

Group 8

Lab 2: MailServer

We attempted four installation methods were attempted, with one final success. They are

- iRedMail on Digital Ocean (CentOS 7x)
- iRedMail on Digital Ocean (Ubuntu 22.04 LTS)
- Mailinabox on Digital Ocean (Ubuntu 23.0)
- Mailinabox on Digital Ocean (Ubuntu 22.04 LTS)
- Mailinabox on IBM Cloud (Ubuntu 22.04 LTS)

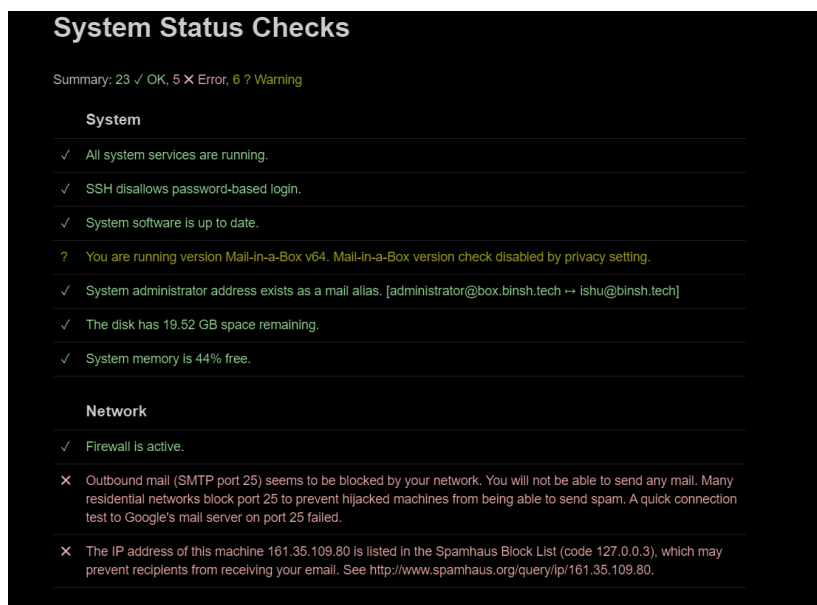
The manual setup is very tedious when using the IRedmail for setting up the mail server. The steps are almost for when it's done on CentOS or Ubuntu only the command 'yum' and 'apt'

For example:

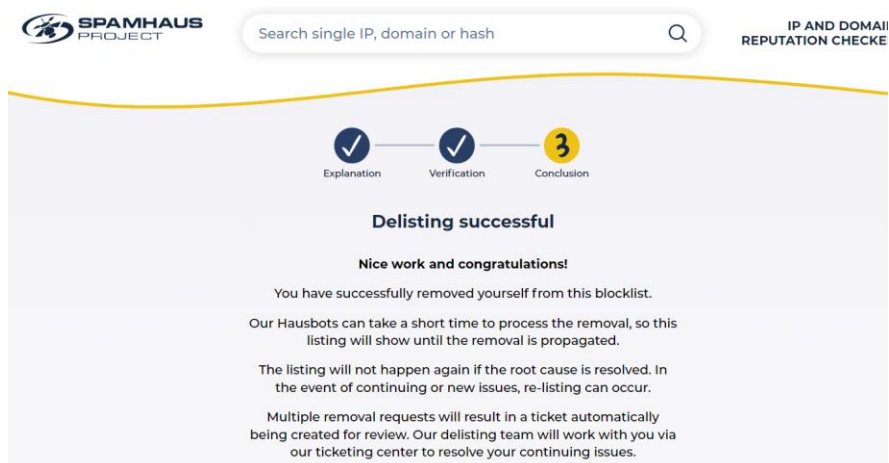
For CentOS: sudo yum update

For Ubuntu: sudo apt update

After that I tried using the mailinabox for server setup with Ubuntu 23x version. Due to the no support of mailinabox for Ubuntu 23 I was not able to properly run the mail server. So, I downgraded to Ubuntu 22 and was able to complete the setup.

