

007WRITE-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.

```
(root@kali)-[/tmp]
# nmap -A -Pn 172.20.46.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-26 17:45 +03
Nmap scan report for 172.20.46.136
Host is up (0.081s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-B9266PTLH5T
| Not valid before: 2024-11-25T22:44:52
|_ Not valid after: 2025-05-27T22:44:52
|_ ssl-date: 2024-11-26T22:46:49+00:00; +8h00m00s from scanner time.
|_ rdp-ntlm-info:
|_ Target Name: WIN-B9266PTLH5T
```

Cevap: WIN-B9266PTLH5T

SORU 2: RDP'nin açılımı nedir?

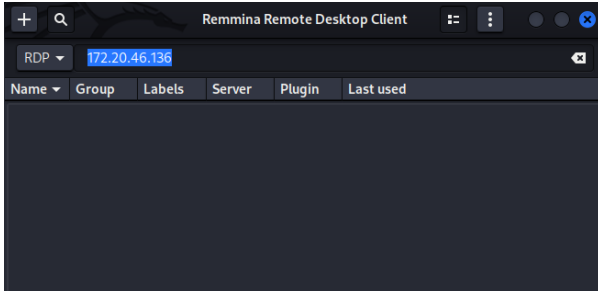
Remote Desktop Protocol

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

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

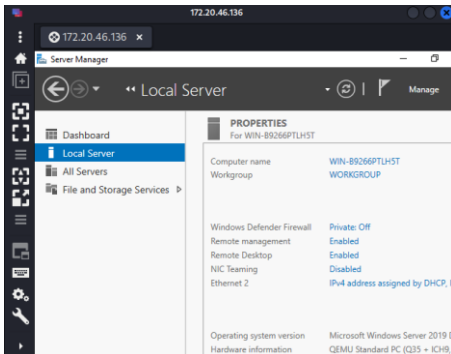
SORU 4: Windows versiyonu nedir?

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.

```
PS C:\Users\Administrator> Get-ComputerInfo | Select-Object WindowsVersion
WindowsVersion
-----
1809
```

Cevap: 1809

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

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

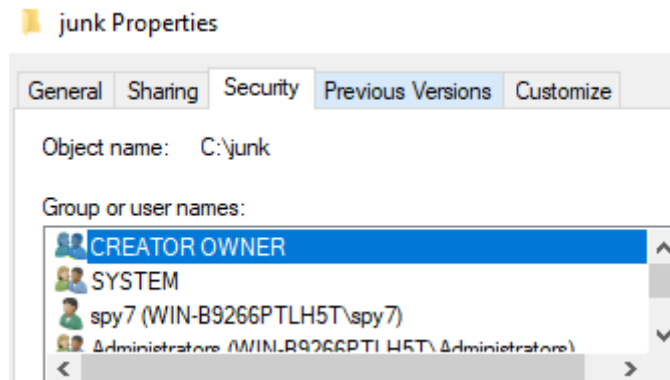
```
PS C:\> dir

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          1/3/2024   8:05 AM             junk
d-----          11/5/2022   11:21 AM             PerfLogs
```

Cevap: JUNK

SORU 6: Which user owns the junk folder?



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