**SMB – Tactic**

**Target: 10.129.86.5**

**What I Was Trying to Do**

My goal was to gain access to the target system and figure out what was exposed. I started with basic reconnaissance to map out what services were running, then moved into exploiting what I found. The whole process was pretty straightforward once I discovered the admin share didn't require authentication.

**Quick Reconnaissance — What I Ran and Found**

I started with a standard Nmap scan to see what was listening on the network.

**Commands I used:**

nmap -Pn 10.129.86.5



**What I found:**

SMB (port 445) was open and responding

The system appeared to be a Windows machine

Anonymous enumeration seemed possible

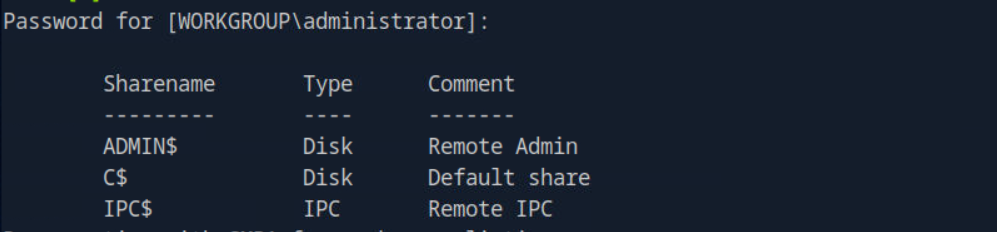
This was a good starting point. SMB often gives you a lot of information if the system is misconfigured.

**Enumerating the SMB Shares**

My next move was to see what shares were actually available on the box without any credentials. I used smbclient with the -N flag (no password) to just list what was there.

**Command I ran:**

smbclient -L //10.129.86.5 -U administrator



**What came back:**

So there were three shares visible:

* **ADMIN$** and **C$** are hidden administrative shares on Windows
* **IPC$** is for inter-process communication

The fact that these were even listed without credentials was already a red flag

**Attempting to Connect to the C$ Share**

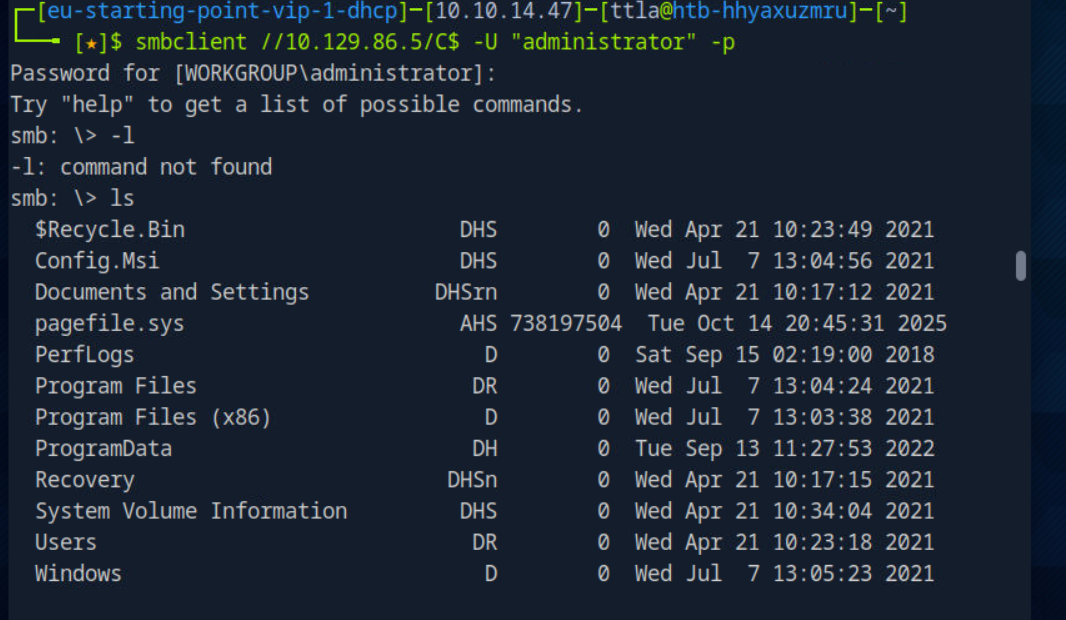
The C$ share is basically the C: drive of the Windows system, and it's normally restricted to administrators. I decided to try connecting as the "administrator" user without providing a password to see if this system had a default or null configuration.

