Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

Purpose: the main aim for this lab for essential to cybersecurity students is to provide hands-on experiences in setting up an SMTP mail server using iRedMail on Kali Linux, while are familiarizing them with the RRs and getting experience with different tools.

Step 1: Sign up for a GitHub student account

To get started, you'll need to sign up for a GitHub student account. You can do this by visiting the GitHub Education page and following the instructions. Once you've signed up, you should be able to access the GitHub Student Developer Pack, which includes a free $50 credit for DigitalOcean.

Step 2: Sign up for a DigitalOcean account

- With your GitHub student account, you can now sign up for a free DigitalOcean account using your student credit. Here's how:
- Go to the DigitalOcean website and click "Sign up" in the top right corner.
- Fill in your information, and make sure to select "GitHub Student Developer Pack" as your promotional code.
- Follow the instructions to verify your account, and you should now have access to your free credit.

Step 3: Create a droplet on DigitalOcean

- Now that you have a DigitalOcean account, you can create a droplet to host your SMTP mail server. Here's how:
- Log in to your DigitalOcean account and click "Create" in the top right corner.
- Select "Droplets" from the dropdown menu.
- Choose a name for your droplet, and select the region closest to you.
- Under "Distributions," select "Ubuntu 20.04" as your operating system.
- Under "Authentication," select "SSH Keys" and add your public key.
- Click "Create Droplet" to create your server.

Step 4: Set up your domain on Namecheap

- To create an SMTP mail server, you'll need a domain name. You can get a free domain name from Namecheap by following these steps:
- Go to the Namecheap website and sign up for an account.
- Use the domain search tool to find a free domain name.
- Follow the instructions to complete your registration and set up your domain.

Sign in to your domain registrar account: Go to your domain registrar's website and sign in to your account.

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

- Access your domain settings: Locate your domain in your account and access its settings. This may be labeled as "Domain Management," "DNS Management," or similar.
- Add MX records: Add an MX (Mail Exchange) record to your domain's DNS settings. The MX record should point to the hostname or IP address of your SMTP mail server. You can usually find this information in the documentation for your mail server software.

- Add SPF records: Add an SPF (Sender Policy Framework) record to your domain's DNS settings. This record specifies which servers are authorized to send email on behalf of your domain. You can usually generate an SPF record using an online tool, such as the SPF Record Generator from EasyDMARC.
- Add DKIM records: Add a DKIM (DomainKeys Identified Mail) record to your domain's DNS settings. This record adds a digital signature to your outgoing email messages, allowing recipients to verify that they were sent by an authorized server. You can usually generate a DKIM record using an online tool, such as the DKIM Record Generator from EasyDMARC.
- Wait for DNS propagation: Once you've added your MX, SPF, and DKIM records, it may take some time for DNS changes to propagate across the internet. This can take anywhere from a few minutes to several hours, depending on your DNS provider.
- Test your setup: Once DNS propagation is complete, you can test your SMTP setup by sending a test email to your own email address. Make sure to check your spam folder, as your email client may mark the message as spam until your SPF and DKIM records have been fully propagated.

Step 5: Install and configure iRedMail on Kali

Now that you have a server and a domain name, you can install and configure iRedMail. Here are the steps:

Connect to your server using SSH.

Run the following command to download the iRedMail installer:

wget https://github.com/iredmail/iRedMail/releases/download/1.4.1/iRedMail-1.4.1.tar.bz2

Extract the files from the archive:

tar xjf iRedMail-1.4.1.tar.bz2

Change to the iRedMail directory:

bash

cd iRedMail-1.4.1/

Run the installer script:

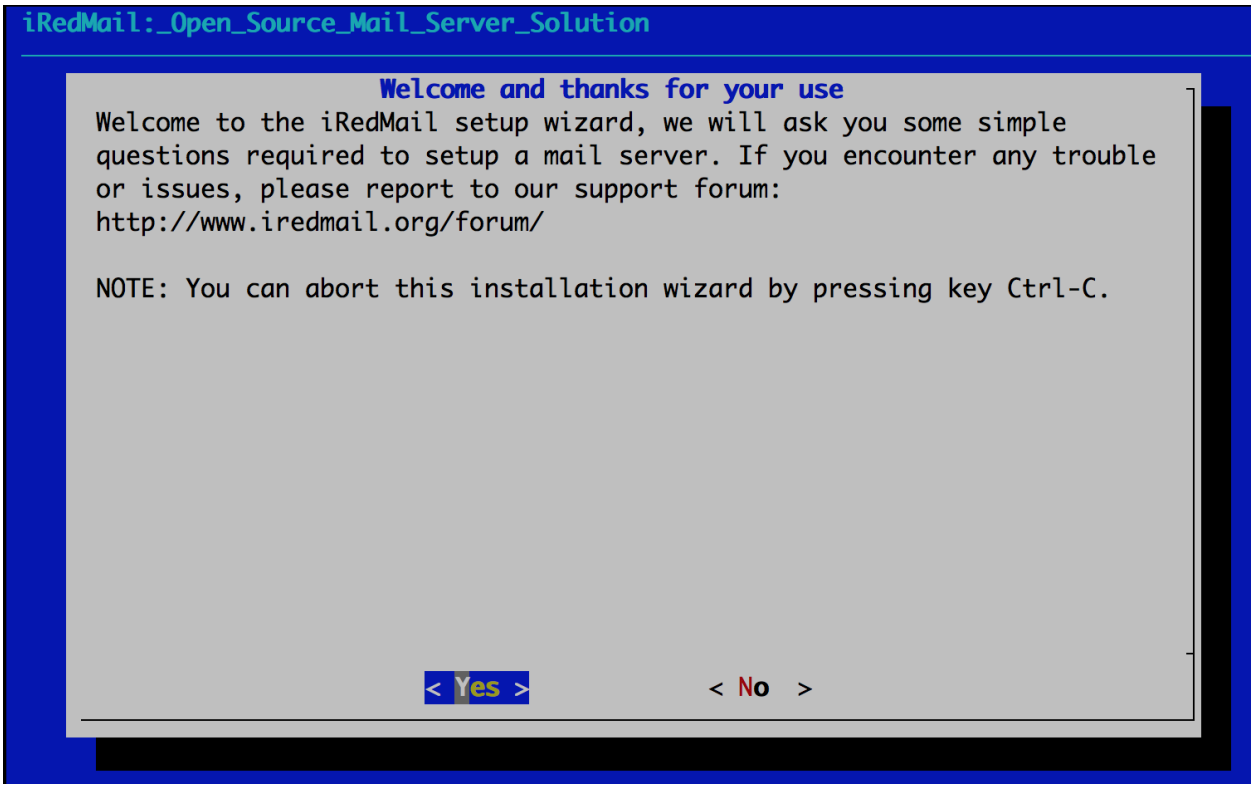
sudo bash iRedMail.sh

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

Follow the prompts to configure iRedMail. When prompted for the hostname, enter your domain name. Make sure to select "OpenLDAP" as the backend.

