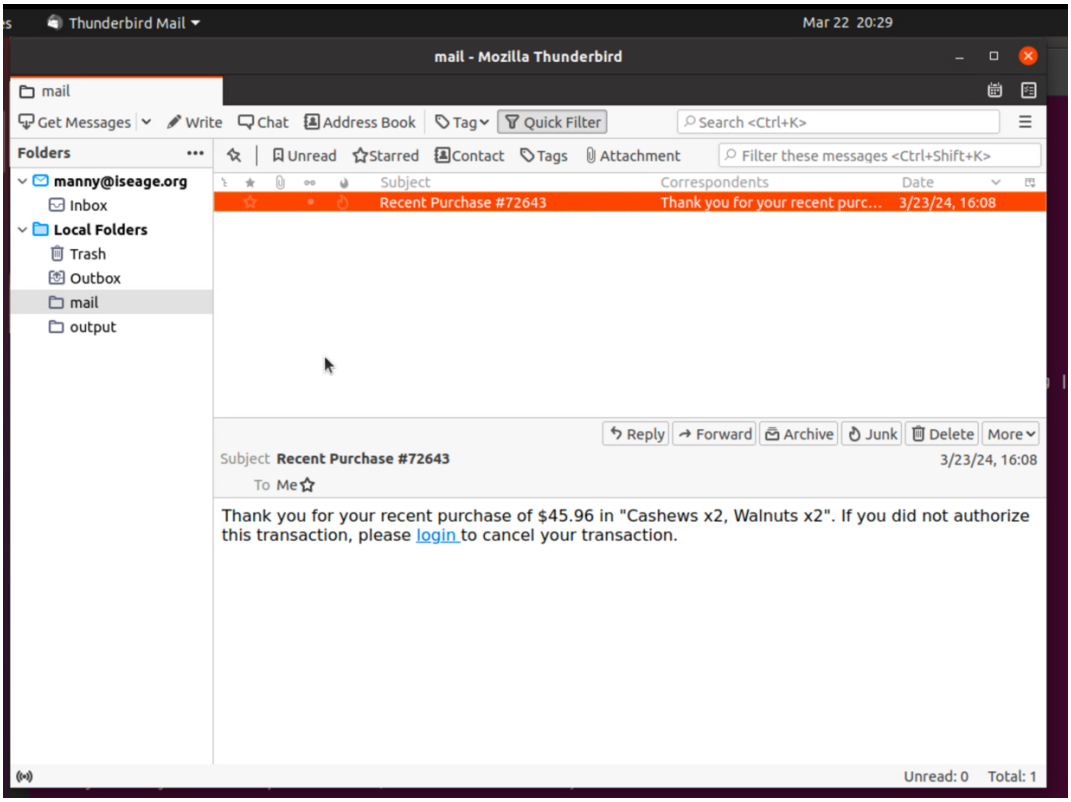
Lab Template: Ethan Roepke

1. **Navigate to www.scratsnutemporium.com in a browser in your Kali VM. Browse the storefront and record the following.**
    a. **Where is Scrat's Nut Emporium physically located?**
    (5 points)
    371A Durham Center
    Iowa State University
    Ames, IA 50010

    b. **What's the most expensive item that is sold?**
    (5 points)
    Pine nuts

    c. **What's the phone number for the shop?**
    (5 points)
    515-294-4000

2. Write an email that you can use to direct Manny to your cloned website (screenshot from Thunderbird).
(15 points)



3. What happens when you try to click the link within Thunderbird directly? What happens when you right-click the link and select "Open Link in Browser"? (2+ sentences) (5 points)

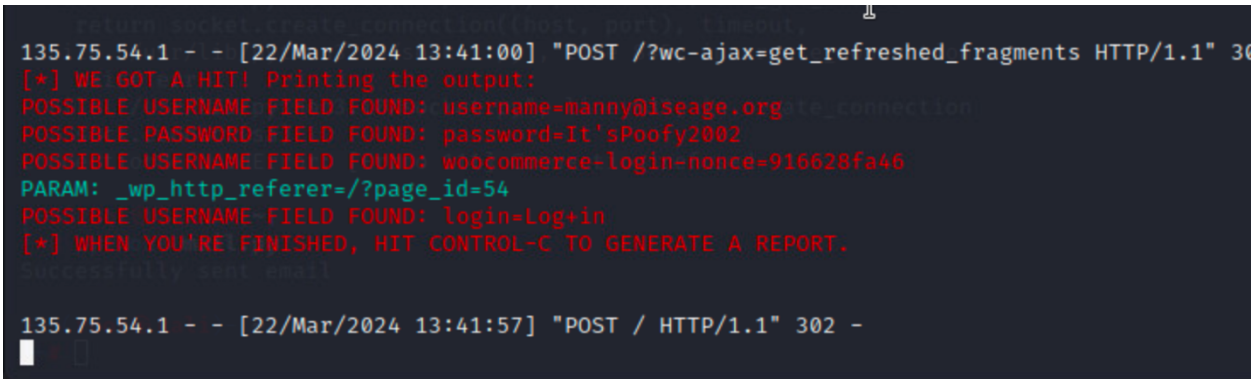
When we click the link directly from the email on thunderbird, it will prompt a message letting us know that this may be a scam. It says this website is trying to impersonate other web pages and letting them know thee web page they may go into which is 135.75.54.2

When we right click the link and open in browser, we are sent to the login page for **www.scratsnutemporium.com**, however it is a copy of the web page with the URL being 135.75.54.2

4. When Manny entered his credentials at the cloned My Account page (no less than two sentences each). From Manny's perspective:

1. **What happened? (5** Points)
   When many entered his credentials on his account in the cloned web page, it looks like the web page got refreshed and removed his credentials from his login try. If you look at the URL, the URL changed from 135.75.54.2 to the real web page URL.
2. **Where was he redirected? (5** points)
   Manny was redirected from 135.75.54.2 login page to the actual web page **www.scratsnutemporium.com** on the login page after he submitted his credentials.
3. **What would a user think? (**5 points)
   A user may think many things, if they do not look at the URL at all, they might think the web paged just refreshed on them and nothing bad happened. The user may also think that they just entered their credentials in wrong so they would reenter their credentials again which would log them in since it directed them to the actual web page URL.

5. Screenshot of logging the username and password for Manny on the Kali box. (10 points)



6. The website at X.X.X.2 did not log Manny in. Please enter these in your lab report, and answer each of these in no less than two sentences each. From the attacker's perspective:

d. What happened?
(5 points)

The user entered his credentials and then was immediately redirected to the real webpage. When the user entered his credentials and creating out Social engineering tool, on out kali box we got an output of the users username and password.

e. Where was he redirected?
(5 points)

The user was redirected to the real web pages **scratsnutemporium.com** login after entering his login credentials on the copy web page.

f. Why is this important?
(5 points)

This is important to have the user redirected to the actual website, because if not, the user would realize that this is a fake/copy website to gather his/her user credentials. Being able to redirect to the actual web page login after the first login try on the fake website will keep the user not suspicious since if they try to login again they will have access to their account.

g. What would a user think?
(5 points)

If a user doesn't look close enough to the URL at all, they may think that the web page either refreshed or accidently input the wrong login credentials. They wouldn't think too much about it because once they try logging in again they will be granted into their account since they are redirected to the real website. However, if the user sees the URL 135.75.54.2, they will think that this is not a real website and research more to figure out if its real or not.

7. Logged in as Manny…

h. What has Manny ordered in the past?
(5 points)

Walnuts

i. What quantity?
(5 points)

2 Walnuts

j. On what date?
(5 points)

March 22, 2020

8. Three domain names that look like scratsnutemporium.com

(5 points)

scratsnuternporium.com

scratsnutemporlum.com

scratsnutemporium.org