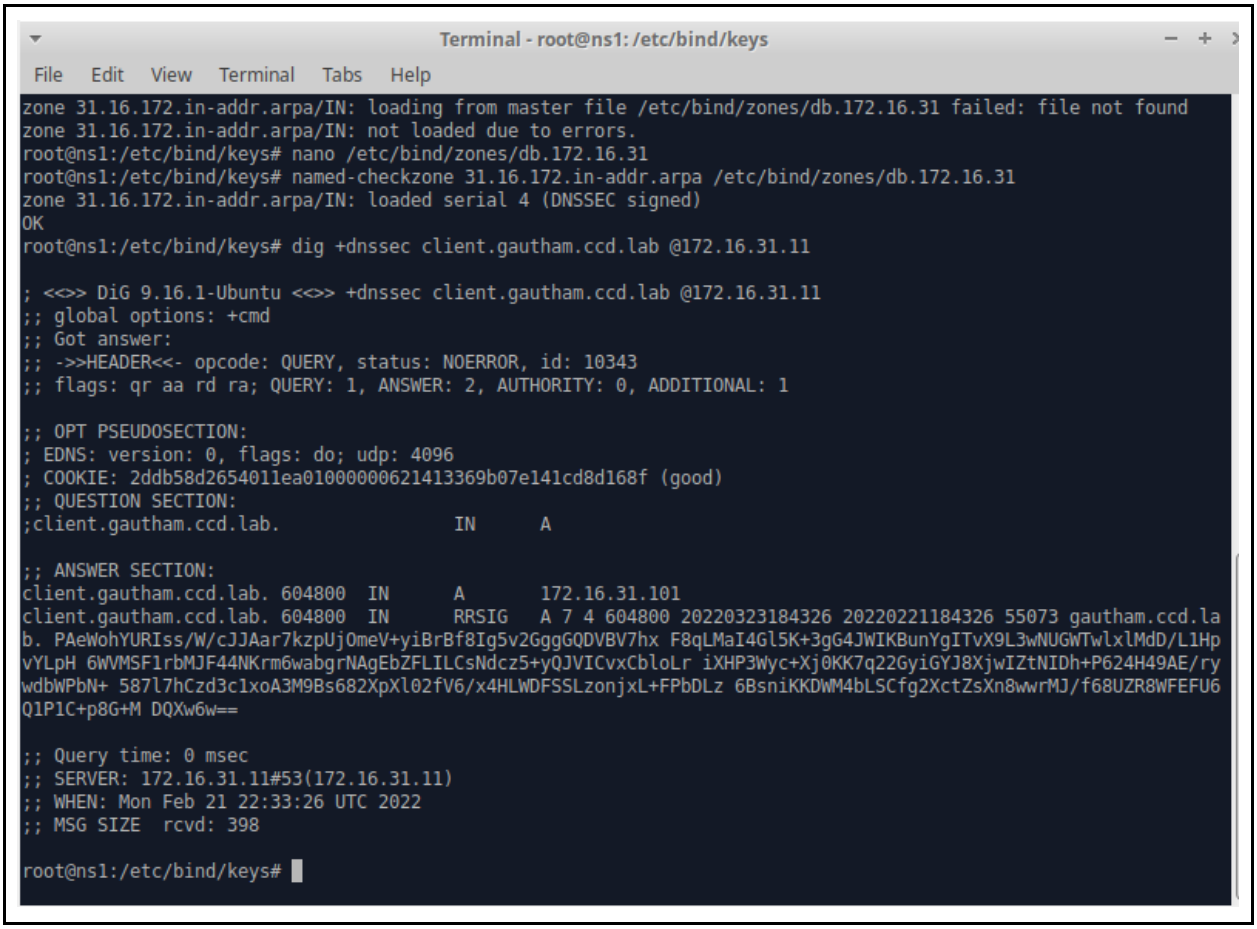
