Dovecot Configuration:

1. Install dovecot-pop3d(Version 2.2.9) on each linux machine
2. Edit the following configuration files in '/etc/dovecot/conf.d folder
    a. 10-ssl.conf (To avoid configuring SSL for dovecot authentication)
        i. Add 'ssl = no '
    b. 10-auth.conf (Enabling authentication with plain text)
        i. disable_plaintext_auth = no
    c. 10-logging.conf (logs username and passwords tried in the format mentioned below)
        i. auth_debug_passwords = yes
    d. 10-mail.conf(configure inbox for successfully logged in users)
        i. mail_location = mbox:~/mail:INBOX=/var/mail/%u
3. Stop dovecot service:
    a. '*doveadm stop*'
4. Start dovecot service:
    a. '*dovecot'*
5. All messages are logged to /var/log/mail.log
6. Log Message Format:
   Apr 1 04:47:21 ip-172-31-18-190 dovecot: auth-worker(28822): pam(apr1,127.0.0.1): pam_authenticate() failed: Authentication failure (password mismatch?) (given password: pass_april)

SSH configuration:

1. Downloaded the source of OPENSSH 6.6.1p1 on each of the VMs.
2. Edited the file auth2-passwd.c in the source directory.
    - Added the following snippet of code at line 75.

```
if(authenticated == 1){
            logit("CSE523 Succesful Authentication attempt using password: %s for %s from
%s port %d",password,authctxt->user,get_remote_ipaddr(),get_remote_port());
      }
      else if(authenticated == 0){
      logit("CSE523 Failed Authentication attempt using password: %s for %s from %s port
%d",password,authctxt->user,get_remote_ipaddr(),get_remote_port());
      }
```

3. In the source directory, build and install as follows
    i. ./configure
    ii. make
    iii. make install
4. This will install the OpenSSH binaries in /usr/local/bin, configuration files in /usr/local/etc, the server in /usr/local/sbin
5. start the server as follows

```
#/usr/local/sbin/sshd &
```

6. Authentication logs are found in /var/log/auth.log
7. Log message format:
   Apr 19 06:51:01 ip-172-31-37-7 sshd[22122]: CSE523 Failed Authentication attempt using password: ketome for root from 43.255.190.92 port 43455 [preauth]

Joomla configuration:

1. Database initialization

mysql -u root -p

- Here we are adding database=joomladb user=joomlauser and password=joomlapassword:
  - *CREATE DATABASE joomladb;*
  - *CREATE USER joomlauser@localhost;*
  - *SET PASSWORD FOR joomlauser@localhost= PASSWORD("joomlapassword");*
- Giving priveleges to the user, here two cases lies if the LAMP is made of Mysql-server:
  - *GRANT ALL PRIVILEGES ON joomladb.* TO joomlauser@localhost IDENTIFIED BY 'joomlapassword';*
- Further moving ahead:
  - *FLUSH PRIVILEGES;*
  - *exit*
- Restart services
  - *service apache2 restart*
  - *service mysql restart*

2. Installation of Joomla

- We will first make a directory temp in which I will the download the latest version of the Joomla as follows:

  mkdir temp
  cd temp
  wget <Joomla download link>
- We need to install unzip as by default it is now installed:

  apt-get install unzip
- Now create a directory /var/www/html/joomla and unzip the Joomla zip file in the newly created folder:

