Connecting to AD CS Attacks
for Red and Blue Teams Lab

Table of Contents

Credentials and VPN Config

Please login to the lab portal (https://adcs.enterprisesecurity.io/) using your registered Google account and download the VPN config. If the email you used to purchase the lab is not connected to a Google account, please sign-up for one and share that with us.

You can either use a Web browser or OpenVPN to access the dedicated VM in the lab using the credentials below. You will find these credentials in the lab portal.

Note that **X** is your userID. If you are student41, your machine is 172.16.100.41 and your username is student41:

VPN credentials:
Username: student**X**
Password: Tdh13SheXS3PnCeC

VM credentials (to be used after connecting to the VPN):
IP: 172.16.100.**X** **Username:** certbulk\student**X**
Password: iWVUCsY36P8xUfTs

Connecting using OpenVPN - Windows setup:

1. First of all download OpenVPN from following website: https://swupdate.openvpn.org/community/releases/OpenVPN-2.5.8-I604-amd64.msi

2. Install the OpenVPN client (default options are fine).

3. After completing the installation, copy the OpenVPN config files that you got to OpenVPN directory “C:\Users\<username>\OpenVPN\config\” or “C:\Program Files\OpenVPN\config”

4. Run OpeVPN GUI as administrator. After running, you can find it in the system tray at bottom right, and click on Connect. If you have existing configurations, choose the one for this lab.

5. Enter the VPN credentials in the credential prompt. If everything is fine, you will be connected to the lab.

6. Now you can RDP to your dedicated VM 172.16.100.**X** in the lab using mstsc or any other RDP client.

Connecting using OpenVPN - Ubuntu/Kali setup:

1. Install openvpn and rdesktop on the machine using following command:

```
sudo apt-get install openvpn -y
sudo apt-get install rdesktop
```

2. Go ahead and connect to the VPN server using openvpn config files. Use it with the below command:

```
sudo openvpn --config <yourlabconfigfile>.ovpn
```

3. Use rdesktop to connect to your dedicated VM 172.16.100.**X** in the lab

```
rdesktop -d certbulk -u studentX -p iWVUCsY36P8xUfTs
172.16.100.X
```

Alternatively, You can use xfreerdp to connect with the dedicated VM -

1. Install xfreerdp package on your machine using the following command -

```
sudo apt install freerdp2-x11
```

2. Use xfreedp to connect to your dedicated VM 172.16.100.X in the lab

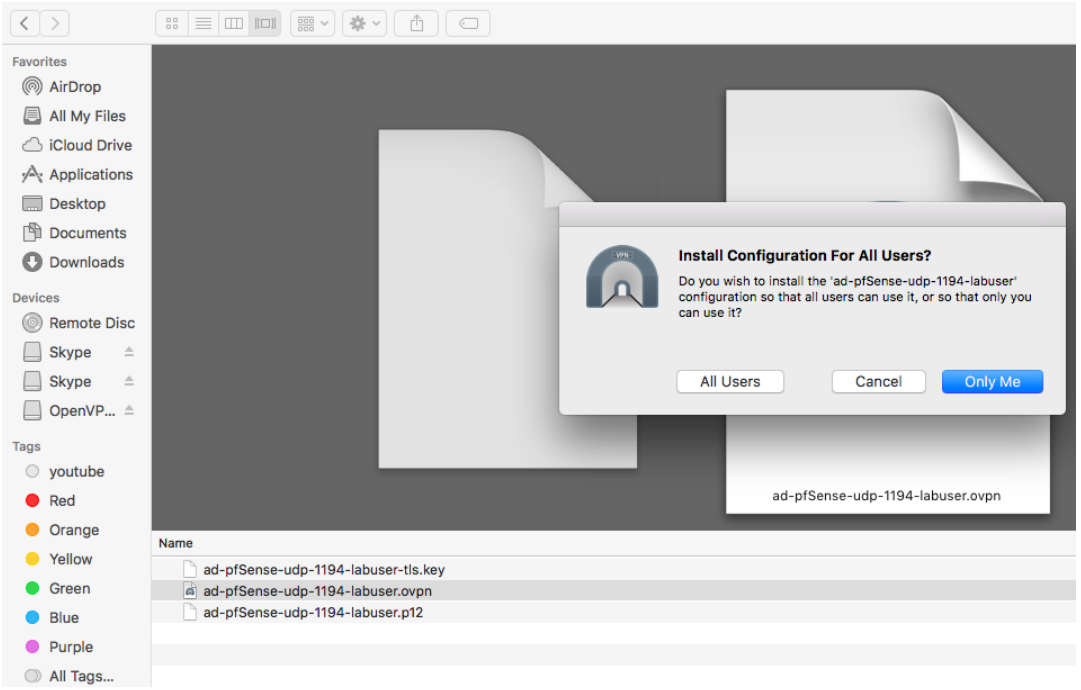
```
xfreerdp /u:'certbulk\studentX' /p:FjVxkzyGQgvYw9nk
/cert-ignore /drive:Tools,/home/user/Desktop/Tools
/v:172.16.100.X +clipboard
```