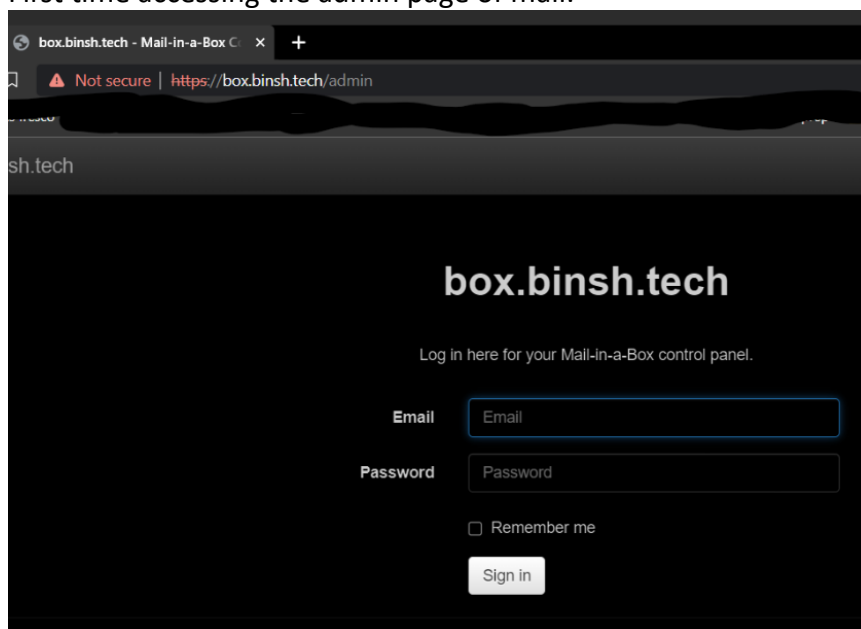


During this process, we found out that the IP addresses assigned to our server is present in one of the block list. We sent a mail to "Spamhaus block list" and got it removed from the block list. I attached the screenshot below which shows our ipaddress is removed from the blacklist success fully.

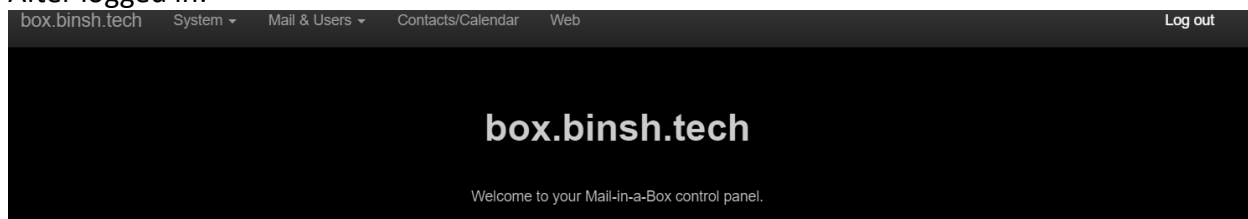


After that I have faced issue with smtp and after doing some research. I got to know that purging the postfix and re-installing the mailinabox fixed the issue.

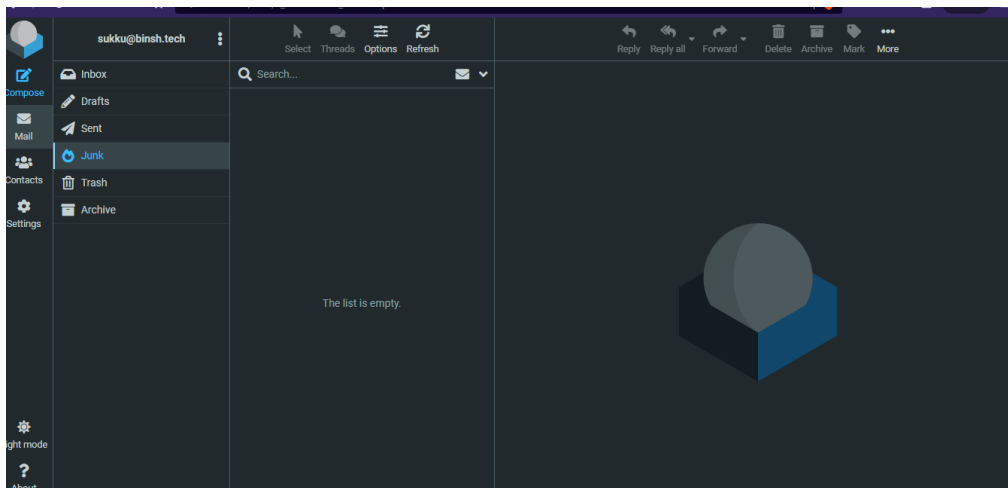
First time accessing the admin page of mail.



