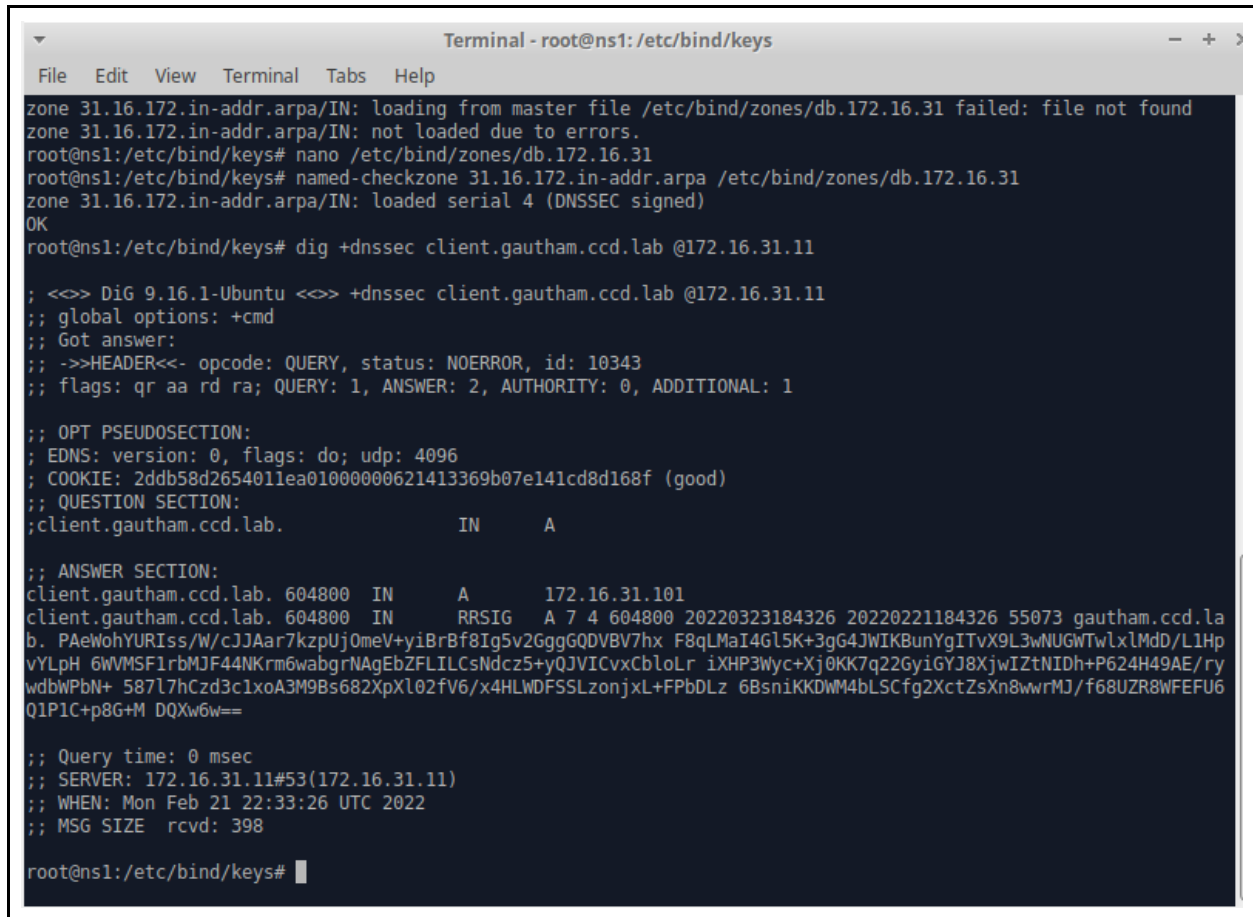


# Securing Network Communications

Gautham Krishna Kumar

1. Upload a screenshot showing the signatures

A terminal window titled "Terminal - root@ns1: /etc/bind/keys" showing the process of verifying a DNS zone. The user runs 'named-checkzone' and 'dig +dnssec' to verify the 'client.gautham.ccd.lab' zone. The output shows the zone is loaded and signed, and the dig command returns a successful response with DNSSEC data.

```
Terminal - root@ns1: /etc/bind/keys
File Edit View Terminal Tabs Help
zone 31.16.172.in-addr.arpa/IN: loading from master file /etc/bind/zones/db.172.16.31 failed: file not found
zone 31.16.172.in-addr.arpa/IN: not loaded due to errors.
root@ns1:/etc/bind/keys# nano /etc/bind/zones/db.172.16.31
root@ns1:/etc/bind/keys# named-checkzone 31.16.172.in-addr.arpa /etc/bind/zones/db.172.16.31
zone 31.16.172.in-addr.arpa/IN: loaded serial 4 (DNSSEC signed)
OK
root@ns1:/etc/bind/keys# dig +dnssec client.gautham.ccd.lab @172.16.31.11

; <<>> DiG 9.16.1-Ubuntu <<>> +dnssec client.gautham.ccd.lab @172.16.31.11
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10343
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: 2ddb58d2654011ea01000000621413369b07e141cd8d168f (good)
;; QUESTION SECTION:
;client.gautham.ccd.lab.                IN      A

;; ANSWER SECTION:
client.gautham.ccd.lab. 604800 IN      A      172.16.31.101
client.gautham.ccd.lab. 604800 IN      RRSIG  A 7 4 604800 20220323184326 20220221184326 55073 gautham.ccd.la
b. PAeWohYURIss/W/cJJAar7kzpUj0meV+yiBrBf8Ig5v2GggGQDVBV7hx F8qLMaI4G15K+3gG4JWIKBunYgITvX9L3wNUGWTwLxLMdD/L1Hp