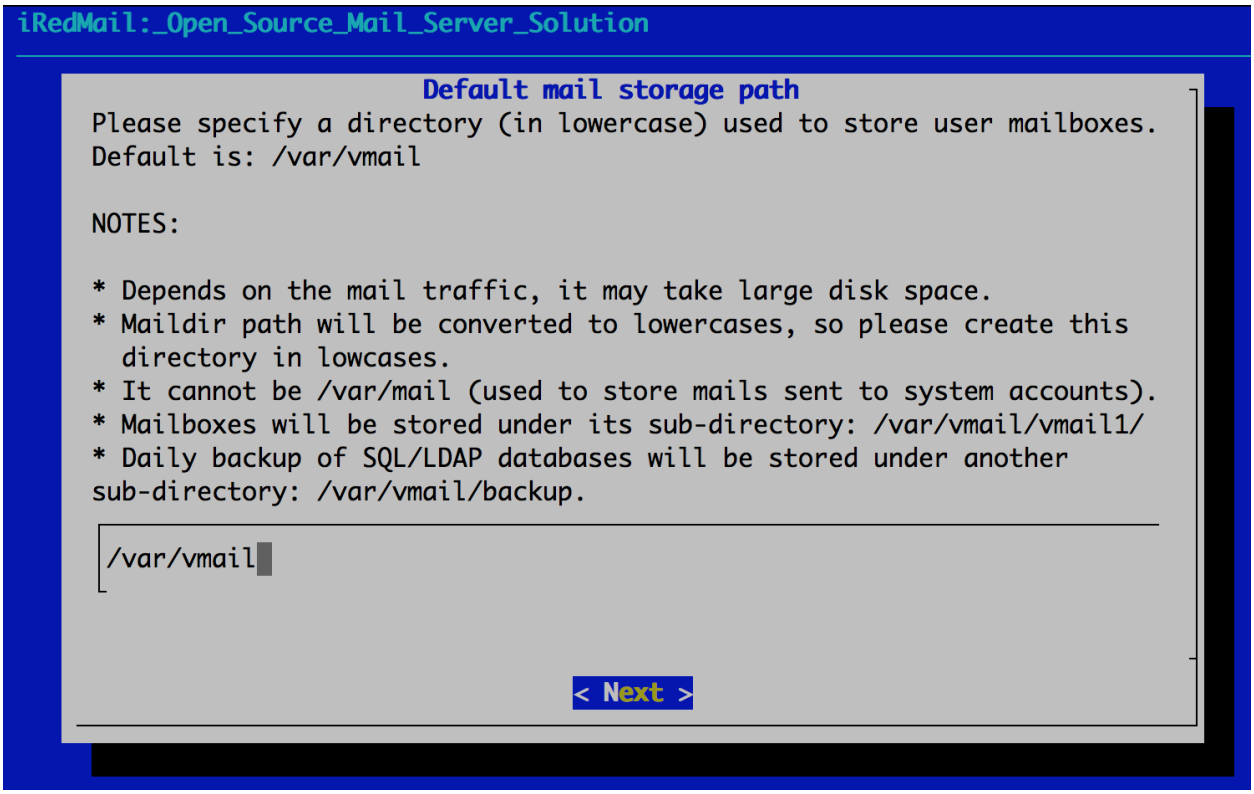
Screenshots of installation:

- Welcome and thanks for your use



- Specify location to store all mailboxes. Default is `/var/vmail/`.