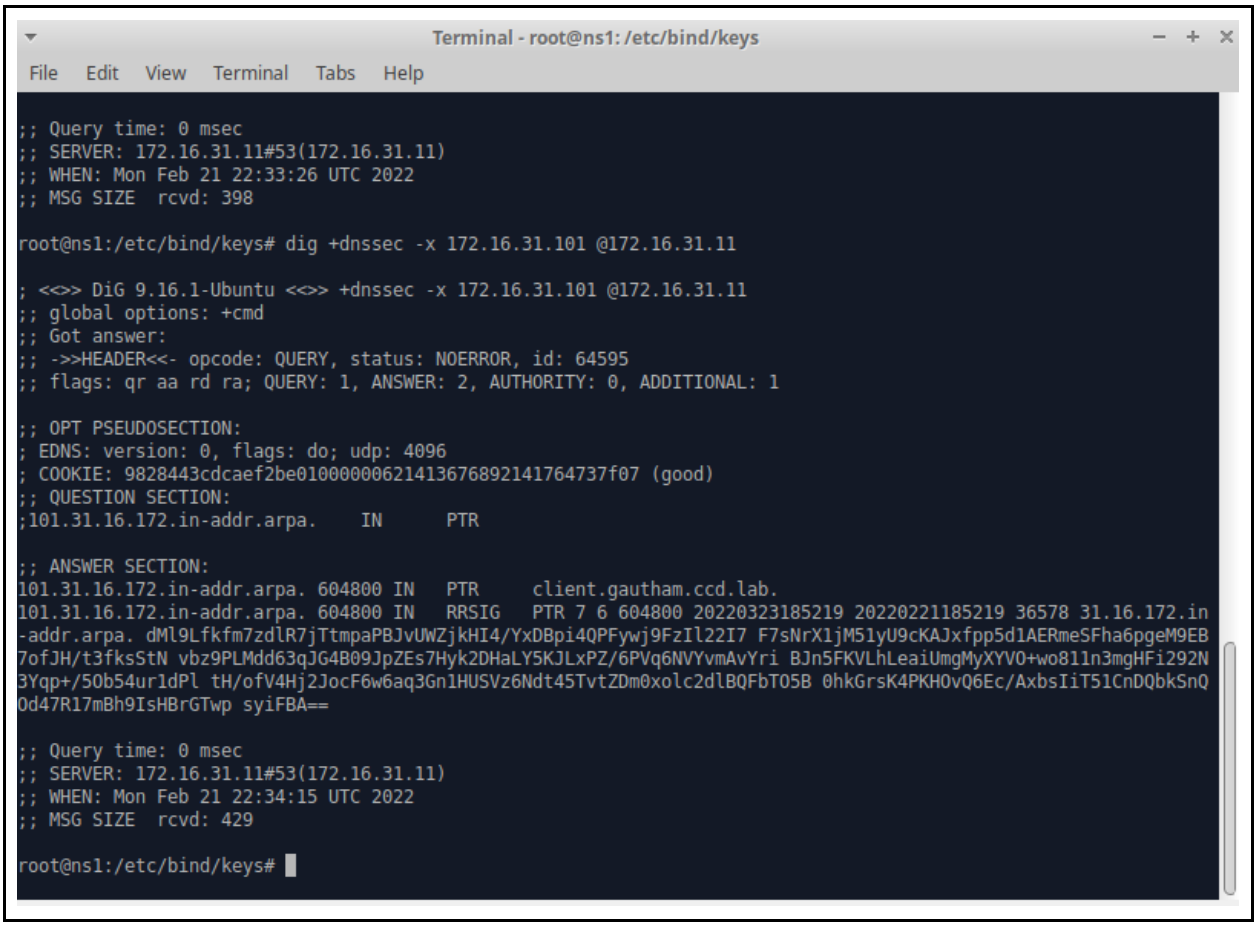
Securing Network Communications

