

Build the Recipient Tracing Lab

From an empty VM to five verified deliveries

Technologies, commands, checkpoints and evidence export

Architecture and technologies	02
Hyper-V and Ubuntu installation	03-04
SSH and local mail service	05-07
Recipients and message preparation	08-09
Submission and recipient tracing	10-11
Evidence export and verification	12
Troubleshooting and references	13

Abdellah Bayar

SOC LAB PORTFOLIO

5 October 2026

What you will build

A local SMTP experiment with observable delivery outcomes and reproducible evidence.

Create an Ubuntu VM on Windows, configure Postfix for local delivery, and send one harmless email to five accounts. Then investigate Alice's copy and reconstruct all successful recipients from the server log.

Technology	What it does
Hyper-V / Ubuntu Server	Provide the virtual machine and Linux operating system.
Postfix / SMTP	Accept a message with a sender and five delivery recipients; route it to local mailboxes.
Swaks	Prepare the message and expose the SMTP conversation.
Maildir / rsyslog	Store received messages as files and record server events.
SSH / SCP	Run Linux commands from Windows and copy the evidence back.
grep / SHA-256	Search the evidence and verify that exported bytes match.

Prerequisites and boundaries

Use a Windows host with Hyper-V available, hardware virtualization enabled, at least 4 GB of RAM available for the VM, and space for a 40 GB virtual disk. Internet access is needed to obtain the Ubuntu ISO and packages. No Microsoft 365 tenant or paid mail service is required.

LAB FLOW

```
Windows PowerShell --SSH--> Ubuntu VM
Swaks --127.0.0.1:25--> Postfix --> five Maildirs
|
+--> /var/log/mail.log
```

Use your own run values. A new run produces different timestamps, Message-IDs, queue IDs and mailbox filenames. The analysis PDF describes the reference run; use the identifiers generated by your reproduction.

Create the Hyper-V VM

Run these steps on the Windows host, using Hyper-V Manager.

- 1 Download Ubuntu Server.** Use the official Ubuntu 24.04 LTS release page linked on page 13. The reference run used 24.04.5; a later point release may show different package versions.
- 2 Start the VM wizard.** In Hyper-V Manager, select the host, then New > Virtual Machine. Give the new machine its own virtual disk.

Setting	Lab value
Name	SOC-Mail-Lab
Generation	Generation 2
Startup memory	4096 MB; disable Dynamic Memory for this configuration
Virtual processors	2; set in Settings after creating the VM
Network connection	Default Switch
Virtual hard disk	New 40 GB VHDX
Installation media	Downloaded Ubuntu Server ISO
Secure Boot	Enabled; template: Microsoft UEFI Certificate Authority

- 3 Set the Linux Secure Boot template.** Open VM Settings > Security and select Microsoft UEFI Certificate Authority. This is the Linux template documented by Microsoft.
- 4 Start the installer.** Connect to the VM and start it. If prompted to boot from the virtual DVD, press a key. Choose the standard Ubuntu Server installation.

Checkpoint: the Ubuntu Server installer opens inside the SOC-Mail-Lab VM. The disk used for this lab is the new 40 GB virtual disk created in the wizard.

Install Ubuntu Server

These choices reproduce the reference environment without adding a desktop interface.

Installer screen	Selection
Language and keyboard	Choose the layout that matches the keyboard you will use.
Type of installation	Ubuntu Server; standard installation.
Network	Use DHCP on eth0. Record the IP later; it may change.
Proxy / archive mirror	Leave the proxy blank; continue after the archive mirror test succeeds.
Storage	Use the new 40 GB virtual disk. For the reference layout, deselect LVM and leave encryption off.
Profile	Hostname: soc-mail-lab. Username: labadmin. Choose a password and keep it private.
Ubuntu Pro	Skip for now.
SSH configuration	Install OpenSSH Server; allow password authentication for this local lab.
Featured server snaps	Leave them unselected.

Finish and reboot

Wait for Installation complete, then select Reboot Now. If the console asks to remove the installation medium, eject the virtual DVD using Media > DVD Drive > Eject, or set the DVD media to None in the VM settings. Return to the console and press Enter.