vYLpH 6WVMSF1rbMJF44NKrm6wabgrNAgEbZFLILCsNdcz5+yQJVICvxCbloLr iXHP3Wyc+Xj0KK7q22GyiGYJ8XjwIZtNIDh+P624H49AE/ry
wdbWPbN+ 587l7hCzd3c1xoA3M9Bs682XpXl02fV6/x4HLWDFSSLzonjxL+FPbDLz 6BsniKKDWM4bLSCfg2XctZsXn8wwrMJ/f68UZR8WFEFU6
Q1P1C+p8G+M DQXw6w==

;; Query time: 0 msec
;; SERVER: 172.16.31.11#53(172.16.31.11)
;; WHEN: Mon Feb 21 22:33:26 UTC 2022
;; MSG SIZE rcvd: 398

root@ns1:/etc/bind/keys#
```

```
Terminal - root@ns1: /etc/bind/keys
File Edit View Terminal Tabs Help

;; Query time: 0 msec
;; SERVER: 172.16.31.11#53(172.16.31.11)
;; WHEN: Mon Feb 21 22:33:26 UTC 2022
;; MSG SIZE rcvd: 398

root@ns1:/etc/bind/keys# dig +dnssec -x 172.16.31.101 @172.16.31.11

; <<>> DiG 9.16.1-Ubuntu <<>> +dnssec -x 172.16.31.101 @172.16.31.11
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64595
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: 9828443cdcaef2be01000000621413676892141764737f07 (good)
;; QUESTION SECTION:
;101.31.16.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
101.31.16.172.in-addr.arpa. 604800 IN PTR client.gautham.ccd.lab.
101.31.16.172.in-addr.arpa. 604800 IN RRSIG PTR 7 6 604800 20220323185219 20220221185219 36578 31.16.172.in-addr.arpa. dMl9Lfkfm7zdLR7jTtpaPBjvUWZjKHl4/YxDBpi4QPFYwj9FzIl22I7 F7sNrXlJm51yU9cKAJxfpp5d1AERmeSFha6pgeM9EB7ofJH/t3fksStN vbz9PLMdd63qJG4B09JpZEs7Hyk2DHaLY5KJLxPZ/6PVq6NVYvmAvYri BJn5FKVLhLeaiUmgMyXYV0+wo811n3mgHFi292N3Yqp+/50b54urldPl tH/ofV4Hj2JocF6w6aq3Gn1HUSVz6Ndt45TvtZDm0xolc2dLBQFbT05B 0hkGrS4PKH0vQ6Ec/AxbsIi51CnDQbkSnQ0d47R17mBh9IsHBrGTwp syiFBA==

;; Query time: 0 msec
;; SERVER: 172.16.31.11#53(172.16.31.11)
;; WHEN: Mon Feb 21 22:34:15 UTC 2022
;; MSG SIZE rcvd: 429

root@ns1:/etc/bind/keys#
```

