ATTACK DEFENSE

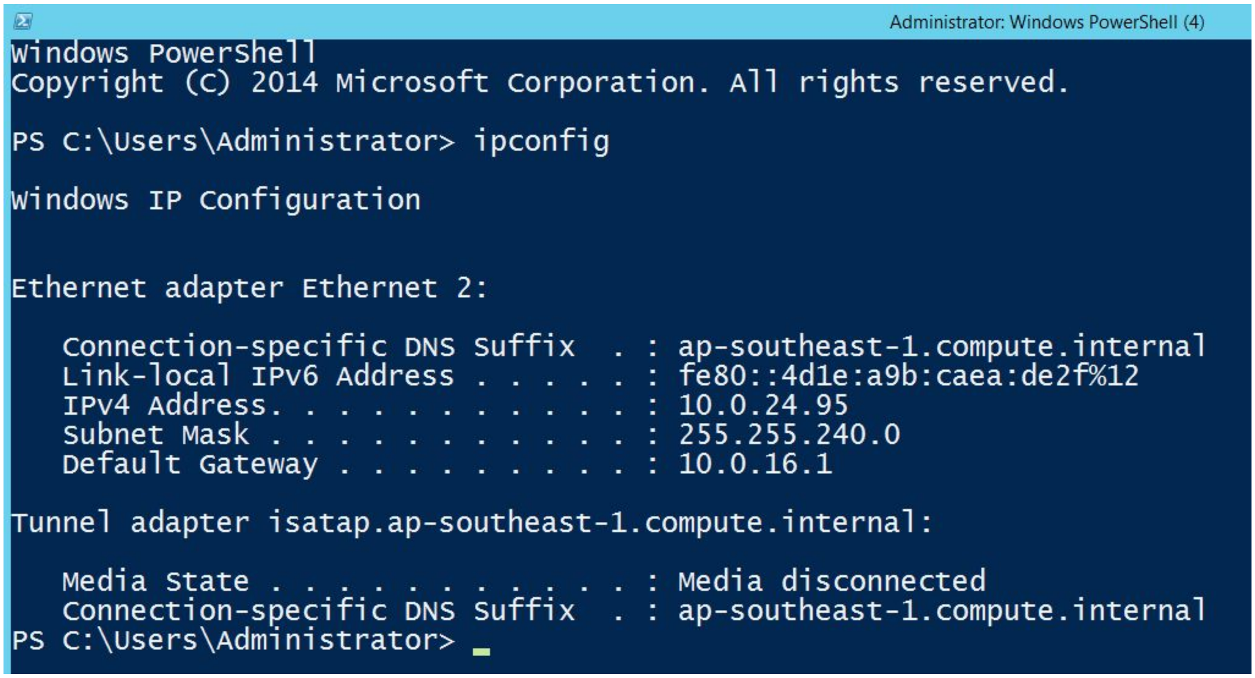
by PentesterAcademy

Name	Windows Recon: SMB: Discover and Mount
URL	https://attackdefense.com/challengedetails?cid=2220
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 IP address.