Storage confirmation: formatting applies to the selected virtual disk. Check that the summary shows the lab's new 40 GB disk before confirming. The reference layout used ext4 for / and FAT32 for /boot/efi.

After reboot, sign in as labadmin. Linux does not display characters while you type a password. A successful login ends at a shell prompt such as labadmin@soc-mail-lab:~\$.

Connect through SSH

Use Windows Terminal to control the VM without typing in the Hyper-V console.

First, in the VM console

UBUNTU VM CONSOLE

```
whoami
hostname -I
```

Expect whoami to return labadmin. Record the IPv4 address shown by hostname -I. Hyper-V's Default Switch assigns this address dynamically; use the current value.

Then, on the Windows host

WINDOWS POWERSHELL - REPLACE YOUR_VM_IP

```
ssh labadmin@YOUR_VM_IP
```

On the first connection, SSH displays the server's host key fingerprint. To verify it, run the following command in the VM console and compare the fingerprint for the key type shown by SSH:

UBUNTU VM CONSOLE - ED25519 FINGERPRINT

```
sudo ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub
```

If the client shows a different key type, check the matching public host key file in /etc/ssh. After confirming the match, accept the host key and enter the password created during installation.

Where you type	What the prompt means
PS C:\...>	Windows PowerShell on the host. Use it for ssh and scp.
labadmin@soc-mail-lab:~\$	Linux shell inside the VM. Use it for all following mail setup and investigation commands.

Checkpoint: the Windows Terminal tab shows labadmin@soc-mail-lab. SSH connects over the VM's network address; the SMTP test later connects to loopback inside that same VM.

Install the mail tools

Run the Linux commands in the SSH session connected to the Ubuntu VM.

UBUNTU SSH SESSION

```
sudo apt update
sudo apt install postfix rsyslog swaks
```

apt update refreshes the package list. apt install adds the mail server, log service and SMTP testing tool. Enter the labadmin password when sudo requests it; confirm the package installation when prompted.

Postfix installation choices

Prompt	Choose
General mail configuration type	Local only
System mail name	lab.test

Local only is appropriate for this experiment: messages are handled for local accounts, and Postfix listens on the VM's loopback interface. lab.test is the address domain used by the five test recipients.

Check the service and versions

UBUNTU SSH SESSION

```
sudo systemctl enable --now rsyslog
sudo systemctl status postfix --no-pager
postconf mail_version
swaks --version
```

Checkpoint: the installation completes and Postfix is running. The reference run used Postfix 3.8.6 and Swaks 20240103.0. Record the versions installed on your own VM.

If Postfix was already installed with different settings, run `sudo dpkg-reconfigure postfix` and select Local only with lab.test. Verify the resulting configuration on the next page.

Configure local delivery

Maildir stores each received message in a separate file under the recipient's home directory.

UBUNTU SSH SESSION

```
sudo postconf -e 'home_mailbox = Maildir/'
sudo systemctl restart postfix
postconf mydestination inet_interfaces default_transport \
    home_mailbox mailbox_command
```

Setting	Expected value or condition
mydestination	Includes lab.test and the local host names.
inet_interfaces	loopback-only
default_transport	error
home_mailbox	Maildir/
mailbox_command	Empty

mydestination defines domains handled as local mail. The Maildir/ setting selects file-based mailbox delivery. The error transport prevents this lab from delivering to external domains. Confirm these values before sending the test.

Verify logging and the listener

UBUNTU SSH SESSION

```
sudo tail -n 10 /var/log/mail.log
sudo ss -ltnp 'sport = :25'
```

The log should contain Postfix service events. The SMTP listener should be on 127.0.0.1:25 and, if enabled, [::1]:25. It should not listen on every interface (0.0.0.0 or [::]) for this setup.

Checkpoint: Maildir delivery is enabled, mail.log exists and SMTP is restricted to loopback. Stop here and correct any mismatch before continuing.

Create five recipients

Local Linux accounts provide the mailboxes used in the experiment.

UBUNTU SSH SESSION - FRESH VM

```
sudo useradd -m -s /usr/sbin/nologin alice
sudo useradd -m -s /usr/sbin/nologin bob
sudo useradd -m -s /usr/sbin/nologin carol
sudo useradd -m -s /usr/sbin/nologin edoardo
sudo useradd -m -s /usr/sbin/nologin vittorio
getent passwd alice bob carol edoardo vittorio
```

The -m option creates each home directory. The nologin shell prevents interactive login for these recipient accounts while local mail delivery can still use their homes. Maildir folders appear on the first successful delivery. If a lab account already exists, keep it and skip its creation command.