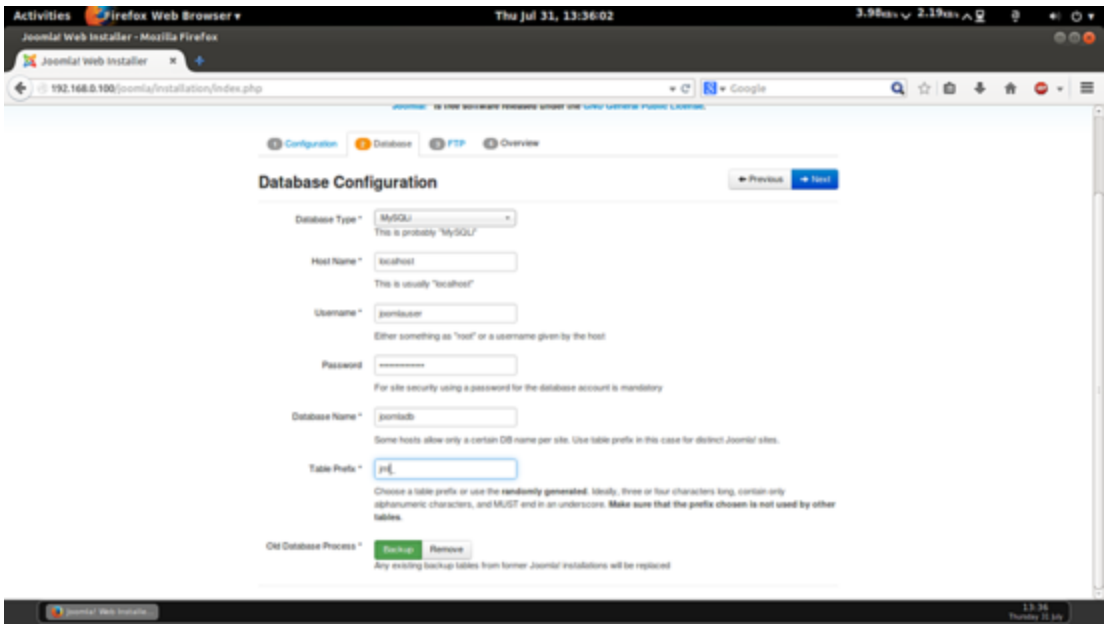
  mkdir -p /var/www/html/joomla
  unzip -q Joomla_3.3.3-Stable-Full_Package.zip -d /var/www/html/joomla
- Now give appropriate permissions in the directory

  chown -R www-data.www-data /var/www/html/joomla
  chmod -R 755 /var/www/html/joomla
- Now proceed to the web installation of Joomla. Go to the URL http://localhost/joomla:

Now give the values as follows

Site Name = joomla_test_site
Description = joomla_test_site
Admin Email = admin@example.com
Admin Username = admin
Admin password = howtoforge
Confirm Admin Password = howtoforge

The above values will differ in you case, you can give any values of your choice. After giving the values press Next:



Further fill the values in next page as you mentioned wile creating the database of the joomla

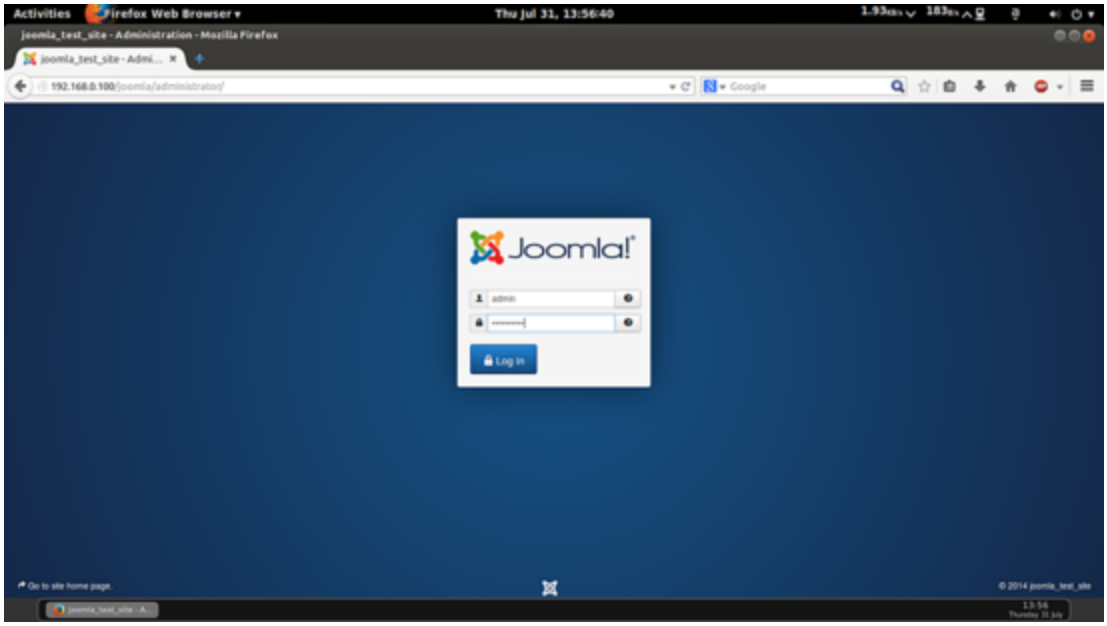
Database Type = MySQLi

hostname = localhost
username = joomlauser
password = joomlapassword
Database Name = joomladb
*Table Prefix = jml_*

For then next tab, select the Brochure English (GB) Sample Data and press Install:

It will install Joomla. Now you need to delete the installation folder by using Remove Installation Folder:

Now you can access the admin panel at http://localhost/joomla/administrator/ give the credentials as you gave at the time of Joomla installation:



In my case values are:
username = admin
password = howtoforge
It will launch the default webpanel of Joomla.