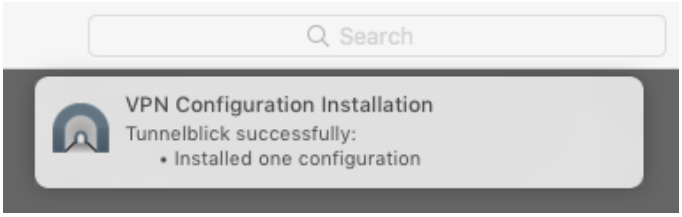
Note - Change the path “/home/user/Desktop/Tools” accordingly, to share local folder with your student VM.

Connecting using OpenVPN - MacOSX Setup:

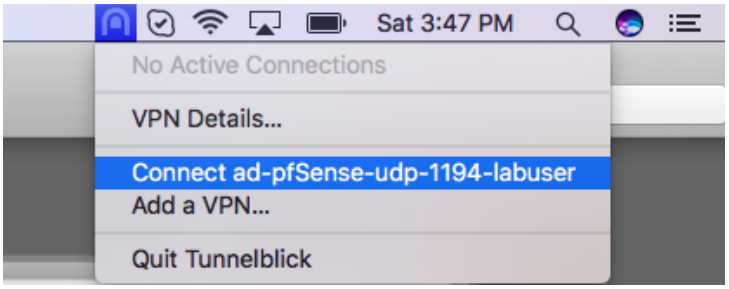
1. Install Tunnelblick and Microsoft Remote desktop
   https://tunnelblick.net/
   https://itunes.apple.com/in/app/microsoft-remote-desktop/id715768417?mt=12

2. Now go ahead and add OpenVPN config file using Tunnelblick





3. Next, click on Connect to connect to the lab



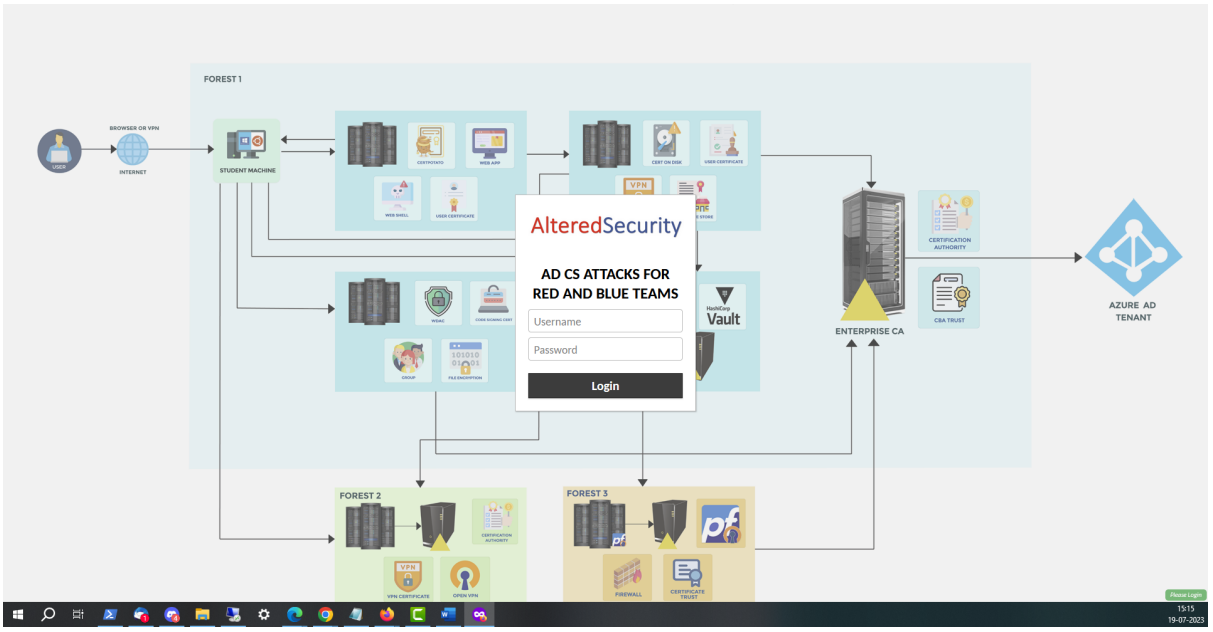
4. Enter the VPN credentials in the credential prompt. If everything is fine, you will be connected to the lab.