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

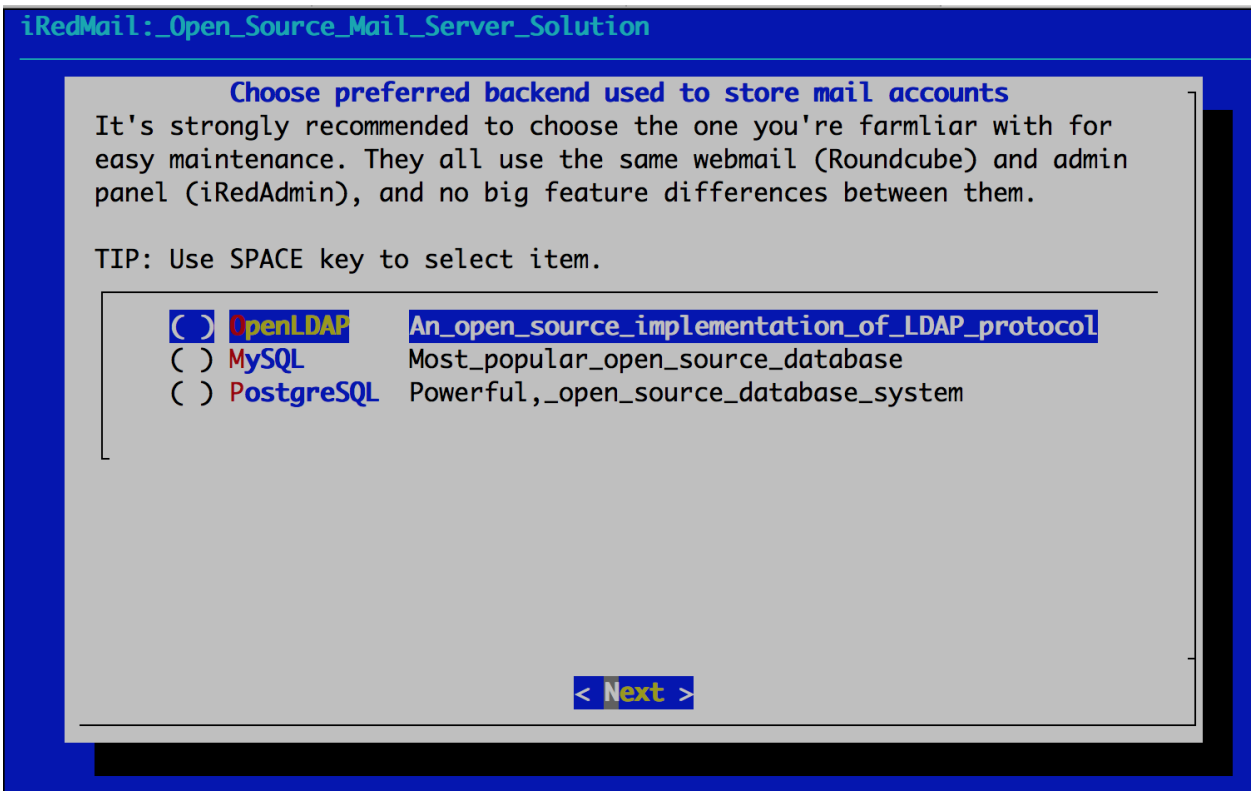


- Choose backend used to store mail accounts. You can manage mail accounts with iRedAdmin, our web-based iRedMail admin panel.

  Note:

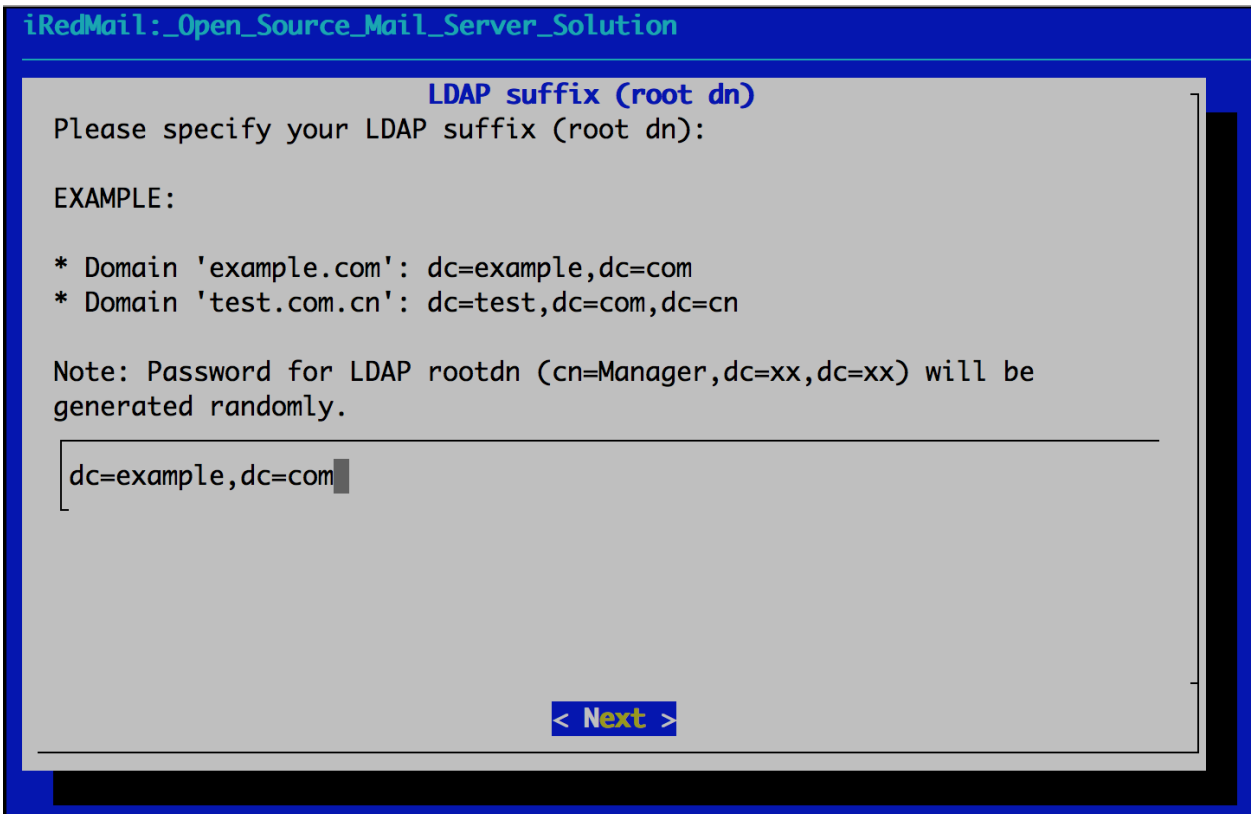
- There's no big difference between available backends, so it's strongly recommended to choose the one you're familiar with for easier management and maintenance after installation.

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs



- If you choose to store mail accounts in OpenLDAP, iRedMail installer will ask to set the LDAP suffix.