3. **Edited file :** /var/www/html/joomla/plugins/authentication/joomla/joomla.php
Added the following snippet of code at line 72.

```
 $response->status       = JAuthentication::STATUS_SUCCESS;
```

```
                        $response->error_message = '';
                        $honeypot_log = "CSE508_joomla successful login from
IP:".$_SERVER['REMOTE_ADDR']." user:".$credentials['username']."
password:".$credentials['password'];
                        syslog(LOG_INFO, $honeypot_log);
                }
                else
                {
                        // Invalid password
                        $response->status       = JAuthentication::STATUS_FAILURE;
                        $response->error_message =
JText::_('JGLOBAL_AUTH_INVALID_PASS');
                        $honeypot_log = "CSE508_joomla unsuccessful login from
IP:".$_SERVER['REMOTE_ADDR']." user:".$credentials['username']."
password:".$credentials['password'];
                        syslog(LOG_INFO, $honeypot_log);
                }
        }
        else
        {
                // Invalid user
                $response->status       = JAuthentication::STATUS_FAILURE;
                $response->error_message = JText::_('JGLOBAL_AUTH_NO_USER');
                $honeypot_log = "CSE508_joomla unsuccessful login from
IP:".$_SERVER['REMOTE_ADDR']." user:".$credentials['username']."
password:".$credentials['password'];
                syslog(LOG_INFO, $honeypot_log);
        }
```

4. To enable comment box. Downloaded and installed jcomment plugin
5. Logging to /var/log/syslog
6. Log message format:

    Mar 30 16:26:58 localhost apache2: CSE508_joomla unsuccessful login from IP:172.24.16.239 user:sddcs password:dsccs

FTP:

1. We are using the **pure-ftpd** daemon
2. Download the pure-ftpd from http://www.pureftpd.org/project/pure-ftpd/download
3. In function “void dopass(char *password)” the below highlighted code was added to log successful and unsuccessful login attempts at line number 1742 in the file *pure-ftpd-1.0.36/src/ftpd.c*

```
//password copied to pwd since it is cleared more memory later on.
char pwd[100];
memset(pwd, '\0', sizeof(pwd));
strcpy(pwd, password);
authresult = pw_check(account, password, &ctrlconn, &peer);
{
    /* Clear password from memory, paranoia */
    volatile char *password_ = (volatile char *) password;

    while (*password_ != 0) {
        *password_++ = 0;
    }
}
//On unsuccessful Login attempt.
if (authresult.auth_ok != 1) {
    logfile(LOG_INFO, "CSE508_FTP Accessed by UserName: %s and Password: %s and
Auth: Failed", account, pwd);
    tapping++;
    randomsleep(tapping);
    addreply_noformat(530, MSG_AUTH_FAILED);
    doreply();
    if (tapping > MAX_PASSWD_TRIES) {
        logfile(LOG_ERR, MSG_AUTH_TOOMANY);
        _EXIT(EXIT_FAILURE);
    }
    logfile(LOG_WARNING, MSG_AUTH_FAILED_LOG, account);
    return;
}
//On successful login attempt.
else
{
    logfile(LOG_INFO, "CSE508_FTP Accessed by UserName: %s and Password: %s and
Auth: Success", account, pwd);
}
```

4. Authentication logs are found in /var/log/syslog

5. Log Format:
   Apr 27 00:34:44 ip-172-31-37-7 pure-ftpd: (?@de222-089.resnet.stonybrook.edu) [INFO] CSE508_FTP Accessed by UserName: admin and Password: root and Auth: Failed

6. To install the pure-ftpd on your system, use the following commands:
   - To build and install
     ./configure
     make install-strip

- To launch the server, just type the following command:
  /usr/local/sbin/pure-ftpd &

WORDPRESS
The below steps are involved to install the wordpress on your system:

1. Create a MySQL Database and User for WordPress

- Install MySQL Database
  To get started, log into the MySQL root (administrative) account by issuing this command:

  mysql -u root -p

- First, we can create a separate database that WordPress can control. You can call this whatever you would like, but I will be calling it wordpress because it is descriptive and simple. Enter this command to create the database:

  CREATE DATABASE wordpressdb;

- Create a new user
  CREATE USER wpuser@localhost IDENTIFIED BY 'NetSec_508';
- Granting our user account access to our database with this command:

  GRANT ALL PRIVILEGES ON wordpressdb. TO wpuser@localhost*;
  FLUSH PRIVILEGES;

2. Download WordPress

wget http://wordpress.org/latest.tar.gz

sudo apt-get update
sudo apt-get install php5-gd libssh2-php

This will allow you to work with images and will also allow you to install plugins and update portions of your site using your SSH login credentials.