Command: ipconfig



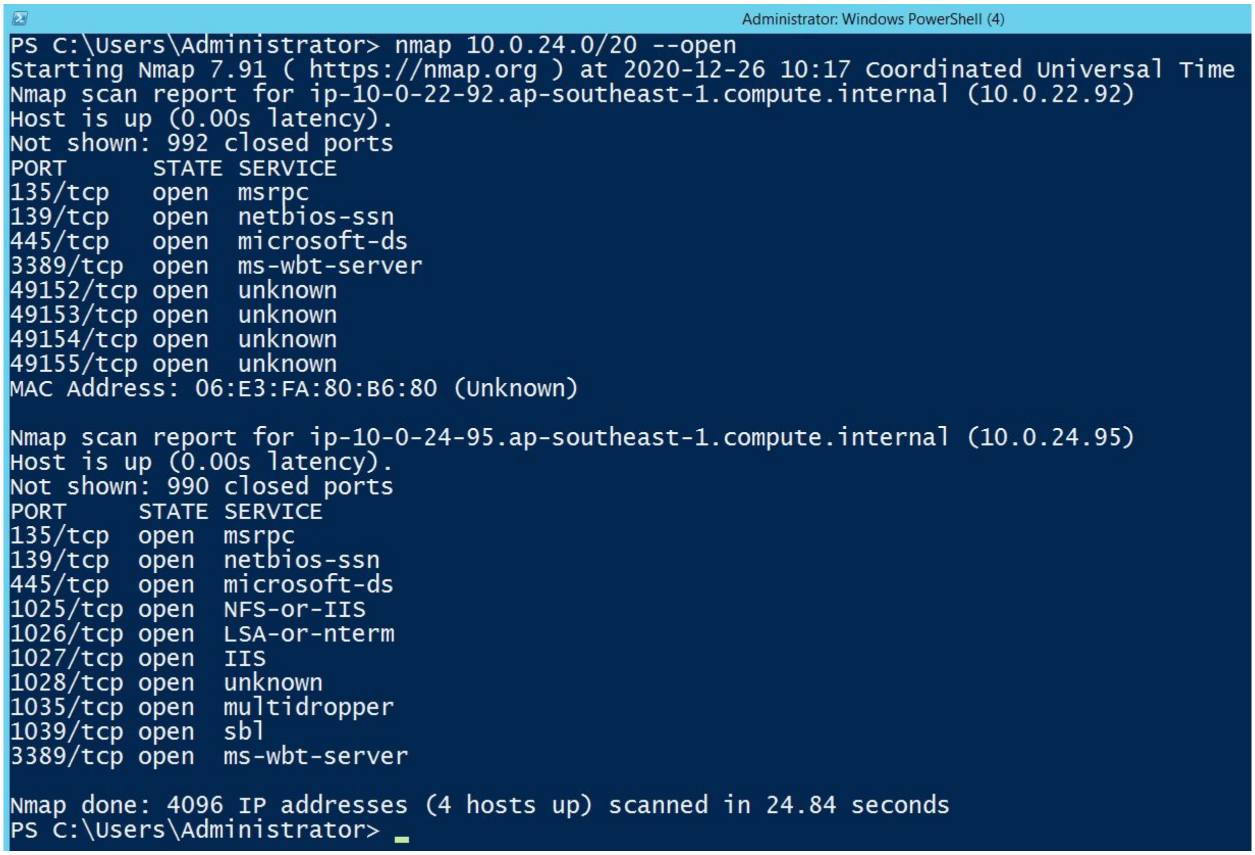
```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::4d1e:a9b:caea:de2f%12
   IPv4 Address. . . . . . . . . . . : 10.0.24.95
   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
PS C:\Users\Administrator> _
```

Step 2: Run Nmap scan against the subnet to discover the target machine’s IP address.

Command: nmap **10.0.24.0/20** --open

The target subnet is "**255.255.240.0**" hence we have mentioned CIDR to 20.

Note: Nmap '**--open**' option would show only exposed ports of the live hosts.



```
PS C:\Users\Administrator> nmap 10.0.24.0/20 --open
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-26 10:17 Coordinated Universal Time
Nmap scan report for ip-10-0-22-92.ap-southeast-1.compute.internal (10.0.22.92)
Host is up (0.00s latency).
Not shown: 992 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
MAC Address: 06:E3:FA:80:B6:80 (Unknown)

Nmap scan report for ip-10-0-24-95.ap-southeast-1.compute.internal (10.0.24.95)
Host is up (0.00s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1035/tcp open  multidropper
1039/tcp open  sbl
3389/tcp open  ms-wbt-server

Nmap done: 4096 IP addresses (4 hosts up) scanned in 24.84 seconds
PS C:\Users\Administrator> _
```

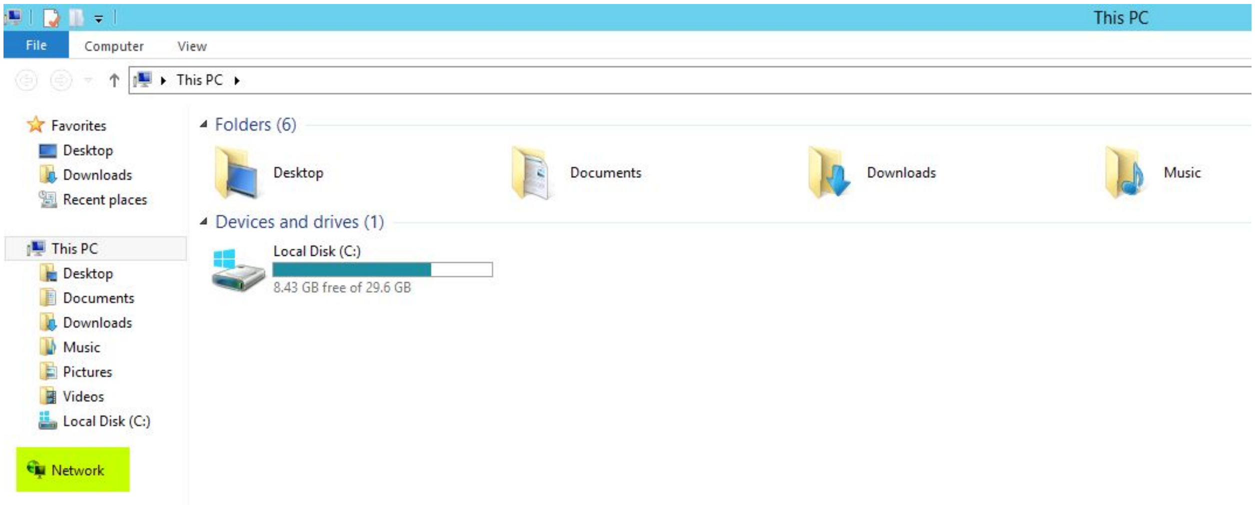
We have discovered the target machine's IP address (**10.0.22.92**) and the target machine exposed to multiple ports. SMB service port 445 is also exposed.

