Assessment Worksheet

Conducting an Incident Response Investigation for a Suspicious Login

Course Name and Number: CSCI 352 Comp Law and Forensics

Student Name: Gary Fowler

Instructor Name: Ismail Guynedas

Lab Due Date: 12/10/2017

Overview

In this lab, you used NetWitness Investigator to analyze the network traffic to identify a suspect's login credentials from an FTP packet trace. You also used P2 Commander to analyze the digital portion of a forensic image and locate the transferred file on the suspect's own evidence drive. You exported the suspect files, added bookmarks in the Case Log, and created a report to detail your findings.

Lab Assessment Questions & Answers

1. What was the username of the FTP client who successfully transferred files on the FTP server? What was the IP address for that account?

   badguy
   172.16.177.132

2. How many e-mails did the alleged offender send to his partner? What are the two e-mail addresses involved in the e-mail conversation?

   3 emails
   badguy11111@gawab.com
   b603358@bofthew.com

3. As a forensic investigator, would you be able to play back an entire TCP session if it is requested under trial?

   Yes

4. What time did the alleged offender choose to perform the actions? Why do you think this is particularly important? Where did you get this information?

   1:08:58
   this is important because it tells us when he commited the crime
   I got this information from the RFC version of the email as well as the right pane of the RSA application

5. What is the name of the "local user" account involved in the alleged actions (*Hint: where in the file structure did you find the suspect files*)? What was the IP address of the alleged offender workstation?

   Administrator
   172.16.177.132

6. How many attempts to access the FTP server did you find during the packet capture analysis? Why is this important for your case?

   4 attempts, 2 unsuccessful 2 successful
   If this attempt was a very large number it could be performed by a program, but a smaller number proves the person at the PC did it.

7. What was the password of the FTP client account used to perform the alleged actions? How were you able to obtain the password?

   you will never guess this !! was the password
   yes