3. Configure WordPress

cd ~/wordpress
cp wp-config-sample.php wp-config.php
nano wp-config.php

- We will need to find the settings for DB_NAME, DB_USER, and DB_PASSWORD in order for WordPress to correctly connect and authenticate to the database we created.
- Fill in the values of these parameters with the information for the database you created. It should look like this:

```
/** The name of the database for WordPress */
define('DB_NAME', 'wordpressdb');

/** MySQL database username */
define('DB_USER', 'wpuser');

/** MySQL database password */
define('DB_PASSWORD','NetSec_508');
```

4. Copy Files to the Document Root

- The location of the document root in the Ubuntu 14.04 LAMP guide is /var/www/html/. We can transfer our WordPress files there by typing:

  sudo rsync -avP ~/wordpress/ /var/www/html/
  cd /var/www/html

You will need to change the ownership of our files for increased security.

*sudo chown -R demo:www-data **

- First, let's manually create the uploads directory beneath the wp-content directory at our document root. This will be the parent directory of our content:

  mkdir /var/www/html/wp-content/uploads

- We have a directory now to house uploaded files, however the permissions are still too restrictive. We need to allow the web server itself to write to this directory. We can do this by assigning group ownership of this directory to our web server, like this:

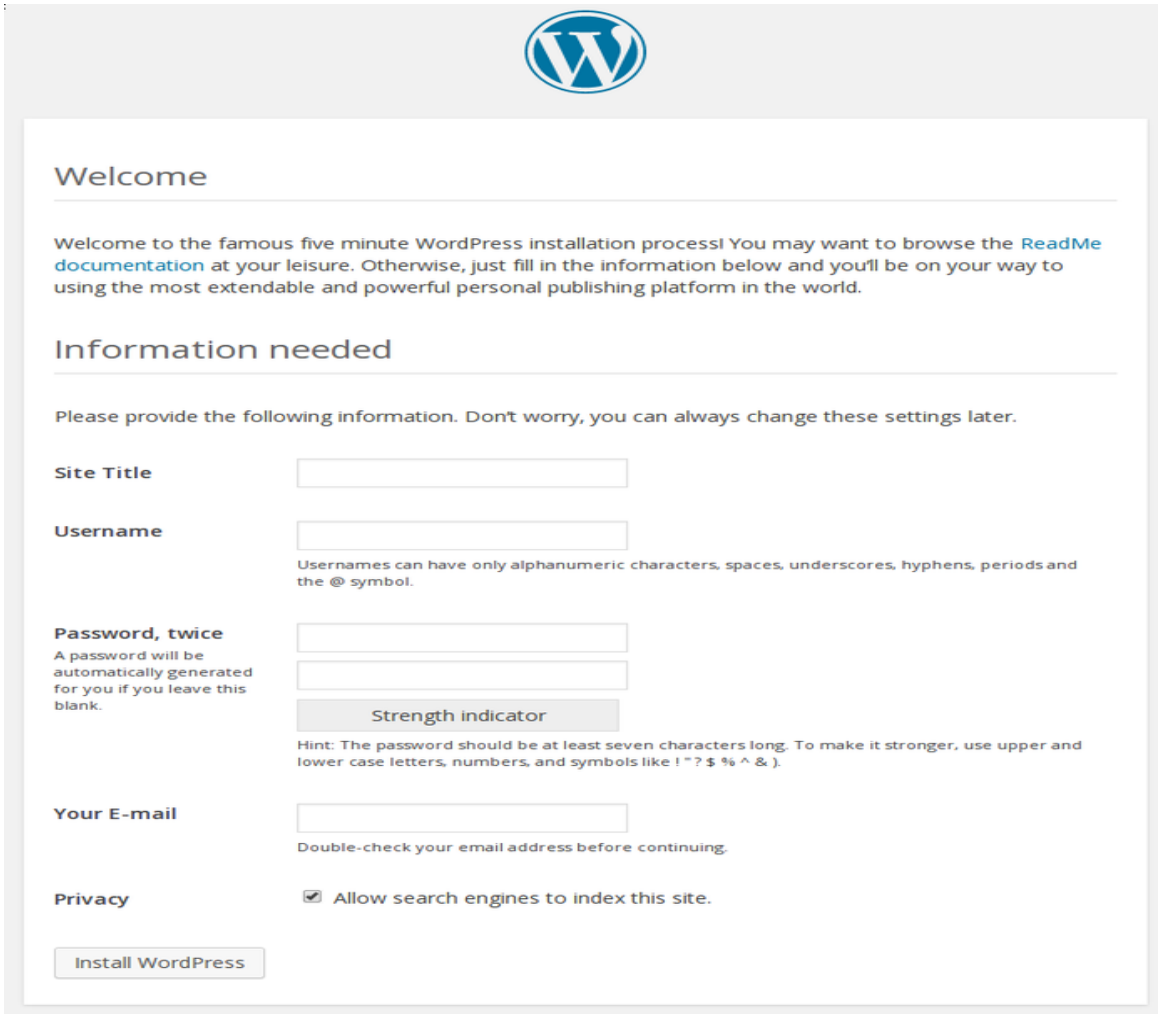
  sudo chown -R :www-data /var/www/html/wp-content/uploads

