Lab – Scenario for assessment

Lab Background

A background to the Laboratory has been provided separately on the Moodle. Students are to complete at least two of the training scenarios which are based on training scenarios produced by George Mason University and made available as Digital Corpora[1] under a National Science Foundation grant. In the laboratory session, student will be completing a scenario based on Digital Corpora's NITROBA training scenario which is extended extended and includes an assessable component which is to be submitted by as part of your major assignment. Otherwise, the laboratory is not assessed.

Scenario

This scenario is based on the NITROBA training scenario. The case is a hypothetical case used for training and competency assessment purposes. The scenario is in two parts:

1. Part 1 – which you are to complete during the laboratory. Although you will be working individually, you are encouraged to collaborate with other students and seek guidance from instructors;
2. Part 2 – which is to be submitted as part of your major assignment. You may commence Part 2 during the laboratory.

Scenario Background

(Review this background in conjunction with the provided Nitroba slide deck)

You are completing your Master of Cyber Security at the fictional Nitroba State University (Nitroba). You are making ends meet by working as a security administrator working in Nitroba's IT Department.

Nitroba's IT department received an email from Lily Tuckrige, a teacher in the Chemistry Department. Tuckride has been receiving harassing emails and she suspects that they are being sent by a student in her class Chemistry 109, which she is teaching this summer. The email was received at Tuckrige's personal email account, lilytuckrige@yahoo.com. She took a screenshot of the web browser and sent it in (slide 2).

The system administrator who received the complaint wrote back to Tuckrige that Nitroba needed the full headers of the email message. Tuckrige responded by clicking the Full message headers button in Yahoo Mail and sent in another screen shot, this one with mail headers (slides 3 and 4).

The mail header shows that the mail message originated from the IP address 140.247.62.34, which is a room in the Nitroba student shared accommodation (see slides 5 and 6). Three

[1] https://digitalcorpora.org/

women share the room. Nitroba provides an Ethernet connection in every room but not Wi-Fi access, so of the occupants have installed a Wi-Fi router in the room, which is a common practice. There is no password on this Wi-Fi (see slide 7).

Because several email messages appear to come from the IP address, Nitroba decides to place a network sniffer on the ethernet port (see slide 8 and 9). All of the packets are logged. On Monday 21 July, Tuckrige received another harassing email (see slide 10). But this time instead of sending it directly, the perpetrator sent it through a web-based service called willselfdestruct.com (see slide 11). The website briefly showed the message to Tuckrige, and then the website reports that the Message Has Been Destroyed (see slide 12 and 13).

You have been given the screen shots (on the slide deck), the packets that were collected from the Ethernet tap (the NITROBA.PCAP file), and the class list for Tuckrige's class Chem 109 (see slide 14).

Part 1

Your task is to determine if one of the students in the class was responsible for the harassing email.

Prior to commencing the technical activity, spend 15 minutes or so considering what you have been asked to do and your suitability to do it. Record your thoughts on the two key considerations and how you might manage them i.e.:

1. Is this within my area of expertise?
2. Is there a conflict of interest?

Complete your technical analysis to discover the email's sender. Make necessary contemporaneous notes and record any data files (which you will need for Part 2).

A step-by-step sample solution is provided (see Appendix A). You are encouraged to spend ½ hour planning your own approach prior to attempting the activity using the sample solution.

NOTE: THIS SAMPLE SOLUTION IS NOT TO BE STORED SEPERATELY TO THIS PASSWORD PROTECTED DOCUMENT

Part 2 (for major assignment)

In Part 1, you identified the email's sender and they have been spoken to and subsequently suspended from the University. They are appealing the suspension and since Nitroba is a state-owned University, the appeal is being heard in the NSW Civil and Administrative Tribunal (NCAT).

After speaking with you, Nitroba's in-house counsel (i.e. lawyer) understands that your preliminary analysis might have been rushed because at the time you were also completing an intensive course as part of your Master's study. Given you have plenty of time, you may want to re-perform all or some of your analysis or conduct further examinations (the NITROBA.PCAP file will be available on Moodle for the duration of the course).

Counsel has now instructed you to:

1. Prepare an expert's report detailing the analysis/examinations that led you to conclude that XXXX was the sender of the email;
2. Demonstrate the reliability of your conclusion by showing an alternate solution or using alternate tools to arrive at the same result – you might also find you arrived at the wrong conclusion first time around;
3. In doing the above, you are to assume that the NITROBA.PCAP file provided to you by the IT Department was reliable up to the time that it was provided to you.