Gautham Krishna Kumar

1. Upload a screenshot showing the signatures





2. Upload a screenshot of the following commands to show that OpenLDAP is correctly configured to use TLS

```
root@ldap:~# ldapsearch -H ldap:// -x -b "dc=gautham,dc=ccd,dc=lab" -LLL dn
Confidentiality required (13)
Additional information: TLS confidentiality required
root@ldap:~# ldapsearch -H ldap:// -x -b "dc=gautham,dc=ccd,dc=lab" -LLL -ZZ dn
dn: dc=gautham,dc=ccd,dc=lab

dn: cn=admin,dc=gautham,dc=ccd,dc=lab

dn: ou=Users,dc=gautham,dc=ccd,dc=lab

dn: ou=Groups,dc=gautham,dc=ccd,dc=lab

dn: cn=ccd_group,ou=Groups,dc=gautham,dc=ccd,dc=lab

dn: uid=jkrishn4,ou=Users,dc=gautham,dc=ccd,dc=lab

dn: cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: cn=GAUTHAM.CCD.LAB,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=K/M@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krbContainer,dc
 =gautham,dc=ccd,dc=lab

dn: krbPrincipalName=krbtgt/GAUTHAM.CCD.LAB@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB
 ,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kadmin/admin@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krbCon
 tainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kadmin/krb.gautham.ccd.lab@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD
 .LAB,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kiprop/krb.gautham.ccd.lab@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD
```

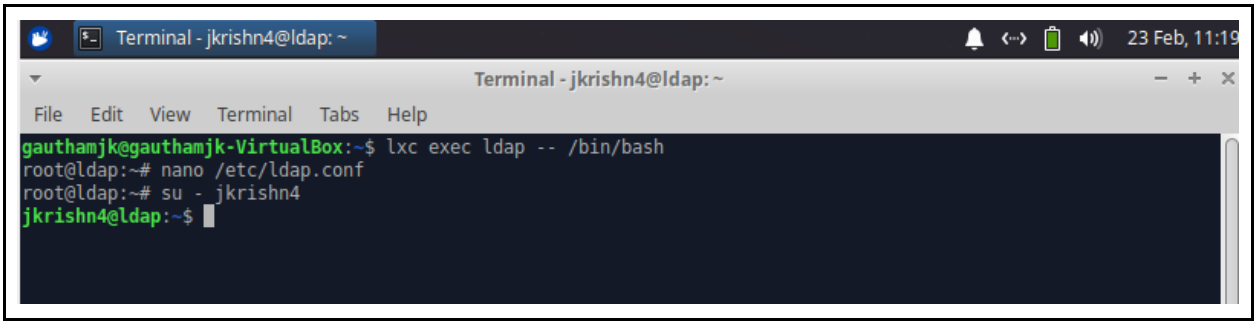
Terminal - root@ldap: ~

File Edit View Terminal Tabs Help

```
dn: uid=jkrishn4,ou=Users,dc=gautham,dc=ccd,dc=lab

dn: cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: cn=GAUTHAM.CCD.LAB,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=K/M@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krbContainer,dc
 =gautham,dc=ccd,dc=lab

dn: krbPrincipalName=krbtgt/GAUTHAM.CCD.LAB@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB
 ,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kadmin/admin@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krbCon
 tainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kadmin/krb.gautham.ccd.lab@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD
 .LAB,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kiprop/krb.gautham.ccd.lab@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD
 .LAB,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kadmin/changepw@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krb
 Container,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=kadmin/history@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krbC
 ontainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=jkrishn4/admin@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krbC
 ontainer,dc=gautham,dc=ccd,dc=lab

dn: krbPrincipalName=host/ssh.gautham.ccd.lab@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.L
 AB,cn=krbContainer,dc=gautham,dc=ccd,dc=lab

root@ldap:~#
```

