007 Write-up

Giriş

007 ısınma makinesi, Uzak Masaüstü Protokolü (RDP) ile ilgili ideal bir başlangıç noktasıdır. Bu makinede, RDP servislerinin yanlış yapılandırılmasından kaynaklanan güvenlik açıklarını belirlemeyi ve bunları nasıl kullanabileceğinizi öğreneceksiniz. Ayrıca, RDP'nin temel işleyişini ve bağlantı kurma yöntemlerini de detaylı bir şekilde keşfedeceksiniz. Bu alıştırma, RDP güvenlik açıklarını anlamanıza ve siber güvenlik becerilerinizi güçlendirmenize yardımcı olacaktır.

Remote Desktop Protocol (RDP)

Uzak Masaüstü Protokolü (RDP), Microsoft tarafından geliştirilen ve kullanıcıların bir ağ üzerinden başka bir bilgisayara uzaktan erişim sağlamasına olanak tanıyan bir protokoldür. RDP, veri şifrelemesi, oturum yönetimi ve cihaz yönlendirme gibi güvenlik ve işlevsellik özellikleriyle donatılmıştır.

Bilgi Toplama

Hedef makinemize yönelik port taraması yaparak bilgi toplamaya başlayalım.

```
root💀hackerbox:~# nmap 172.20.3.146
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-06 06:51 CST
Nmap scan report for 172.20.3.97
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 52:54:00:E0:92:52 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
```

Yaptığımı port taraması sonucunda 4 adet port açık olduğunu keşfediyoruz. Açık olan 3389 portu ile ilgili araştırma yaptığımızda, bilgisayara uzak masaüstü bağlantısı kurabileceğimiz RDP servisinin çalıştığını tespit ettik.

Görev 1
Hedef makinenin NetBIOS servisi üzerinden hostname bilgisini öğrenebiliriz. Bunun için basitçe **`nmblookup`** aracını kullanabiliriz.

nmblookup

```
nmblookup [options] <netbios-name>
```

```
-A : Bir bilgisayarın IP adresinden NetBIOS adını öğrenmek için kullanılan parametredir.

-B : Bir bilgisayarın NetBIOS adından IP adresini öğrenmek için kullanılan parametredir.
```

```
root💀hackerbox:~# nmblookup -A 172.20.3.146
Looking up status of 172.20.3.146
 WIN-B9266PTLH5T <20> -         B <ACTIVE>
 WIN-B9266PTLH5T <00> -         B <ACTIVE>
 WORKGROUP       <00> - <GROUP> B <ACTIVE>

 MAC Address = 52-54-00-E0-92-52
```

Görev 2
RDP'nin açılımı **`Remote Desktop Protocol`**'dür.

Görev 3
Windows bilgisayarlarda genellikle varsayılan olarak yetkilil kullanıcı **`Administrator`** kullanıcısıdır.