We have the credentials to access the target server. First, we will access SMB service using GUI. i.e administrator:smbserver_771

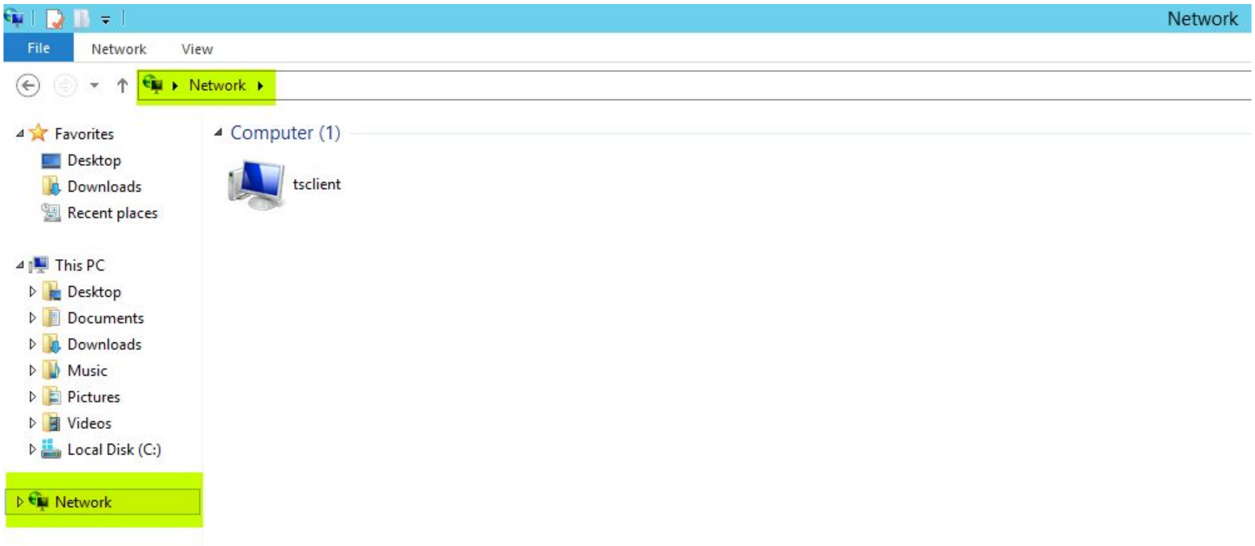
Step 3: Open "**Map Network Drive**"