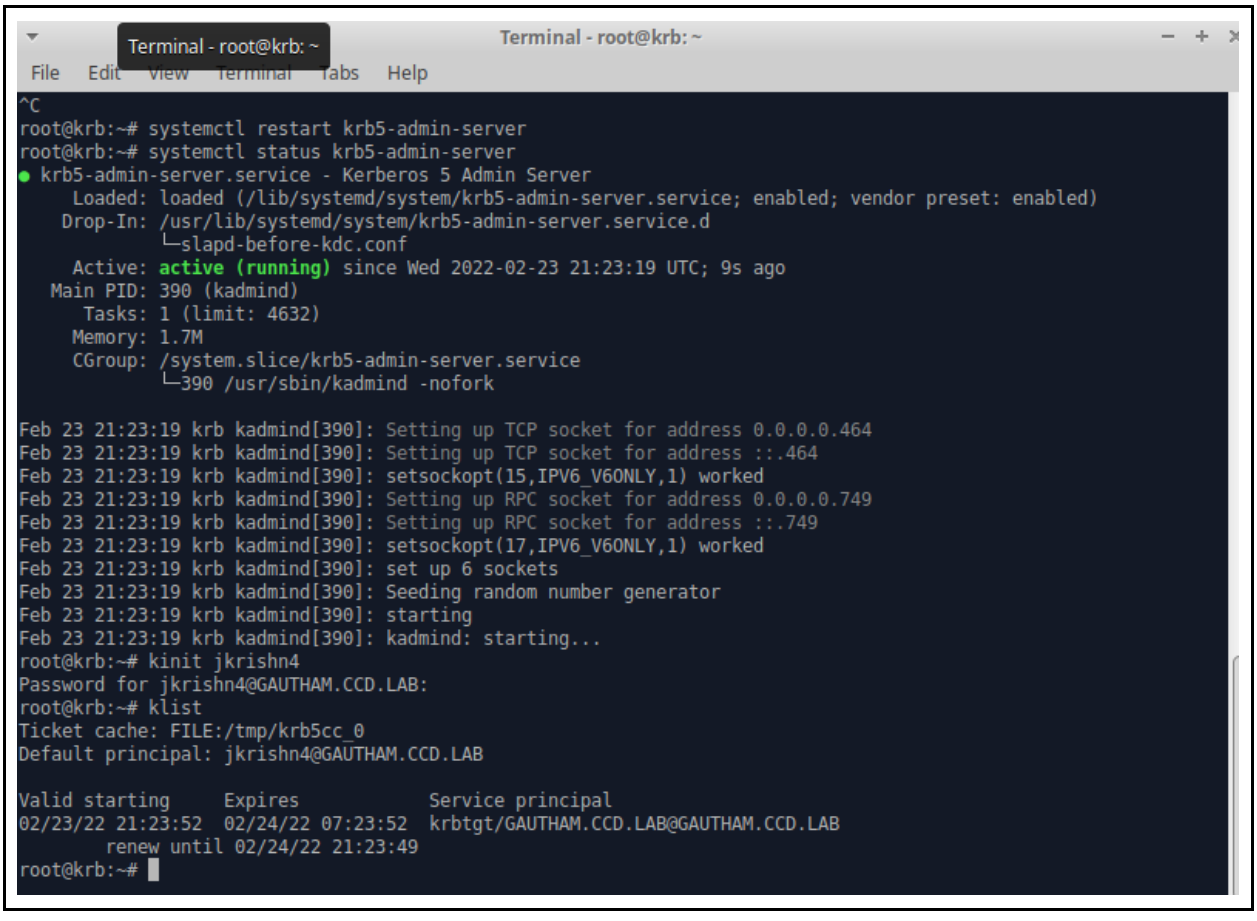
```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfreetype6
Use 'apt autoremove' to remove it.
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aebd88e-1ubuntu1 [196
kB]
Fetched 196 kB in 1s (243 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 32184 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
root@ldap:~# netstat -plant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      524/slapd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      169/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      225/sshd: /usr/sbin
tcp        0      0 0.0.0.0:88              0.0.0.0:*               LISTEN      268/krb5kdc
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      524/slapd
tcp        0      0 172.16.31.16:55514      91.189.88.142:80        TIME_WAIT   -
tcp6       0      0 :::389                  :::*                    LISTEN      524/slapd
tcp6       0      0 :::22                   :::*                    LISTEN      225/sshd: /usr/sbin
tcp6       0      0 :::88                   :::*                    LISTEN      268/krb5kdc
tcp6       0      0 :::636                  :::*                    LISTEN      524/slapd
root@ldap:~#
```

