Carnival Write-up

Introduction

The Carnival warmup machine is an ideal starting point for practicing with the Server Message Block (SMB) protocol. On this machine, you will learn how to identify vulnerabilities of the SMB service and how to work around them. You will also learn about the basic principles of SMB and its interactions on the network. This exercise will help you increase your knowledge of the security of the SMB protocol.

Server Message Block (SMB)

The SMB protocol is a network file sharing protocol that allows files, printers and other resources to be shared between devices on a network. Originally developed by IBM, it was adopted by Microsoft for widespread use on Windows operating systems. SMB makes it possible for users to access, open and edit files on different computers and use printers on the network.

The main function of SMB is to facilitate file and resource sharing between devices on a network. For example, in an office environment, employees can access files stored on a central server from different computers.

However, the SMB protocol can have some security vulnerabilities. In particular, older versions contain vulnerabilities and may be susceptible to cyber-attacks.

There are various types of access to shared resources over the SMB protocol, such as anonymous access, guest access, authenticated access. Anonymous access means accessing shared resources without authentication.

Some common sharenames encountered in the SMB protocol are C$, D$, ADMIN$, IPC$.

C$

It is a hidden network share in Windows operating systems that gives privileged access to system administrators. It provides access to the root directory of the C drive.

D$
It is a hidden share for system administrators in Windows that gives access to the root directory of drive D.

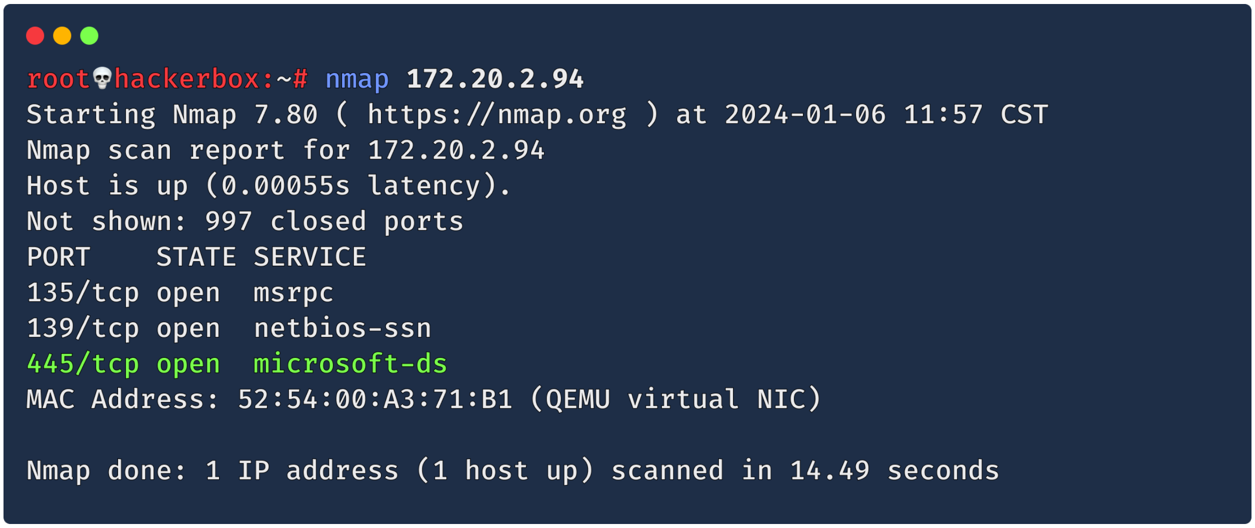
ADMIN$
On Windows operating systems, it is a hidden network share used for system administration purposes. It usually provides access to the %WINDIR% (for example, C:\Windows) directory, which is the installation directory of Windows.

IPC$
It stands for "Inter-Process Communication Share" and is used for inter-process communication in Windows operating systems. This share is used for anonymous logins and other temporary network operations over the network and does not provide file or directory access.

PRINT$
It is a private network share where printer drivers and printer configuration files are stored and managed, making it easy to access and manage printers over the network.

Information Gathering

Let's run a port scan on our target machine



```
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
```

Task 1
As can be seen in the open ports above, `SMB (Server Message Block)` service is running on port 445.

System Access

Let's try to access resources through the SMB service running on the target machine.

