

Report of Assignment 2: Manual Spam

By Piyusha Jaisinghani (UCFID - 4736715)

Manual Spam Steps

Objective- Manually send a pure text-based spam email to "ucf.cap6135@gmail.com" using telnet to CS department email server.

Following are the steps that I performed to send a spam email:-

1. Connected to the eustis machine and to find out the CS department email server used the command:

dig mx cs.ucf.edu

```

Welcome to eustis.eecs.ucf.edu.

Please use your NID and NID password to log in.

pi846531@eustis.eecs.ucf.edu's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Last login: Sat Feb 16 12:21:08 2019 from 172.31.5.212
pi846531@net1547:~$ dig mx cs.ucf.edu

; <<>> DiG 9.11.3-1ubuntu1.3-Ubuntu <<>> mx cs.ucf.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14062
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cs.ucf.edu.                IN      MX

;; ANSWER SECTION:
cs.ucf.edu.                 3600    IN      MX      10 longwood.cs.ucf.edu.

;; AUTHORITY SECTION:
cs.ucf.edu.                 3600    IN      NS      longwood.cs.ucf.edu.
cs.ucf.edu.                 3600    IN      NS      server.cs.ucf.edu.

;; ADDITIONAL SECTION:
longwood.cs.ucf.edu.        3600    IN      A       10.173.204.10
server.cs.ucf.edu.          3600    IN      A       10.173.204.13

;; Query time: 0 msec
;; SERVER: 10.173.204.10#53(10.173.204.10)
;; WHEN: Sat Feb 16 13:50:40 EST 2019
;; MSG SIZE rcvd: 131

```

2. Connected to the CS department email server using the below telnet command:

telnet longwood.cs.ucf.edu 25

```

pi846531@net1547:~$ telnet longwood.cs.ucf.edu 25
Trying 10.173.204.10...
Connected to longwood.cs.ucf.edu.
Escape character is '^]'.
220 longwood.cs.ucf.edu ESMTP Sat, 16 Feb 2019 13:51:26 -0500 (EST)

```

- Used the helo command to get the domain name of the sending host to SMTP. Below is the command:

helo get.fakedomain

```
[pi846531@net1547:~]$ telnet longwood.cs.ucf.edu 25
Trying 10.173.204.10...
Connected to longwood.cs.ucf.edu.
Escape character is '^]'.
220 longwood.cs.ucf.edu ESMTP Sat, 16 Feb 2019 13:51:26 -0500 (EST)
[helo get.fakedomain
250 longwood.cs.ucf.edu Hello [10.173.204.63], pleased to meet you
```

- Now specified the mail from and rcpt to addresses. Below are the addresses given:

mail from: accountmanager@be.com

rcpt to: ucf.cap6135@gmail.com

rcpt to: piyushajaisinghani@knights.ucf.edu

rcpt to: piyushajaisinghani@gmail.com

```
mail from: accountmanager@be.com
250 2.1.0 accountmanager@be.com... Sender ok
rcpt to: ucf.cap6135@gmail.com
250 2.1.5 ucf.cap6135@gmail.com... Recipient ok
rcpt to: piyushajaisinghani@knights.ucf.edu
250 2.1.5 piyushajaisinghani@knights.ucf.edu... Recipient ok
rcpt to: piyushajaisinghani@gmail.com
250 2.1.5 piyushajaisinghani@gmail.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
from: IT-support@bankofEarth.com
to: spamHW@CAP6135
subject: CAP6135: Piyusha Jaisinghani

Dear Customer,
This is to inform you that your account has been locked due to multiple invalid login attempts.
Please contact 012-345-6789 to unlock your account.

Thanks and regards,
Account Manager
Bank of Earth
```

- To type the data that needs to be sent in the mail used the command "data" and began typing the email. Below are the details:

data

from: IT-support@bankofEarth.com
to: spamHW@CAP6135"
subject:CAP6135: Piyusha Jaisinghani

Dear Customer,

This is to inform you that your account has been locked due to multiple invalid login attempts.

Please contact 012-345-6789 to unlock your account.

Thanks and regards,

Account Manager

Bank of Earth

.

“.” to send the mail and quit to exit session.

```
mail from: accountmanager@be.com
250 2.1.0 accountmanager@be.com... Sender ok
rcpt to: ucf.cap6135@gmail.com
250 2.1.5 ucf.cap6135@gmail.com... Recipient ok
rcpt to: piyushajaisinghani@knights.ucf.edu
250 2.1.5 piyushajaisinghani@knights.ucf.edu... Recipient ok
rcpt to: piyushajaisinghani@gmail.com
250 2.1.5 piyushajaisinghani@gmail.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
from: IT-support@bankofEarth.com
to: spamHW@CAP6135
subject: CAP6135: Piyusha Jaisinghani

Dear Customer,
This is to inform you that your account has been locked due to multiple invalid login attempts.
Please contact 012-345-6789 to unlock your account.

Thanks and regards,
Account Manager
Bank of Earth
.
250 2.0.0 x1GJxvtQ000111 Message accepted for delivery
quit
221 2.0.0 longwood.cs.ucf.edu closing connection
Connection closed by foreign host.
pi846531@net1547:~$
```

6. Please find the screenshots of the mail received in my knights mail account:-

