**FIND AND CRACK WRİTE-UP**

Bugünkü yazımda Hackviser platformu üzerinde bulunan Find and Crack isimli warmup’ın çözümünü anlatacağım. Bu ısınmayı çözebilmemiz için bize verilen komutu /etc/hosts dosyasına ekliyoruz ve başlıyoruz.

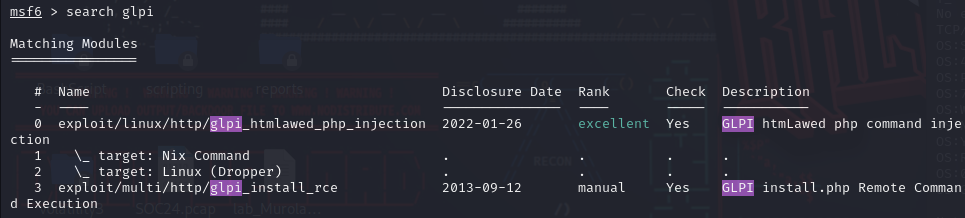
**SORU 1:** Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?

Sitemize erişim sağlayıp giriyoruz.

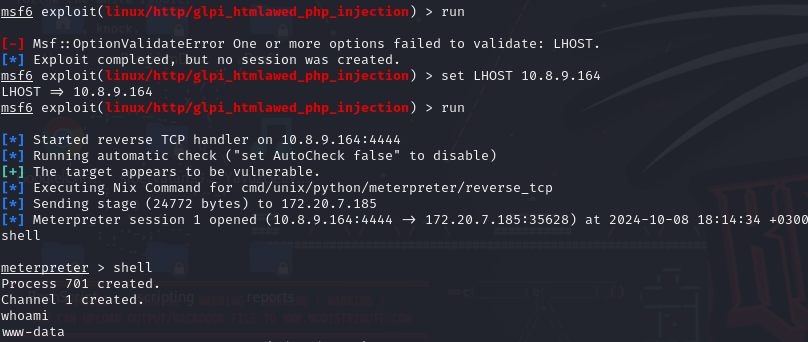
 tıkladıktan sonra cevap URL üzerinde  Cevap: **glpi**

**SORU 2:** Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?

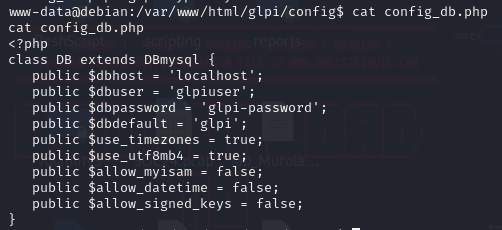
Elimizde glpi diye bir yazılım ismi var. Bu yüzden burası ile ilgili bir açık var mı yok mu diye msfconsole ile metasploit framework’e bağlanıp aramalar yapacağım.



Bir açık mevcutmuş. Şimdi bu kısmı biraz inceleyelim. Biraz daha ileri gidip Shell almayı deneyelim.



Başarılı bir şekilde Shell almayı başardık. Şimdi veritabanı ile bilgi istiyor. Bu yüzden config dosyası var mı yok mu onu kontrol edip içini okuyup cevaba ulaşmaya çalışacağım.

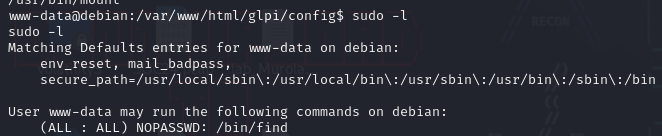


/var/html/glpi/config klasörü içerisinde config\_db.php dosyasını buldum ve içini gösterdiğimizde cevaba ulaşmış olduk.

Cevap: **glpiuser**

**SORU 3:** Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?

Bu sorunun cevabını bulabilmek için “*sudo –l*” komutunu çalıştıralım.



Burada **find** komutunu kullanabileceğimizi görüyoruz.

**SORU 4:** backup.zip parolası nedir?

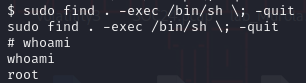
Backup.zip dosyasının nerede olduğunu bulmak için biraz gezinelim.



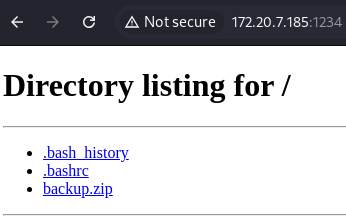
Burada /home dizini altında lost+found dizinine giremediğimi gördüm. O yüzden artık yetki yükseltmem gerekiyor. Kullanacağımız komut da find komutu. Hadi başlayalım.

[GTFOBins](https://gtfobins.github.io/gtfobins/find/#suid) sayfası üzerinde find komutu için yetki yükseltme yolları arasında:

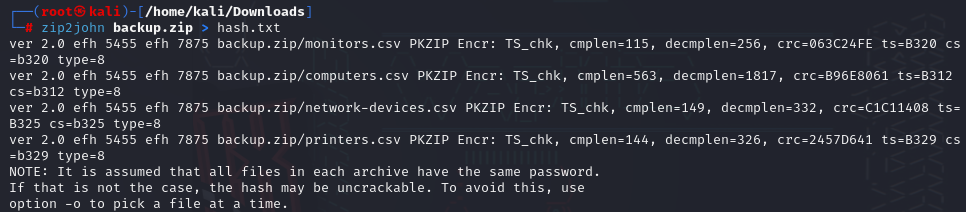
“*sudo find . -exec /bin/sh \; -quit*” komutunu buldum ve denedim.

 ARTIK ROOT KULLANICISIYIZ ☺

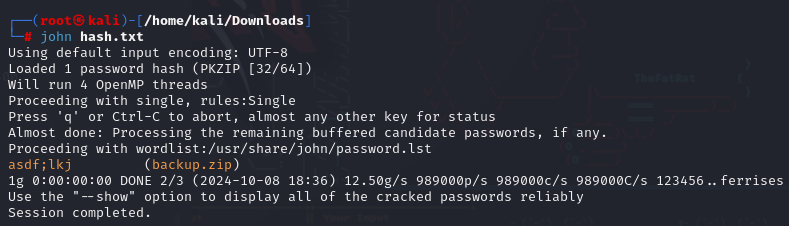
Root dizini içerisinde dosyamızı buldum.  Şimdi bunu ana makinemize indirmemiz gerek. Bu yüzden geçici bir sunucuyu hedef makinede açıyoruz ve Google tarayıcısı üzerinden gidiyoruz.(kodumuz: python3 –m http.server 1234)

 Şimdi indiriyoruz. Elimizde zip dosyası var ve şifrenin ne olduğunu bilmiyoruz. Bunun için john aracı ile şöyle bir yöntem uygulayacağım.

Öncelikle zip dosyasının hash değerini hash.txt içerisine kaydediyoruz.



Daha sonra hash değerini çözmek için yine john aracını kullanıyorum.



Burada zip dosyasının şifresine ulaşmış olduk.

Cevap: **asdf;lkj**

**SORU 5:** Kimin madencilik yaptığından şüpheleniliyor?

Şimdi şifreyi deneyerek dosyaları zipten çıkaralım ve tek tek dosyaların içini kontrol edelim.



Burada **Ethan Friedman** adlı kişi “He may be mining.” Cümlesinden cevabı buluyoruz.