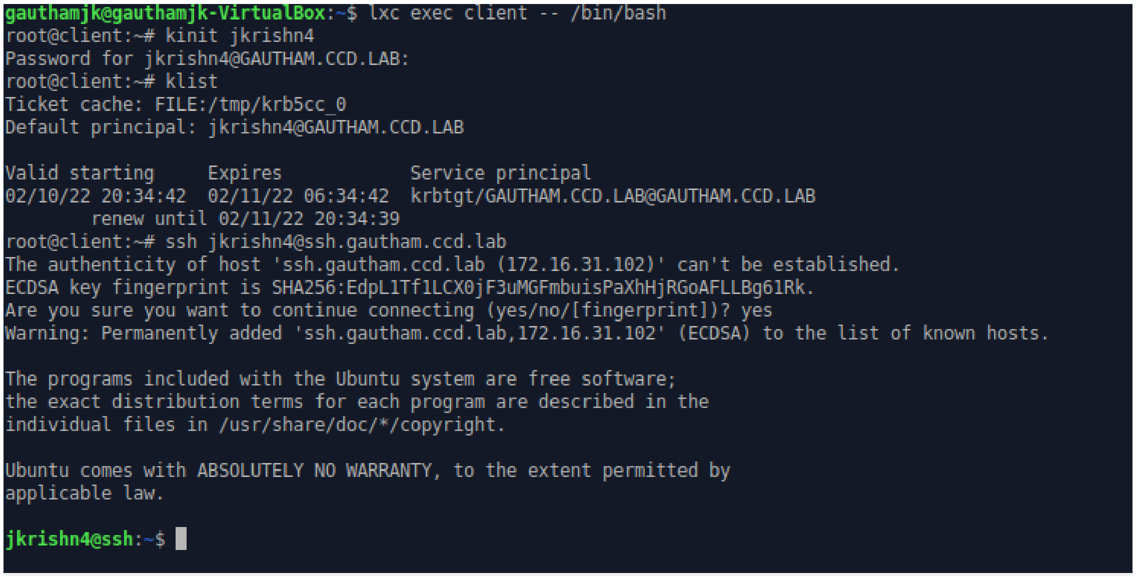
Single-sign-on Services

Name: Gautham Krishna Kumar

1. Upload a screenshot showing that you can successfully login without using a password to your ssh container.



```
gauthamjk@gauthamjk-VirtualBox:~$ lxc exec client -- /bin/bash
root@client:~# kinit jkrishn4
Password for jkrishn4@GAUTHAM.CCD.LAB:
root@client:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: jkrishn4@GAUTHAM.CCD.LAB

Valid starting     Expires            Service principal
02/10/22 20:34:42  02/11/22 06:34:42  krbtgt/GAUTHAM.CCD.LAB@GAUTHAM.CCD.LAB
        renew until 02/11/22 20:34:39
root@client:~# ssh jkrishn4@ssh.gautham.ccd.lab
The authenticity of host 'ssh.gautham.ccd.lab (172.16.31.102)' can't be established.
ECDSA key fingerprint is SHA256:EdpL1Tf1LCX0jF3uMGFmbuisPaXhHjRGoAFLLBg61Rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ssh.gautham.ccd.lab,172.16.31.102' (ECDSA) to the list of known hosts.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jkrishn4@ssh:~$
```

2. Explore other services that support Kerberos, such as an email server, an NFS server, and a web server. Identify one of each of the mentioned services and describe how to enable support for Kerberos authentication for these services. Include links to documentation that you find.

Web Server: https://plugins.miniorange.com/guide-to-setup-kerberos-single-sign-sso

1) First, the kerberos client libraries must be installed on the web server.
2) Then, the Active Directory domain in the Kerberos Configuration File needs to be configured.
3) Since this is an Apache Web Server, install the auth_kerb module.
4) A keytab file on the AD domain controller needs to be created.
5) Finally, we can configure Kerberos Single sign on for the site directory.

NFS Server: https://docs.oracle.com/cd/E19253-01/816-4557/setup-237/index.html

1) Before configuring the Kerberos NFS server, the master KDC must be configured. Several clients are needed to test this process.
2) Configure the NFS server as a kerberos client.
3) Start kadmin and create the server's NFS service principal and add it to the server's keytab file.
4) Share the NFS file system with Kerberos security modes.

Email Server: https://mailtrap.io/blog/smtp-auth/

1) GSSAPI is almost exclusively used with Kerberos.
2) These are used in Microsoft Windows Servers just like NTLM.
3) The client and server negotiate a shared secret key, cipher, and hash for the session.
4) A host key is then provided by the server.
5) And finally, the authentication is done by the client.