CARNIVAL WRİTE-UP

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

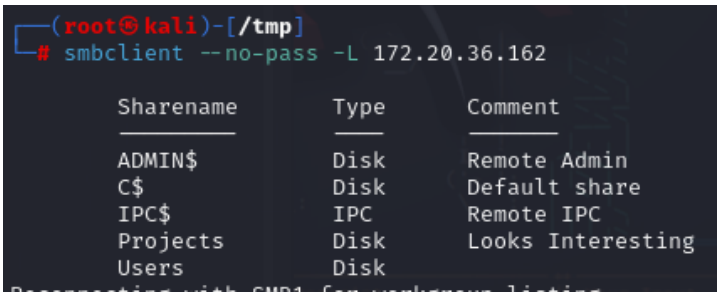
SORU 1: Genellikle 445 portunu kullanan SMB servisinin açılımı nedir?

SERVER MESSAGE BLOCK

SORU 2: "Looks interesting" yorumunu içeren paylaşılan klasörün adı nedir?

Bu sorunun cevabını bulabilmemiz için öncelikle smb bağlantısı kurmamız gerekmektedir. Uzun araştırmalarım sonucunda "smbclient" aracı ile bunu yapabildiğimizi buldum.

Smbclient –no-pass –L <IP_ADDRESS> komutu ile giriş yapmayı deneyelim.



Ve başarılı. Cevap: **Projects**

SORU 3: SMB bağlantısından sonra hangi komutları çalıştırabileceğimizi gösteren yardımcı komut nedir?

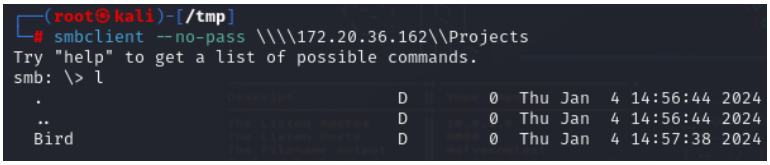
Linux'ta neredeyse birçok tool'da olduğu gibi bu tool içinde **help** komutu kullanılır.

SORU 4: Projenin ismi nedir?

Bu sorunun cevabını bulmak için smbclient –help yaparak biraz kurcalıyoruz.

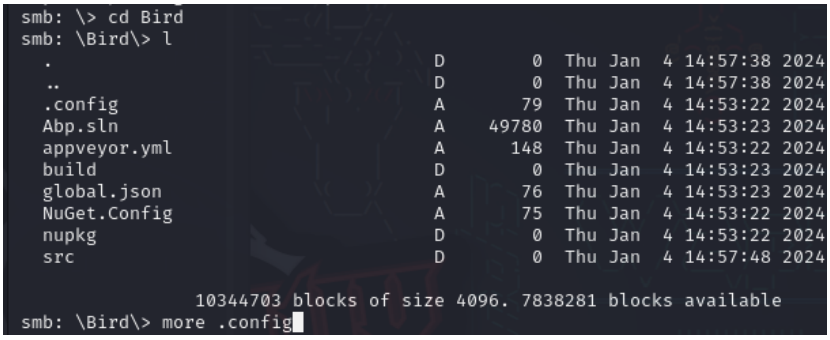
"smbclient –no-pass \\\\<IP_ADDRESS>\\<Foldername>"

Komutu ile cevaba ulaşmaya çalışalım. Şimdi tam olarak bağlantı kurmuş olduk. "l" ile cevaba gidelim.

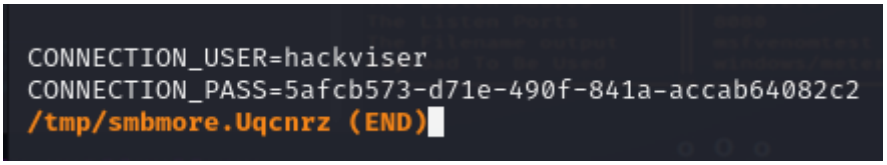


Cevap: **Bird**

SORU 5: .config dosyası içindeki bağlantı şifresi nedir?



.config dosyası Bird klasörü içerisinde. More .config komutu ile içini görüntüleyelim.



Cevap: **5afcb573-d71e-490f-841a-accab64082c2**