**Command I ran:**

smbclient //10.129.86.5/C$ -U "administrator" -p

When I hit enter without typing a password, the system accepted it. No error. No "access denied." I was just... in.

I had unauthenticated access to the entire C: drive.



**Exploring the Filesystem**

Once connected to the C$ share, I had access to standard filesystem commands. I could navigate around, list directories, and download files.

**Commands available to me:**

ls # See what's in the current folder

cd [directory] # Move into subdirectories

pwd # See where I am

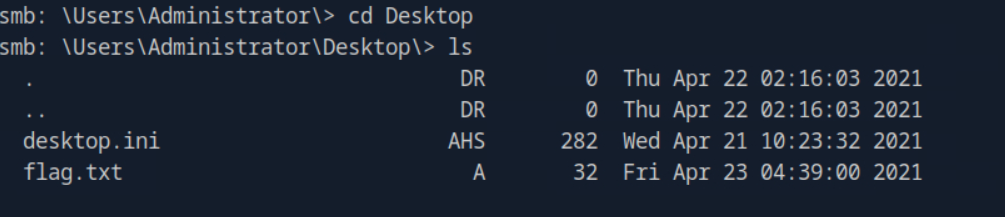
get [filename] # Download files to my machine

exit # Disconnect

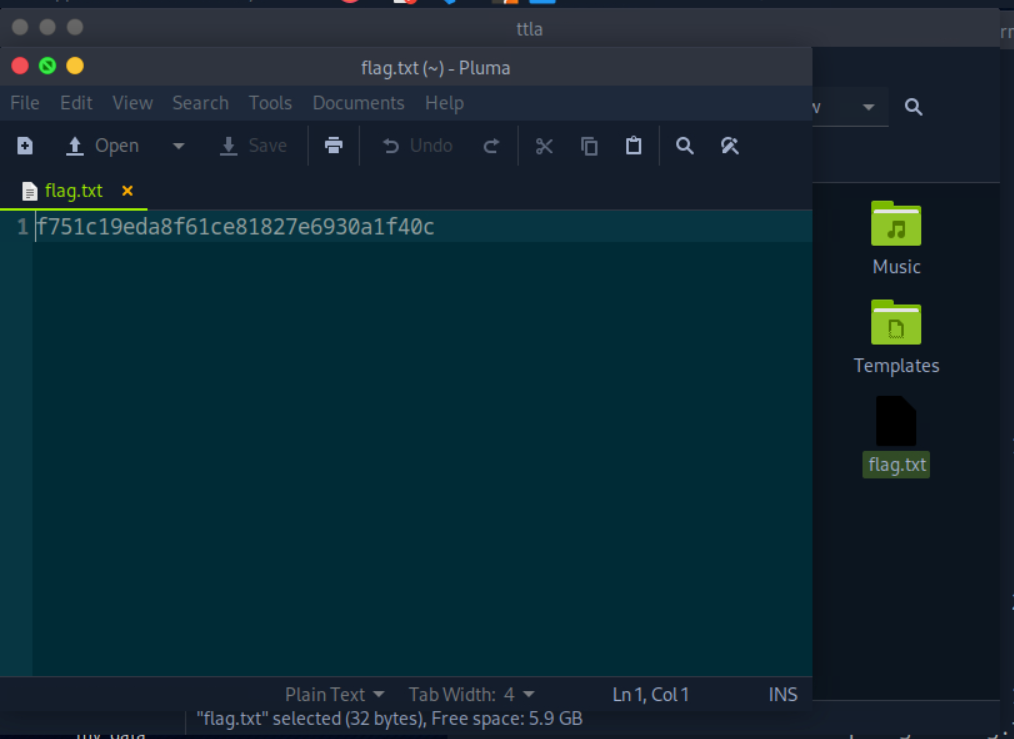
I started browsing the directory structure that appeared after connecting. From the root of C$, I could see the typical Windows folders:

* Users
* Windows
* Program Files
* System directories

The filesystem was fully accessible for reading (and potentially writing).



I then use Get method to download it:



**What This Means**

This was a serious misconfiguration. The administrator account has no password protection, and the administrative share is exposed. That means:

* Anyone who can reach port 445 can access the entire C: drive
* I can read any file stored on this system
* I can potentially write files to system locations
* User data, configuration files, and sensitive information are all exposed
* Next steps could include extracting credentials, finding flags, or establishing persistence