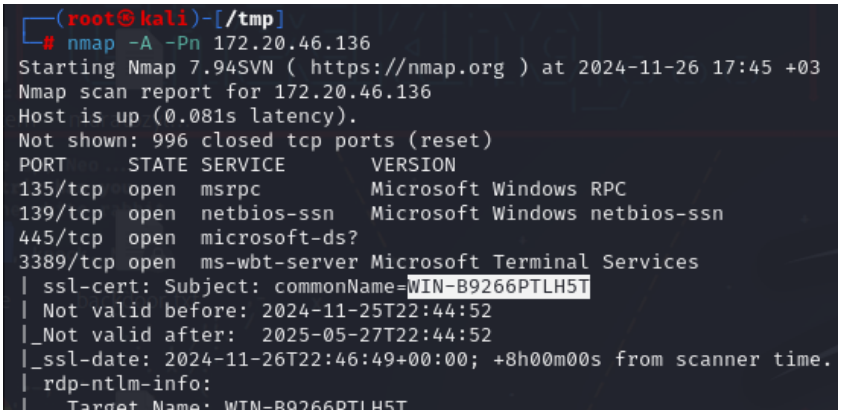
007WRİTE-UP

Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan 007 adlı Warmup' ını yazacağım.

SORU 1: Hedef bilgisayarın adı nedir?

Öncelikle hedef hakkında bilgi toplama işlemleri yapalım. Nmap taraması ile başlayalım.



Cevap: **WIN-B9266PTLH5T**

SORU 2: RDP'nin açılımı nedir?

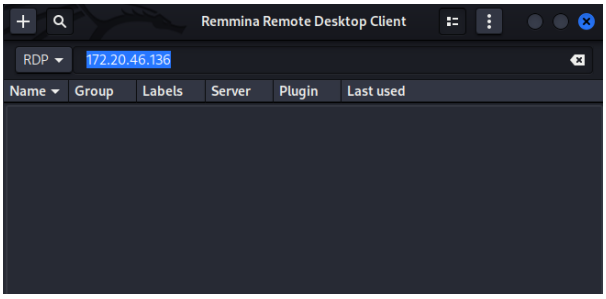
Remote Desktop Protocol

SORU 3: Windows'ta, genellikle kullanılan en ayrıcalıklı kullanıcı adı nedir?

Windows İşletim Sistemi'nde en ayrıcalıklı kullanıcı **Administrator**' dur.

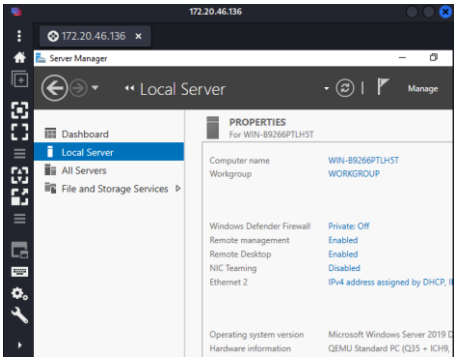
SORU 4: Windows versiyonu nedir?

Bunun için RDP bağlantısı yapmamız gerekiyor. Şimdi "Remmina" adlı uygulamayı Linux makinemize indiriyoruz ve başlatıyoruz.



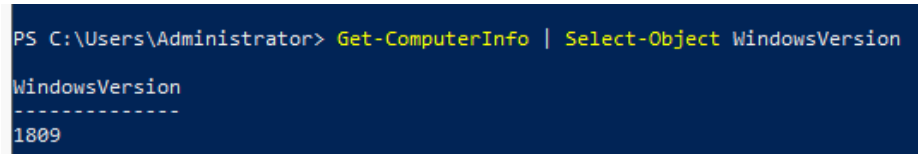
Hedef IP adresini giriyoruz.

Daha sonra doğrulama kısmında kullanıcı adına "Administrator" yazıp diğer kısımları boş bırakarak bağlantı kurmayı deniyoruz.



Böylelikle bağlantı başarılı oldu. ☺

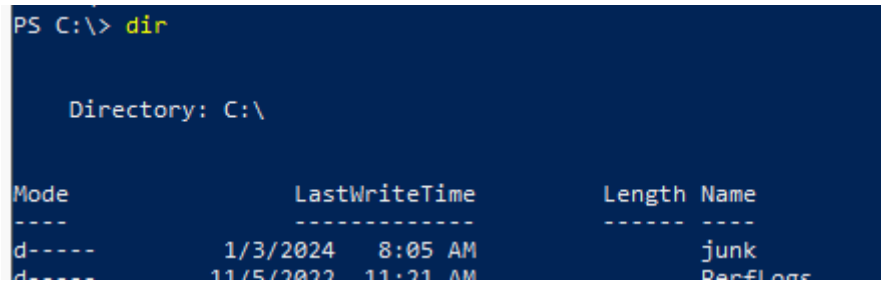
Şimdi powershell içerisine “Get-ComputerInfo | Select-Object WindowsVersion” komutunu yazarak Windows versiyonunu öğrenelim.



Cevap: **1809**

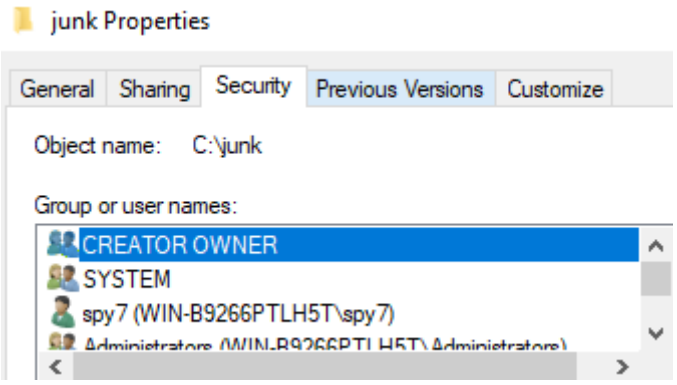
SORU 5: C:\ dizini altındaki şüpheli görünen klasörün adı nedir?

Cd .. diyerek geri klasörlere gidiyoruz. Ve sonra “dir” komutu ile dosyaları listeliyoruz.



Cevap: **JUNK**

SORU 6: Which user owns the junk folder?



Dosyaya girip sağ tık yaparak özellikler sekmesine girdiğimizde burada gözümüze çarpan kullanıcı **spy7**