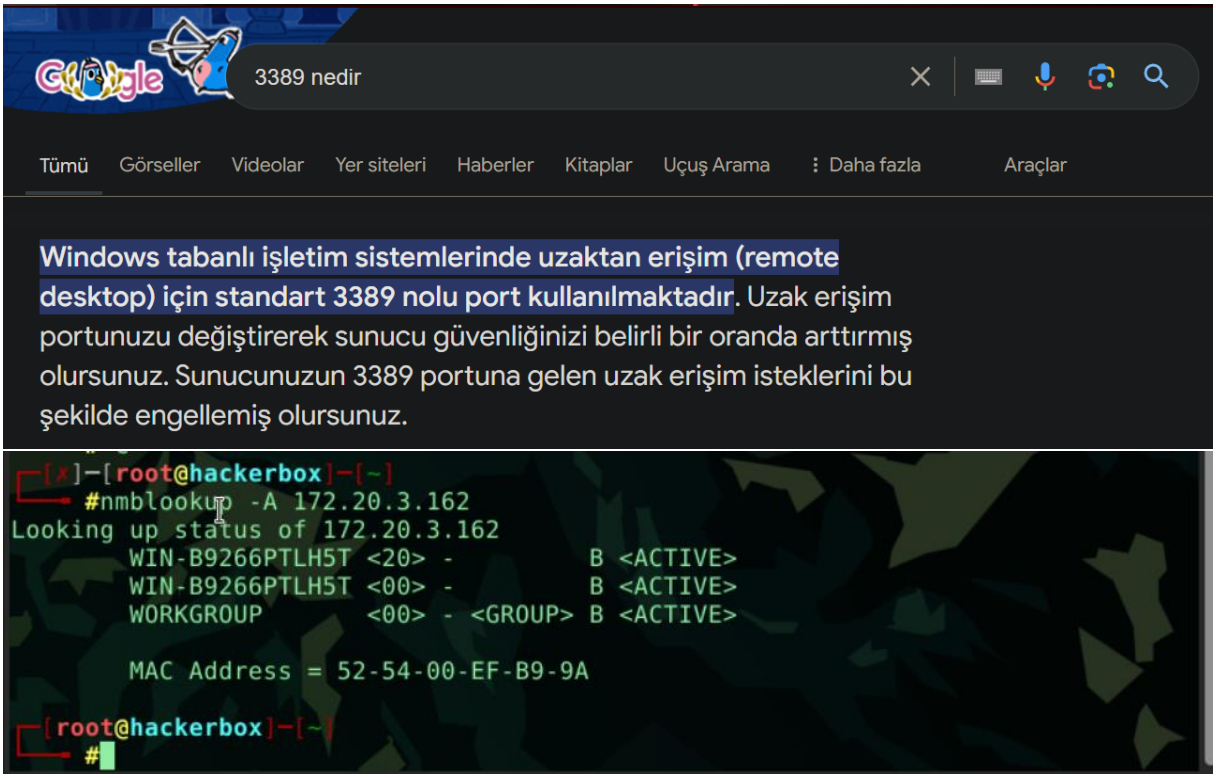
007 ISINMASI

Isınma ile ilgili bilgi: Remote Desktop Protocol (RDP), kullanıcıların bir bilgisayara uzaktan bağlanıp kontrol etmesine olanak tanıyan bir protokoldür.

RDP ile ilgili temel alıştırmalar yapmak için önerilir.

1. *Hedef bilgisayarın adı nedir?*
   Bilgi: **`nmblookup`** komutu, NetBIOS ad çözümlemesi yapmak için kullanılan bir araçtır. Bu araç, NetBIOS adları ile IP adresleri arasında eşleşmeler bulmak ve ağ üzerindeki bilgisayarların NetBIOS adlarını sorgulamak için kullanılır.
   Kullanımı: nmblookup -A <IP_adresi> (bash) : Belirtilen IP adresinin NetBIOS adlarını ve bilgilerini arar.



Görüldüğü üzere hedef bilgiyarın adı "WIN-B9266PTLH5T"dir.