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=krbContainer,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=kinrop/krb.gautham.ccd.lab@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,cn=krbContainer,dc=gautham,dc=ccd,dc=lab
```

```
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=krbContainer,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=kinrop/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=krbContainer,dc=gautham,dc=ccd,dc=lab

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

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

dn: krbPrincipalName=host/ssh.gautham.ccd.lab@GAUTHAM.CCD.LAB,cn=GAUTHAM.CCD.LAB,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 0.0.0.0:53:53          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

```

Terminal - jkrishn4@ldap: ~
File Edit View Terminal Tabs Help
gauthamjk@gauthamjk-VirtualBox:~$ lxc exec ldap -- /bin/bash
root@ldap:~# nano /etc/ldap.conf
root@ldap:~# su - jkrishn4
jkrishn4@ldap:~$

```

```

gauthamjk@gauthamjk-VirtualBox:~$ lxc exec server -- /bin/bash
root@server:~# su - jkrishn4
jkrishn4@server:~$ logout
root@server:~# exit
gauthamjk@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:~# exit
gauthamjk@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:~# exit
gauthamjk@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

```

Terminal - root@krb: ~
File Edit View Terminal Tabs Help
^C
root@krb:~# systemctl restart krb5-admin-server
root@krb:~# systemctl status krb5-admin-server
● krb5-admin-server.service - Kerberos 5 Admin Server
   Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; vendor preset: enabled)
   Drop-In: /usr/lib/systemd/system/krb5-admin-server.service.d
            └─slapd-before-kdc.conf
   Active: active (running) since Wed 2022-02-23 21:23:19 UTC; 9s ago
     Main PID: 390 (kadmind)
       Tasks: 1 (limit: 4632)
      Memory: 1.7M
    CGroup: /system.slice/krb5-admin-server.service
            └─390 /usr/sbin/kadmind -nofork

Feb 23 21:23:19 krb kadmind[390]: Setting up TCP socket for address 0.0.0.0.464
Feb 23 21:23:19 krb kadmind[390]: Setting up TCP socket for address ::.464
Feb 23 21:23:19 krb kadmind[390]: setsockopt(15,IPV6_V6ONLY,1) worked
Feb 23 21:23:19 krb kadmind[390]: Setting up RPC socket for address 0.0.0.0.749
Feb 23 21:23:19 krb kadmind[390]: Setting up RPC socket for address ::.749
Feb 23 21:23:19 krb kadmind[390]: setsockopt(17,IPV6_V6ONLY,1) worked
Feb 23 21:23:19 krb kadmind[390]: set up 6 sockets
Feb 23 21:23:19 krb kadmind[390]: Seeding random number generator
Feb 23 21:23:19 krb kadmind[390]: starting
Feb 23 21:23:19 krb kadmind[390]: kadmind: starting...
root@krb:~# kinit jkrishn4
Password for jkrishn4@GAUTHAM.CCD.LAB:
root@krb:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: jkrishn4@GAUTHAM.CCD.LAB

Valid starting    Expires          Service principal
02/23/22 21:23:52 02/24/22 07:23:52 krbtgt/GAUTHAM.CCD.LAB@GAUTHAM.CCD.LAB
        renew until 02/24/22 21:23:49
root@krb:~# █