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

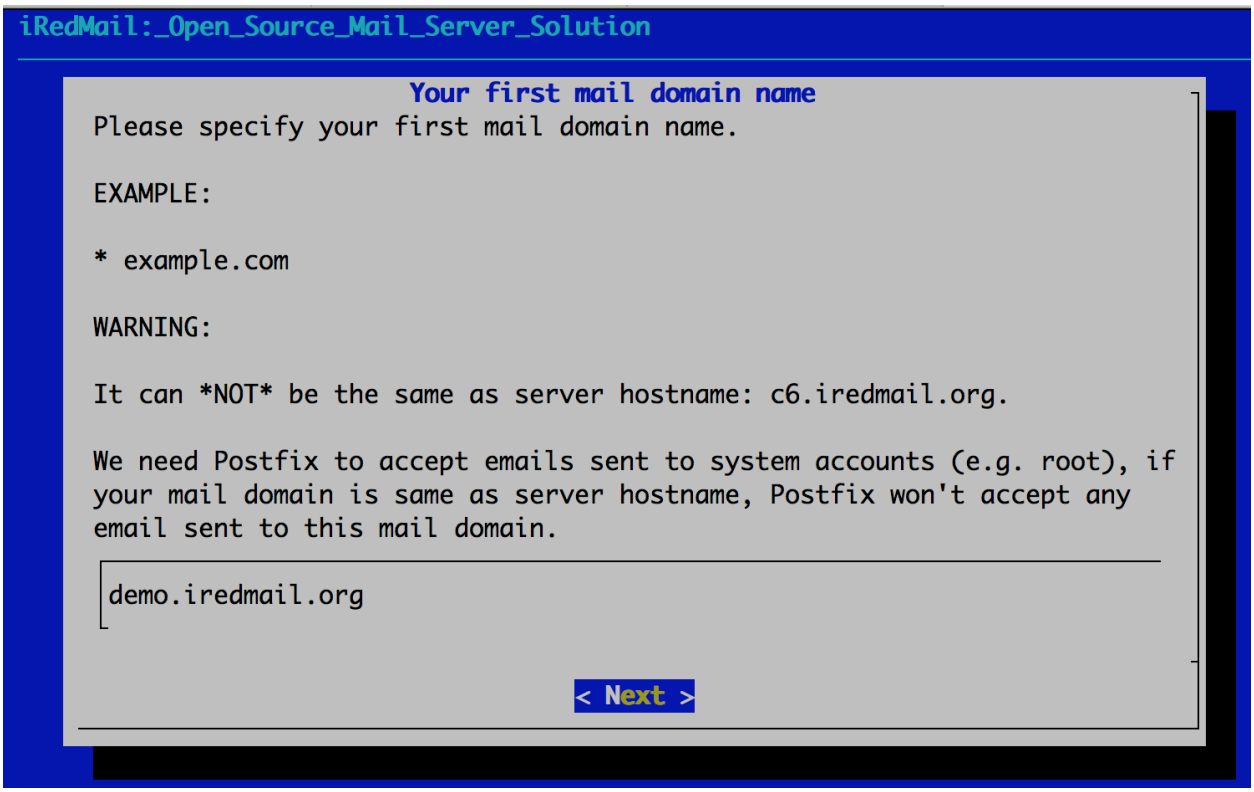


To MySQL/MariaDB/PostgreSQL users

If you choose to store mail accounts in MySQL/MariaDB/PostgreSQL, iRedMail installer will