Module 2.0 – How Email Works

This module consists of several micro-modules. We'll begin with taking a look at how email works, from there will look at the Postfix mail server, eMail Protocols, and finally will look at a few email best practices.

This module has two sections that must be completed in order. In section 1 we will discuss how email works. In section two, you will apply the principles discussed and introduced in section 1 in a live laboratory environment. When you have completed your lab assignments, be sure to submit them to your instructor for evaluation. If your instructor indicates that you have successfully completed your assignment, you can then move on to the next module in this course.

Introduction

We have all used email by this time to communicate with others. You more than likely received and sent an email to confirm your participation in this course. The transmission of electronic messages on the Internet is one of the most commonly used methods of communications between people using electronic devices. Email messages may contain text, files, images, music, programs, or other attachments.

But exactly how are these messages transmitted from one person's device to another?

Step A - The process begins with the sender creating an email in their Mail User Agent or MUA, also referred to as an email client. The mail user agent is a software application or web service that allows you to send and retrieve email. Some common MUAs include: Outlook, Thunderbird, and Mail on the Apple platform. A Mail User Agent can be a freestanding application like Thunderbird or a web application like Roundcube.. There are also MUAs that are integrated with various email solutions such as Zimbra. You can have multiple MUAs on one system.

Step B - The Sender's Mail Transfer Agent sends the email to a Mail Delivery Agent or MDA, which can also act as the Mail Transfer Agent or MTA.

Once the email is received by the Mail Delivery Agent, it routes the email to the recipient's local mailbox. In instances where the recipient's mailbox is not local the email will be forwarded by the sender's MTA.

Step C - When the email clears the queue it enters the internet where it is routed through several servers using Simple Mail Transfer Protocol. The sending MTA handles all aspects of mail delivery

until the message has been either accepted or rejected by the receiving MTA. Each MTA in the Internet needs to stop and ask directions from the DNS in order to identify the next MTA in the delivery sequence.

Step D - As the email progresses through the transfer process, it is likely to pass through at least one firewall that contains spam and virus filters that will screen the message for viruses or malware. If the message contains malware the file is quarantined, and the sender is notified; if the message is identified as spam it will likely be deleted.

Step E - The MTA contacts the MX servers on the MX record in order of priority until it finds the designated host for that address domain. The sending MTA asks if the host accepts messages for the recipient's username at that domain (i.e., username@domain.tld) and transfers the message. The email is finally received by the Recipient’s Mail Transfer Agent and is then routed through the company’s network to the Recipient’s mail delivery agent and finally to the recipient’s mail user agent/client.

Now, let's take a closer look at how the email message is formatted.

Message Format

The format of the email message was originally defined in RFC 822 and the most recent guideline can be found in RFC 6854, published in 2013.

An email message is quite similar to a physical letter. You have a message header, message body, and the envelope. Click each section to learn more.

The Message Header includes the sender, or mail from information, the recipient, and a portion of the email content, including the subject, date, etc. This is the routing information that instructs the "postman" where to deliver the email. The MUA adds the Headers before sending the email. There is one header per email message.

The Message Body contains the email content which can be free text or a structured document

The Envelope contains the actual routing information that is communicated from the email client to the mail server. This information is usually the same as the routing information in the header, with some exceptions. For example, when you send a Blind Carbon Copy (BCC), the actual recipient address (derived from the envelope) is not the same as the "To" address that is displayed in the recipient's email client, which is derived from the header.

Simple Mail Transfer Protocol (SMTP)

There are two types of protocols that govern how email is sent:

Simple Mail Transfer Protocol, and Extended Simple Mail Transfer Protocol.

Simple mail transfer protocol is an internet standard communication protocol for transmitting email messages. Mail servers and mail transfer agents use SMTP to send and receive email messages.

SMTP is a push protocol and is used to send the mail whereas POP3 or, post office protocol version 3, or IMAP, internet message access protocol, are used to retrieve those mails at the receiver's side.

An SMTP session is initiated when a mail sender issues a series of commands which are communicated to the mail receiver. The receiving server responds with a series of numerical codes.

One of the disadvantages of SMTP is that users are not verified when a connection is established, meaning that the sender of an email might not be a trustworthy source. As a result, open SMTP relays are often used to send spam on a massive scale.

Extended Simple Mail Transfer Protocol (ESMTP)

In response to the rampant spam problem on the internet, an extension of SMTP was released in 1995: extended SMTP or ESMTP. This protocol was defined in RFC 1651.

ESMTP added additional commands to the protocol which enabled new functions to save bandwidth and protect servers which included:

- Authentication of the sender
- SSL encryption of e-mails
- Possibility of attaching multimedia files to e-mails
- Restrictions on the size of e-mails according to server specifications
- Simultaneous transmission to several recipients
- Standardized error messages in case of undeliverability

There are three phases in the ESMTP Protocol:

- The ESMTP handshake is where the sender's server establishes a TCP connection to the recipient's server to identify themselves and the sender and recipient of the email.
- The message transfer which starts when Alice's server responds with code 250 indicating that it's ready to receive the message. When the sending server receives this code it begins sending the message out line by line. When the sending server sends the end of mail special line, the receiving server begins processing the message.

Lastly, the sending server sends a QUIT command to Alice's mail server to indicate its intention to close the connection to which Alice's mail server responds with a code 221.

Conclusion

This concludes section 1 of this module. Now, it's your turn to put what we have discussed into practice by completing the lab assignments. Click the proceed to lab assignment button to continue.