3. Upload a screenshot showing that you can still successfully login after editing the configuration



```
gauthamjk@gauthamjk-VirtualBox:~$ lxc exec server -- /bin/bash
root@server:~# su - jkrishn4
jkrishn4@server:~$ logout
root@server:~# exitgauthamjk@gauthamjk-VirtualBox:~$ lxc exec krb -- /bin/bash
root@krb:~# su - jkrishn4
jkrishn4@krb:~$ logout
root@krb:~# exit
exit
gauthamjk@gauthamjk-VirtualBox:~$ lxc exec ns1 -- /bin/bash
root@ns1:~# su - jkrishn4
jkrishn4@ns1:~$ logout
root@ns1:~# exitgauthamjk@gauthamjk-VirtualBox:~$ lxc exec ns2 -- /bin/bash
root@ns2:~# su - jkrishn4
jkrishn4@ns2:~$ logout
root@ns2:~# exit
exit
gauthamjk@gauthamjk-VirtualBox:~$ lxc exec client -- /bin/bash
root@client:~# su - jkrishn4
jkrishn4@client:~$ logout
root@client:~# exitgauthamjk@gauthamjk-VirtualBox:~$ lxc exec ssh -- /bin/bash
root@ssh:~# su - jkrishn4
jkrishn4@ssh:~$ logout
root@ssh:~# exit
exit
gauthamjk@gauthamjk-VirtualBox:~$
```

