CSE 127 Week 9 Discussion

Recap

List of tools you might need to use:

- ssh - Connect to servers over shell
- tcpdump - View network traffic on machine
- nmap - Scan ports/IPs (locally and externally)
- nc - Allows you to make connections locally
- wget - Download files from the internet

Final Goal:

Download a token somewhere

Be careful: submit the last token you download

Email Spoofing

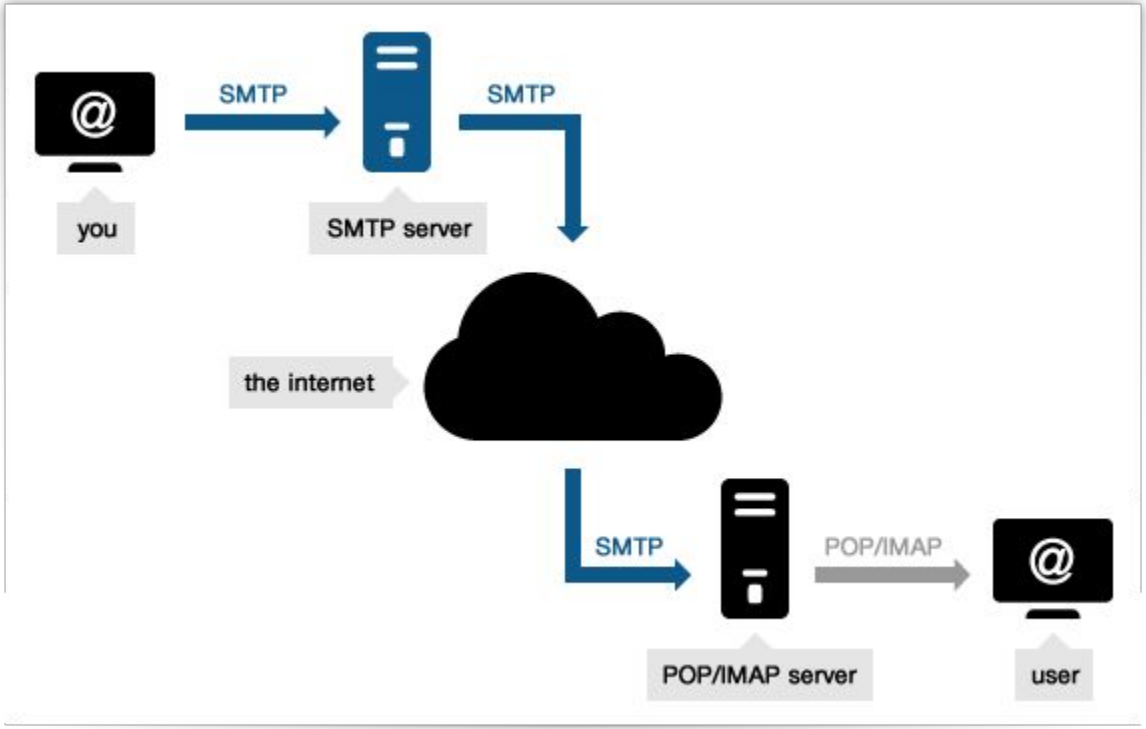
- Pretend to be a legit sender
- Phishing and spam

“Hey, this is your TA Zijie, something went wrong on Gradescope. Could you send your current PA back through email?”

SMTP

- Simple Mail Transfer Protocol
- A protocol for sending mail
- SMTP servers commonly use TCP on port 25
- SMTPS (S for secure) is often on port 465 as well
- The remote machine for this PA has a smtp server setup

SMTP


SMTP
SMTP
you
SMTP server
the internet
SMTP
POP/IMAP
POP/IMAP server
user

SMTP Commands

- **MAIL FROM**
- **RCPT TO**
- **DATA**
  - **From**
  - **To**
  - **Reply-To**
  - **Return-Path**
  - **Date**
  - **Subject**
  - **…**
  - **The Message**

SMTP Fields

- **FROM**: this is the field that indicates where the mail is from. This is our traditional notion of who the mail's sender is
- **RETURN-PATH**: Does not need to be the same as FROM. This field indicates where emails should bounce back to if they cannot reach the recipient. Think of this as the return address equivalent of snail mail.
- **REPLY-TO**: This is added by the sender to indicate where human replies should be addressed to. When you press the "Reply" button on, say, your Gmail client, the email in this field will show up as you compose your reply

SMTP Fields: MAIL FROM vs. FROM

- MAIL FROM and RCPT TO are both fields in the “envelope” of the email address whereas FROM and other fields are in the “letter” of the email
- MAIL FROM is the one used by SMTP servers to transport the mail
- But when it shows up in the client, typically the envelope is discarded and only the FROM is shown

Spoofing

- MAIL FROM is not checked :(
- FROM is not checked :(
- REPLY-TO is not checked :(

wget

- Need to use https://[some address]
- Need to specify --no-check-certificate
- No need to try to find all possible files in the beginning

Misc

- SSH permission too open on WSL: try to ssh from Windows directly
- If you are stuck staring at some chat log, re-read what Nadia says
- Don’t send email to Nadia (e.g. nadiah at cs.ucsd.edu). The email addresses used in this PA are local and the format is for you to figure out.