5. Use Remote desktop application and configure the IP (PC name) and credentials. Click on start to connect.

See Microsoft's documentation for more details:
https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-mac

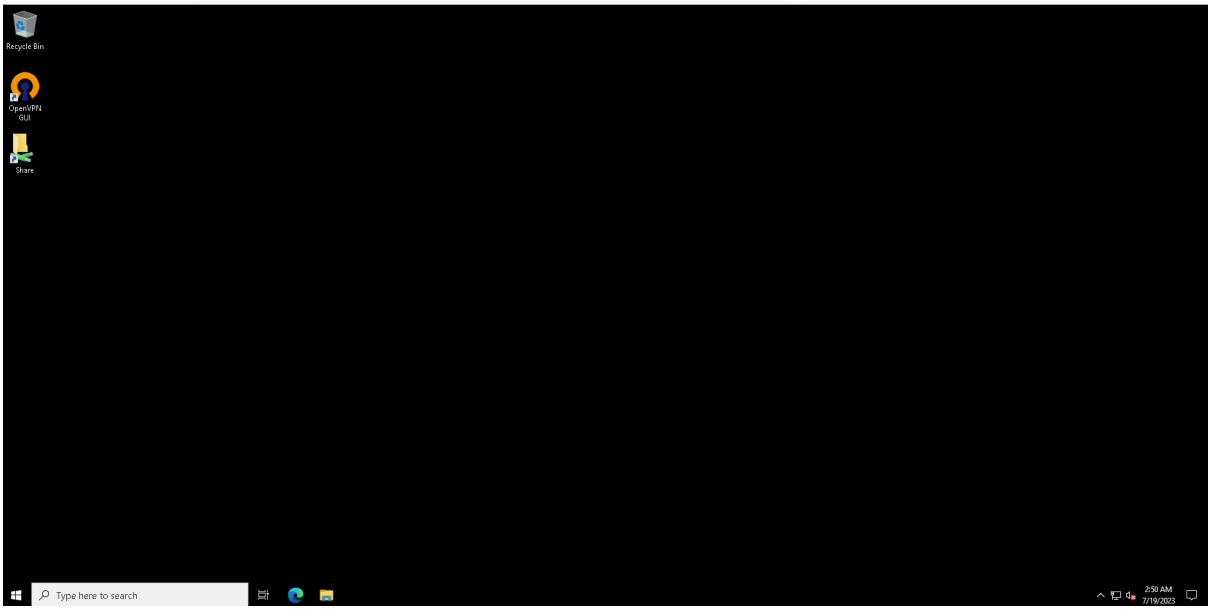
Login using web browser

Step 1: Browse to the server URL 'https://<ServerIP>:Port' and accept the certificate warning to open the login page:



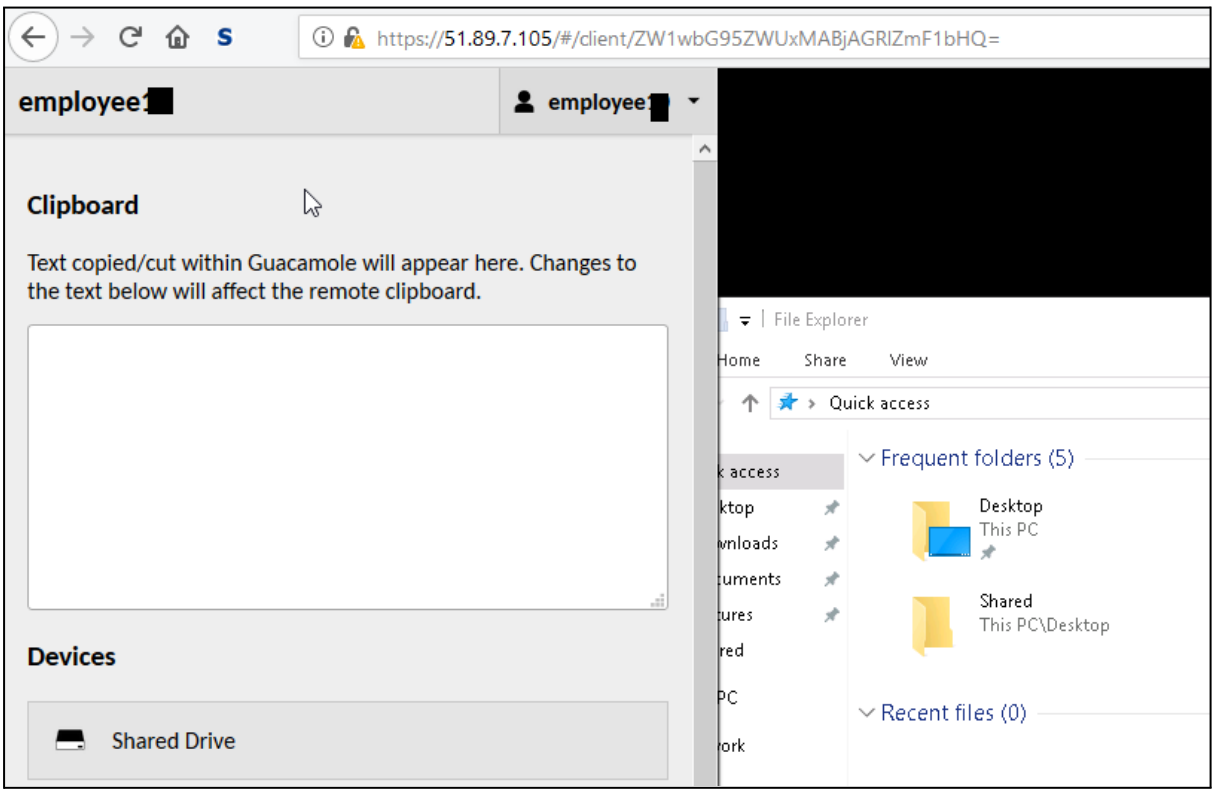
Step 2: Enter the username and password shared with you or generated in the portal to login:

Step 3: Enter the Windows username and password shared with you. You can now access the lab VM without needing anything else.

