**Discover Lernaean**

Bu yazımda Hackviser platformunda bulunan Discover Lernaean adlı warmup’ın çözümünü anlatacağım.

**SORU 1:** Hangi port(lar) açık?

Nmap taraması yaparak bu sorunun cevabını bulmaya çalışacağım.



Burada **22(**ssh) ve **80**(http) portlarının açık olduğunu buluyoruz.

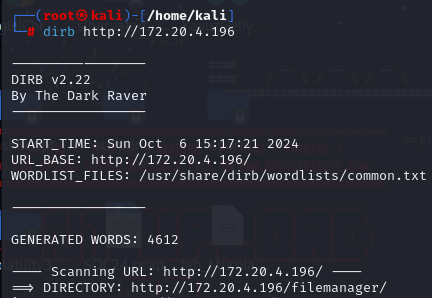
**SORU 2:** 80 portunda çalışan servisin versiyonu nedir?

80 portunun açıklama kısmında çalışan servisin versiyonunun **2.4.56** olduğunu bulduk.

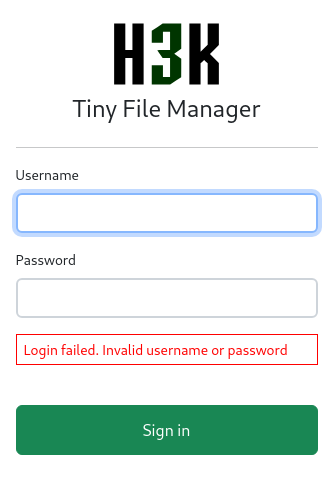
**SORU 3:** Dizin tarama aracını kullanarak bulduğunuz dizin nedir?

Dizin tarama aracı olarak dirb aracını kullanıyorum.

Dirb ile tarama yaparak sonucu görelim:

 filemanager dizinini bulduk.

**SORU 4:** File manager'a giriş yapmak için kullandığınız username:password nedir?

 filemanager dizinini açmak istediğimizde böyle sayfaya gidiyoruz.

Burada OSINT dediğimiz bilgi toplama yöntemini kullanacağız. Login sayfasının başında Tiny File Manager ismi benim dikkatimi çekiyor. Bunu araştırıyoruz. Bir github buldum.

<https://github.com/prasathmani/tinyfilemanager>

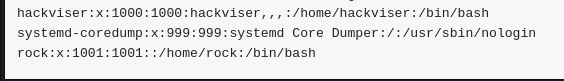
Burada default username:password var.

 Deniyoruz.

**User:12345** deneyerek giriş yaptım.

**SORU 5:** Bilgisayara eklenen son kullanıcı adı nedir?

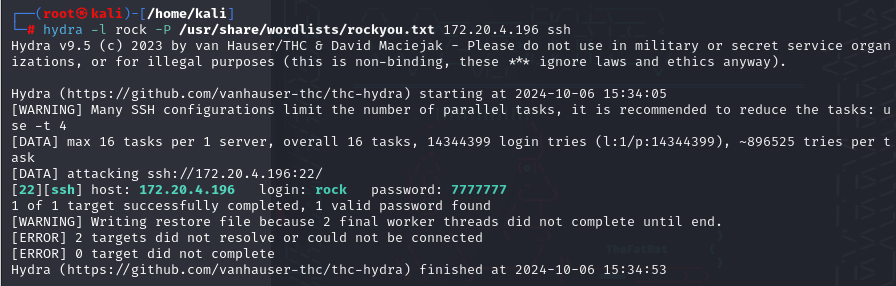
Bilgisayardaki kullanıcılar /etc/passwd dosyası altında toplanır. Buraya gidiyoruz.



Bu dosyayı görüntülediğimizde en son eklenen kullanıcının **ROCK** olduğunu görüyoruz.

**SORU 6:** rock kullanıcısının parolası nedir?

Bu sorunun cevabını bulmak için 22 portunun açık olduğunu 22 portunun da ssh’a ait olduğunu tekrardan gözden geçiriyoruz. Ve ssh ile bağlanmaya çalışacağım. Şifreyi bilmediğimiz için brute-force attack dediğimiz saldırı yöntemini kullanacağım. Hydra aracı ile yapacağım.



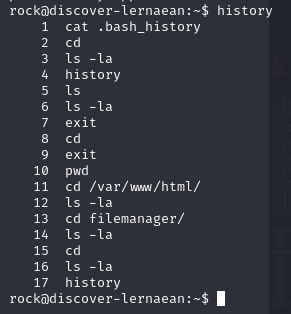
-l: kullanıcı ismini biliyorsak kullanırız.

-P: kullanacağımız wordlist’i belirtiriz. Rockyou.txt en fazla kullanılan wordlist olduğu için seçtim.

Parolanın **7777777** olduğunu bulduk.

**SORU 7:** rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

SSH ile bağlantı yapıyoruz.



History: Bizim terminaldeki yazdığımız komut geçmişini gösterir. İlk yazılan komutu sorduğu için

Cevap: **cat .bash\_history**