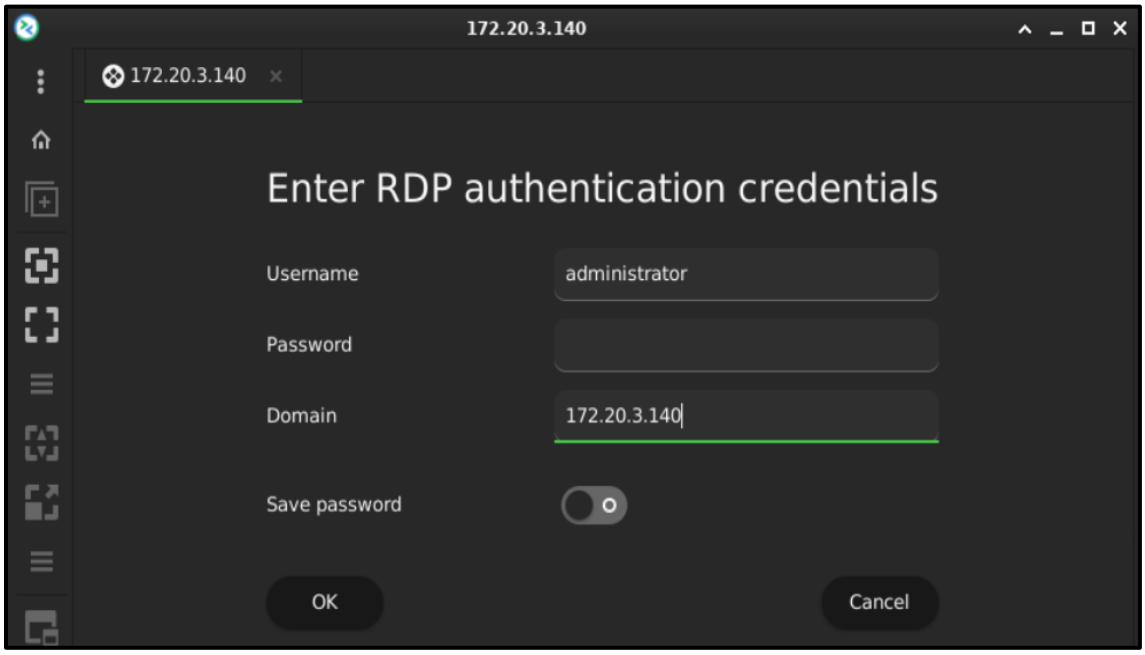
2. *RDP'nin açılımı nedir?*
   Bilgi: RDP'nin açılımı "Remote Desktop Protocol"dür. Bu protokol, bir bilgisayara uzaktan bağlanıp kontrol etmenizi sağlar, genellikle Windows işletim sistemlerinde kullanılır. RDP, kullanıcılara uzak bir bilgisayarın masaüstüne erişim sağlar, bu sayede sanki bilgisayar doğrudan kullanılıyormuş gibi çalışabilirler.

3. *Windows'ta, genellikle kullanılan en ayrıcalıklı kullanıcı adı nedir?*
   Bilgi: Windows'ta, genellikle kullanılan en ayrıcalıklı kullanıcı adı `Administrator`dır. Bu kullanıcı adı, sistemde tam yönetim haklarına sahip olan ve tüm sistem ayarlarını değiştirme, yazılım yükleme ve tüm kullanıcı hesaplarına erişim sağlama yetkisine sahip bir hesaptır.