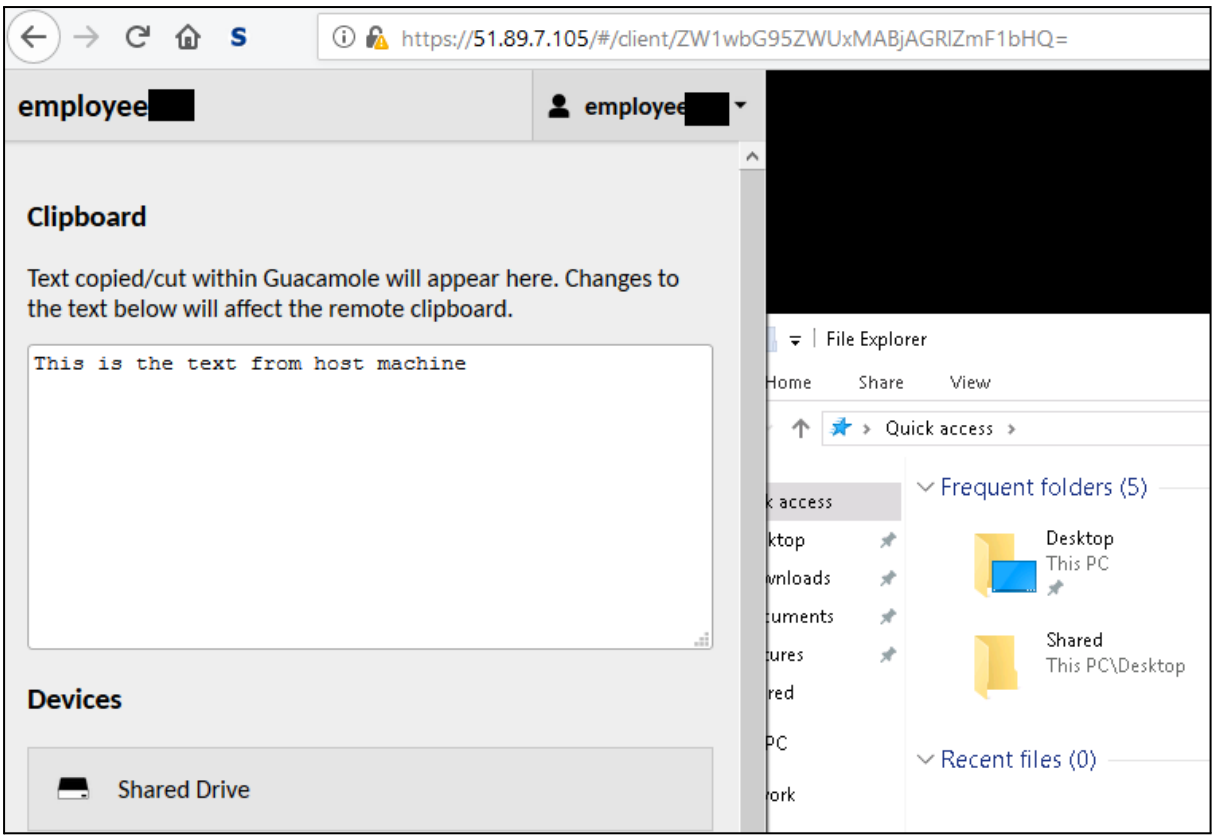


Copying text from host machine to lab VM

Step 1: After login, use **Ctrl + Alt + Shift** on the browser to open clipboard:

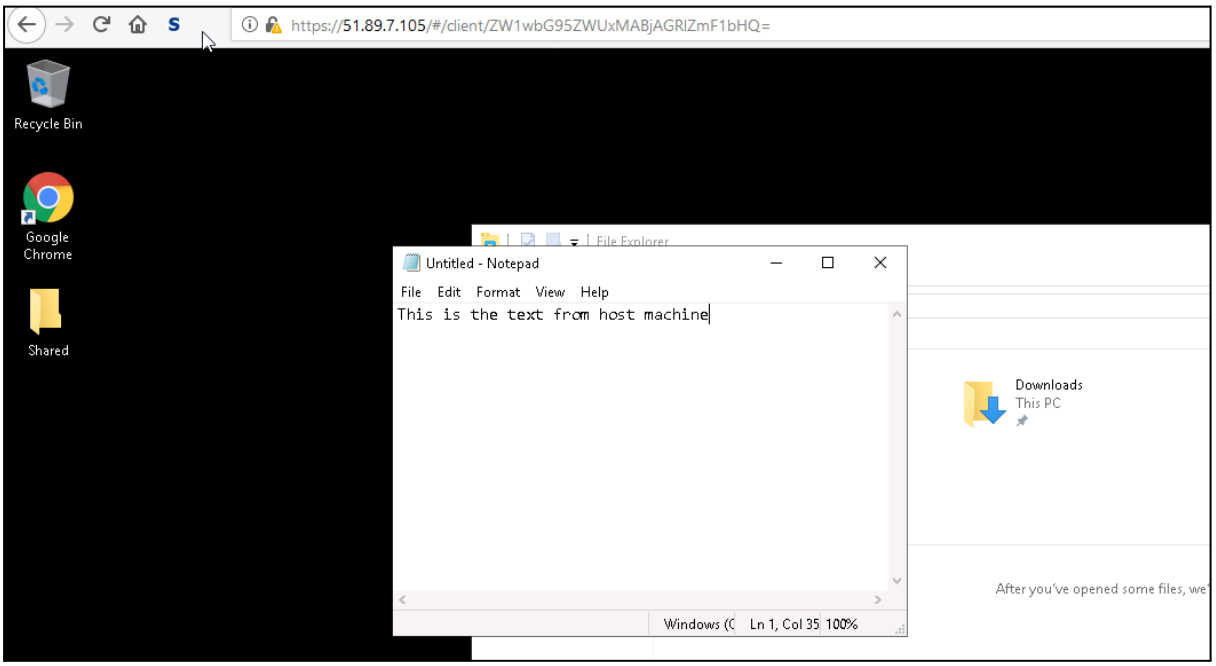


Step 2: Copy text from host machine and paste in the clipboard:



Step 3: Press **Ctrl + Alt + Shift** on the browser to copy the text to lab VM's clipboard.

