**ECE435: Network Engineering – Homework 4**
e-mail, DNS

**Due: Friday, 18 February 2022, 5:00pm**

For this assignment create a document with your answers (text, pdf, libreoffice, MS Office if you must) and e-mail them to *vincent.weaver@maine.edu* by the homework deadline. Title your e-mail "ECE435 Homework 4" and be sure your name is included in the document.

1. **E-mail Headers (5pts)**

   (a) You receive an e-mail claiming to be from a bank. You turn extended e-mail headers on and below is what you see.

```
Return-Path: <starwood@dental.ufl.edu>
Delivered-To: vince@deater.net
Received: from pop.deater.net [64.26.60.216]
    by pianoman.cluster.toy with POP3 (fetchmail-6.3.26)
    for <vince@localhost> (single-drop); Wed,
    16 Nov 2016 21:48:21 -0500 (EST)
Received: from stor32.mfg.siteprotect.com ([192.168.31.39])
    by stor15.mfg.siteprotect.com (Dovecot) with LMTP id
    uahOABj4LFjrQQAA9Krtqg
    for <vince@deater.net>; Wed, 16 Nov 2016 18:21:44 -0600
Received: from mx.siteprotect.com (unknown [192.168.33.227])
    by stor32.mfg.siteprotect.com (Postfix) with ESMTP id 8C23A1001FED
    for <vince@deater.net>; Wed, 16 Nov 2016 18:21:38 -0600 (CST)
Received: from smtp.ufl.edu (smtp-prod06.osg.ufl.edu [128.227.74.254])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
    (No client certificate requested)
    by mx.siteprotect.com (Postfix) with ESMTPS id 3905955C087
    for <vince@deater.net>; Wed, 16 Nov 2016 18:21:38 -0600 (CST)
X-UFL-GatorLink-Authenticated: authenticated as starwood () with LOGIN
    from 69.70.91.146
Received: from localhost (modemcable146.91-70-69.static.videotron.ca
    [69.70.91.146])
    (authenticated bits=0)
    by smtp.ufl.edu (8.14.4/8.14.4/3.0.0) with ESMTP id uAH0K1dd032514
    (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256
    verify=NOT);
    Wed, 16 Nov 2016 19:20:20 -0500
Message-ID: <0603B5E6ED391784585D14AA1EA70F57@dental.ufl.edu>
From: "Maybank2u.com" <starwood@dental.ufl.edu>
Subject: Transaction alert
Date: Wed, 16 Nov 2016 19:20:18 -0500
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="0c69c634b31bc1d0b1050909ca80"
X-Proofpoint-Virus-Version: vendor=fsecure engine=2.50.10432:,,
    definitions=2016-11-16_07:,,
 signatures=0
X-Proofpoint-Spam-Details: rule=notspam policy=default score=1 spamscore=1
    suspectscore=10
 malwarescore=0 phishscore=0 adultscore=0 bulkscore=0 classifier=spam
 adjust=0 reason=mlx scancount=1 engine=8.0.1-1609300000
 definitions=main-1611170005
```

```
X-Spam-Level: *
X-UFL-Spam-Level: *
X-CTCH-RefID: str=0001.0A020205.582CF817.018C,ss=3,re=0.000,recu=0.000,
    reip=0.000,vtr=str,vl=0,cl=3,cld=1,fgs=0
X-Mail-Filter-Gateway-ID: 8C23A1001FED.A1639
Mail-Filter-Gateway: Scanned OK
X-Mail-Filter-Gateway-SpamDetectionEngine: NOT SPAM,
    MailFilterGateway Engine (score=2.318, required 3,
    autolearn=disabled, CTASD_SPAM_BULK 4.00, MISSING_HEADERS 1.21,
    RP_MATCHES_RCVD -2.90, T_OBFU_PDF_ATTACH 0.01)
X-Mail-Filter-Gateway-SpamScore: **
X-Mail-Filter-Gateway-From: starwood@dental.ufl.edu
X-Mail-Filter-Gateway-To: vince@deater.net
X-Spam-Status: No
Parts/Attachments:
   1 Shown     ~9 lines  Text (charset: windows-1251)
   2          156 KB     Application
----------------------------------------

An incoming transaction to your account was declined.
```

i. Is this likely a legitimate e-mail? Why or why not?
(Hint: you can see in the `Subject` and `From` headers the claim to be from a bank. Does anything in the rest of the headers contradict this?)

ii. The e-mail had a .pdf file attached. Should you open it? Why or why not?

(b) You look at a raw e-mail you received and it contains the following:

```
Content-Type: image/jpeg;
        name="26993963_n.jpg"
Content-Description: 26993963_n.jpg
Content-Disposition: attachment;
        filename="26993963_n.jpg"; size=228405;
        creation-date="Tue, 23 Jan 2018 16:48:41 GMT";
        modification-date="Tue, 23 Jan 2018 16:48:41 GMT"
Content-Transfer-Encoding: base64

/9j/4AAQSkZJRgABAgAAAQABAAD/7QCcUGhvdG9zaG9wIDMuMAA4QklNBAQAAAAAAIAcAmcAFHpZ
ejRabS1UVmw2ejBfS3FMYnBhHAIoAGJGQk1EMDEwMDBhOWUwZDAwMDBjNjMzMDAwMGFkOGEwMDAw
Njk4ZjAwMDA5MDk3MDAwMGJkMjMwMTAwZTZmMjAxMDAwOGZiMDEwMDhhMDQwMjAwOTYxMjAyMDAz
NTdjMDMwMP/iC/hJQ0NfUFJPRklMRQABAQAAC+gAAAAAgAAAG1udHJSR0IgWFlaIAfZAAMAGwAV
ACQAH2Fjc3AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD21gABAAAAANMtAAAAACn4Pd6v
...
KMzUXkeXneFRVnYMq9ns4x7FBiYHDp+GWSOgsUpXZ1iEWuh5H/WC5AFE+j5Zx5yvPTW6NmPZWcsP
7e/jP//Z
```

i. What is this section of the e-mail all about?

ii. Why is there a large seemingly random jumble of letters and numbers?

2. **DNS (5pts)**

(a) Look up the domain registration info for the **maine.edu** domain. There are various ways to do this; on Linux you can use the `whois` utility: `whois maine.edu`
(you might need to install it first, `apt-get install whois`)

i. When was the maine.edu domain *first* created/activated?

ii. What is the name of the domain registrar that maine.edu uses? This is the top-level registry that holds the info for the top-level `.edu` domain.

(b) Use DNS requests to look up some information on various domains. On Linux you can use a utility named `dig` to do this easily. You might need to install the dnsutils package first `apt-get install dnsutils`. In the examples replace HOSTNAME with the name of the system you are asking about.

i. What is the IP address of weaver.eece.maine.edu? Use a command line like below, but replace HOSTNAME with in this case weaver.eece.maine.edu
`dig HOSTNAME A`, look for answer in the ANSWER section.

ii. What is the IPv6 address of google.com?
`dig HOSTNAME AAAA`

iii. What is the name of the UMaine nameservers? (maine.edu)
`dig HOSTNAME NS`

iv. What is the name of the UMaine mailservers?
`dig HOSTNAME MX`

v. Do you notice anything odd about the UMaine mailservers?

(c) Finally, name one security issue that exists with standard DNS. What can be done to avoid this issue?