generate a random, strong password for you. You can find it in file `iRedMail.tips`.

- Add your first mail domain name

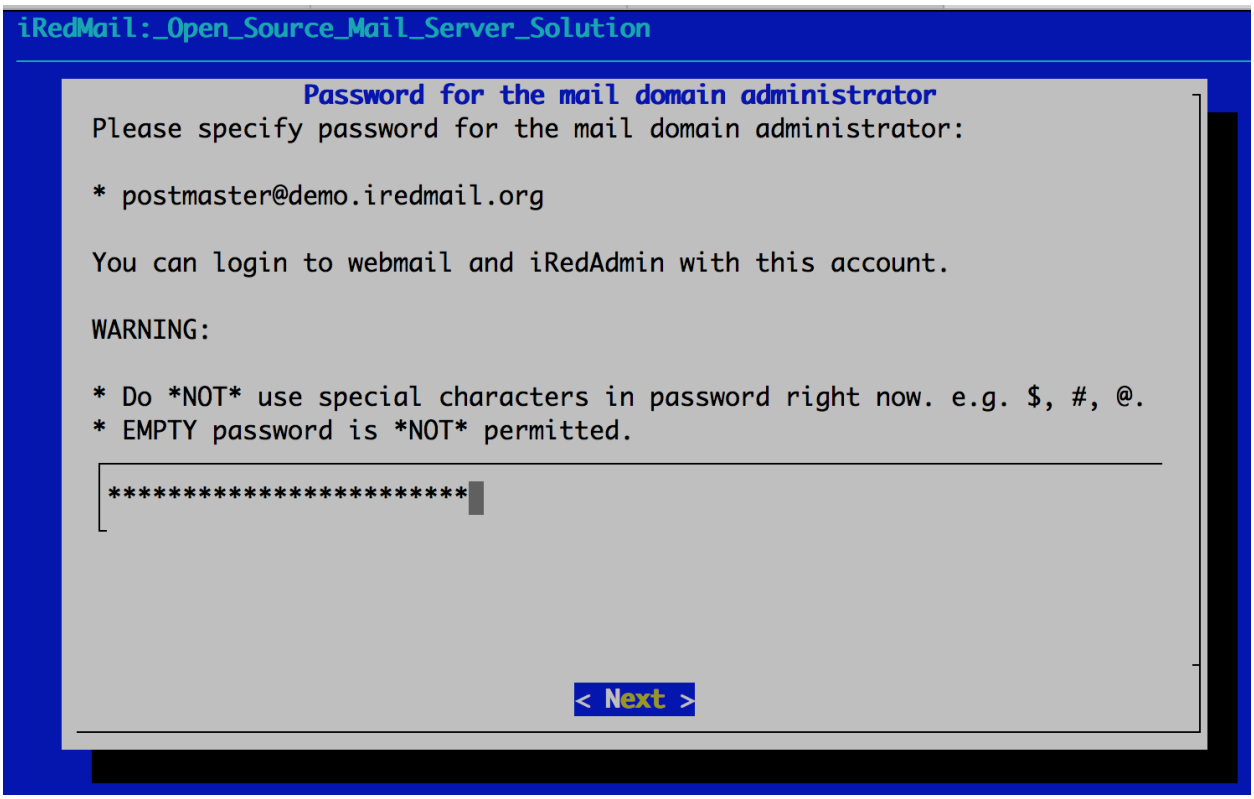
Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs



- Set password of admin account of your first mail domain.

Note: This account is an admin account and a mail user. That means you can login to webmail and admin panel (iRedAdmin) with this account, login username is full email address.

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

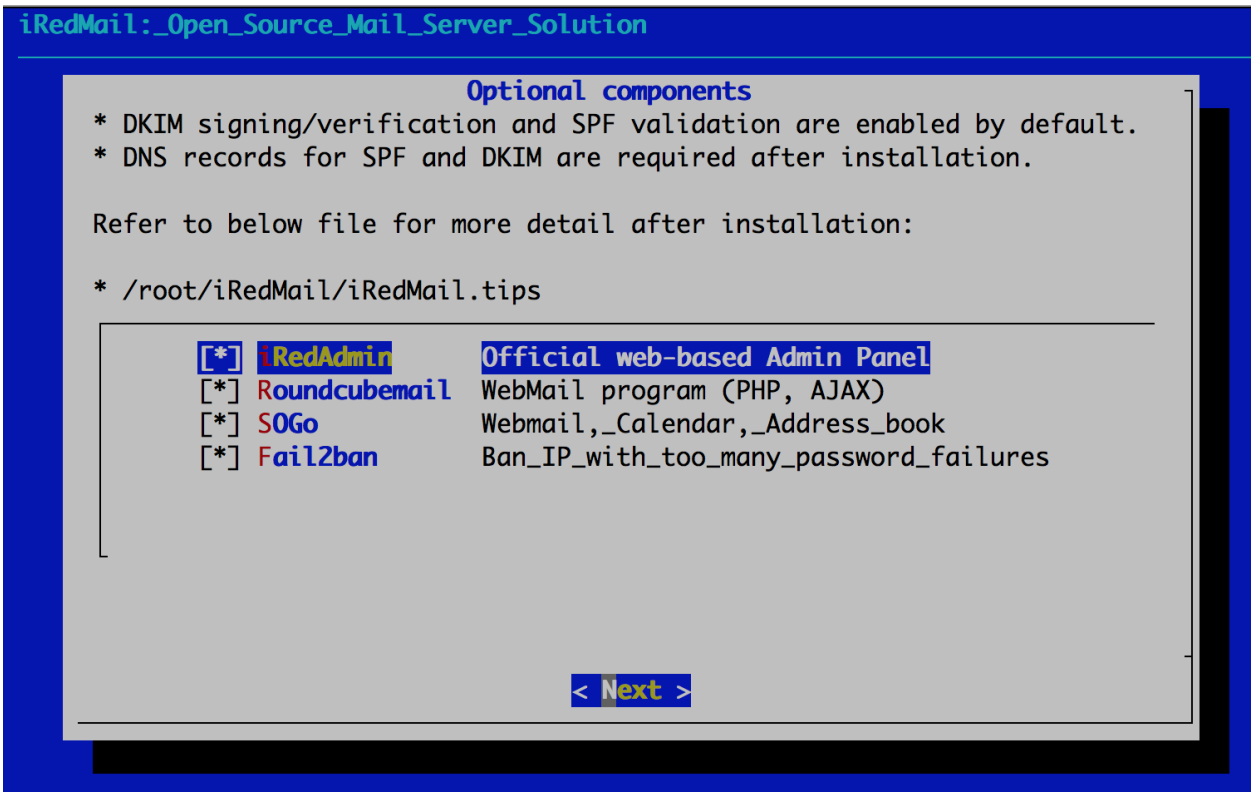


Choose optional components

Which webmail should you choose? Roundcube or SOGo?

- Roundcube is a fast and lightweight webmail, and webmail only. If all you need is a webmail to access mailbox and manage mail filters, then Roundcube is the best option.
- SOGo offers webmail, calendar (CalDAV), contacts (CardDAV) and ActiveSync. If you need calendar and contacts support, also syncing them to mobile or PC mail client applications, then SOGo is the one to go. Note: If you have many ActiveSync clients, it requires a lot RAM.
- It's ok to install both, but you can only manage mail filters with Roundcube in this case, because the filter rules generated by Roundcube and SOGo are not compatible. You can force to enable it in SOGo, but please inform end users and ask them to stick to one of them for managing mail filters.

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs



After answered above questions, iRedMail installer will ask you to review and confirm to start installation. It will install and configure required packages automatically. Type `y` or `Y` and press `Enter` to start.

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

```
*************************************************************************
***************************** WARNING ***********************************
*************************************************************************
*                                                                       *
* Below file contains sensitive infomation (username/password), please  *
* do remember to *MOVE* it to a safe place after installation.         *
*                                                                       *
*   * /root/iRedMail/config                                             *
*                                                                       *
*************************************************************************
********************** Review your settings *****************************
*************************************************************************

* Storage base directory:              /var/vmail
* Mailboxes:                           /var/vmail/vmail1
* Daily backup of SQL/LDAP databases:  /var/vmail/backup
* Store mail accounts in:              MySQL
* Web server:                          Nginx
* First mail domain name:              demo.iredmail.org
* Mail domain admin:                   postmaster@demo.iredmail.org
* Additional components:               "iRedAdmin" "Roundcubemail" "SOGo" "Fail2ban"

< Question > Continue? [y|N]
```

Once the installation is complete, you should be able to access the iRedMail web interface by navigating to https://yourdomain.com/iredadmin/.

Step 6: Configure your mail client.

Finally, you'll need to configure your mail client to send and receive email through your new iRedMail mail server. You can do this using the settings provided by iRedMail, or by following the instructions for your specific mail client.

That's it! You've now created an SMTP mail server using iRedMail on Kali, with a GitHub student account, DigitalOcean, and Namecheap.

References:

https://docs.iredmail.org/install.iredmail.on.debian.ubuntu.html

Lab#2: Designing SMTP MAIL SERVER USING IREDMAIL with its RRs

these questions should be answer by students to ensure that you understand the key concepts and steps involved in setting up an SMTP mail server using IredMail.

1. **Set up your domain on Namecheap**
    a. **Why do you need a domain name to create an SMTP mail server?**
    b. **Explain the purpose of MX, SPF, and DKIM records in the context of email security.**
    c. **What is DNS propagation, and why do you need to wait for it after making DNS changes?**
2. **Install and configure iRedMail on Kali**
    a. **Why is SSH used to connect to the server for installing iRedMail?**
    b. **What is the significance of choosing "OpenLDAP" as the backend for storing mail accounts?**
    c. **Compare and contrast Roundcube and SOGo as webmail options. When would you choose one over the other?**
    d. **What is the importance of reviewing and confirming the installation choices before proceeding?**
3. **Configure your mail client**
    a. **Why is it necessary to configure your mail client after setting up the SMTP mail server?**
    b. **What specific information or settings would you need to configure your mail client to work with the iRedMail server?**