Legal Notice

This lecture will be recorded and made available to registered students on Canvas.
Agenda

1) SMTP Overview
2) SMTP Demo
3) tcpdump & Wireshark demo
4) Questions/OH
SMTP Overview

- 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 Confusing Difference between SMTP Fields

- **FROM:** This is the field in 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 the 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.
MAIL FROM vs FROM

- MAIL FROM and RCPT TO are both fields in the “envelope” of the email 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.
- For more on the SMTP Protocol: https://www.ietf.org/rfc/rfc2821.txt
- For more on the letter format: https://www.ietf.org/rfc/rfc2822.txt
SMTP Demo
nmap Demo
TCPDump & Wireshark Demo
Questions / Office Hours