Harassment at NITROBA State University
The case

You are a staff member at the Nitroba University Incident Response Team.

Lily Tuckrige is teaching chemistry CHEM109 this summer at NSU. Tuckrige has been receiving harassing email at her personal email address.

- Tuckrige's personal email is lilytuckrige@yahoo.com
- She thinks that it is from one of the students in her class.

Tuckrige contacted IT support.

- She sent a screen shot of one of the harassing email messages.
- She wants to know who is doing it.
The email message.

From: nobody@nitroba.org
To: lilytuckrige@yahoo.com

Subject: we don't like your class

Sun, 7/13/08 5:21 PM 1KB

we don't like your class

"nobody@nitroba.org" <nobody@nitroba.org> [Add]  To: lilytuckrige@yahoo.com

Please stop teaching it. You aren't very good. We hate you.
Nitroba's IT wrote back to Lily.

The IT tech told Lily:

- The screen shot wasn't tremendously useful.
- Can you get the full headers?

Lily sent back a screen shot with the headers:
Nitroba's IT wrote back to Lily.

The IT tech told Lily:

- The screen shot wasn't tremendously useful.
- Can you get the full headers?

Lily sent back a screen shot with the headers:
The IP address points to a nitroba dorm room.

$ host 140.247.62.34
34.62.247.140.in-addr.arpa domain name pointer G24.student.nitroba.org
$
The Dorm Room

Three women share the room:

- Alice
- Barbara
- Candice

Nitroba provides 10mbps Ethernet in every room but no Wi-Fi. Barbara's boyfriend Kenny installed a Wi-Fi router in the room. There is no password on the router.
To find out what's going on, Nitroba's IT sets up a packet sniffer.

Who is sending the harassing mail?
Now we wait
The guy attacked!
And here is the message:

You have been sent a secure e-mail from someone you know.

To view the message please click here.

If the above link does not work, you can paste the following address into your browser:

http://www.willsselfdestruct.com/secure/inkeys834

You may view this message only once for 30 second(s), after which it will self-destruct.

If you leave this page or refresh the page the message will self-destruct.

Will Self-Destruct has forwarded this message on behalf of the author. We do not send our own messages nor do we store the message or your email after your message has been viewed.

If you would like to no longer receive mails from Will Self-Destruct please click the following link

http://www.willsselfdestruct.com/secure/block?email=lilytuckrige@yahoo.com

Kind Regards,
Will Self-Destruct
No, here is the message

This message will self-destruct in 4 second(s). If you leave this page or refresh the message will be destroyed.

From: [Undisclosed Sender]
To: lilytuckrigge@yahoo.com
Subject: you can't find us

Message:

and you can't hide from us.
Stop teaching.
Start running.
And there goes the message:
So who did it?

Chemistry 109 class list:

Teacher: Lily Tuckrige

Students:
  Amy Smith
  Burt Greedom
  Tuck Gorge
  Ava Book
  Johnny Coach
  Jeremy Ledvkin
  Nancy Colburne
  Tamara Perkins
  Esther Pringle
  Asar Misrad
  Jenny Kant
How to solve this problem:

1. Map out the Nitroba dorm room network.
2. Find who sent email to lilytuckrige@yahoo.com
   - Look for a TCP flow that includes the hostile message
   - Find information that can tie that message to a particular web browser.
3. Identify the other TCP connections that belong to the attacker
4. Find information in one of those TCP connections that IDs the attacker.