Johnny Rivera

Dr. Walden

CIT 485

04/19/22

# Incident Report

## Introduction

Nitroba State University’s (NSU) Information Technology (IT) department received an email from one of their teachers, Lili Tuckrige, in the chemistry department regarding emails the teacher has been receiving. These emails were suspected to be sent by one of the students in her classroom chemistry 109. The system administrator that first received the complaint was able to pinpoint that the attacker sends the harassing emails from the student dorm rooms and the website that they used to launch the attack. This was done by the system administrator by placing a network sniffer on the ethernet port to log the packets that were being sent and received. The investigation materials that we will analyze and use to find the culprit were provided by the teacher and the system administrator. After investigating this incident, we will be able to find out who sent these emails, when the attacks started/stopped and what happened on the network when they sent out these emails.

## Investigation Process

In order to fully understand where to start it is best to organize the data that was presented into a more friendly view so that we can connect pieces of information better.

Diagram, text

Description automatically generated

The diagram shown is a very simple visual aid on how the network works at NSU dorms. The tools I used to investigate this case were Wireshark [1] and the information provided by the System administrator at NSU [2]. While looking through the network sniffing capture that the system administrator obtained, we were able to find the following:

|  |  |  |
| --- | --- | --- |
| User Agent | Given Name | Owner |
| Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) | User 1 | Johnny Coach |
| Mozilla/4.0 (compatible; MSIE 5.5) | User 2 | Amy Smith |

Graphical user interface, text, application, email

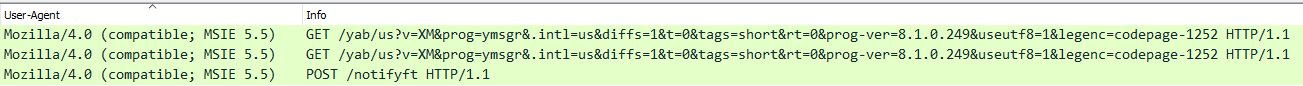
Description automatically generatedText, letter

Description automatically generatedThese were the users that were able to be filters out and discovered with the packets we received. There were instances where users would search online through shopping websites and online videos, but their activity would end there. There were no instances of these excluded users going to any website that deals with emails. The users that are included used email services online, but only one user did the attack. In order to validate that these users could have sent the attack to the victim it was necessary to search time related to the attack. The attack was mentioned to be launched on July 21 but was discovered to be sent around 6 am on July 22nd. The following information was discovered in a packet which shows the details of the attack.

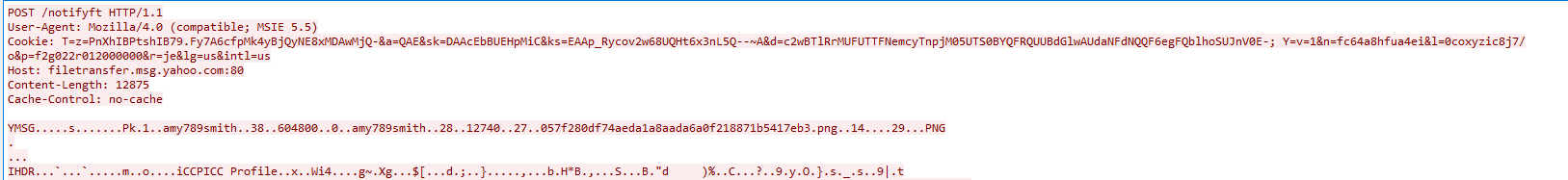
The image(left) provided is a snippet of the information inside the website http packet which provides the text that the user sent inside the website application form. The image (right)[2] above shows the website form that the attacker would have seen and filled out. After analyzing the packets around the attack and the two suspecting user’s network activity it was deduced that User 1, Johnny Coach, launched the attack against Lily Tuckrige. The following chart shows User 1’s relevant network activity:

|  |  |  |  |
| --- | --- | --- | --- |
| Time (07/22/08) | Source | Destination | Comment |
| 05:56:23.54 | 192.168.15.4 | 207.46.19.190 | The user opened his internet browser. |
| 05:57:38.54 | 192.168.15.4 | 74.125.19.104 | Searched: “how to annoy people” on www.google.com |
| 05:58:01.43 | 192.168.15.4 | 74.125.19.104 | Searched “sending anonymous mail” on www.google.com |
| 05:58:07.82 | 192.168.15.4 | 74.125.19.104 | Searched “I want to harass my teacher” on www.google.com |
| 05:58:32.66 | 192.168.15.4 | 74.125.19.104 | Searched “can I go to jail for harassing my teacher” on www.google.com |
| 06:00:44.47 | 192.168.15.4 | 74.125.19.104 | Went to their google calender. NOTE: Email [jcoachj@gmail.com](mailto:jcoachj@gmail.com) found packet from same user\_agent. |
| 06:01:24.25 | 192.168.15.4 | 74.125.19.104 | Searched “send anonymous mail” on www.google.com |
| 06:03:16.82 | 192.168.15.4 | 192.217.199.107 | Visited email.about.com regarding sending anonymous email messages after previous query search. |
| 06:03:43.82 | 192.168.15.4 | 69.25.94.22 | Clicked on ad about [www.willselfdestruct.com](http://www.willselfdestruct.com) from email.about.com |
| 06:04:24.31 | 192.168.15.4 | 69.25.94.22 | Sent harass email to Lily Tuckrige. |
| 06:04:55.38 | 192.158.15.4 | 74.125.19.17 | Checked google mail one last time then disappeared from the network. |

As previously mentioned, the only other suspect that had any network activity regarding mail services was User 2, Amy Smith. User 2’s activity only revolved around what seemed to be a privacy settings change on yahoo. The image below shows the request to yahoo for the p3p which was the privacy preferences.



Looking at the image below we can see some plain text inside the package data which shows User 2’s email url “amy789smith” as well as “iCCPICC Profile” (ICC Color profile [3]). We can infer that she was messing with some of her yahoo user settings in general using the data before and the data collected from this packet. Thus, removing suspicion of User 2.



## Conclusion

A picture containing graphical user interface

Description automatically generated

In conclusion, after looking through the packet capture that was provided by NSU’s system administrator we were able to deduce who the culprit was that sent the harassment email. While looking through the packages that were captured by the network sniffing tool, we were able to find out that the attack happened at 06:04:24 am UTC. The network user that sent the email through the website “www.willselfdestruct.com” was Johnny Coach. This was found out after we investigated the user-agents (browsers) that communicated with the internet. After filtering out the browsers with services such as web servers and other devices we found out that Johnny’s web browser matched the one that the attacker used. Upon tracing Johnny’s network activity, it was found evident due to his suspicious searches related to the attack method/goal that he launched the attack. The activity that gave the user away was the packet pertaining his email information. The user logged onto his email several times, the most relevant ones were noted in the time table showing him checking his calendar and finally getting off his computer. The user did have extra activity after his attack which was found irrelevant to the data, mostly YouTube video searches and a search case “where do the cool kids go to play”. The last email check was most likely to confirm that the service he used to launch the attack did not use his personal email while the previous activity was him feeling good about himself after harassing his teacher. Using all this data I was able to pinpoint that Johnny Coach was the student in CHE 109 that was harassing the teacher Lily Tuckrige.

References

[1] Download. Wireshark · Go Deep. (n.d.). Retrieved April 20, 2022, from https://www.wireshark.org/

[2] Digital corpora. Digital Corpora " 2008 Nitroba University Harassment Scenario. (n.d.). Retrieved April 20, 2022, from https://digitalcorpora.org/corpora/scenarios/nitroba-university-harassment-scenario

[3] Wikimedia Foundation. (2022, April 7). Portable network graphics. Wikipedia. Retrieved April 20, 2022, from https://en.wikipedia.org/wiki/Portable\_Network\_Graphics#File\_header