

CARNIVAL ISINMASI

INFO: SMB (Server Message Block) protokolü, bir ağ üzerindeki bilgisayarların dosya, yazıcı ve diğer kaynakları paylaşımlarını sağlayan bir iletişim protokolüdür. SMB ile ilgili temel alıştırmalar yapmak için önerilir.

1. Genellikle 445 portunu kullanan SMB servisinin açılımı nedir?

Bilgi: SMB (Server Message Block), bir ağ iletişim protokolüdür. Özellikle dosya paylaşımı, yazıcı paylaşımı ve diğer kaynak erişim işlemleri için kullanılır. SMB, Windows işletim sistemleri ve diğer birçok ağ cihazı tarafından desteklenir. 445 numaralı port genellikle SMB trafiklerinin iletimi için kullanılır ve SMB protokolünün modern sürümleri genellikle bu port üzerinden iletişim kurar.

2. "Looks interesting" yorumunu içeren paylaşılan klasörün adı nedir?

Bilgi: Öncelikle nmap taraması yapılır ve açık portlar bulunur. Ardından SMB protokolünün açık olduğu keşfedilir. Ardından SMB bağlantısı kurularak istenilen şeye ulaşılmaya çalışılır.

Kullanımı: Öncelikle nmap atılır. Nmap <ip-adresi> .Linux sisteminde, SMB paylaşımına bağlanmak için smbclient aracını kullanabiliriz.

```
[root@hackerbox]# nmap 172.20.3.162
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-01 13:25 CDT
Nmap scan report for 172.20.3.162
Host is up (0.0010s latency).
Not shown: 996 closed tcp ports (reset)
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:EF:B9:9A (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 15.59 seconds
```

```
[root@hackerbox]# smbclient --no-pass -L 172.20.3.52

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

smbclient --no-pass -L <sunucu_adi_veya_IP_adresi>

- smbclient: SMB paylaşımına bağlanmak için kullanılan komuttur.
- --no-pass: Bu seçenek, bağlantı sırasında şifre girilmesini istemediğinizi belirtir. Yani, komut çalıştırıldığında şifre girmeniz gerekmez. Bu genellikle, anonim (şifresiz) erişim için kullanılır.
- -L <sunucu_adi_veya_IP_adresi>: Bu seçenek, belirtilen SMB sunucusunun paylaşımlarını listelemek için kullanılır. Sunucu adı veya IP adresini belirtmeniz gerekir. Bu komut, sunucuda mevcut olan tüm paylaşımların listesini döndürür.

Görüldüğü üzere klasörün adı "projects"dir.

3. SMB bağlantısından sonra hangi komutları çalıştırabileceğimizi gösteren yardımcı komut nedir?

Bilgi: SMB bağlantısından sonra kullanabileceğiniz komutların listesini görmek için smbclient komutunun yardım seçeneği kullanılır.

Kullanımı:

```
[*]-[root@hackerbox]-[~]
#smbclient --no-pass '\\172.20.3.52\projects
Try "help" to get a list of possible commands.
smb: \> help
?               allinfo          altname          archive          backup
blocksize       cancel           case_sensitive   cd               chmod
chown           close           del              deltrees         dir
du              echo            exit             get              getfacl
geteas          hardlink        help             history          iosize
lcd             link            lock             lowercase        ls
l               mask            md               mget             mkdir
more            mput            newer            notify           open
posix           posix_encrypt   posix_open       posix_mkdir      posix_rmdir
posix_unlink    posix_whoami    print            prompt           put
pwd             q               queue            quit             readlink
rd              recurse         reget            rename           reput
rm              rmdir           showacls         setea            setmode
scopy           stat            symlink          tar              tarmode
timeout         translate       unlock           volume           vuid
wdel            logon           listconnect     showconnect      tcon
tdis            tid             utimes          logoff           ..
!
smb: \>
```

Görüldüğü üzere kullanılan komut "help" komutudur.

4. Projenin ismi nedir?

Bilgi: l komutu, smbclient aracıyla SMB paylaşımlarına bağlandığınızda dosya ve klasörleri listelemek için kullanılan bir komuttur. Ancak, smbclient'in yardım seçeneklerinde l komutuna doğrudan bir referans bulamayabilirsiniz. Bu durumda, bazı kaynaklarda ls komutu yerine l olarak kısaltmalar kullanılabilir.

Kullanımı:

```
smb: \> l
.                  D          0   Thu Jan  4 05:56:44 2024
.                  D          0   Thu Jan  4 05:56:44 2024
Bird               D          0   Thu Jan  4 05:57:38 2024
10344703 blocks of size 4096. 7834531 blocks available
smb: \>
```

Görüldüğü üzere proje adı "bird"dir.

5. .config dosyası içindeki bağlantı şifresi nedir?

Bilgi: Dosya listesi görüntülenerek, istenilen dosya seçilir ve okunur.

Kullanımı: smb: \> ls : dosyaları listelemek için , smb: \> get .config : dosyanın içeriğini görmek için

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

Görüldüğü üzere bağlantı şifresi ekran görüntüsünde bulunmaktadır.

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser'in Carnival ısınmasını başarıyla tamamladı