Go to This PC → Network → Right Click on Network → Map Network Drive

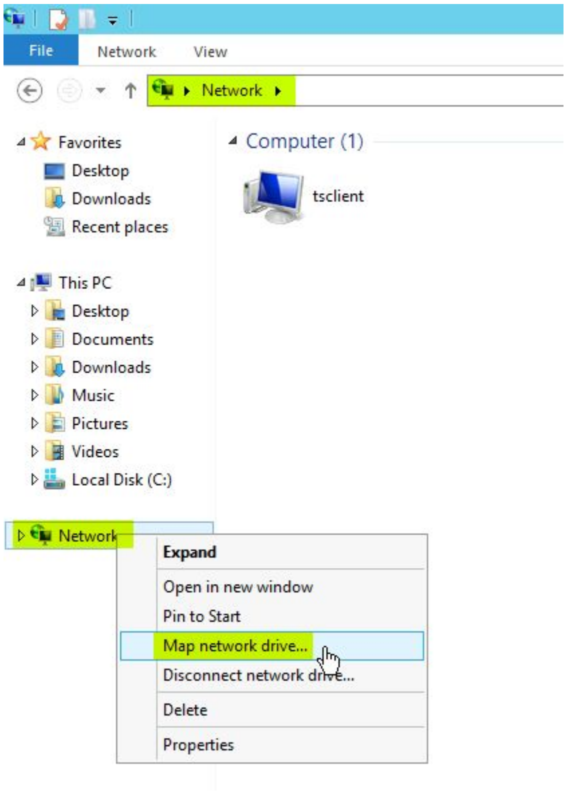
This PC

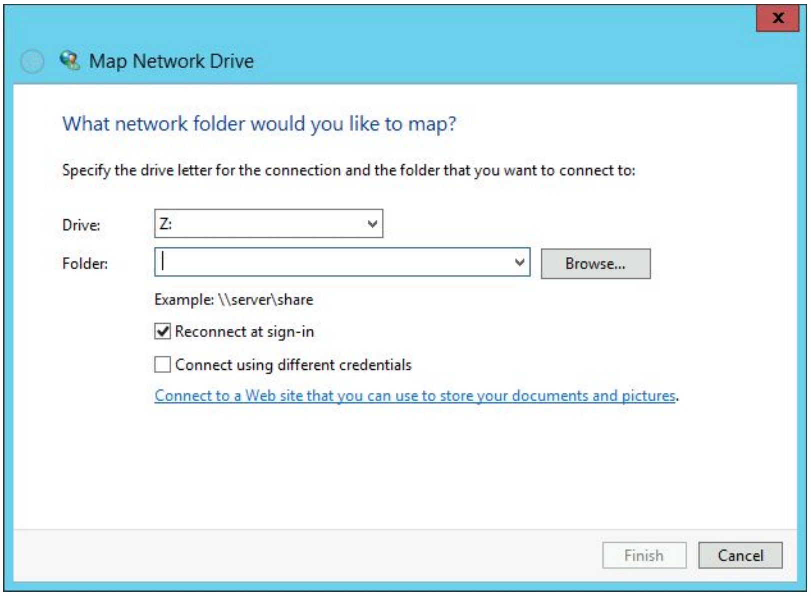


Network

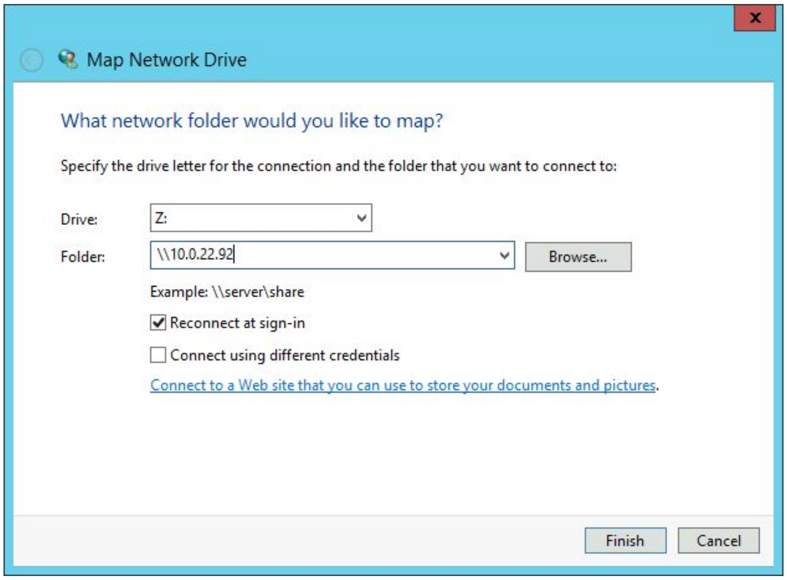


Right Click on Network and select the “**Map Network Drive**” option:




Map Network Drive
What network folder would you like to map?
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
Z:
Folder:
Browse...
Example: \\server\share
☑ Reconnect at sign-in
□ Connect using different credentials
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

Type target machine IP address “\\10.0.22.92” in **Folder:** field and hit **Browse...**



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

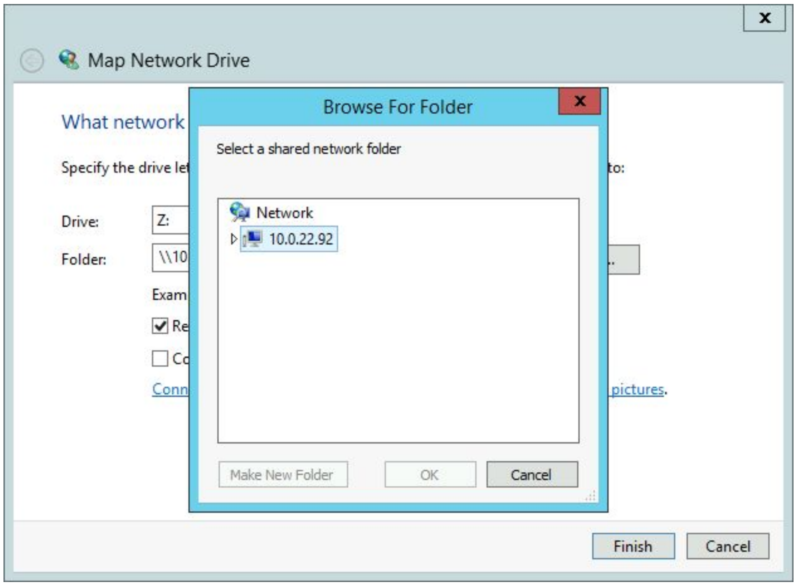
Folder: \\10.0.22.92

Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.



