Carnival Write-up

Giriş

Carnival ısınma makinesi, Server Message Block (SMB) protokolü ile ilgili pratik yapmak ideal bir başlangıç noktasıdır. Bu makinede, SMB servisinin güvenlik açıklarını nasıl tespit edebileceğinizi ve bu açıkların üzerinden nasıl ilerleyebileceğinizi öğreneceksiniz. Ayrıca, SMB'nin temel prensipleri ve ağ üzerindeki etkileşimleri hakkında bilgi edineceksiniz. Bu alıştırma, SMB protokolünün güvenliğine dair bilginizi artırmanıza yardımcı olacaktır.

Server Message Block (SMB)

SMB protokolü, ağ üzerindeki cihazlar arasında dosya, yazıcı ve diğer kaynakların paylaşılmasını sağlayan bir ağ dosya paylaşım protokolüdür. Başlangıçta IBM tarafından geliştirilmiş olan bu protokol, Microsoft tarafından Windows işletim sistemlerinde geniş çaplı kullanım için benimsenmiştir. SMB, kullanıcıların farklı bilgisayarlardaki dosyalara erişimini, bunları açıp düzenlemesini ve ağ üzerindeki yazıcıları kullanmasını mümkün kılar.

SMB'nin temel işlevi, bir ağdaki cihazların dosya ve kaynak paylaşımını kolaylaştırmaktır. Örneğin, bir ofis ortamında, çalışanlar farklı bilgisayarlardan merkezi bir sunucuda depolanan dosyalara erişebilir.

Ancak, SMB protokolü bazı güvenlik zafiyetlerine sahip olabilir. Özellikle, eski sürümleri güvenlik açıkları içerir ve siber saldırılara açık olabilir.

SMB protokolü üzerinden paylaşılan kaynaklara **`anonim erişim`**, misafir erişimi, kimlik doğrulamalı erişim gibi çeşitli erişim türleri vardır. Anonim erişim, kimlik doğrulaması yapılmadan paylaşılan kaynaklara erişim sağlamak anlamına gelir.

SMB protokolünde karşılaşılan bazı yaygın paylaşım adları; C$, D$, ADMIN$, IPC$.

C$

Windows işletim sistemlerinde bulunan ve sistem yöneticilerine ayrıcalıklı erişim sağlayan gizli bir ağ paylaşımıdır. C sürücüsünün kök dizinine erişim sağlar.

D$
Windows'ta sistem yöneticilerine yönelik gizli bir paylaşımdır ve bu paylaşım D sürücüsünün kök dizinine erişim sağlar.

ADMIN$
Windows işletim sistemlerinde, sistem yönetim amaçlı kullanılan bir gizli ağ paylaşımıdır. Genellikle, Windows'un kurulum dizini olan %WINDIR% (örneğin, C:\Windows) dizinine erişimi sağlar.

IPC$
"Inter-Process Communication Share" anlamına gelir ve Windows işletim sistemlerinde işlemler arası iletişim için kullanılır. Bu paylaşım, ağ üzerinden anonim oturum bilgileri ve diğer geçici ağ işlemleri için kullanılır, dosya veya dizin erişimi sağlamaz.

PRINT$
Yazıcı sürücülerinin ve yazıcıların yapılandırma dosyalarının saklandığı ve yönetildiği özel bir ağ paylaşımıdır, bu sayede ağ üzerinden yazıcılara erişim ve onların yönetimi kolaylaştırılır.

Bilgi Toplama

Hedef makinemiz üzerinde port taraması yaparak bilgi toplamaya başlayalım.

```
root💀hackerbox:~# nmap 172.20.2.94
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-06 11:57 CST
Nmap scan report for 172.20.2.94
Host is up (0.00055s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 52:54:00:A3:71:B1 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds
```

Görev 1
Yukarıdaki açık portlar içerisinde de görüldüğü üzere 445 portunda **`SMB (Server Message Block)`** servisi çalışıyor.

Sisteme Erişim

Hedef makinede çalışan SMB servisi üzerinden kaynaklara erişmeyi deneyelim.

Görev 2

Bu görevi tamamlayabilmek için SMB servisi üzerinden paylaşılan dosya ve klasörleri listelememiz gerekiyor. Bunun için **`smbclient`** aracını kullanabiliriz.

smbclient

Sunuculardaki SMB kaynaklarına erişmek için kullanılan FTP benzeri bir istemcidir.

```
smbclient [options] <netbios-name|ip-address>
```

```
--no-pass : Parola gerektirmeyen bir kaynağa erişirken kullanılmalıdır. Bu parametre belirtilmezse istemci tarafından parola istenecektir.

-L : Bu seçenek, bir sunucuda hangi kaynakların mevcut olduğunu listeler.
```

```
root💀hackerbox:~# smbclient --no-pass -L 172.20.2.94

 Sharename       Type      Comment
 ─────────       ────      ───────
 ADMIN$          Disk      Remote Admin
 C$              Disk      Default share
 IPC$            IPC       Remote IPC
 Projects        Disk      Looks Interesting
 Users           Disk
SMB1 disabled -- no workgroup available
```

Yukarıdaki komut çıktısında da görüldüğü üzere “Looks Interesting” yorumunu içeren kaynağın adı **`Projects`** dir.

Görev 3
Parolasız bir şekilde SMB kaynağına ya da servisine bağlanmak için aşağıdaki komut dizesi kullanılabilir.

```
smbclient -no-pass \\\\<netbios-name|ip-address>\\<sharename>
```

```
root💀hackerbox:~# smbclient --no-pass \\\\172.20.2.94\\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            deltree        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         ..
!
```

Yukarıdaki gibi bir kaynağa bağlandıktan sonra **`help`** komutu ile çalıştırabileceğimiz komutlar ile ilgili bilgi alabiliriz.

Görev 4
Projects kaynağındaki dosya ve klasörleri listelemek için **`l`** komutunu kullanabiliriz.

```
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. 7466576 blocks available
```

Görev 5

```
smb: \> cd Bird
smb: \Bird\> l
  .                                   D        0  Thu Jan  4 05:57:38 2024
  ..                                  D        0  Thu Jan  4 05:57:38 2024
  .config                             A       79  Thu Jan  4 05:53:22 2024
  Abp.sln                             A    49780  Thu Jan  4 05:53:23 2024
  appveyor.yml                        A      148  Thu Jan  4 05:53:22 2024
  build                               D        0  Thu Jan  4 05:53:23 2024
  global.json                         A       76  Thu Jan  4 05:53:23 2024
  NuGet.Config                        A       75  Thu Jan  4 05:53:22 2024
  nupkg                               D        0  Thu Jan  4 05:53:22 2024
  src                                 D        0  Thu Jan  4 05:57:48 2024

  10344703 blocks of size 4096. 7466576 blocks available
smb: \Bird\> more .config
CONNECTION_USER=hackviser
CONNECTION_PASS=5afcb573-d71e-490f-841a-accab64082c2
```

💪 Bağlantı parolasını bulduk.

-

Tebrikler 🙌

✨ Bu alıştırmadaki tüm görevleri başarıyla tamamladınız.