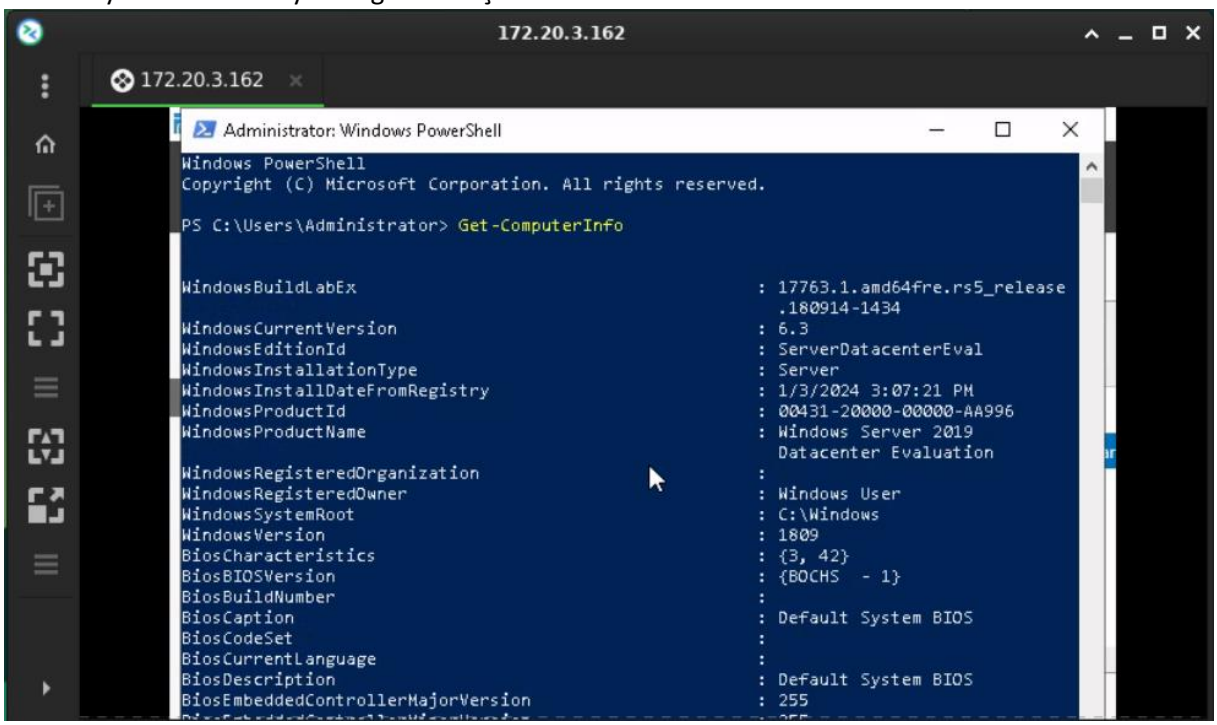
4. Windows versiyonu nedir?

Bilgi: Uzak bir bilgisayara RDP bağlantısı kurmak için çeşitli araçlar mevcuttur. Linux üzerinde, “Remmina” gibi araçlar, RDP bağlantısı kurmak için oldukça kullanışlıdır. Remmina, kullanıcı dostu bir arayüze sahip olup, çeşitli uzak masaüstü protokollerini destekleyerek uzak bilgisayarlara erişimi kolaylaştırır. Diğer popüler RDP araçları arasında Microsoft Remote Desktop, FreeRDP ve rdesktop da bulunmaktadır.

Kullanımı: Öncelikle hacker-box içindeki remina aracına bağlanmaya çalışılır.