4. Upload a screenshot of the above commands showing your new TGT

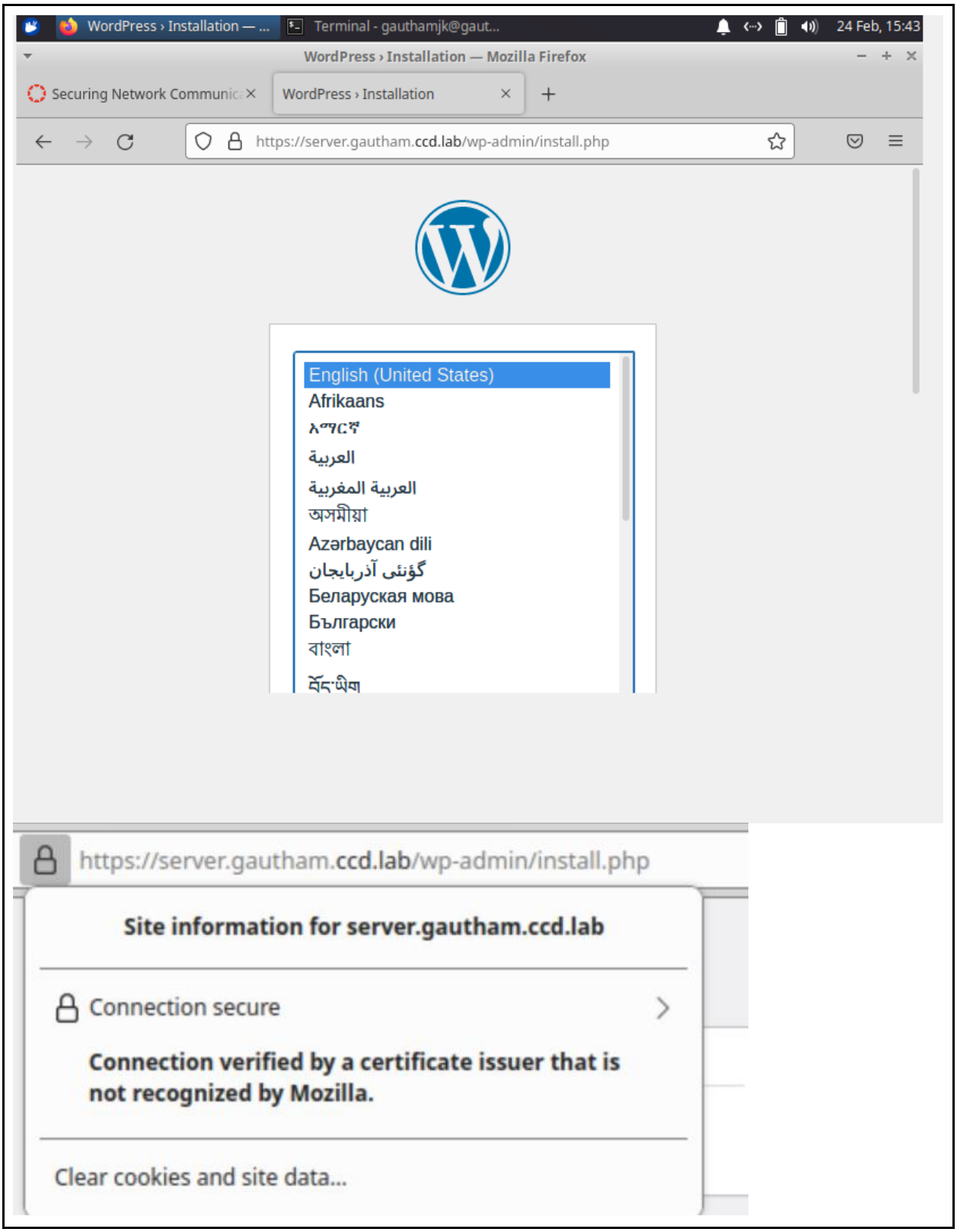


5. Explain what the two server blocks in the above configuration file do. Also explain what each location block does. You will likely have to read the nginx documentation to figure all of this out

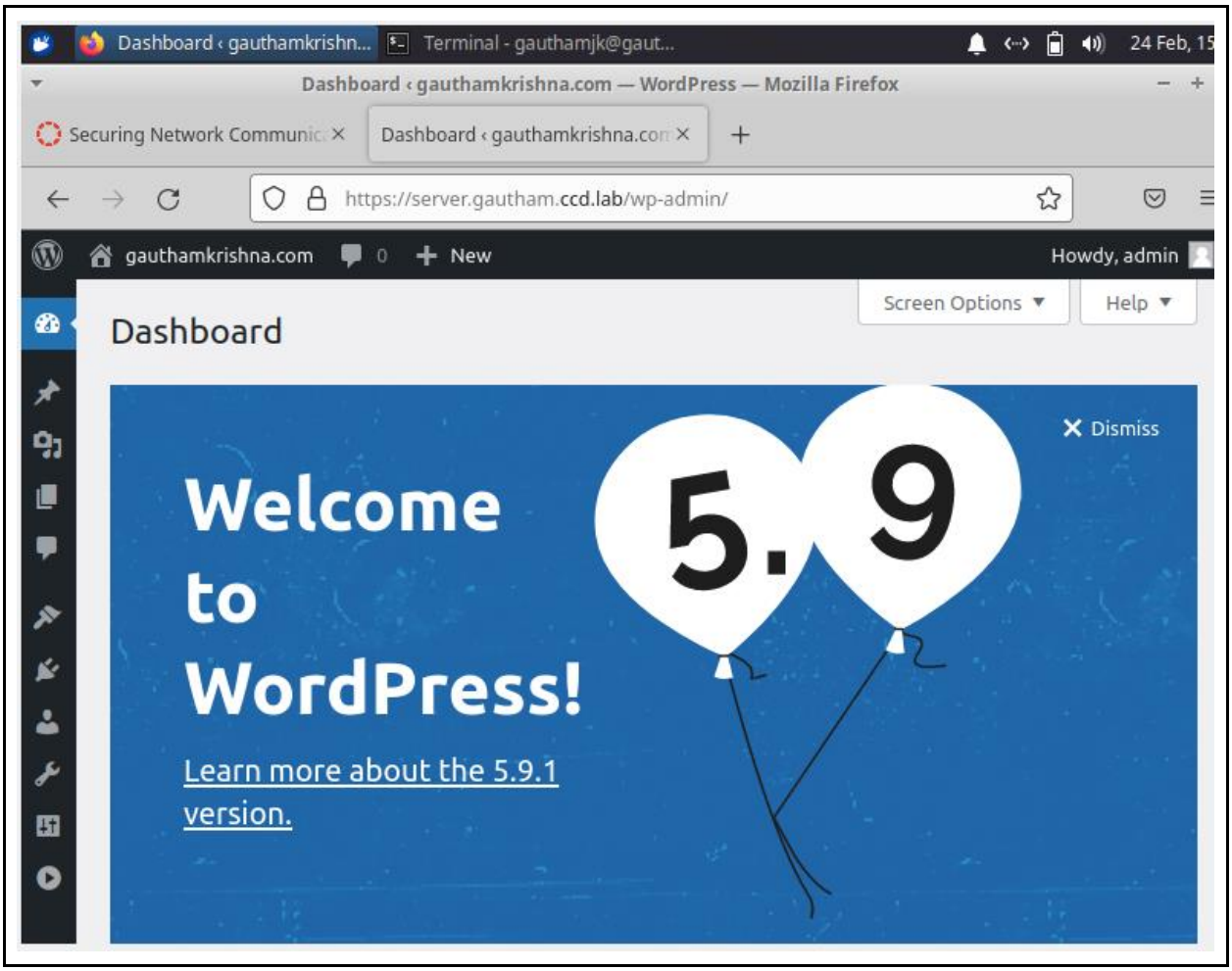
- The configuration file may include quite a few server blocks distinguished by ports on which they listen to and by server names. Nginx will first determine which server will process the request.
- The first block will redirect the requests to HTTPS (443) and will return a code 301, which indicates permanent URL redirection.
- In the second block, the first four lines define the SSL parameters such as the SSL Certificate and the SSL Certificate Key. Then, the WordPress HTML file location will be mentioned.
- The location block defines how nginx should handle requests for different resources and URIs for the parent server.
- From the first location, the command try_files checks the existence of index.php and if found, it will process the file.
- From the second location, the fastcgi configuration file is used and nginx is assigned the task to proxy requests to it using the FCGI command.