5. Complete Installation through the Web Interface

In your web browser, navigate to your server's domain name or public IP address:

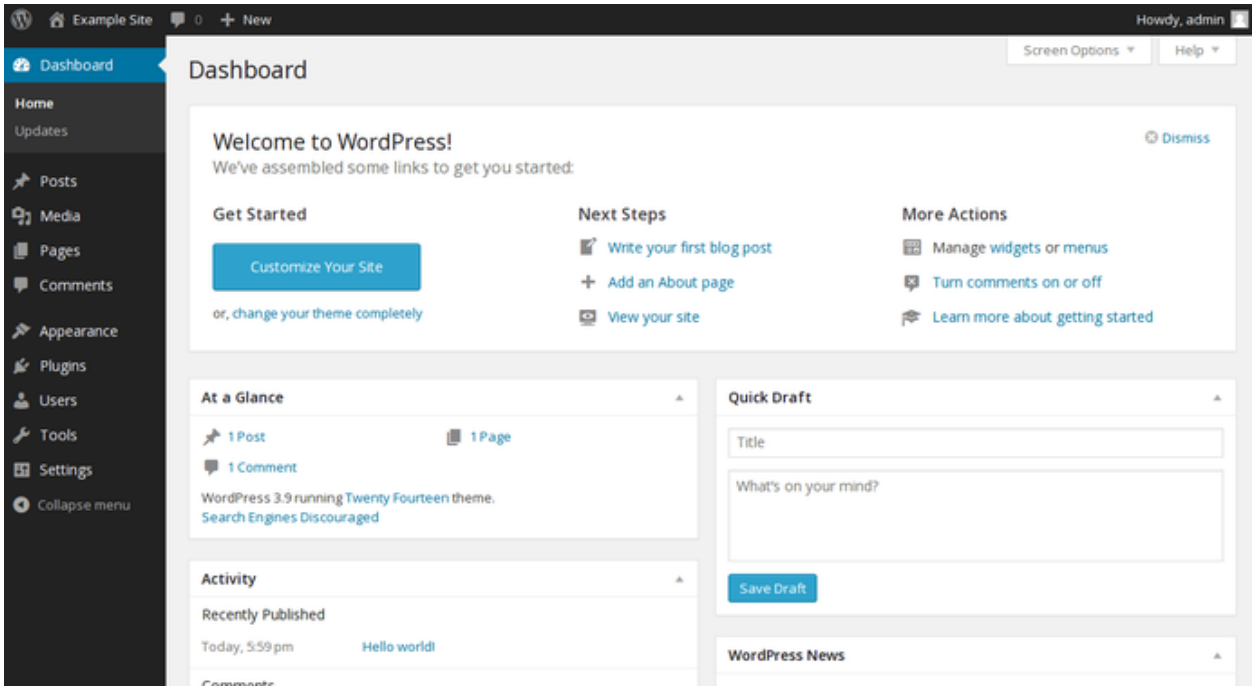
http://server_domain_name_or_IP

You will see the WordPress initial configuration page, where you will create an initial administrator account:



Hit the button at the bottom and then fill out your account information:

You will be presented with the WordPress interface:



6. Code changes to WordPress in the file /var/www/html/wp-login.php at line number 748:

```
//Logging userName and password to syslog
$uName = $_POST['log'];
$passwd = $_POST['pwd'];
$ip = $_SERVER['REMOTE_ADDR'];
if(!empty($uName))
{
syslog(LOG_INFO, "CSE508_wordpress Accessed with UserName: $uName and Password: $passwd from IP:$ip");
}
```

7. Authentication logs are found in /var/log/syslog
8. Log Format:

Apr 27 01:03:07 ip-172-31-37-7 apache2: CSE508_wordpress Accessed with UserName: admin and Password: root123 from IP:130.245.222.89