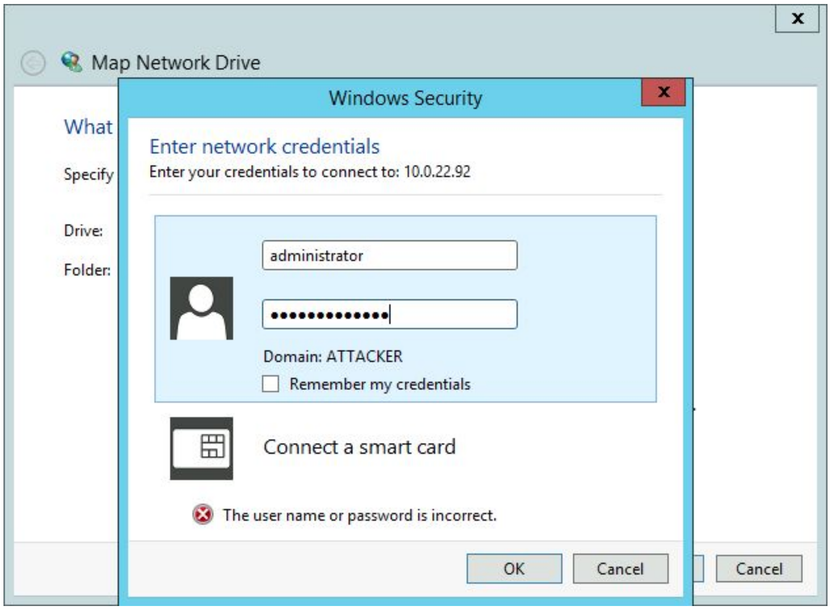
Browse For Folder

Select a shared network folder

Network
10.0.22.92

We can observe, we have discovered a network share on the machine **10.0.22.92**.

Select the target machine IP address and we would expect a network credential prompt. Here, we need to enter target machine credentials which are provided to you i.e **administrator:smbserver_771**



Windows Security

Enter network credentials

Enter your credentials to connect to: 10.0.22.92

administrator

••••••••••••••

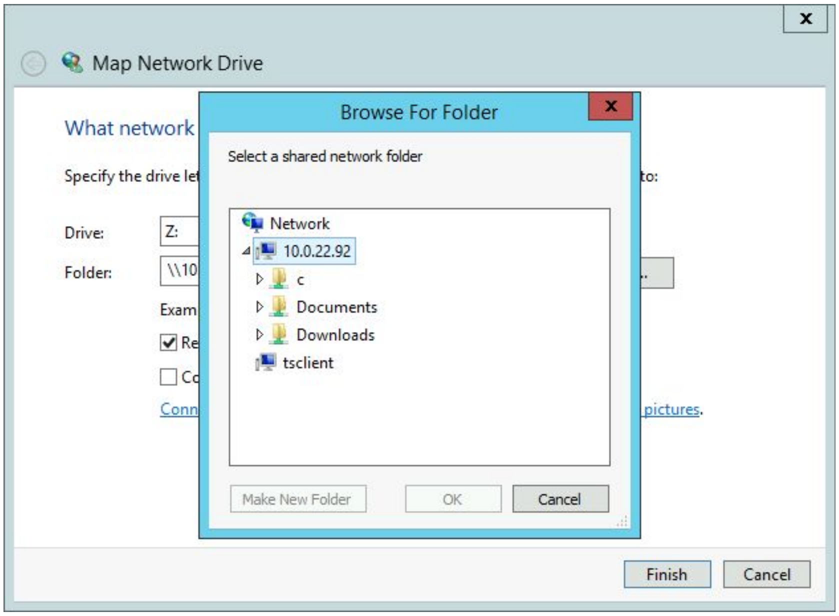
Domain: ATTACKER

□ Remember my credentials

Connect a smart card

The user name or password is incorrect.

Click “**Ok**”



Drive: Z:

Folder: \\10

☑ Re

□ Co

Browse For Folder

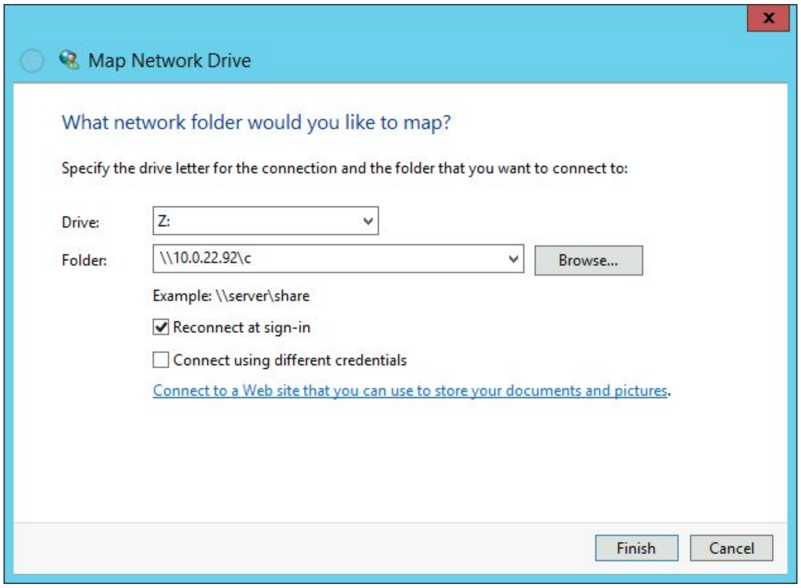
Select a shared network folder

- Network
  - 10.0.22.92
    - c
    - Documents
    - Downloads
  - tsclient

We can notice, we have received all the shared folders from the target machine.

We can select any folder to create a network drive. In this case, we are selecting the “C:\” drive of the target machine.

Select the folder and click “**Ok**” → **Finish**



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

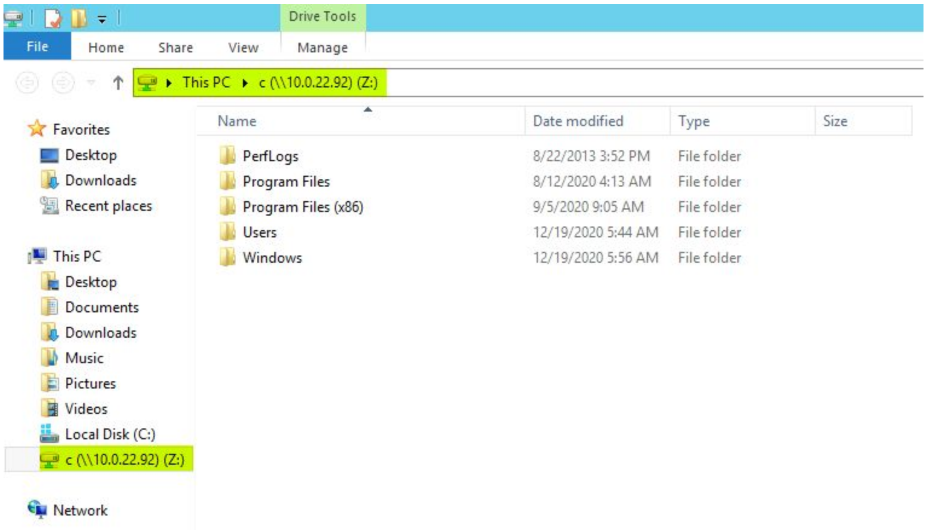
Folder: \\10.0.22.92\c

Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.



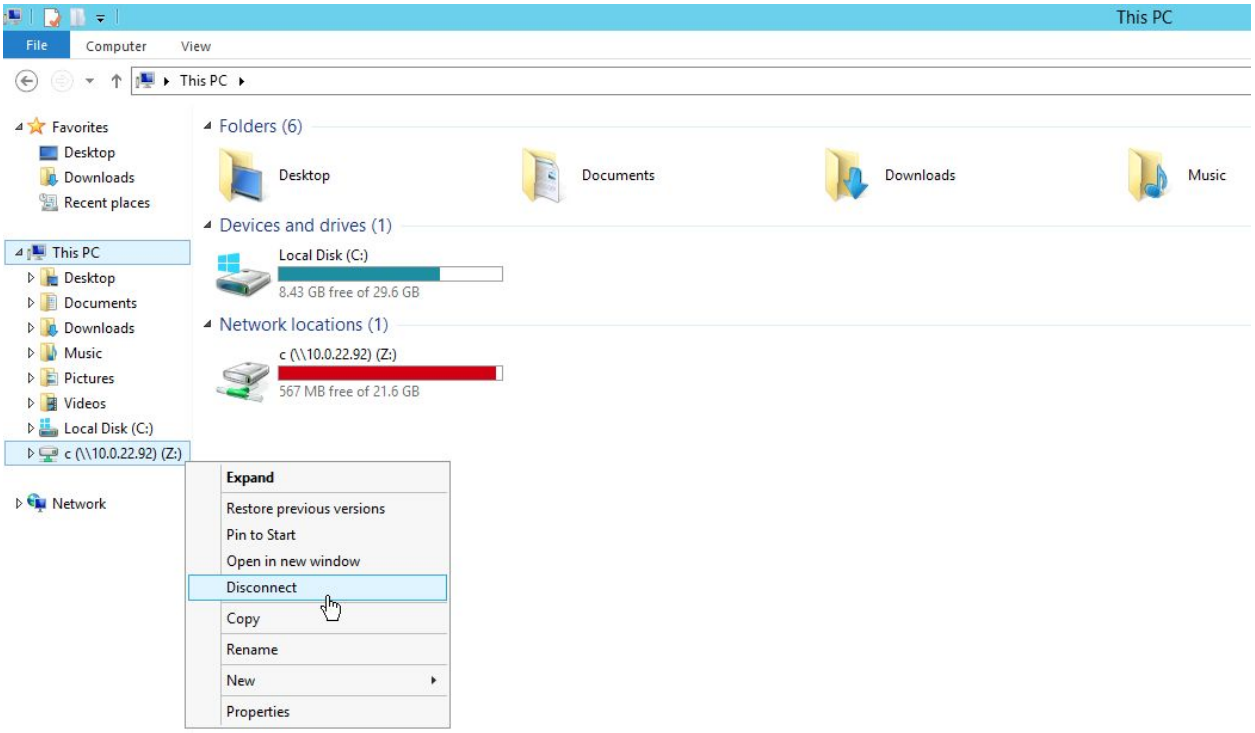
This PC ▸ c (\\10.0.22.92) (Z:)

Name	Date modified	Type	Size
PerfLogs	8/22/2013 3:52 PM	File folder	
Program Files	8/12/2020 4:13 AM	File folder	
Program Files (x86)	9/5/2020 9:05 AM	File folder	
Users	12/19/2020 5:44 AM	File folder	
Windows	12/19/2020 5:56 AM	File folder	

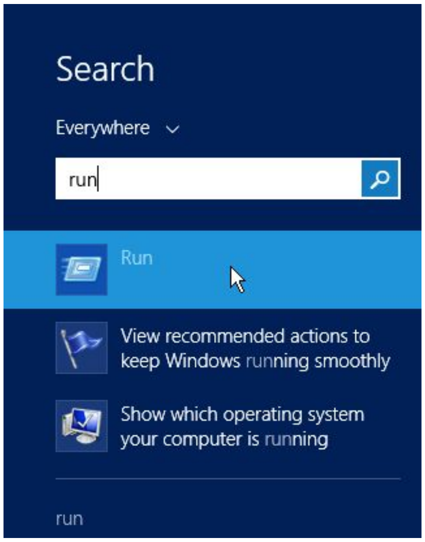
We have successfully mounted the target machine shared folders.

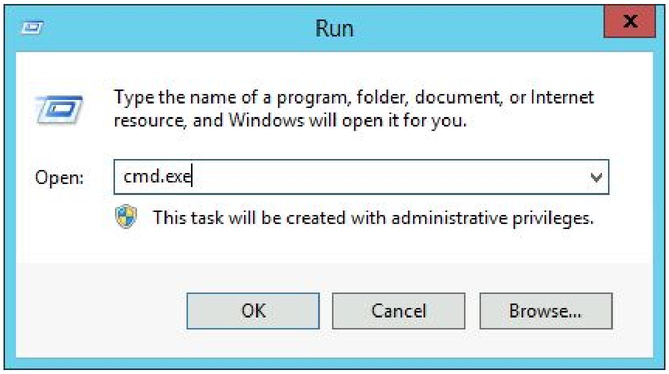
Step 4: We could also mount the drive using the Windows command prompt.

Go to “**This PC”** and disconnect the network drive.



Step 5: Open Run and type cmd.exe to access the windows command prompt.

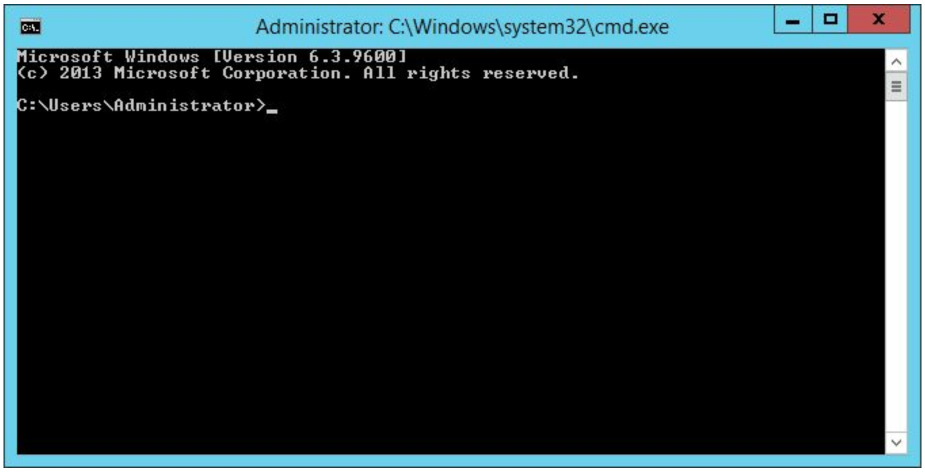

Search
Everywhere
run
Run
View recommended actions to keep Windows running smoothly
Show which operating system your computer is running
run