6. Upload a screenshot of your browser window showing a successful TLS connection and the Wordpress setup screen

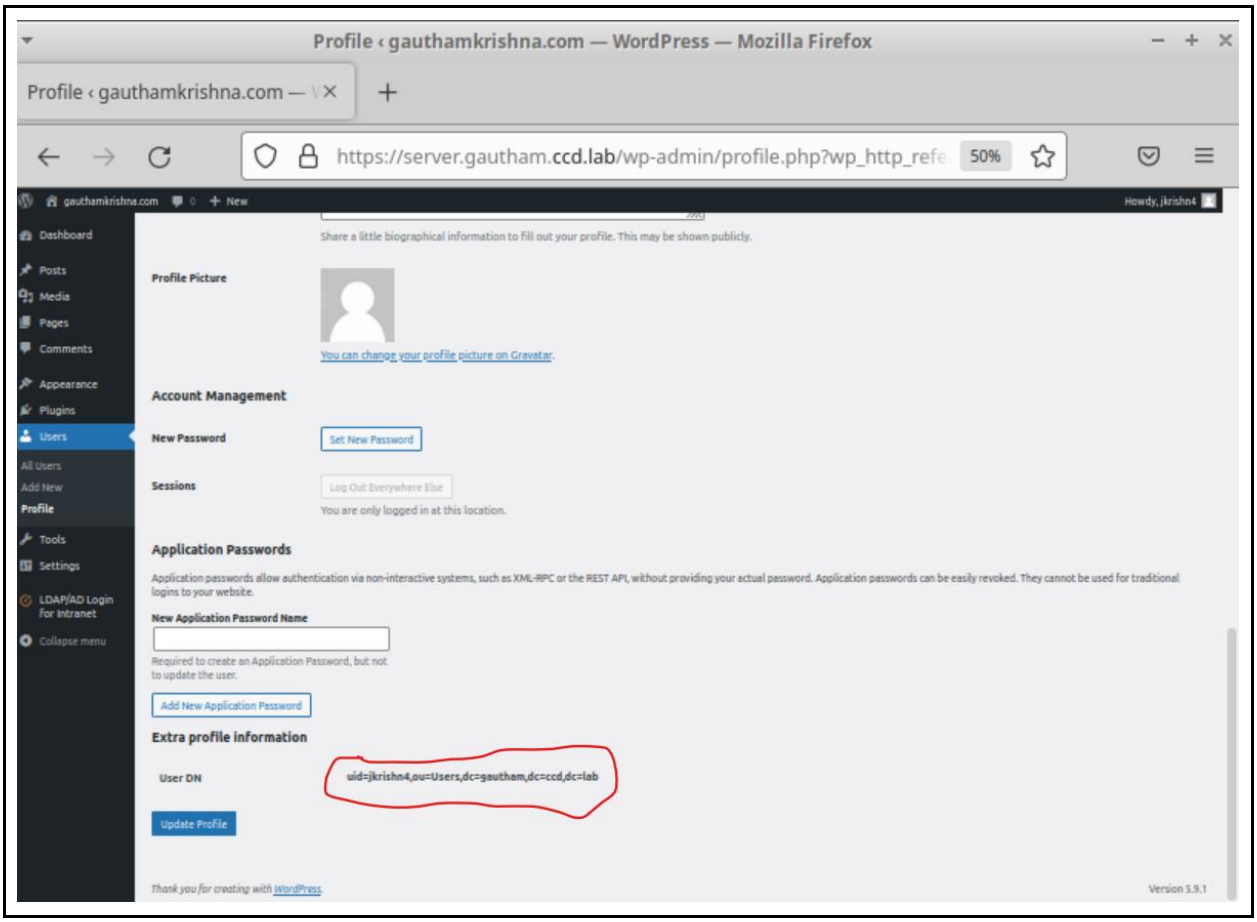
Next Page


WordPress › Installation — ...
Terminal - gauthamjk@gaut...
24 Feb, 15:43
WordPress › Installation — Mozilla Firefox
Securing Network Communic...
WordPress › Installation
https://server.gautham.ccd.lab/wp-admin/install.php
English (United States)
Afrikaans
አማርኛ
العربية
العربية المغربية
অসমীয়া
Azərbaycan dili
گؤنئی آذربایجان
Беларуская мова
Български
বাংলা
https://server.gautham.ccd.lab/wp-admin/install.php
Site information for server.gautham.ccd.lab
Connection secure
Connection verified by a certificate issuer that is not recognized by Mozilla.
Clear cookies and site data...

7. Finish the setup of Wordpress and upload a screenshot of the dashboard after you have successfully logged in. Create an admin account and remember the password



8. Upload a screenshot of this page showing that your Wordpress user is mapped to your LDAP user DN.


Profile ‹ gauthamkrishna.com — WordPress — Mozilla Firefox
Profile ‹ gauthamkrishna.com —
https://server.gautham.ccd.lab/wp-admin/profile.php?wp_http_refe
50%
gauthamkrishna.com
New
Howdy, jkrishn4
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
Users
All Users
Add New
Profile
Tools
Settings
LDAP/AD Login for Intranet
Collapse menu
Share a little biographical information to fill out your profile. This may be shown publicly.
Profile Picture
You can change your profile picture on Gravatar.
Account Management
New Password
Set New Password
Sessions
Log Out Everywhere Else
You are only logged in at this location.
Application Passwords
Application passwords allow authentication via non-interactive systems, such as XML-RPC or the REST API, without providing your actual password. Application passwords can be easily revoked. They cannot be used for traditional logins to your website.
New Application Password Name
Required to create an Application Password, but not to update the user.
Add New Application Password
Extra profile information
User DN
uid=jkrishn4,ou=Users,dc=gautham,dc=ccd,dc=lab
Update Profile
Thank you for creating with WordPress.
Version 5.9.1