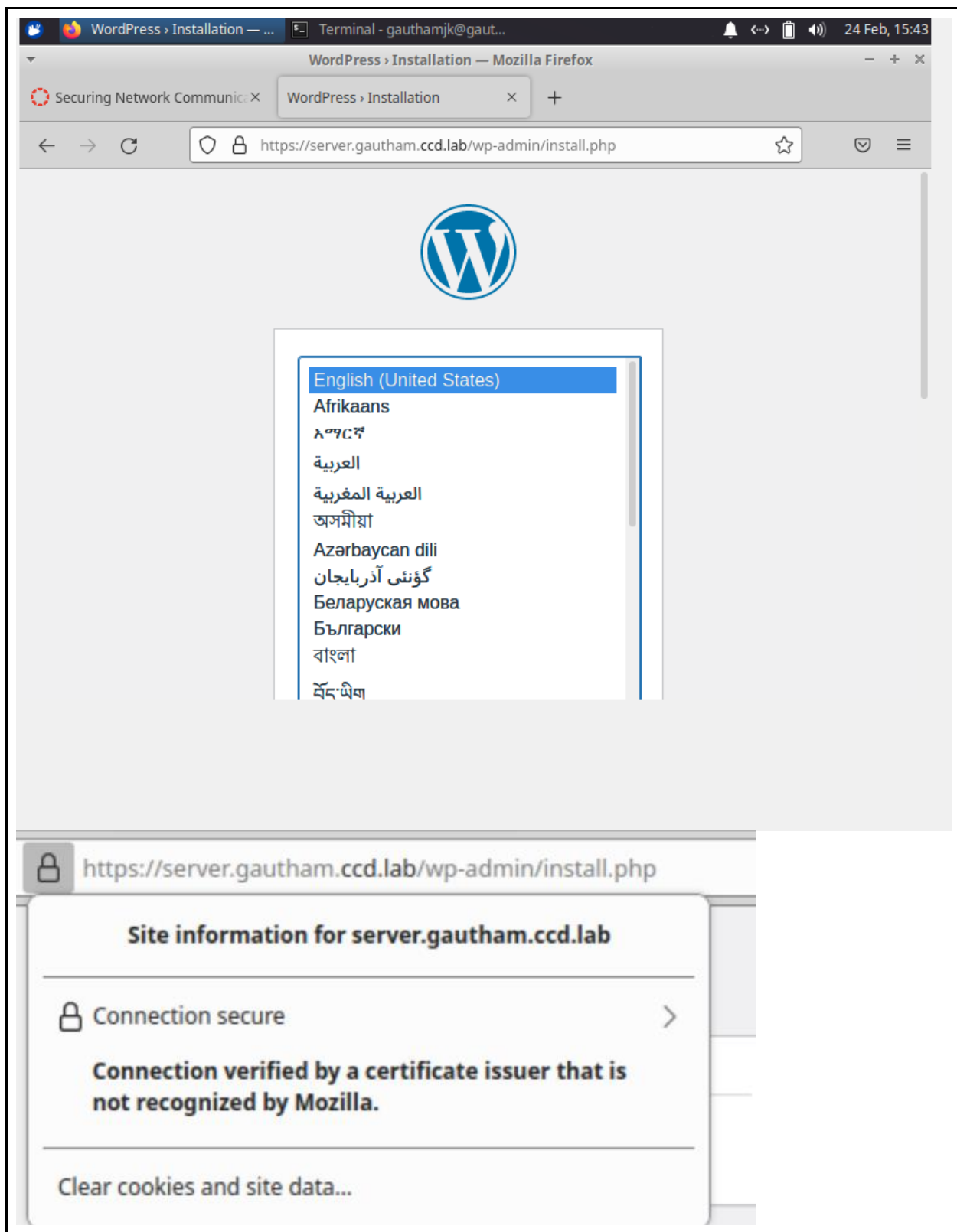
```

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.

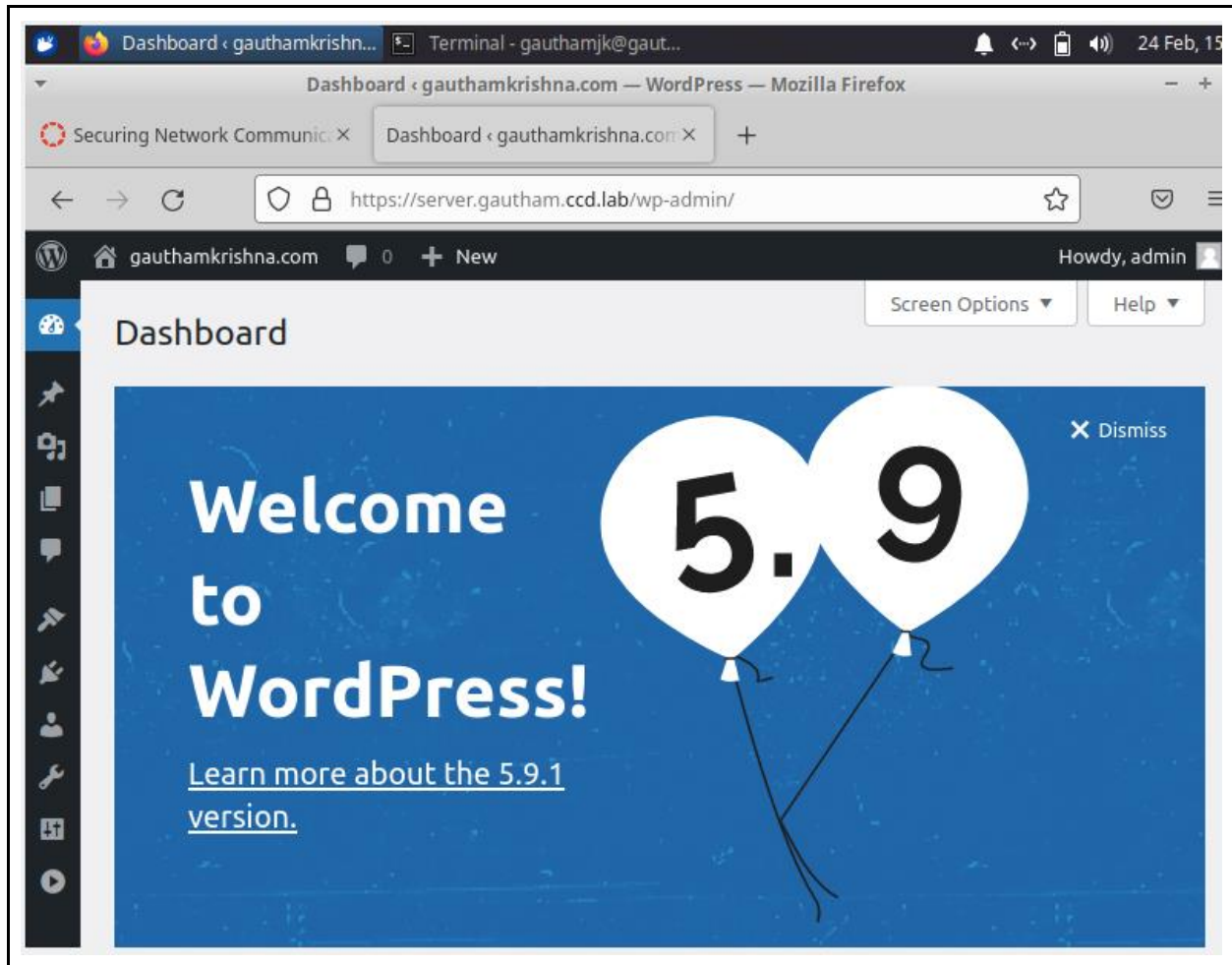
6. Upload a screenshot of your browser window showing a successful TLS connection and the Wordpress setup screen

Next Page





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\_refer= 50% ☆

🔒 📄

gauthamkrishna.com 0 + 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

Profile

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