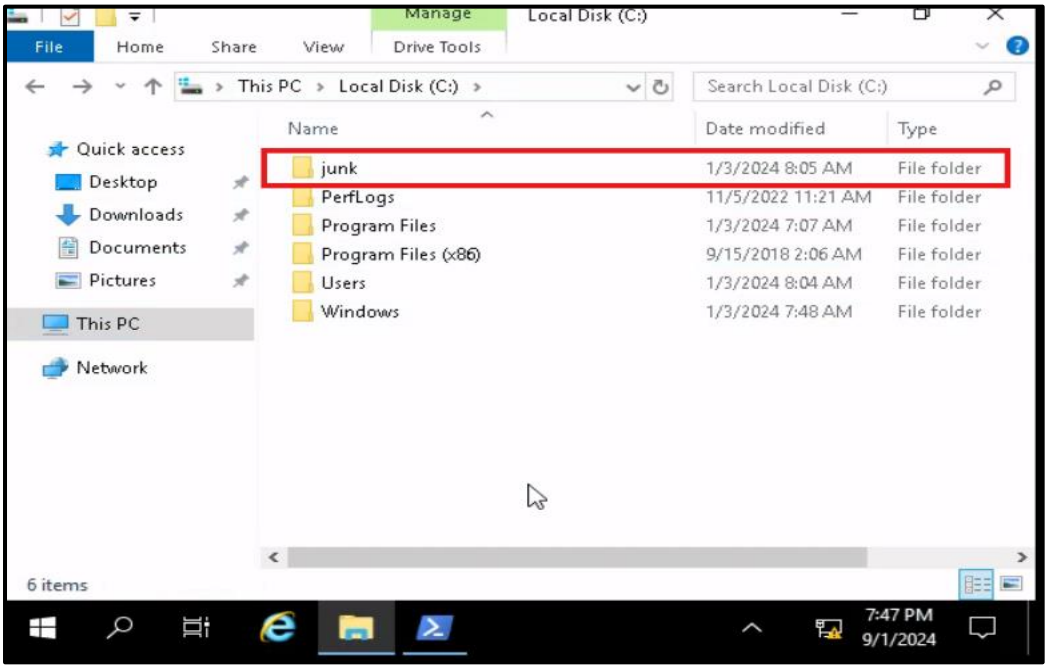


Ardından başarılı bir şekilde bağlandığı görülür ve sürüm aramasına geçilir. Bunun için Powershell ya da cmd kullanılabilir. Burada PowerShell kullanıldı. “Get-ComputerInfo” komutu yardımı ile versiyon bilgisine ulaşılır.



Görüldüğü üzere versiyonu 6.3’tür.

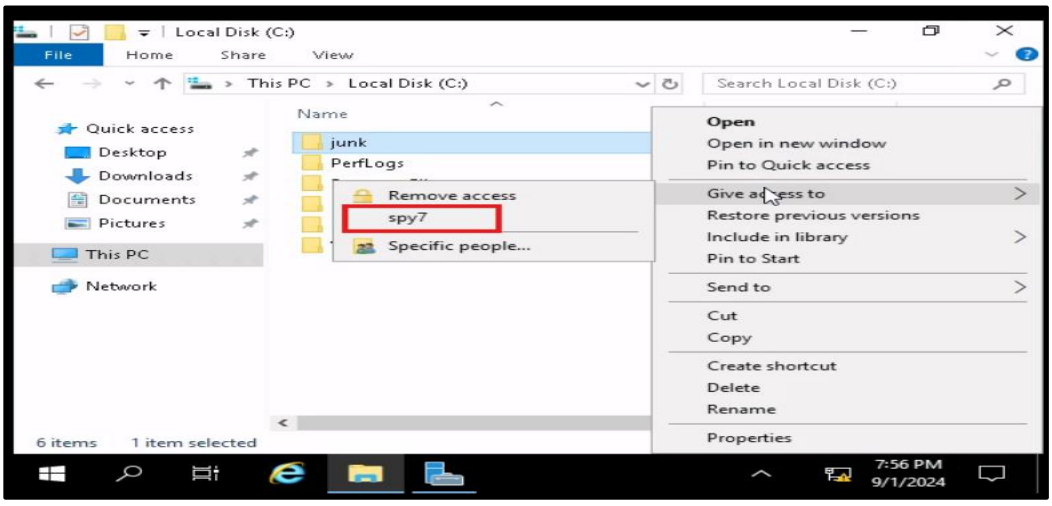
5. *C:\ dizini altındaki şüpheli görünen klasörün adı nedir?*
   Bilgi: *C:*\ dizininde şüpheli görünen klasörler genellikle sistemde olağan dışı veya yetkisiz değişikliklerin izlerini taşıyabilir.
   Kullanımı: C:\ dizinine gidilir ve şüphe uyandıracak dosyalar incelenir.



Görüldüğü üzere tüm dosyalar sistem dosyaları ile ilgiliyken-normal görünürken "junk" dosyası dikkat çekmektedir.

6. *Which user owns the junk folder?*
   Bilgi: Dosya Gezgini Kullanarak tespit edebiliriz:
   - C:\junk gibi ilgili klasöre sağ tıklayın ve "Özellikler" seçeneğine tıklayın.
   - "Güvenlik" sekmesine gidin.
   - "Gelişmiş" düğmesine tıklayın.
   - Açılan "Gelişmiş Güvenlik Ayarları" penceresinde, en üstte klasörün mevcut sahibi görüntülenir. Buradan sahibini değiştirme seçenekleri de mevcuttur.

   Kullanımı:



Görüldüğü üzere dosyanın sahibi "spy7"dir.

- ***007 TAMAMLANMIŞTIR –***