After logged in:



Accessing the mail.



I was able to send and receive mails internally between the mails of my own mail server. But unable to send to people who using mails like Gmail, outlook etc., after going through few things and looking over different forums of digital ocean. They have blocked the SMTP port 25 for purpose of reducing the email spams. So, we came to conclusion that the problem is not with the setup of the server but the server provider itself. I have attached the forum link in the reference section as well.

So, next after talking to one of the student (Nicholas). He informed, they have used IBMcloud doing the server setup. And we decided to use IBM Cloud to run our Ubuntu instance, as they did not block port 25 for SMTP protocol. We used the Mailinabox it's easy of installation and setup process.

We used name cheap and hover for getting our domain names. After using them both for the building the mail server. We think Hover has better UI and easy access.

1. Set up your domain on Namecheap.

a. Domain Name Necessity for SMTP Mail Server

I used both Namecheap and Hover and for the IBMcloud I used the hover for buying the domain. The domain name serves as the address for your mail server on the internet which can be used instead of IP addresses which are easy to remember. Without a domain name, the server would only be reachable by its IP address, which is not user-friendly and impractical for widespread use.

b. Purpose of MX, SPF, and DKIM Records

- MX Records (Mail Exchange Records): Directs email to your mail server. Without MX records, other servers won't know where to send emails for your domain.
- SPF Records (Sender Policy Framework): Helps to prevent email spoofing by specifying which mail servers are permitted to send email on behalf of your domain.
- DKIM Records (DomainKeys Identified Mail): Provides a method to validate a domain name identity that is associated with a message through cryptographic authentication.

c. DNS Propagation

After making DNS changes, we need to wait for DNS propagation setup to complete. In some cases it can more than a day to complete. It is the process by which the updated DNS records are spread on internet. It takes long time because the process take time to update their cached information with the new settings from the DNS server for the domain.

2. Install and configure iRedMail on Kali

a. SSH for iRedMail Installation

We used Ubuntu instead of Kali and we used Mailinabox instead of IRedMail. Commands for installing the server are as follows:

```
curl -s https://mailinabox.email/setup.sh | sudo -E bash
```

I added the other required commands link in the reference section.

b. Significance of "OpenLDAP" as Backend

- "OpenLDAP" is the backend for storing mail accounts, because it is an open-source implementation of the LDAP. It's used for directory services, which allows for a centralized database for usernames and passwords.
- In our case the the database is already set by the mailinabox setup. So, It's easy to configure and use it.

c. Roundcube vs. SOGo

- Roundcube: A browser-based IMAP client with an app-like user interface. It's known for its user-friendly design and simplicity.
- SOGo: Provides more than just webmail, including calendar and address book integration, making it suitable for organizations looking for a groupware solution that integrates with other systems.
- In our case we the the NxtCloud client for the interface which is built in the Mailinabox setup

d. Importance of Reviewing Installation Choices

- It is important to review and confirm installation processes to ensure that all configurations are correct before proceeding.
- This step minimizes the risk of errors and potential security vulnerabilities.
- In our case, we found three issues in different stages.
 - Blacklist of the IP address
 - Issue with version of postfix installed in the server.
 - Digital Ocean blocking the SMTP port 25.

3. Configure your mail client

a. Necessity of Mail Client Configuration

After setting up the SMTP mail server, configuring your mail client is necessary to send and receive emails through your server. This process is simplified with the help of Mailinabox, which gives us GUI for setting up the server and configuring the mail server with minimal interaction.

b. Information for Mail Client Configuration

- SMTP server name and port: For sending emails.
- IMAP/POP3 server name and port: For receiving emails.
- Security settings: Such as SSL/TLS for encryption.