Task 2

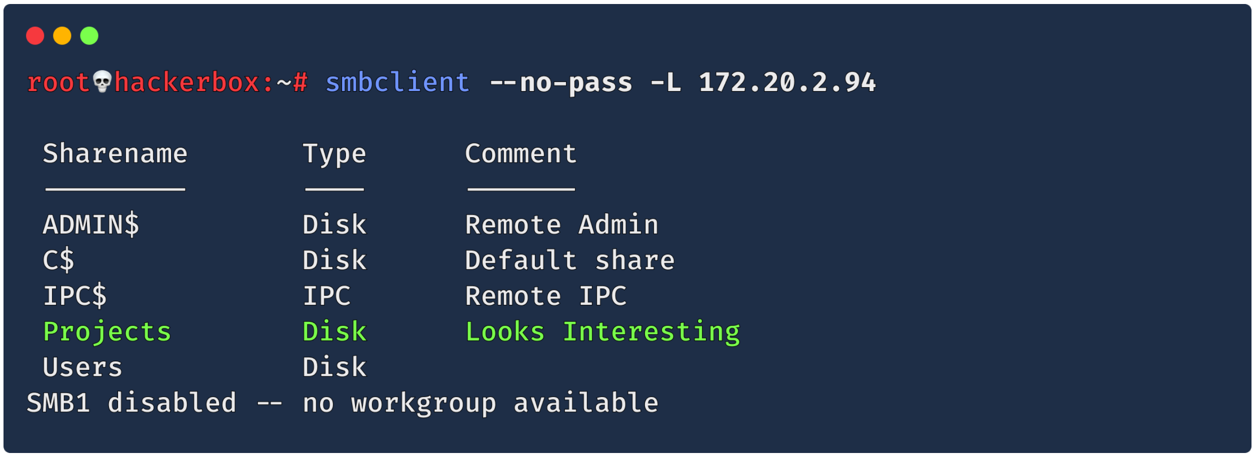
To complete this task, we need to list the files and folders shared via the SMB service. For this we can use the **`smbclient`** tool.

smbclient

It is an FTP-like client used to access SMB resources on servers.

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

```
--no-pass : Should be used when accessing a resource that does not require
a password. If this parameter is not specified, the client will ask for a
password.

-L : This option lists which resources are available on a server.
```



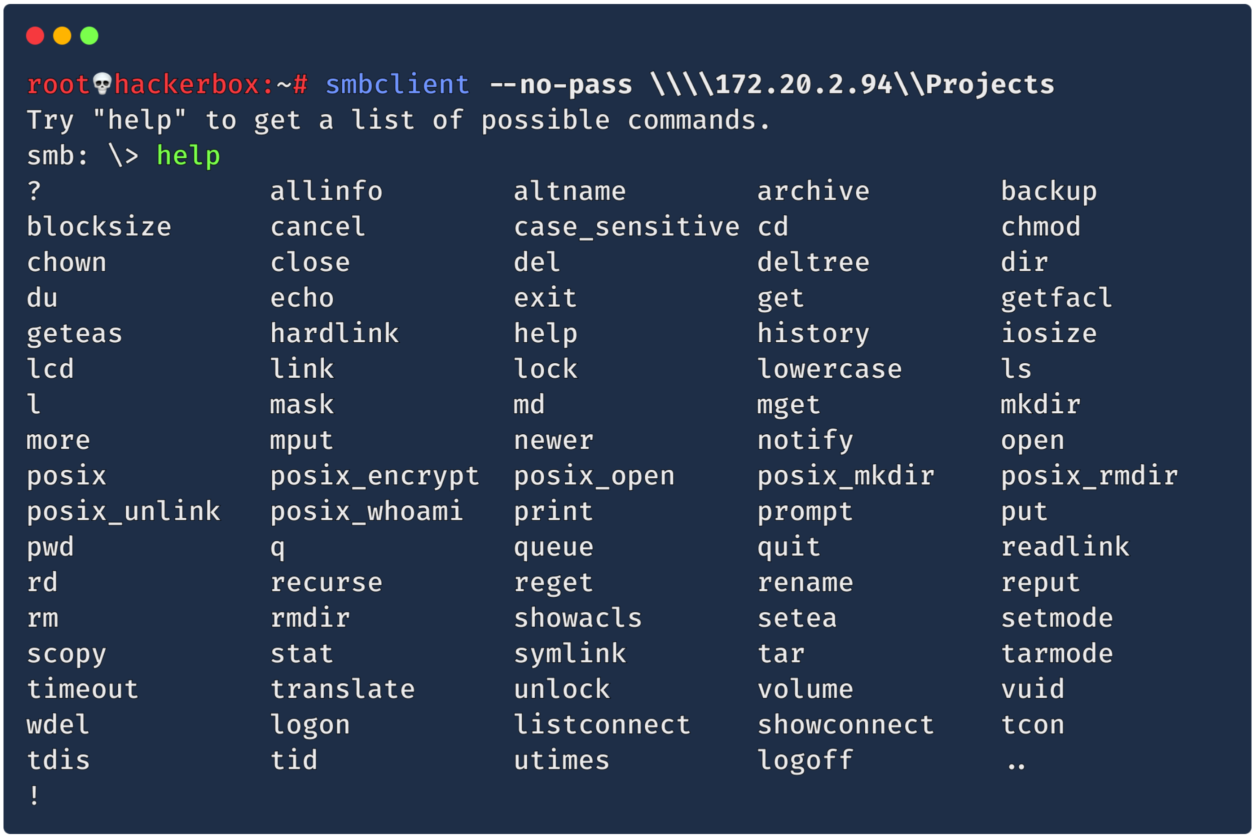
```
root💀hackerbox:~# smbclient --no-pass -L 172.20.2.94

  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
```

As can be seen in the command output above, the name of the resource containing the comment "Looks Interesting" is **`Projects`**.