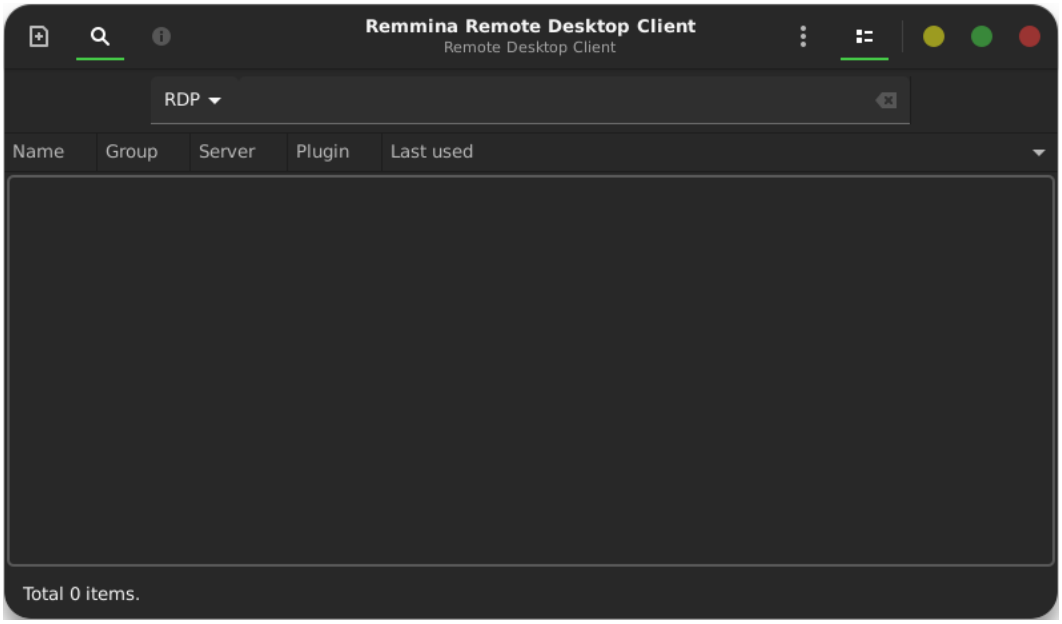
Sisteme Erişim

Hedef makineye, RDP protokolü üzerinden tahmin ettiğimiz Administrator kullanıcısı olarak bağlanmayı deneyelim.

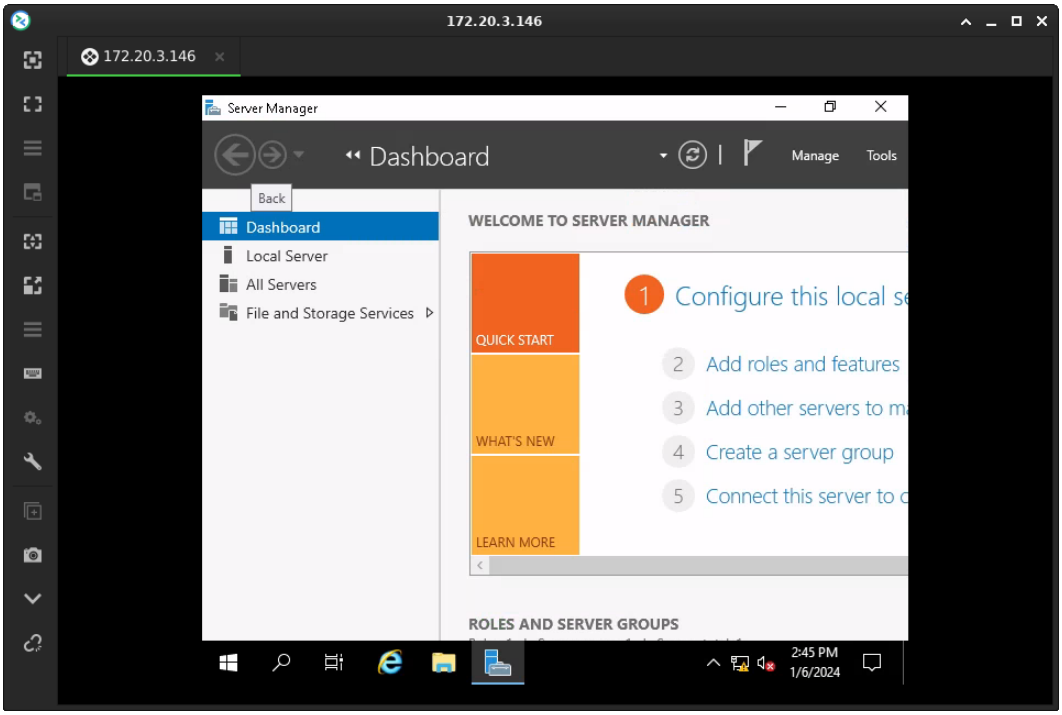
Uzak bir bilgisayara RDP bağlantısı kurmak için kullanılabilecek bir çok araç vardır. Microsoft Remote Desktop, FreeRDP, rdesktop, Remmina gibi araçlar RDP bağlantısı için kullanılabilecek araçlardan bazılarıdır.

Görev 4
Açık-kaynaklı bir proje olan Remmina ile RDP bağlantısı kurmayı deneyelim.

Bunun için HackerBox içerisinde yüklü olarak gelen Remmina aracını başlatalım.