We can see from the above screenshot we have TLS certificate signed and validated with TTL as 86 at the time of screenshot taken.

- Authentication credentials: Typically, the email address and password.

box.binsh.tech
System
Mail & Users
Contacts/Calendar
Web

Users

Add a mail user

Add an email address to this system. This will create a new login username/password.

Normal User
Add User

- Passwords must be at least eight characters consisting of English letters and numbers only. For best results, [generate a random password](#).
- Use [aliases](#) to create email addresses that forward to existing accounts.
- Administrators get access to this control panel.
- User accounts cannot contain any international (non-ASCII) characters, but [aliases](#) can.

Existing mail users

Email Address	Actions
binsh.tech	
ishu@binsh.tech	admin (remove privilege) set password archive account
sukku@binsh.tech	set password make admin archive account

Mail user API (advanced)


Use your box's mail user API to add/change/remove users from the command-line or custom services you build.

From the GUI, we can add new users and they can access the mail.

Mail to TA:

Reply
Reply all
Forward
Delete
Archive
Mark
More

Group-8 Mail server



To [aiswaryapalla@my.unt.edu](#), 3 more... on 2023-11-02 11:53

Details
Headers

Hi Karthik,

This is Group -8 form Cybersecurity Essentials class of Monday session..

Regards,
AIswarya. P

Reply form TA:

Re: Group-8 Mail server



From ishu@binsh.tech on 2023-11-03 22:02

[Details](#) [Headers](#) [Plain text](#)

Hello Group 8,

You can take a screenshot of this email and update your submission on canvas.

Regards,

Karthik

On Fri, Nov 3, 2023 at 9:49 PM Aiswarya <ishu@chef.net> wrote:

Hi Karthik,

This is Group -8 form Cybersecurity Essentials class of Monday session..

Regards,

Aiswarya. P

Sample Mail header:

Message headers

Return-Path: <aiswarya.palla6@gmail.com>

Delivered-To: ishu@binsh.tech

Received: from box.binsh.tech ([127.0.0.1])

by box.binsh.tech with LMTP

id nqh6AmWwRWWmuQAAkQqNeg

(envelope-from <aiswarya.palla6@gmail.com>)

for <ishu@binsh.tech>; Fri, 03 Nov 2023 21:45:57 -0500

X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on box.binsh.tech

X-Spam-Level:

X-Spam-Status: No, score=-0.3 required=5.0 tests=DKIM_SIGNED,DKIM_VALID,DKIM_VALID_AU,DMARC_PASS,FREEMAIL_FROM,HTML_MESSAGE,RCVD_IN_DNSWL_NONE,RCVD_IN_MSPIKE_H2,SPF_HELO_NONE,SPF_PASS,T_SCC_BODY_TEXT_LINE autolearn=ham autolearn_force=no version=3.4.6

X-Spam-Report:

- * -0.1 DMARC_PASS DMARC check passed
- * -0.1 SPF_PASS SPF check passed
- * 0.0 SPF_HELO_NONE SPF: HELO does not publish an SPF Record
- * 0.0 FREEMAIL_FROM Sender email is commonly abused enduser mail provider
- * [[aiswarya.palla6\[at\]gmail.com](mailto:aiswarya.palla6[at]gmail.com)]
- * 0.0 HTML_MESSAGE BODY: HTML included in message
- * 0.1 DKIM_SIGNED Message has a DKIM or DK signature, not necessarily

Reference:

- <https://www.digitalocean.com/community/questions/outbound-mail-smtp-port-25-seems-to-be-blocked-by-your-network-mail-in-a-box>
- <https://discourse.mailinabox.email/t/incoming-mail-smtp-postfix-is-not-running-port-25-after-upgrade-to-0-40/4340/3>
- <https://mailinabox.email/>
- <https://mailinabox.email/maintenance.html#upgrade>