Nitroba Investigation

Austin Wolfe CIT-485

Introduction

This investigation is being carried out by the Nitroba University Incident Response team in response to an incident involving Lily Tuckrige, who teaches CHEM109 at Nitroba University. Tuckrige has been receiving harassing email at her personal email address, lilytuckrige@yahoo.com; she believes the email is from a student in her class. Tuckrige contacted IT support with a screenshot of the harassing email, wanting to know the identity of the harasser. As the email body text was not very helpful, the system administrator who received the complaint wrote back to Tuckrige asking for the full email message headers. Tuckrige responded with a screenshot of the mail headers, having obtained them by pressing the “Full message headers” button in Yahoo Mail. Inside the email header is the IP address 140.247.62.34, which points to a Nitroba student dorm room that is shared by three women: Alice, Barbara, and Candice. Since Nitroba provides no Wi-Fi, only Ethernet, in every room, Barbara’s boyfriend, Kenny, installed a Wi-Fi router inside the room with no set password.

There are several email messages appearing to come from the IP address, so a network sniffer was set up on the ethernet port at the dorm, logging packets, waiting for the harasser to send another email. On 7/21 Tuckrige received another harassing email, only this time the message was sent through a website called “willselfdestruct.com”, which shows the message to Tuckrige, but soon after stops displaying the message, displaying instead the text “Message Has Been Destroyed”.

The goal of this investigation is to find clear evidence of the harasser using the email screenshots, the packets collected from the network sniffer, and the class roster...

Investigation Process

Upon opening the packet capture, nitroba.pcap, inside Wireshark, the 140.247.62.34 address was first investigated. Using the display filter **ip.addr==140.247.62.34**, it can be seen that the address 192.168.15.4, which is a well-known private IP address, is communicating with the public 140.247.62.34 address over tcp, the public address. Upon further investigation of the packets provided in the current display filter, it can be seen from the details pane, under Ethernet II, that 192.168.15.4 has the layer 2 address Apple_e2:c0:ce (00:17:f2:e2:c0:ce) and 140.247.62.34 has the layer 2 address HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60). With the HonHaiPr_2e:4f:60 device being the destination layer 2 address for packets in this capture, it is identified as

a local endpoint for the network; the 192.168.15.4 is one of the private addresses being used by a device behind the router in the dorm room.

To see all the local addresses that are in use, the display filter **ip.src==192.168.15.4/16** is used to get a range of all the local addresses that initiate any kind of communication with another device (the network ranged being controlled with the /16). There are a few other IP addresses in this local range, one to note being 192.168.1.254 with the mac address HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60), which identifies this as the local address of the router.

Having an idea of what local addresses to look out for, the next part of the investigation was to look for tcp streams containing information on who the harasser could be. The display filter **frame contains "tuckrige"** was used and returned two frames relating the Apple_e2:c0:ce device at address 192.168.15.4 to the harassing email. Upon following the tcp stream at frame 80614, occurring on 2008-07-22 06:02:57.548149 UTC, a post request to the website at "sendanonymousemail.net" contains an HTML form. Inside the form contains the email address, "lilytuckrige@yahoo.com"; the sender address, "the_whole_world_is_watching@nitroba.org"; the subject of the email, "Your class stinks"; and the message body, "why do you persist in teaching a boring class? We don't like it. We don't like you." The following table is an overview of the devices in this communication.

date	time	frame	source	dest	dest-host	protocol	info
7/22/2008	6:02:58 UTC	80614	192.168.15.4	69.80.225.90	www.sendanonymousmail.com	http	post
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			

In the other tcp stream, found at frame 83601 occurring at 06:04:24.311700 UTC, is another post request, but this time to the website "willselfdestruct.com", the same website as in the email received by Lily Tuckrige (as seen in the screenshots). Inside the request is an HTML form addressed to lilytuckrige@yahoo.com, with no sender address, and the subject "you can't find us". The message section of the email form contains the text, "and you can't hide from us. Stop teaching. Start running", matching the email received by Lily Tuckrige.

date	time	frame	source	dest	dest-host	protocol	info
7/22/2008	06:04:24 UTC	83601	192.168.15.4	69.25.94.22	www.willselfdesctruct.com	http	POST
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			

Looking closer at the two previous tcp streams and doesn't show any direct personal identifiable information, but the web browser that is being used by the person at his address can be seen, Mozilla/4.0, and can be used to filter packets only involving this particular web browser. During this investigation, before using the web browser as a display filter, while looking through more frames for the Apple_e2:c0:ce device at the 192.168.15.4 address, it was discovered that two different web browsers were being used. After investigating the other web browser, Mozilla/5.0, and finding no evidence of the harasser, one specific to the two previously found tcp streams, Mozilla/4.0, was used. This indicates that there could be two different users on this device.

After using the display filter **http.user_agent == "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"** and scrolling through the returned packets, a few frames were directly of interest and their tcp streams were investigated. The first one in frame 74920, occurring on 2008-07-22, at 05:58:32.660583 UTC, shows a GET request for the host answers.yahoo.com, that includes the text “can I go to jail for harassing my teacher”.

date	time	frame	source	dest	dest-host	protocol	info
7/22/2008	05:58:33 UTC	74920	192.168.15.4	209.73.187.220	answers.yahoo.com	HTTP	GET
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			

In another tcp stream located at frame 74644 occurring on 2008-07-22 05:58:14.137736, in the GET request in the “referer” section, the following can be seen: Referer: http://www.google.com/search?hl=en&q=i+want+to+harass+my+teacher. Someone using this computer, in this web browser, searched on the web, “I want to harass my teacher.”

date	time	frame	source	dest	dest-host	protocol	info
7/22/2008	05:85:14 UTC	74644	192.168.15.4	209.73.187.220	answers.yahoo.com	HTTP	GET
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			

There is now evidence that someone using this this computer not only sent the email but was also actively searching on the topic of harassing their teacher; however, it doesn’t identify the user responsible. Scrolling through the packets filtered based on the web browser a little more reveals http packets for google mail. Following the tcp stream at frame 79292, 192.168.15.4 can be seen communicating with mail.google.com, and inside the GET request for /mail/im/emotispirites/crab.png, the gmailchat cookie can be seen: gmailchat=jcoachj@gmail.com/475090.

date	time	frame	source	dest	dest-host	protocol	info
7/22/2008	06:01:10 UTC	79292	192.168.15.4	74.125.19.17	mail.google.com	HTTP	GET
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			

Conclusion

In the list of Chem 109 students, there is listed “Johnny Coach”, and the email address jcoachj@gmail.com corresponds closely to that name. This makes Johnny Coach a high priority suspect in this investigation, with all the gathered evidence pointing towards this student. The following is a table demonstrating the timeline of the gathered evidence, all gathered while the device at 192.168.15.4 had this web browser description: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1).

date	time	frame	source	dest	dest-host	protocol	info
7/22/2008	05:58:14 UTC	74644	192.168.15.4	209.73.187.220	answers.yahoo.com	HTTP	GET
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			
7/22/2008	05:58:33 UTC	74920	192.168.15.4	209.73.187.220	answers.yahoo.com	HTTP	GET
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			
7/22/2008	06:01:10 UTC	79292	192.168.15.4	74.125.19.17	mail.google.com	HTTP	GET
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			
7/22/2008	6:02:58 UTC	80614	192.168.15.4	69.80.225.90	www.sendanonymousmail.com	http	POST
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			
7/22/2008	06:04:24 UTC	83601	192.168.15.4	69.25.94.22	www.willselfdesctruct.com	http	POST
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60			

As seen in the table above, all of the evidence gathered is within a close timeframe, making it likely that all of this internet traffic belongs to the same person, that person being Jeremy Coach. Based on this evidence, Johnny Coach sought content regarding harassment on “answer.yahoo.com”, and then obfuscated and sent harassing email using the websites “sendanonymousmail.com” and “willselfdestruct.com”.

Other students discovered in packets during this investigation include: Amy Smith, based on the username amy789smith found in a yahoo messenger authentication packet; Ava Book, found inside an HTTP/XML packet. No conclusive evidence was found that these two students sent the harassing emails.

date	time	frame	source	dest	dest-host	protocol	info	student name
7/22/2008	06:09:59 UTC	90388	192.168.15.4	66.163.181.179		YMSG	Authentication	Amy Smith
			Appl_e2:c0:ce	HonHaiPr_2e_4f_60				
7/22/2008	06:09:59 UTC	90471	209.191.93.51	192.168.15.4	address.yahoo.com	HTTP/XML	HTTP/1.0 OK	Ava Book
			HonHaiPr_2e_4f_60	Appl_e2:c0:ce				

In closing, it should be mentioned that there are still things to be investigated more closely on this network in regard to the pcap data provided. When investigating arp packets, it was discovered in frame 14157 the duplicate use of the IP address 192.168.1.64, belonging to both the devices HonHaiPr_2e:4f:61 (00:1d:d9:2e:4f:61) and Apple_5a:77:9b (00:1f:f3:5a:77:9b). While the HonHaiPr_2e:4f:61 was involved in a lot of normal looking traffic, the Apple_5a:77:9b device showed up mainly in arp requests and in multiple packets like the one in frame 13937, with the source address 24.64.79.171 and destination address 198.168.1.64 belonging to the Apple_5a:77:9b device, the protocol being Messenger, carrying this “critical message”:

RITICAL ERROR MESSAGE! - REGISTRY DAMAGED AND CORRUPTED.

To FIX this problem:

Open Internet Explorer and type: www.registrycleanerxp.com

Once you load the web page, close this message window

After you install the cleaner program you will not receive any more reminders or pop-ups like this.

VISIT www.registrycleanerxp.com IMMEDIATELY!

This activity should be investigated further, since the duplicate ip address issue could arp spoofing, leading to session hijacking, and possibly more. Though it seems that Johnny Coach is clearly the person sending the harassing email, an accusation should be postponed until more investigating can be done, just in case something more sinister is happening on the Nitroba network.