Address	Visible in message headers
alice@lab.test	To
bob@lab.test	Cc
carol@lab.test	Absent; envelope recipient only
edoardo@lab.test	Cc
vittorio@lab.test	Absent; envelope recipient only

Create a folder for this run

UBUNTU SSH SESSION

```
mkdir ~/recipient-tracing-run
cd ~/recipient-tracing-run
```

Checkpoint: getent lists all five accounts and their home directories. Use a different working folder name if this example already exists, so the next run does not overwrite earlier evidence.

Prepare the test message

Generate a harmless plain-text email without transmitting it yet.

UBUNTU SSH SESSION - IN THE WORKING FOLDER

```
swaks --server 127.0.0.1 --port 25 \  
  --from labadmin@lab.test \  
  --to alice@lab.test,bob@lab.test,carol@lab.test,edoardo@lab.test,vittorio@lab.test \  
  --header 'To: alice@lab.test' \  
  --header 'Cc: bob@lab.test, edoardo@lab.test' \  
  --header 'Subject: [SOC-LAB] Recipient tracing test 02' \  
  --body 'Controlled lab message for recipient tracing. No action is required.' \  
  --dump-mail | tee message.eml
```

Option	Purpose
--to	Supplies the five SMTP envelope recipients when this message is sent.
--header To / Cc	Controls the visible recipient fields inside the message.
--body	Sets the harmless message content.
--dump-mail / tee	Prints the generated email without sending it, and saves those bytes to message.eml.

Record the generated Message-ID

UBUNTU SSH SESSION

```
grep -i '^Message-ID:' message.eml  
grep -ic '^Message-ID:' message.eml
```

The second command should print 1. Record the complete identifier from the first command, including the < and > characters. Let Swaks generate it automatically; do not add another Message-ID header.

Checkpoint: message.eml contains one Message-ID, Alice in To, Bob and Edoardo in Cc, and the benign body. Carol and Vittorio are omitted from the visible fields by design.

Send and inspect the message

Submit the prepared file, then start the investigation from Alice's received copy.

UBUNTU SSH SESSION - IN THE WORKING FOLDER

```
swaks --server 127.0.0.1 --port 25 \  
  --from labadmin@lab.test \  
  --to alice@lab.test,bob@lab.test,carol@lab.test,edoardo@lab.test,vittorio@lab.test \  
  --data @message.eml \  
  2>&1 | tee smtp-session.txt
```

Confirm that five RCPT TO commands receive successful responses and the final DATA response says 250 ... queued as followed by a queue ID. Save that ID. The transcript records server acceptance; check delivery separately.

Locate Alice's copy

Replace YOUR_MESSAGE_ID with your complete generated identifier, including angle brackets. Keep the single quotes shown in the commands.

UBUNTU SSH SESSION - REPLACE BOTH PLACEHOLDERS

```
sudo grep -rIF 'YOUR_MESSAGE_ID' /home/alice/Maildir/  
sudo cat 'PATH_RETURNED_BY_SEARCH'
```

In the second command, replace PATH_RETURNED_BY_SEARCH with the actual matching path from the first command. Inspect Delivered-To, To, Cc, Message-ID and Received. In this setup, the visible fields identify three distinct recipients.

Checkpoint: Alice's received copy contains your Message-ID, and its Received header contains the queue ID reported by the SMTP server. The server-added headers identify local delivery to Alice.

The message Date reflects preparation time. Use the server's Received timestamp and delivery log records for the actual submission and delivery timeline.

Trace every delivered recipient

Use the received message's identifiers to connect the mailbox evidence with server events.

UBUNTU SSH SESSION - REPLACE THE IDENTIFIERS

```
sudo grep -F 'message-id=YOUR_MESSAGE_ID' /var/log/mail.log
sudo grep -F 'YOUR_QUEUE_ID:' /var/log/mail.log \
| tee delivery.log
```

The first command finds the cleanup event linking your Message-ID to a queue ID. In the second command, replace YOUR_QUEUE_ID with that identifier, keeping the colon. Use the records from this test's time window if an older run shares an identifier.