Task 3

The following command string can be used to connect to an SMB resource or service without a password.

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

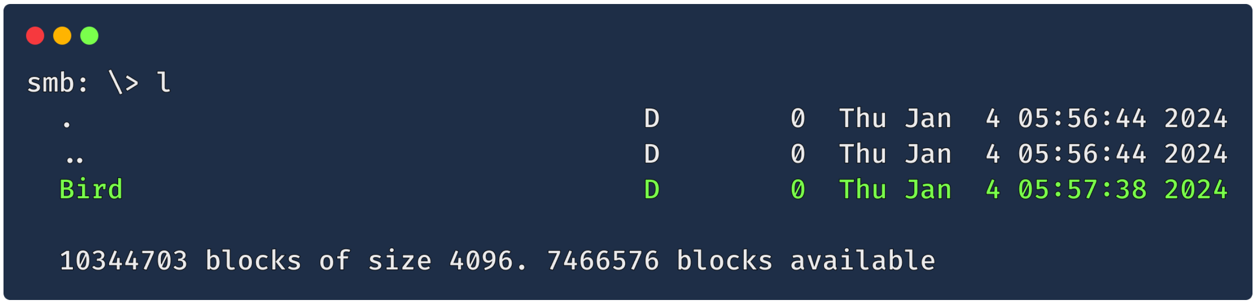


```
root💀hackerbox:~# smbclient --no-pass \\\\172.20.2.94\\Projects
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            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         ..
!
```

After connecting to a source as above, we can get information about the commands we can run with the **help** command.

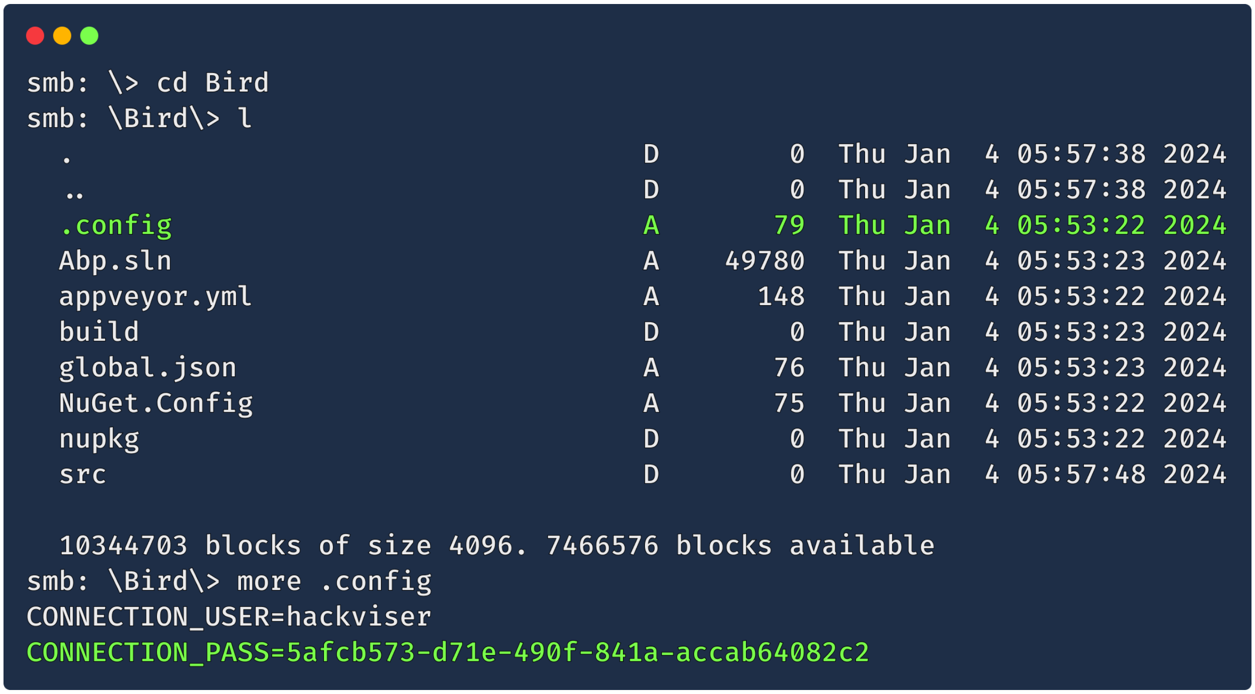
Task 4

We can use the **l** command to list the files and folders in the Projects resource.



```
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
```

Task 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
```

💪 We found the connection password.

-

Congratulations 🙌

✨ You have successfully completed all tasks in this warmup.