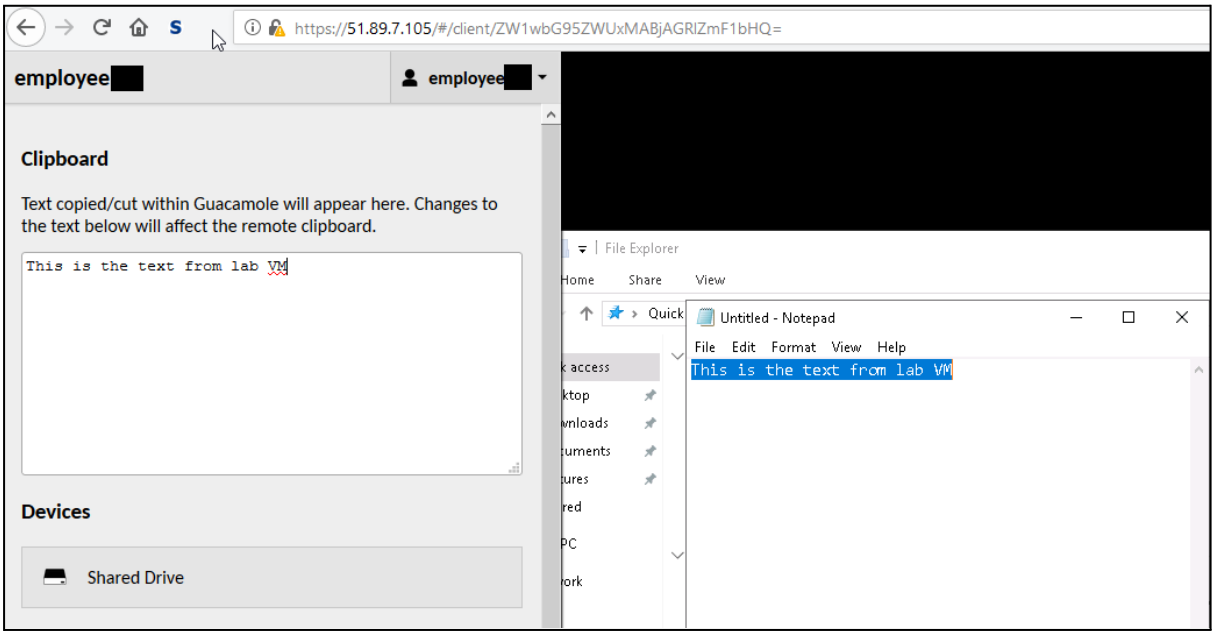
Step 4: Press **Ctrl + v** to paste the text in notepad or any other application on the lab VM. It is recommended to use notepad when copying multiline commands.



Copying text from Lab VM to host machine

Step 1: Copy text from the lab VM.

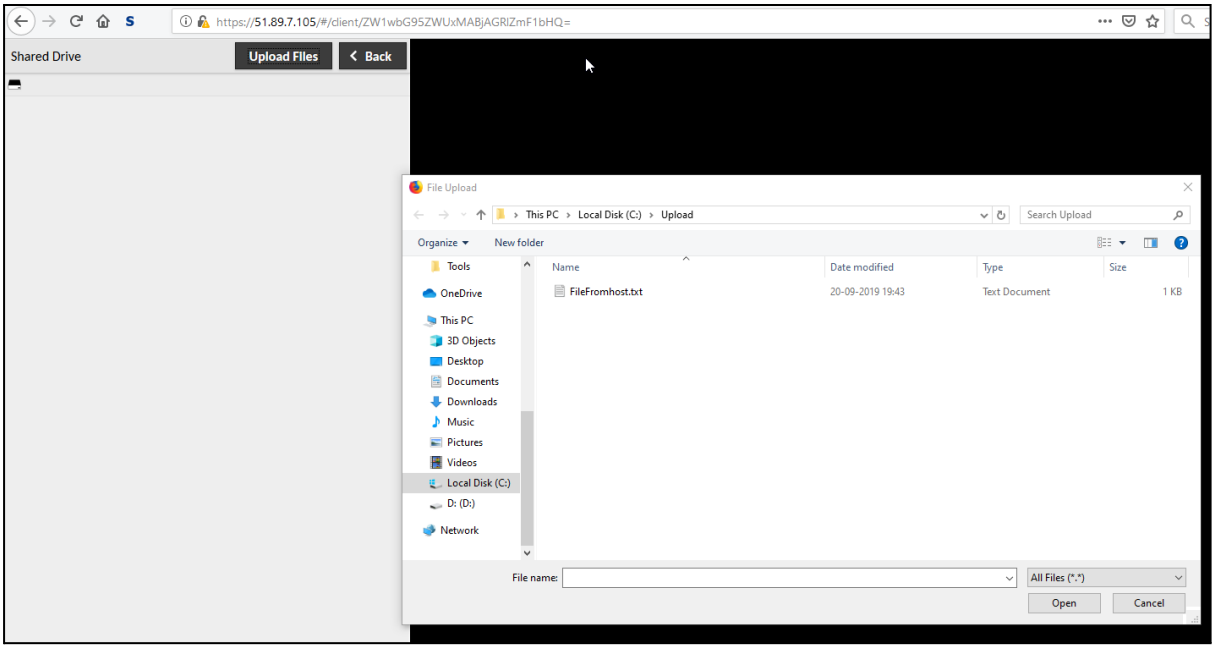
Step 2: Press **Ctrl + Alt + Shift** to open the clipboard. The text you copied from the lab VM will be there.