Record or field	Read it as
cleanup / message-id	The connection between message headers and the server queue.
qmgr / nrcpt	Number of queued envelope recipients.
local / to=<address>	A delivery attempt for that particular local recipient.
status=sent (delivered to maildir)	Successful delivery to the local recipient mailbox.
status=deferred / bounced	A delayed or failed outcome requiring investigation.
qmgr / removed	Queue processing finished; not deletion from a mailbox.

List the distinct successful addresses

UBUNTU SSH SESSION

```
grep -F 'status=sent (delivered to maildir)' delivery.log \
| sed -n 's/.*to=<([^\>]*)>.*\1/p' \
| sort -u | tee delivered-recipients.txt
wc -l < delivered-recipients.txt
```

Expected result: five distinct addresses, including Carol and Vittorio. Compare this list with Alice's To and Cc. Report the observed delivery outcomes if your result differs; delivery does not establish opening or clicking.

Preserve and export evidence

Keep the original mailbox file intact and verify the bytes of the exported copies.

From the working folder, copy Alice's matching mailbox file using the path found on page 10. The copy is owned by labadmin with restricted permissions.

UBUNTU SSH SESSION - IN THE WORKING FOLDER

```
sudo install -o labadmin -g labadmin -m 600 \  
  'PATH_RETURNED_BY_SEARCH' alice-received.eml \  
sha256sum message.eml alice-received.eml \  
  smtp-session.txt delivery.log > evidence.sha256 \  
sha256sum -c evidence.sha256
```

All four checks should report OK. Editing the evidence or changing its line endings changes its SHA-256 hash.

Copy the run to Windows

Open a new Windows PowerShell tab. Use the current VM address and your working folder name. This command exports the run into your Windows Documents folder:

WINDOWS POWERSHELL

```
scp -r "labadmin@YOUR_VM_IP:/home/labadmin/recipient-tracing-run" \  
  "$env:USERPROFILE\Documents"
```

The final backtick continues the command on the next line. Enter the VM password when prompted. Keep each run in its own folder.

Verify an exported file

WINDOWS POWERSHELL

```
$runFolder = "$env:USERPROFILE\Documents\recipient-tracing-run" \  
Get-FileHash -Algorithm SHA256 -LiteralPath \  
  "$runFolder\alice-received.eml"
```

Compare the hash with the alice-received.eml entry in evidence.sha256; letter case is irrelevant. Repeat for the other three evidence files.

Checkpoint: all evidence files and their checksums are on Windows. Preserve their bytes when sharing them.

Troubleshooting and completion

Use the relevant check below, then repeat only the step affected by the issue.

Issue	Check or correction
Ubuntu does not boot	Confirm the ISO is attached and the Linux Secure Boot template is selected.
SSH cannot connect	Check hostname -I in the VM, confirm OpenSSH is running with <code>sudo systemctl status ssh</code> , and use the current address.
Permission denied at login	Use labadmin and the installation password. Check the keyboard layout. Password input is invisible.
No <code>/var/log/mail.log</code>	Confirm rsyslog is active, restart Postfix, and check Ubuntu's mail logging configuration. A journal-only system needs a log export appropriate to that setup.
SMTP connection refused	Check Postfix status and the loopback port 25 listener. Run Swaks inside the VM.
Recipient rejected / no Maildir	Check the account exists and lab.test is in mydestination. Maildir appears after the first successful local delivery.
No identifier match / wrong count	Use the current run's Message-ID and queue ID, check the time window, and inspect each delivery outcome.

Completion check

A complete reproduction has one message identifier, one matched queue, five distinct successful local deliveries, and two delivered recipients absent from To and Cc. Preserve the native files and report any differences from the reference run.

Official references

[Ubuntu 24.04 LTS releases](#) - installation ISO

[Ubuntu Server installation](#) - installer workflow

[Microsoft: Generation 2 VM security](#) - Linux Secure Boot template

[Ubuntu Server: Postfix](#) - Maildir and logs

[Swaks reference](#) - dump-mail, data and header options

[OpenSSH: SCP manual](#) - file export over SSH