MAIL DELIVERY SUBSYSTEMS EMAIL SPOOFING AND TROUBLESHOOTING

BY

Rodney Barnes

Computer Janitor

1

What is the process of sending and receiving e-mail?

- How to compose an e-mail:
  - You compose an e-mail using either an e-mail client like Outlook or Thunderbird.
  - You compose an e-mail using a web browser and logging into Gmail, Yahoo or some other email web site.

2

What happens when you click on send?

- When you are using an e-mail client like Outlook or Thunderbird:
  - The message gets stored on your computer.
  - The message is then sent to the e-mail post office of your internet provider.
  - The message gets logged in on a log file at the provider.
  - Additional information is added to the message.
  - The message gets sent to another e-mail post office of the provider the person you are sending the e-mail to.
  - It gets logged and the receiver either retrieves the e-mail using a client or by web browser.

3

This is the header information from Tom's e-mail to me

- X-Apparently-To: **barnes_rodney@yahoo.com**; Wed, 19 Jun 2019 22:38:11 +0000
- Return-Path: **<pleasenior@gmail.com>**
- Received-SPF: pass **(domain of gmail.com designates 209.85.167.170 as permitted sender)**
- X-YMailISG: sOSnnlwWLDtU18cw7AJErVHfk6jASUKQYRLwC048fIvDBeqX JFVLIAZjBEDR8EaBtvH1Zp6oxg87MGl.RlHEaF8bN6ZBEFgbCf6nn7PQCxQZ srRWNMU64SUqUggdxUUyJk1Xs7UBY_bIVEsGwIzWuoZQq.K3SLc1SG4MQFR4 YusnLqjYmeYn5YBd1_zsurD9yp6dJQ1230nPerhew0WjySNlawkbMtchRgDc fL3XCac1BtHEbQgV61N41oCBhDrgdijRk94VbsIWY20lxxwbJtZO5a7OVMJh ESwa5f3qlafSEcQ8h2Ie0MlPk95yGP1PFmxad9.7JIFIEuhYLbGBi9AkJDWB sy6cqDdjuWa7czulpB7SdZCqH4NtUivahbdF6Knis89_g1nDIRUaaXRgoSop aCyeLmVFKaWKtbYQAAGBctmlMDoQZTLhXpd.4SzAocfBWI_ZjIiLvIHe720T _O6T0tNiCsHHgporJQmUAoPiM7UjIOLsIDcaHz8R_I4ST_Gu6Fwsf_xV/i1 ukd12tIHkfc.VugVL8Obuylgm4rAVVvmLvCrZTHuS2seBvcgBvGsS2a_ mfIN r7q2ENxTib_JsqbFvqKFW8_.zaiYkpFhetvl9Ay_zEISJk8_8SHQpzVSw31P cQkUwAL507LrMjedHo9.AXjVLlu_fGYSZY.raVzwHfnvr3XymVEx.mqtZ_Ph OKv2SxlmrPullqpxgG1ChAVjtzgpAgSwv12vS9gUzvaqCdkgLrLU3kB37E0D 2iwEbsIZtpftdWhUfIEjIYlCLNyf72L1iiCHLbgMEFsjcn1FhbYXpoee0hx YBXmzfGennCRtUeXInvsBEDrUWTmHpxWjtoCjrHkklPEpISFkZJ5uL2qDb8t etG.OwfPKSytbNNNYyiP.PCEeNjLguYSYbe2FQslOwwCZ7_WkVUjVGrMjvQP7 Jo4cB7xv9LH4TM6L5kQ6uLE7ADwGy_k.mZeqhYYC4Lb0E1_ICTo3QOA1QFr0 VlCvK7BbbD7Xy4gTrqdfnHdVV38r69I1EpfM482F5mOJF_P0JXlGsVhDd wpxagWgcvd2AOf80tsOHWP8bDdlz2LYyuJ2RnRaIctnJ0a0WQHoFI8Dw18wq jwIMa.QHxTIATm6j8KjmYZe3csCjOgpAeZMy0Ep3clczrDjWKUSDvSHWKJSu ZOum

- **X-Originating-IP: [209.85.167.170]**
- Authentication-Results: **mta4345.mail.gq1.yahoo.com** header.i=**@gmail.com**; header.s=20161025; dkim=pass (ok)
- **Received: from 10.213.245.191 (EHLO mail-oi1-f170.google.com) (209.85.167.170) by mta4345.mail.gq1.yahoo.com with SMTPS; Wed, 19 Jun 2019 22:38:11 +0000**
- **Received: by mail-oi1-f170.google.com with SMTP id a127so643456oii.2 for <barnes_rodney@yahoo.com>; Wed, 19 Jun 2019 15:38:11 -0700 (PDT)**
- DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20161025; h=mime-version:from:date:message-id:subject:to; bh=URLsQQbI+LgbAjpWiV0zZAnAZAk6Drdf/Sjfx7s0ejM=; b=N/JeI1CCfuuXBOKNhG0M8LfN+1dozTa7fDftD650kE0t+7WZAYJR0+pUb+K1PxrpBT PGqWgEtKj/qHRqu74FH0KOjPrCkQlnf/wUocU1eYp1KFKr1aTh3dJKvftHt4lCMPo32A q1k5VH/Mhw3kXfKgU+vUk6LVUI1BjO1zwQo61Anv3lCHLlIrVs0BLjpBovHux54NJ9o8 5UCfh9MzBTgnI0jZfk4zx8wk+pcvz9LT0NGAj6cC5tPmN3zK3D5WScFfSPThzNExvAbq Mg+9ZDW6hohabc6qvTaceaVG29KArHC38bPfesE/B8G0LfMrIbc1Nijo9LInQOmKc8rJ Qu7g== X-Google-
- DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20161025; h=x-gm-message-state:mime-version:from:date:message-id:subject:to; bh=URLsQQbI+LgbAjpWiV0zZAnAZAk6Drdf/Sjfx7s0ejM=; b=Vast/GeD5oEggaVNCWDfPavloj1nr2kD34+VfygHX7XaswmPzTnDHiSIRkHzpTN8Tk w0e7cpJXGuC+qPrHsShbqOyxLjho54KfKVJtobx9F4UjwgbeNXOeRpDm+2KkQ9rBbWSN hch56I8Nu4rgYyVbltKhWeZLQCbvg3WW8KAqUrnGTe3PQKy5tCmEBoSBIUgvd4IIL0LQ VDDfOPyToqyQj7WGouz7Wlkx+HZbdW+5vLG2MmfjHQHPapzi1322JM58QEPn+dGkj6vy Oabp3Ge3k5C4QXF6xOxg/FB6hDKooEGLypyUBzbATvFBX5XnbU7ABprVwwFEfIlZnapP pfGQ== X-Gm-Message-State: APjAAAW6VeWx37gDdK4LnnB+HXYLWBIsDpDnyUA5/HmMrduRiTQpMHqP Hk6QSw/gcQW2oPN4u6Dk3MG0OOURDOwVvejiKUY=
- X-Google-Smtp-Source: APXvYqye9kYgDj9/J7UaXB8K72cJnWWI3bUu5cTKTvGdUEks/282mApRHAdykU/fSdG12yQI3GGEiMJDrPCU9x2m0=
- **X-Received: by 2002:aca:4ad2:: with SMTP id x201mr4485719oia.129.1560983890902; Wed, 19 Jun 2019 15:38:10 -0700 (PDT) MIME-Version: 1.0**
- From: **Tom Reif <pleasenior@gmail.com>**
- Date: **Wed, 19 Jun 2019 15:37:33 -0700 Message-ID: <CAPWQG=Shw46mnzRMMki_Tg09gPwnMPS=cfk_TsXWOGm92xJVLg@mail.gmail.com>**
- Subject: Personal Technology Users Group --- Agenda for June 27th Meeting
- To: **Tom Reif <tom@reif.us>** Content-Type: multipart/alternative; boundary="0000000000005147790 58bb4e2ea"
- Bcc: **barnes_rodney@yahoo.com**
- Content-Length: 4640 --0000000000005147790 58bb4e2ea Content-Type: text/plain; charset="UTF-8" Content-Transfer-Encoding: quoted-printable

4

What happens when you log into your e-mail server by a browser

- Instead of storing your e-mail on the computer or phone you are logging into the post office of your provider.
- The provider composes the header and then sends the e-mail on it's way to the destination.
- The folder structure is on the server.
- There are no archives on your machine.

5

What is Spoofing

- A spoofing attack is an attack in which one person or program successfully acts as another by falsifying data.
- Spoofing is an art of faking a real identity.
- The main purpose is to trick the authenticator to release sensitive information or to gain unauthorized access.
- https://www.youtube.com/watch?v=YKH2VJvQJfc

6

E-mail Spoofing

- Pretending to be someone else.
- Using some other IP address.
- Changing your IP address to be something else.
- It's a way to send someone an e-mail that makes them think something that is not real.
- There are web sites that provide this service.

7

The process of Spoofing

- Basically you create an SMTP account that you send e-mails to.
  - Some uses an SMTP account that is free.
  - Some uses an SMTP account that they have the log in information on.

8

Some ideas on how to protect yourself from Spoofing

- Be aware of questionable e-mails.
- Don't open unknown or unexpected file attachments.
- Don't click on website links in e-mails that you have not validated by someone you know.
- Don't be afraid to contact the sender if you get an e-mail from them that you don't trust.
- Don't enable macro's if prompted.

9

How to they get your e-mail address?

- Some people send out jokes with multiple e-male addresses.
- Some people harvest e-mail addresses from web sites.
- Some people purchase valid e-mail addresses from the dark web.
- Some people sign up for ads that are fishing sites for valid e-mail addresses.

10