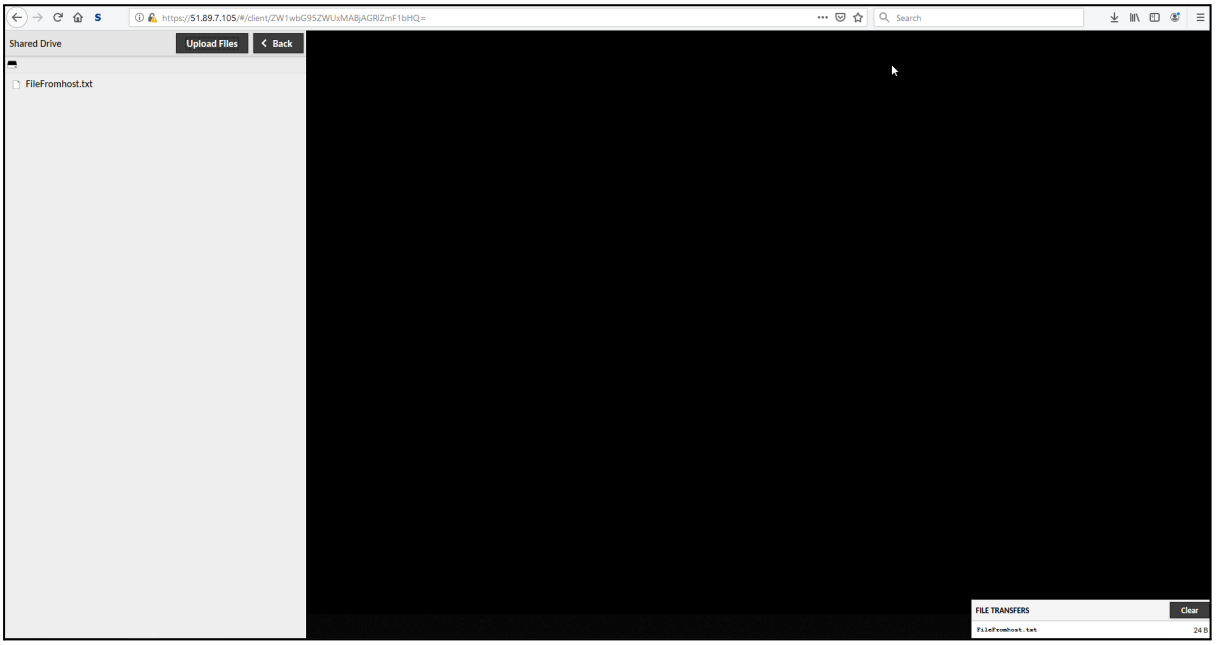
Step 3: Copy the text from the clipboard using Ctrl + c and paste it in any application on your host machine.

