilgi edinmeyi amaçlıyoruz. Yapacağımız taramalarla, Telnet servisinin sürümü, çalıştığı portlar ve sistem üzerindeki çalışan diğer servis bilgileri gibi daha spesifik bilgiler elde edilir.

Bu süreçte kullanılacak araçlar ve metodlar, hedef sistemin yapısına ve güvenlik düzeyine göre değişiklik gösterebilir. Örneğin **nmap**, **rustscan** gibi popüler port tarama araçları bu aşamada kullanılabilir.

nmap

Nmap (Network Mapper), ağ güvenliği alanında yaygın olarak kullanılan güçlü bir open source araçtır. Temel işlevi, ağ taramaları yaparak cihazların ağ üzerindeki varlıklarını, çalıştırdıkları servisleri ve açık portları tespit etmektir. Siber güvenlik uzmanları tarafından güvenlik açıklarını bulmak, ağ yapılarını haritalamak ve savunma sistemlerini test etmek için kullanılır.

Nmap, komut satırı tabanlı bir arayüze sahip olup, esnek ve çok çeşitli tarama seçenekleri sunar.

Nmap aracının kullanımı ve bazı önemli parametreleri aşağıdaki gibidir.

```
nmap <TARGET>
```

```
-sS : TCP SYN paketleri ile hedef makinenin portlarını tarar.  
      nmap -sS <TARGET>  
  
-sT : TCP Connect paketleri ile hedef makinenin portlarını tarar.  
      nmap -sT <TARGET>  
  
-sV : Hedef makinede çalışan servislerin sürümlerini tespit eder.  
      nmap -sV <TARGET>  
  
-A : Agresif tarama. Hedef üzerinde kapsamlı bir tarama yapar. Servis  
      sürümü, işletim sistemi tespiti ve script taraması gerçekleştirir.  
      nmap -A <TARGET>  
  
-O : Hedef sistemde çalışan işletim sistemini tespit etmeye çalışır.  
      nmap -O <TARGET>  
  
-p : Belirli portları ya da port aralığını taramak için kullanılır.  
      nmap -p 80,443 <TARGET> // 80 ve 443 portlarını tarar.  
      nmap -p 1-2000 <TARGET> // 1 ile 2000 arasındaki portları tarar.  
      nmap -p- <TARGET> // Tüm portları (65.536) tarar.
```

Görev 1, Görev 2

Açık port ve servis bilgilerini öğrenmek için hedef makineye nmap taraması yapıyoruz.

```
root@hackerbox:~# nmap 172.20.24.47  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-16 09:08 CST  
Nmap scan report for 172.20.24.47  
Host is up (0.00027s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
23/tcp    open  telnet  
MAC Address: 52:54:00:E9:C7:20 (QEMU virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Sisteme Erişim

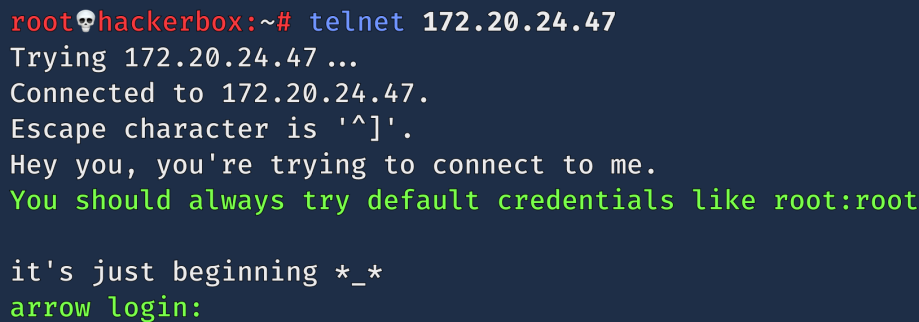
Bu aşama, daha önceki bilgi toplama aşamasında elde edilen bilgilerin pratik uygulamaya döküldüğü, hedef sistem üzerinde ilk somut etkileşimin başladığı noktadır. Bu süreç, sistemin güvenlik durumunun kapsamlı bir değerlendirmesini yapabilmek için kritik bir adımdır.

Sisteme erişim aşamasında gerçekleştirilen faaliyetler, genellikle zafiyetlerin istismarı, güvenlik duvarlarını aşma ve sistemde yetki yükseltme gibi unsurları içerir. Bu süreçte, etik hackerlar veya güvenlik analistleri, hedef sistemdeki güvenlik önlemlerini test eder, potansiyel güvenlik zafiyetlerini belirler.

Görev 3, Görev 4

Bir önceki aşamada port taraması yaparak çalıştığını keşfettiğimiz telnet servisine bağlanmayı deneyeceğiz. Bunun için aşağıdaki komutu çalıştıralım.

```
telnet 172.20.24.47
```

A terminal window with a dark blue background and three colored window control buttons (red, yellow, green) in the top left corner. The terminal shows the command 'telnet 172.20.24.47' being executed. The output includes connection status, escape character information, and a message from the remote host suggesting default credentials. The prompt 'arrow login:' is visible at the bottom.

```
root@hackerbox:~# telnet 172.20.24.47
Trying 172.20.24.47 ...
Connected to 172.20.24.47.
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:
```

Telnet ile hedef makineye bağlanmaya çalışırken bir ipucu yakalıyoruz. İpucu; kullanıcı adı için **root**, parola için **root** gibi varsayılan olarak kullanılabilecek çok basit parolaları denememizi söylüyor.

Ayrıca **arrow login** yazan satırda da bağlanmaya çalıştığımız makinenin hostname bilgisinin **arrow** olduğunu görüyoruz.

Görev 5

5.görevi tamamlayabilmek için ipucu olarak bize verilen **root:root** oturum bilgileriyle oturum açalım.

```
root@hackerbox:~# telnet 172.20.24.47
Trying 172.20.24.47 ...
Connected to 172.20.24.47.
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: root
Password:
Linux arrow 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) 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: Thu Nov  2 10:03:57 EDT 2023 on tty1
root@arrow:~# pwd
/root
root@arrow:~#
```

Oturum açtıktan sonra çalışma dizinimizi görüntülemek için **pwd** komutunu çalıştırmamız yeterli.

-

Tebrikler 🎉

✨ Bu ısınma makinesindeki tüm görevleri başarıyla yerine getirdiniz.