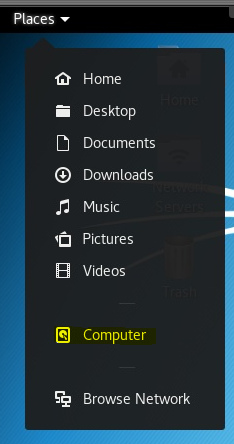
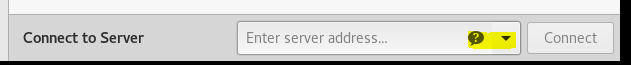
Cracking the ticket.

In the previous lab you used mimikatz to extract a Kerberos ticket from a system. Now you will attempt to crack the password using tgsrepcrack which is available on git hub

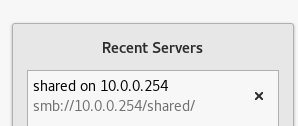
1. Launch into the KaliVirtual Machine using the Skytap link provided.
2. Click on Places 🡪 Computer



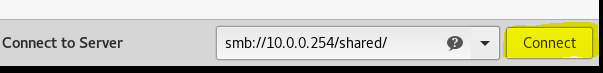
1. Click on Other Locations
2. Next to the Connect to Server Dialog box click the drop down.



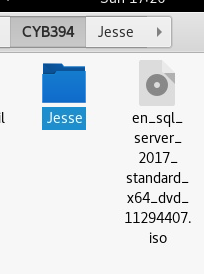
1. Select the shared on 10.0.0.254



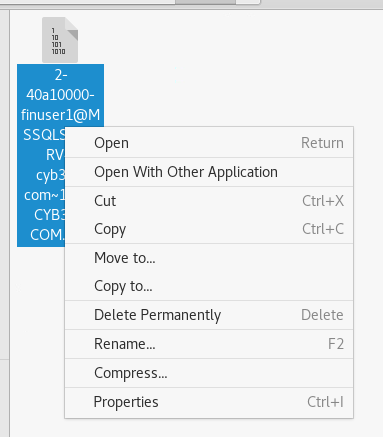
1. Click Connect



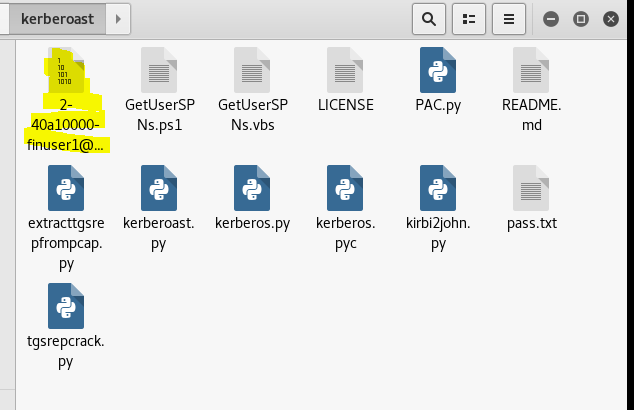
1. When prompted for credentials click Connect
2. Navigate into the cyb394 folder then into your own folder



1. Right click and copy the extracted ticket from the previous lab



1. Back on the Desktop Double Click on the Home folder
2. Then double click on the kerberoast folder
3. Paste your captured ticket into this folder



1. Open a terminal to this location
2. Type in the terminal **python tgsrepcrack.py pass.txt *nameofyourfile.kirbi***

\*You can use tab complete to type in your file name



1. Press enter to run the cracking program.
2. You should get a found password for ticket 0 response.