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd.exe

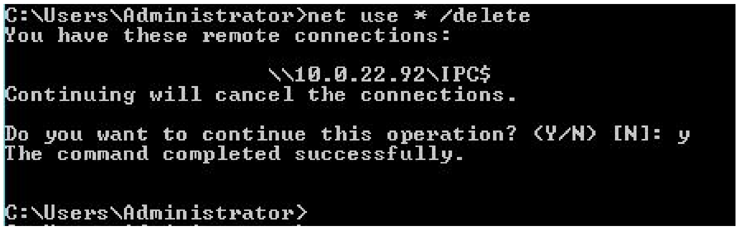
This task will be created with administrative privileges.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>_
```

Step 5: Clear the stored session.

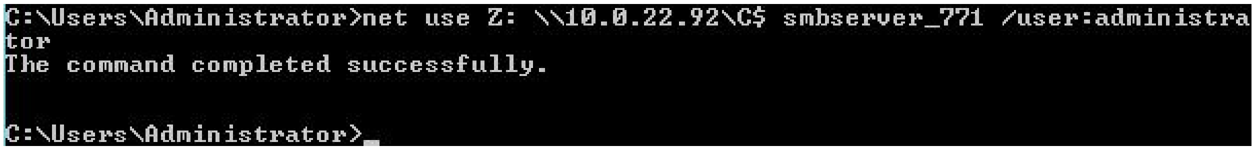
Command: net use * /delete



```
C:\Users\Administrator>net use * /delete
You have these remote connections:

                    \\10.0.22.92\IPC$
Continuing will cancel the connections.

Do you want to continue this operation? (Y/N) [N]: y
The command completed successfully.


C:\Users\Administrator>
```

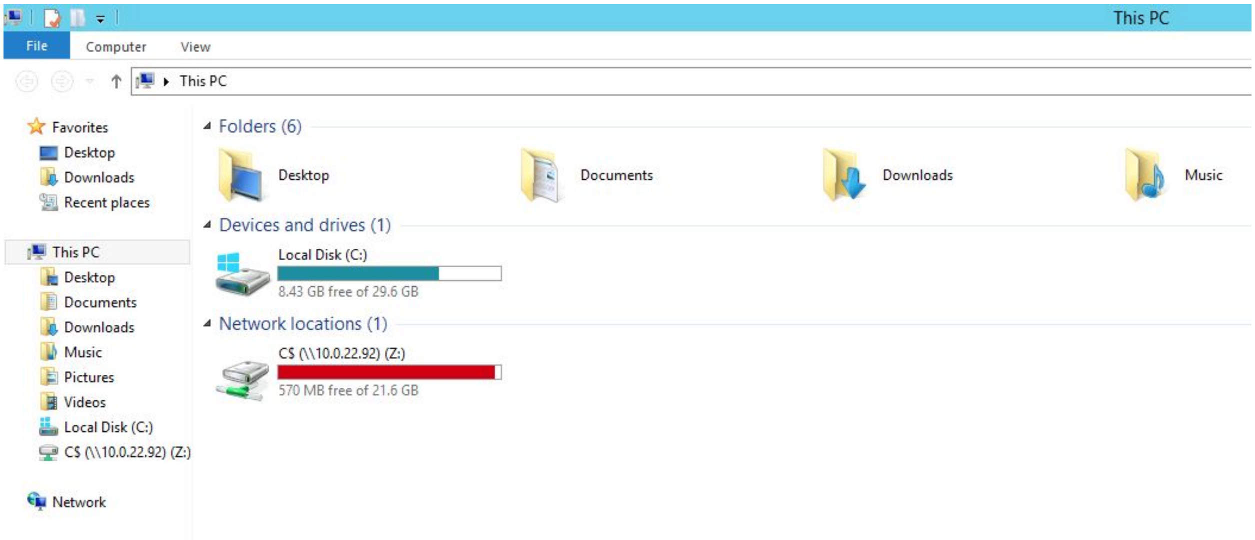
Step 6: Mount the target folder.

Command: net use Z: \\10.0.22.92\C$ smbserver_771 /user:administrator



```
C:\Users\Administrator>net use Z: \\10.0.22.92\C$ smbserver_771 /user:administra
tor
The command completed successfully.


C:\Users\Administrator>_
```

Again, visit This PC and we can notice, there is a new network shared drive i.e Z:\



We have successfully discovered a target host machine and mounted their network shared folder to the attacker machine i.e local machine.

References:

1. Microsoft SMB Protocol and CIFS Protocol Overview (https://docs.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview#:~:text=The%20Server%20Message%20Block%20(SMB,is%20a%20dialect%20of%20SMB.)