Copy files from host machine to lab VM

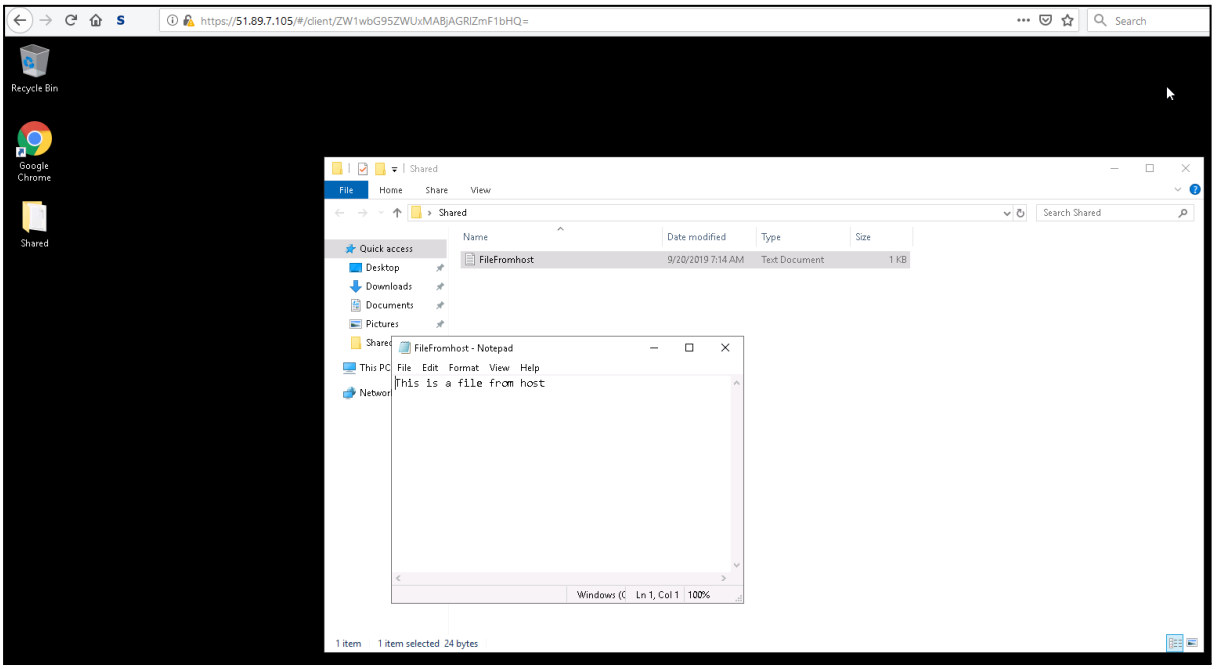
Step 1: Press **Ctrl + Alt + Shift** in the browser window and click on Shared Drive. Click on 'Upload Files' and browse to the file that you want to upload:



Step 2: You can check the file transfer status at the bottom right corner:

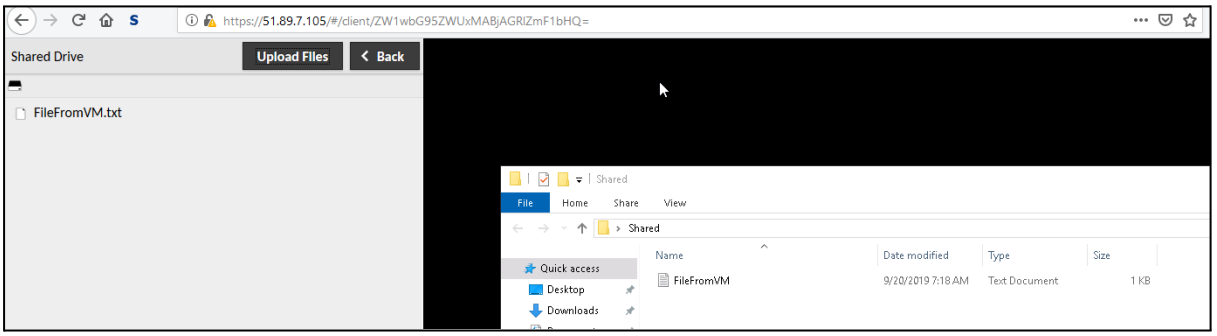


Step 3: Access the file from a folder called 'Shared' on user Desktop on lab VM.



Copy files from lab VM to host machine

Step 1: Copy the file you want to download to the folder named 'Shared' on user Desktop on the lab VM. Press **Ctrl + Alt + Shift** on the browser window and click on 'Shared Drive'. The file you copied to the 'Shared' folder will be visible:



Step 2: Double click the file you want to download: