Obfuscation and Steganography

Tools that obfuscate URLs:

http://tinyurl.com/
http://www.shadyurl.com/

Tools that hide data in images:

OpenPuff http://embeddedsw.net/OpenPuff_Steganography_Home.html

Try hiding a .zip file in a .gif

There are two tiny facts about GIF files and ZIP files you might like to know about: GIF files have their length defined at the start of the file; any bytes after are ignored. ZIP files have a table at the end; anything at the start of the file is ignored. The result is that a file can be both a GIF and a ZIP, just change the extension.

```
cat somefile.zip >> somefile.gif
copy /B source.gif+source.zip target.gif
```

As a proof of concept, try sending the .gif to someone as an email attachment. It should look to them just like a picture. Then have them rename the file with a .zip extention. You may need a tool like WinRAR to open it.

Browsing the internals of your web browser:

http://sourceforge.net/projects/sqlitebrowser/

Try opening your firefox profile .sqlite files, such as downloads.sqlite and places.sqlite. These are located:

OS X: `~/Library/Application Support/Firefox/afe7adfqer.default/`

Windows: `C:\Users\Adminstrator\AppData\Local\Firefox\...`
-probably need to view hidden and system files

How sketchy is a site?

http://www.siteadvisor.com/sites/
http://safeweb.norton.com

Try csusb.edu vs p2pshare.org

mailing lists:

http://www.securityfocus.com/ (Bugtraq)
http://www.us-cert.gov/ (General and Technical bullitens, awareness material)
http://listserv.educause.edu/cgi-bin/wa.exe?A0=SECURITY (Educause security)

Subscribe to these for a month or two, see how relevant they are to your work

Google and Pastebin Alerts

pastebin.com -- search for things like “@csusb.edu” and “username md5”

google alerts a la http://isc.sans.edu/diary.html?storyid=3928

Sometimes you’ll need to do a combo, such as searching google using “csusb.edu site:pastebin.com”

Also checkout http://archive.org

irc is still in use

From Firefox, use the Add-ons menu to downoad ChatZilla
Change your handle (aka nickname)
Connect to a server (eg freenode)
IRC -> Join channel

know how to read email headers

There is evidence of where the email was sent from, but you need to examine the Received: headers carefully. There ordered like pancakes, oldest at the bottom. You'll need to follow the recived from... trail until we see where it entered the csusb.edu network.

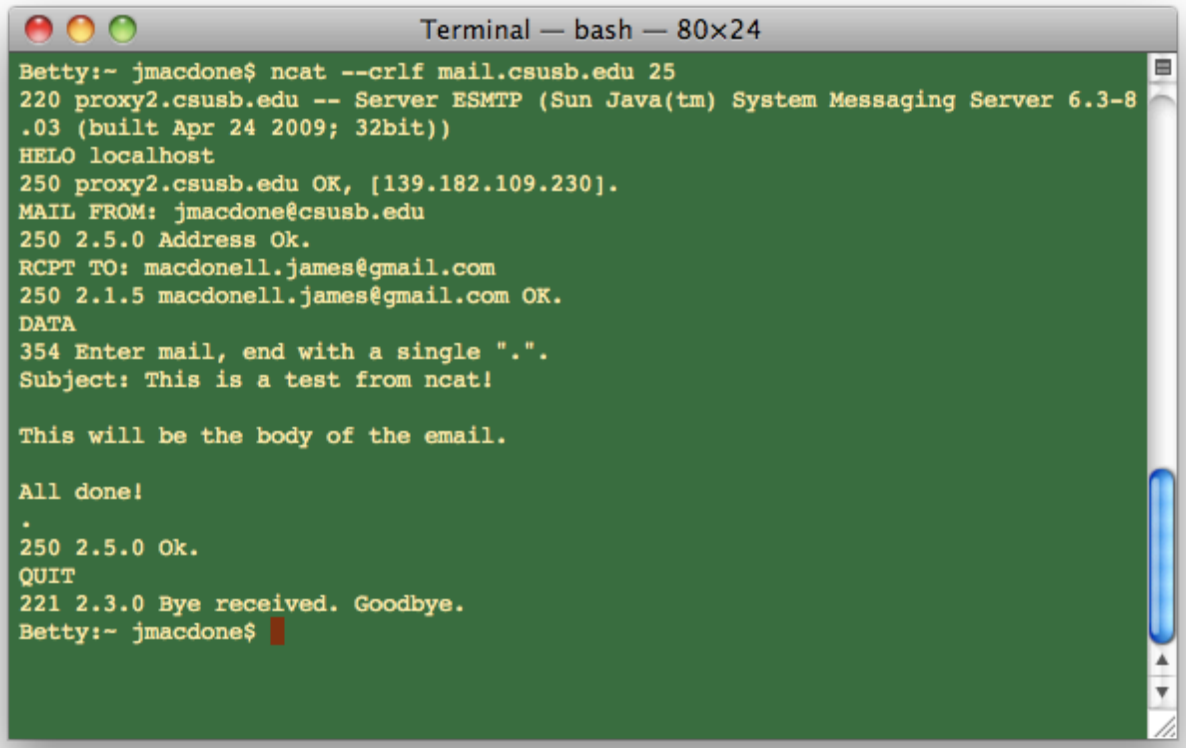
Who was the last IP to send the email?
Who should we contact to report the phishing?
Note other suspicious signs such as random-looking hostnames, long To: lists, non-standard X-mailer clients (typically Outlook, thunderbird, gmail, etc)

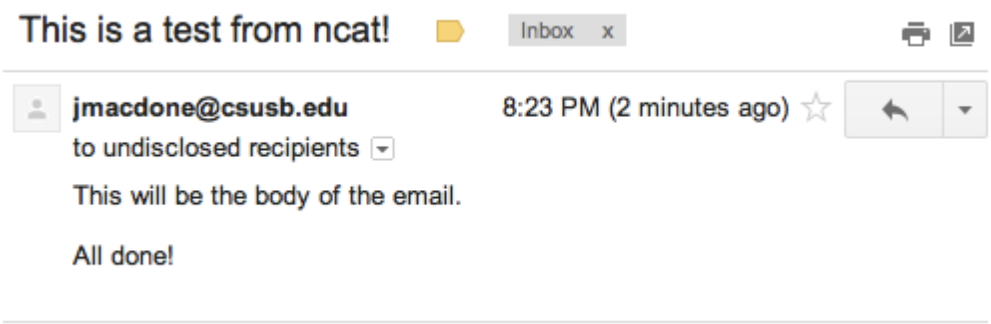
```
Return-path: <icare7@amcustomercare.att-mail.com>
Received: from proxy2.csusb.edu ([139.182.2.66])
  by mailstore.csusb.edu (Oracle Communications Messaging Exchange Server
  7u4-18.01 64bit (built Jul 15 2010))
  id <0M2R00E00YPQR900@mailstore.csusb.edu>; Fri,
  20 Apr 2012 04:08:28 -0700 (PDT)
Original-recipient: rfc822;alert@csusb.edu
Received: from proxy2.csusb.edu ([139.182.2.66])
  by mailstore.csusb.edu (Oracle Communications Messaging Exchange Server
  7u4-18.01 64bit (built Jul 15 2010))
  with ESMTP id <0M2R00EXBYY43PE0@mailstore.csusb.edu> for alert@csusb.edu; Fri,
  20 Apr 2012 04:08:28 -0700 (PDT)
Received: from mx3.csusb.edu ([139.182.2.20])
  by proxy2.csusb.edu (Sun Java(tm) System Messaging Server 6.3-8.03 (built Apr
  24 2009; 32bit)) with ESMTP id <0M2R001YPYY4MC20@proxy2.csusb.edu> for
  alert@csusb.edu (ORCPT alert@csusb.edu); Fri, 20 Apr 2012 04:08:28 -0700 (PDT)
Received: from 111.24.10.93.rev.sfr.net
  (111.24.10.93.rev.sfr.net [93.10.24.111]) by mx3.csusb.edu with ESMTP id
  AiEL2vsrWmcr9Hny; Fri, 20 Apr 2012 04:08:25 -0700 (PDT)
Received: from [28.89.124.89] (helo=bdkdwqd.dsehwxfeynv.info)
  by 111.24.10.93.rev.sfr.net with esmtpa (Exim 4.69) (envelope-from )
  id 1MMGID-8239bl-AP   for valenzum@csusb.edu; Fri, 20 Apr 2012 12:09:36 +0100
Date: Fri, 20 Apr 2012 12:09:36 +0100
From: AT&T Customer Care <icare7@amcustomercare.att-mail.com>
Subject: [Spam]  Your AT&T wireless bill is ready to view
To: valenzum@csusb.edu, vasquez6@csusb.edu, vcoffey@csusb.edu, vossc@csusb.edu,
  vseitz@csusb.edu, vwashing@csusb.edu, waguilar@csusb.edu, tbenson@csusb.edu,
  alert@csusb.edu, algarcia@csusb.edu, allavore@csusb.edu, ablanco@csusb.edu,
  ablesn@csusb.edu, abodman@csusb.edu, abrahamg@csusb.edu, abutler@csusb.edu
Message-id: <3651713031.W1FV83OC839786@xbnqwartpiaen.gujebssgtyonksg.net>
MIME-version: 1.0
X-Mailer: oychnhobqh 30
Content-type: multipart/alternative; boundary="----=_yxogmrvt_81_21_76"
Importance: Low
```

send an email using ncat

ncat --crlf mail.csusb.edu 25
HELO localhost
MAIL FROM: from@example.org
RCPT TO: toaddr@example.com
DATA
Subject: Your subject here!

Body comes after a single blank line.
.
QUIT

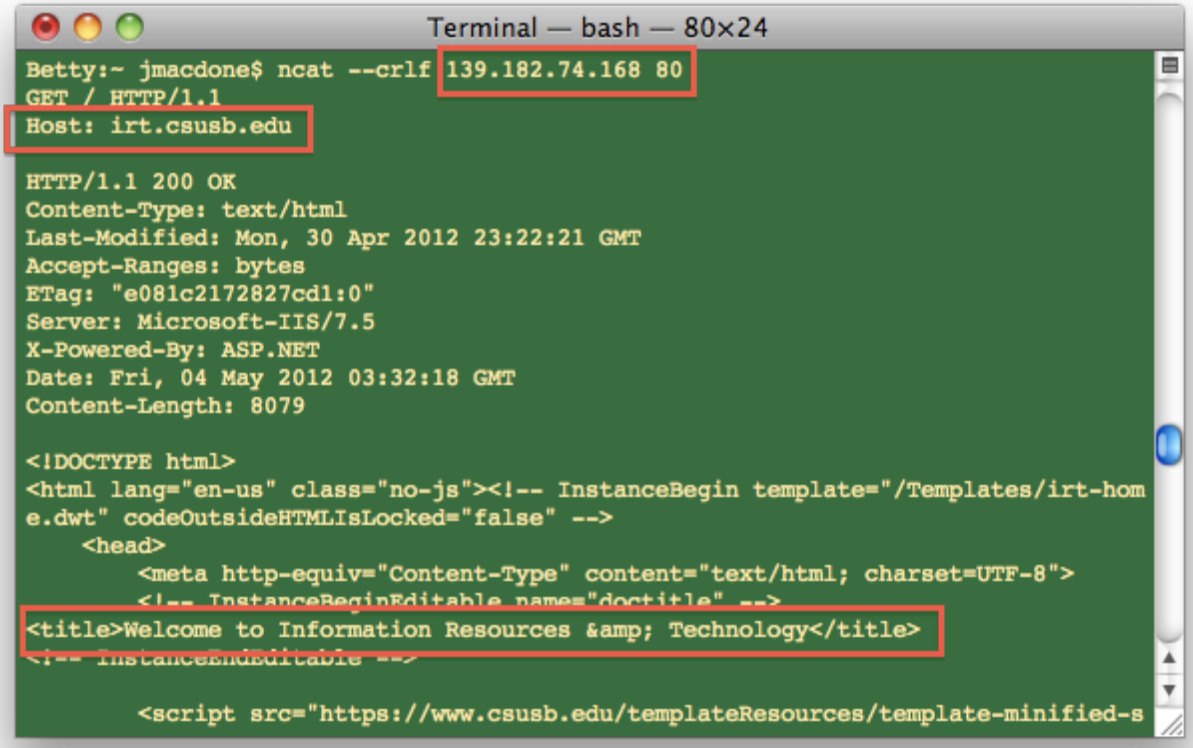


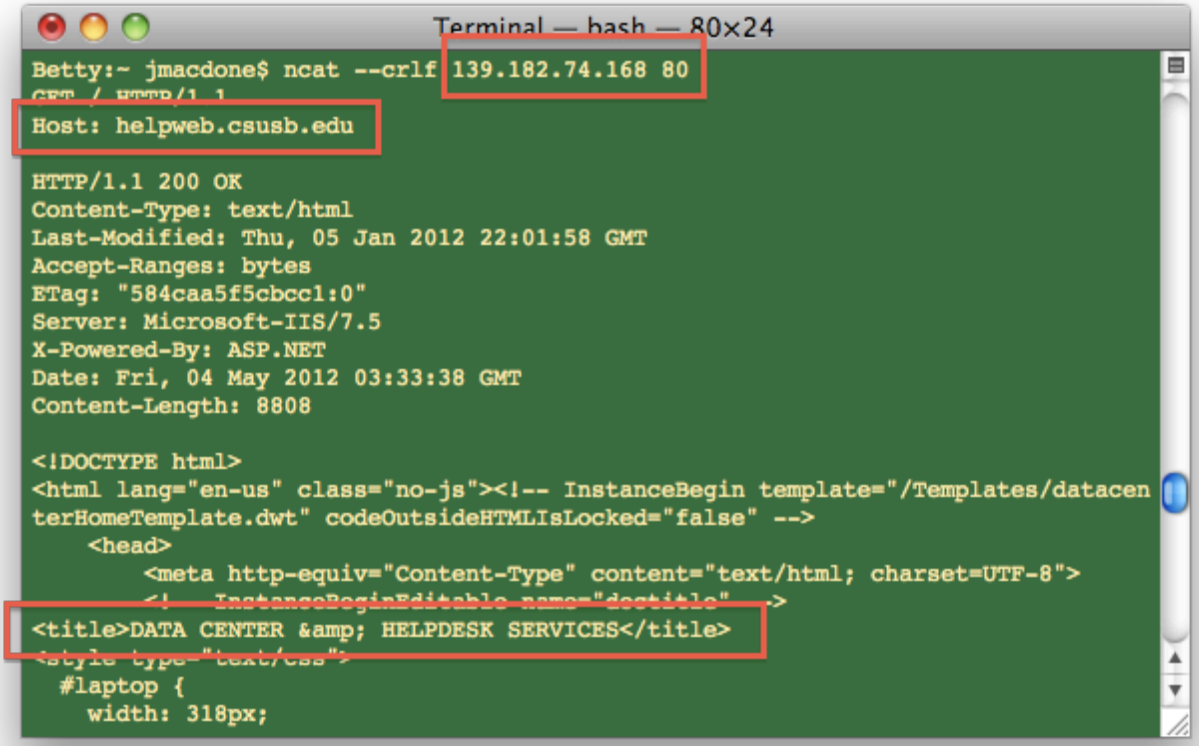


get a web page using ncat

ncat --crlf 139.182.74.168 80
GET / HTTP/1.1
Host: irt.csusb.edu

Try the same command, but use:
Host: helpweb.csusb.edu




Terminal — bash — 80×24
Betty:~ jmacdone$ ncat --crlf 139.182.74.168 80
Host: helpweb.csusb.edu
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Thu, 05 Jan 2012 22:01:58 GMT
Accept-Ranges: bytes
ETag: "584caa5f5cbcc1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Fri, 04 May 2012 03:33:38 GMT
Content-Length: 8808
<!DOCTYPE html>
<html lang="en-us" class="no-js"><!-- InstanceBegin template="/Templates/datacen
terHomeTemplate.dwt" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>DATA CENTER & HELPDESK SERVICES</title>
#laptop {
width: 318px;

Checking on how things look on the “outside”

The DMCA notification page should only be available on campus. Use the following tools to verify that and compare the results

Test http://iso.csusb.edu:8888/ and http://www.csusb.edu/ using the following

http://validator.w3.org/
http://www.downforeveryoneorjustme.com/

Super Advanced -- Amazon ssh tunnel

http://lifehacker.com/237227/geek-to-live--encrypt-your-web-browsing-session-with-an-ssh-socks-proxy
http://docs.amazonwebservices.com/AWSEC2/latest/GettingStartedGuide/GetStartedLinux.html

-Use the free teir

-On the Connect to Your Instance Step, follow either the “Connect... using a Standalone SSH Client” for OS X or “Connect... Using PuTTY

-Don’t terminate the instance.

-Once you can successfully SSH, reconnect but specify the -D dynamic port forwarding option, for example:
Command line:
`ssh -i GSG_Keypair.pem -D 10000 ec2-user@1-2-3-34-3.amazon.aws.example.com`
For putty, see http://mattfleming.com/node/145

-If you get this far, follow the firefox proxy settings stated at http://lifehacker.com/237227/geek-to-live--encrypt-your-web-browsing-session-with-an-ssh-socks-proxy

Check your results by googling “ip address”

ARPWatch

This is a tool that checks for new additions and mysterious disappearances of network devices

Get a compiler (use xcode if you have it, otherwise use:)
https://github.com/kennethreitz/osx-gcc-installer

Pull down source code:
ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

Use the typical configure, make, make install sequence

```
cd Downloads/arpwatch-2.1a15
./configure
make
sudo ./arpwatch -i en1
tail -f /var/log/system.log
sudo killall arpwatch
```

The “-i en1” specifies to use the wireless interface on a Mac (en0 would be the wired ethernet)
“sudo killall” is a command line method of stopping a daemon process like this. You could also use the Activity Monitor.