Email and Firewalls

Module 7

Module 7 Agenda

- Email
- Email Protocols
- Firewalls
- Postfix and Dovecot

Email

Email

- Email is one of the most common Internet applications used worldwide.
  - It is used for business, personal, and retail/client use.

- So how does Email actually work?

  The Email system is make up of two components
  - Message Transfer Agent (MTA)
  - User Agent (UA) or Email Client

Email

- Message Transfer Agent (MTA)
  - Stores and transports messages
- MTAs are similar to post offices…
  - They receive and send mail.
  - They communicate with other MTAs through Simple Mail Transfer Protocol (SMTP). This is similar to the postal service.
  - Mail being sent is transported from one MTA to another until it reaches its destination.
  - MTAs also store messages waiting to be delivered or downloaded by the user.
  - They require authorization (username and password) to open the user's mail.

Email

- User Agent (UA)
  - Supports user interactions between the user and MTAs
  - Allows users to access their individual accounts, read, write, send, and manage emails

- There are two types of User Agents:
  - Private (application based)
  - Web based (accessed through web browser)

Email

- User Agent (UA)
  - **Private (application based):**
    - Examples: Outlook, Thunderbird, iMail)
    - Similar to having mail shipped directly to your house

- **Web based (accessed through web browser):**
    - Examples: Gmail, AOL, Hotmail, Yahoo!
    - Similar to having mail be shipped to the post office to pick up

Email

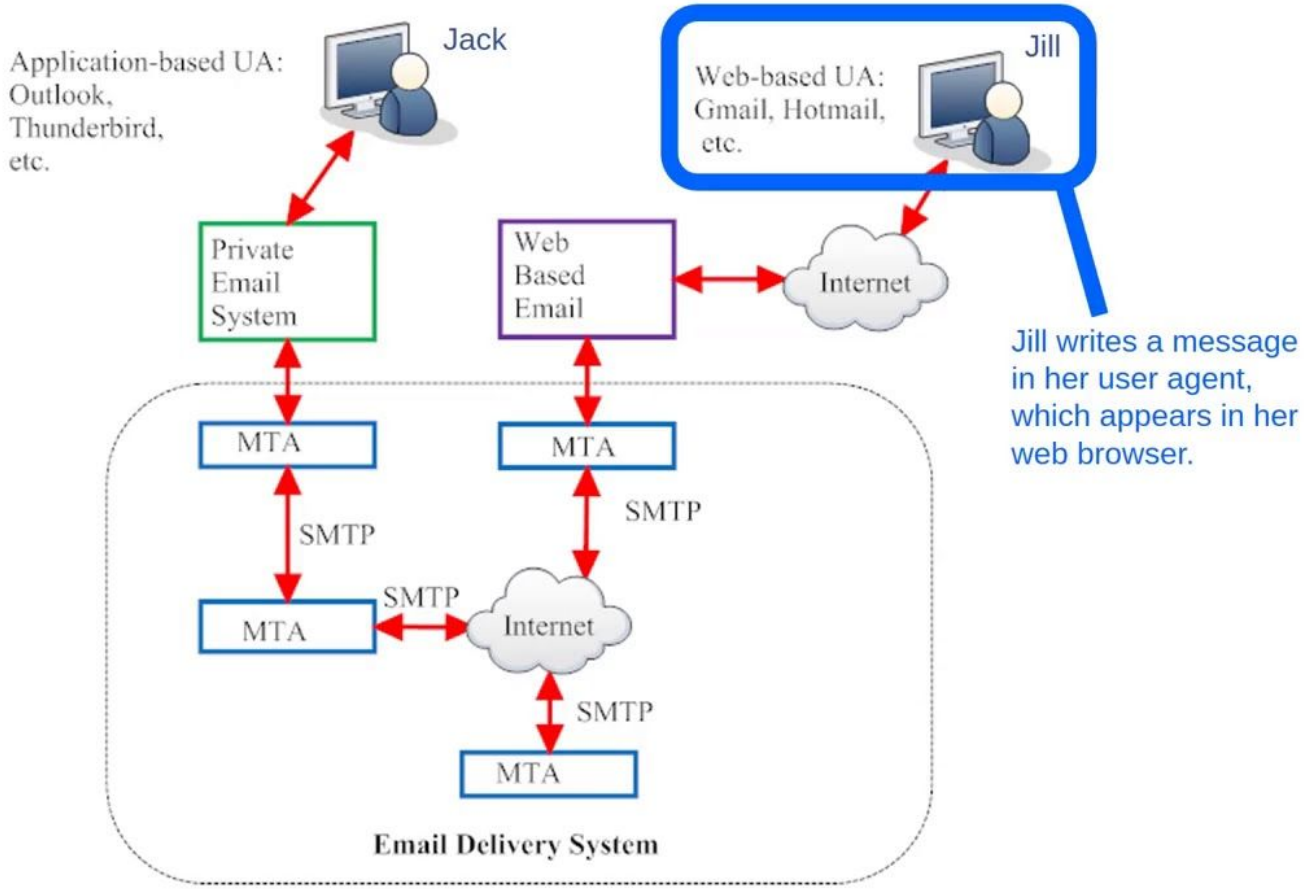
- Email System
  - Email users all have a unique mailing address

    username@domain_name

    - Examples: example@gmail.com, cookiesandcream@outlook.com, ita@iastate.edu

- UA's will send emails from MTA to MTA through the Simple Mail Transfer Protocol (SMTP).
  - Emails of private UA's are sent directly to their MTA
  - Web based emails send the UA's through intermediate MTA's

Email



https://i.ytimg.com/vi/Il0R5blCvO0/maxresdefault.jpg

Email

- Since email is used by the majority of internet users, it is a common medium for criminals to use to carry out cyber-attacks.

- Common email threats:
  - **Eavesdropping**: Hackers can observe user's actions on an insecure network
  - **Spamming/Phishing**: An attacker will pretend to be your bank or a person in "need" in order to trick you into providing them sensitive information or even have you send money.

Email

- Common email threats:
  - **Address Spoofing:**
    - the username is not really who they say there are
    - mikey@gmail could disguise themselves as manager@bank.com
  - **Malicious Attacks:**
    - emails containing links or attachments with viruses and worms

Email

Internet safety message of the day:

- Do not open emails from recipients that you do not know.
- Do not click on any buttons or fields on a suspicious email, simply delete the message.
- Do change your email password if you believe that a stranger has somehow been able to access your account.

Email Protocols

Email Protocols

Before explaining the following concepts watch these two videos to familiarize yourself with the topic of Protocols.

Videos:

IMAP vs. POP3

(https://www.youtube.com/watch?v=SBaARws0hy4)

Simple Mail Transfer Protocol

(https://www.youtube.com/watch?v=PJo5yOtu7o8)

Email Protocols

- **POP3**: Post office protocol (version 3) is used to retrieve email from email server.
- Simplest of the email protocols, and is best when a barebones email implementation is required.
- Downloads new emails to your device from your inbox folder. That's it. It doesn't manage any changes on your other email folders such as sent or drafts.
- In other words, POP3 does not synchronize.
- To save space, emails are deleted off of the email server once downloaded to a device.

Email Protocols

IMAP: Internet Message Access Protocol.

- With this protocol, multiple devices can view the content of the email message
  - Your folder's contents are synchronized.
  - If POP3 seemed strange to you, this is probably an email protocol that you might be more used to.
- The protocol you choose to use really depends on your situation, but at the end of the day, these two are used only to retrieve email from an email server.

Email Protocols

SMTP: Simple Mail Transfer Protocol

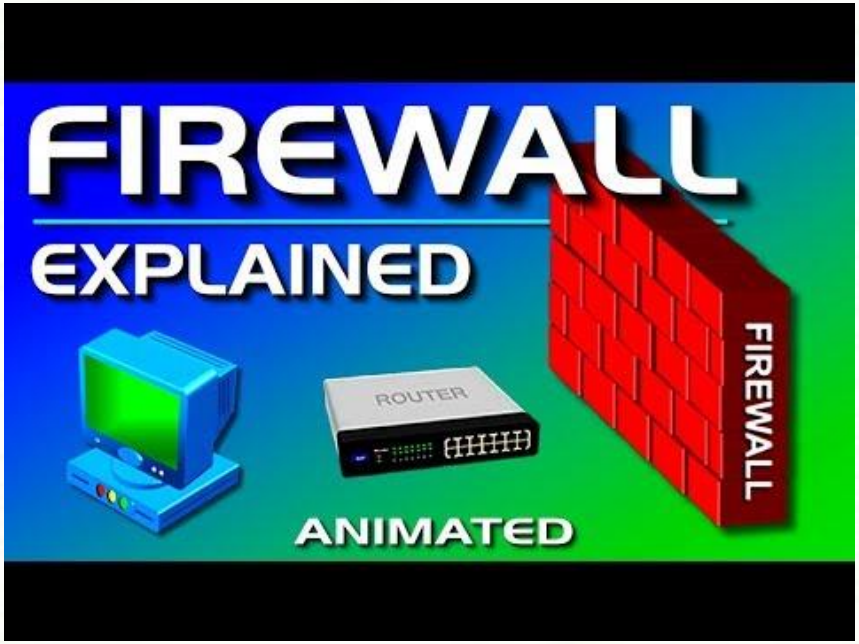
- Protocol used to send emails.
- The basic idea is that an email from your device will travel to your local email server before heading off to the recipients server, and being downloaded or viewed.

Firewalls

Firewalls

- Some computers/networks have a software that will help protect them from hackers trying to get in.

Here is a quick video to understand the concept of firewalls



https://youtu.be/kDEX1HXybrU

Firewalls

- Module 7 Activity 2
  - Teams will research a firewall for Linux they can implement: pfSense, IPTables, IPFire.
  - Each team will pick a firewall.
  - Team Members will take on different rules of research and documentation.
  - They will research pros and cons and how to install their personal firewall.

Postfix and Dovecot

Postfix and Dovecot

Postfix is the common Mail Transfer Agent (MTA) or mail server application for Linux.

- Postfix offers features that make long term maintenance easy.
- Postfix will allow you to send messages to your classmates through our network.

We will be installing Postfix on our VMs in Activity 1

To Do

- Complete Activity One
- Get a good start on Activity two
- Watch the videos in the Powerpoint

End of Module 7!

What questions do you have?

Next Module Topic:

7 Layers of Cyber Security & Web Vulnerabilities

Questions?

Contact IT-Adventures support staff!

email:
ita@iastate.edu

Your school's IP-Range can be found at:
http://www.it-adventures.org/ip-ranges/