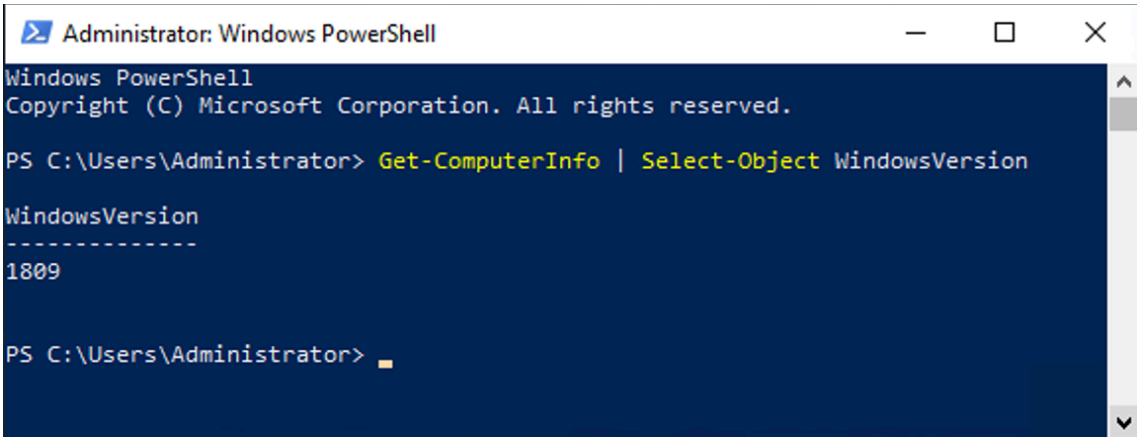


RDP kısmına hedef makinenin IP adresini yazıp ardından kullanıcı adını Administrator olarak girip parolayı da boş bırakıp bağlanmaya çalışalım.

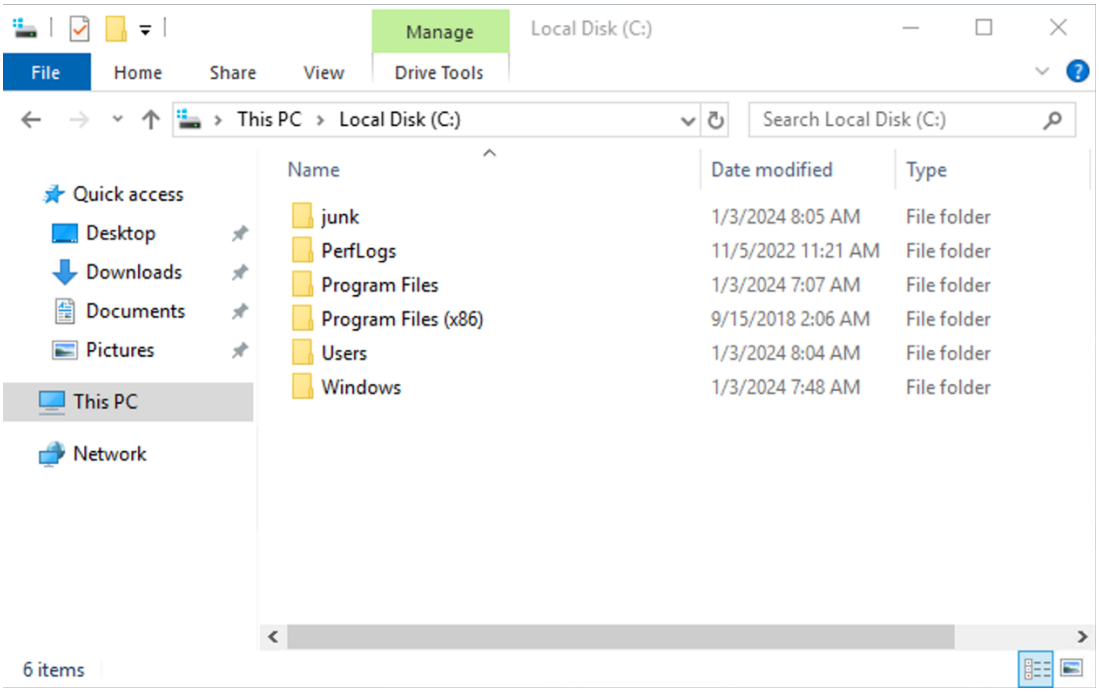


RDP servisi açık kalmış olan bu Windows bilgisayar, parolasız bağlantıya izin verdiği için hatalı konfigüre edilmiş olduğunu söyleyebiliriz. Hatalı konfigürasyondan dolayı uzak masaüstü bağlantısını parolasız olarak başarılı bir şekilde kurduk.

Şimdi Windows versiyonunu öğrenmek için PowerShell'de **`Get-ComputerInfo | Select-Object WindowsVersion`** komutunu çalıştıralım.



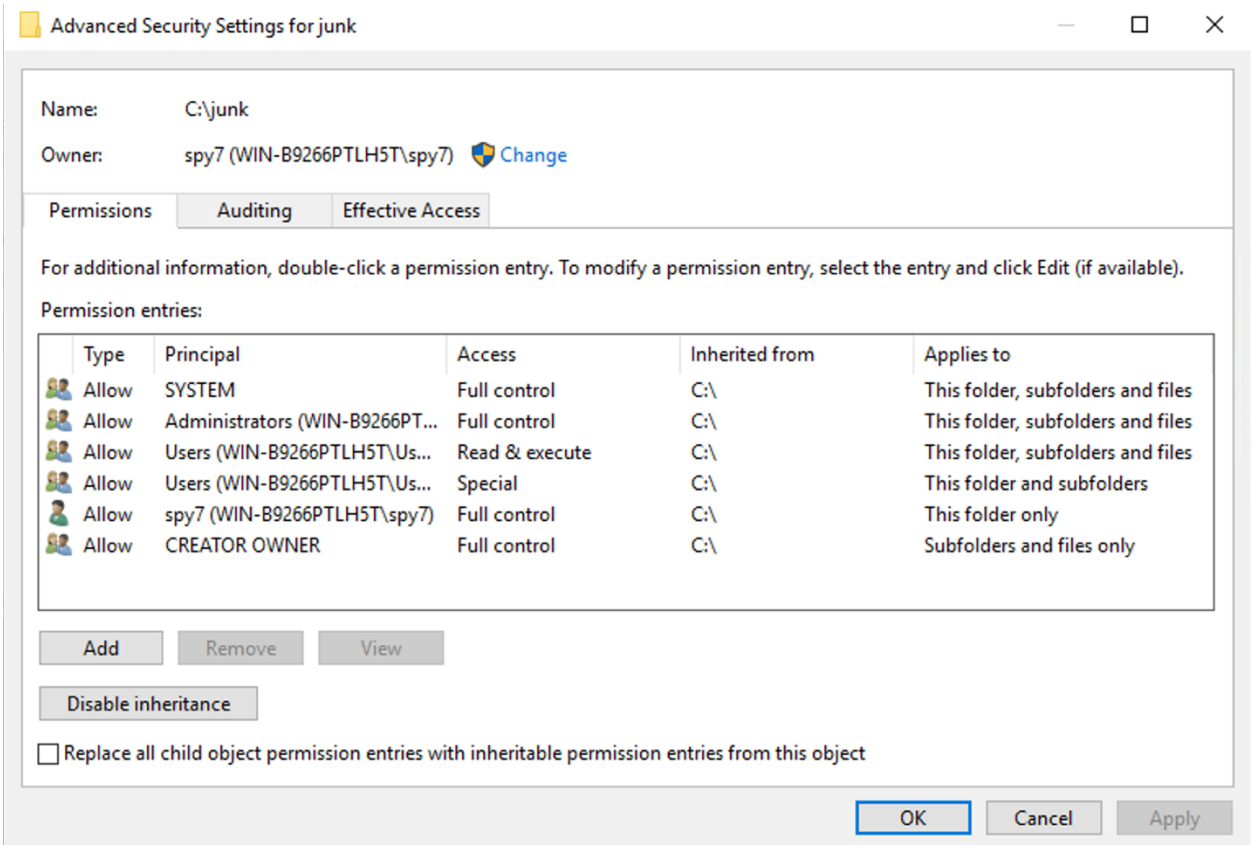
Görev 5
C dizini altındaki dosya ve klasörleri kontrol edelim.



Listeye baktığımızda **`junk`** klasörü şüpheli gözüküyor.

Görev 6

Bu klasörün sahibi olan kullanıcıyı tespit etmek için Properties -> Security -> Advanced yolunu izliyoruz.



Yukarıda da görüldüğü gibi klasörün sahibi **spy7** kullanıcısıdır.

💪 Şüpheli klasörün sahibi olan kullanıcıyı tespit ettik.

-

Tebrikler 🙌

✨ Bu alıştırmadaki tüm görevleri başarıyla tamamladınız.