Lab 10 - Assessment Worksheet

Conducting an Incident Response Investigation for a Suspicious Login

Course Name and Number:

CYBS 7359 - 010

Student Name:

Natnael Kebede

Instructor Name:

Dr. Renita Murimi

Lab Due Date:

04/13/2020

Lab Assessment Questions

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?

   The username of the FTP client who successfully transferred files on the FTP server is badguy. The IP address for this account was 172.16.177.132

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

   Yes. As a forensic investigator, I would be able to play back an entire TCP session if it is requested under trial. There are tools such as NetWitness Investigator which can be employed by forensic specialists to playback an entire TCP session to trace file transfers. Consequently, the information collected from such tools can be used as a starting point for continuing the investigation into the suspects own computer.

3. 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 from?

   The alleged offender performed the actions at 01:08:58 on 2010-Jul-31. This information is particularly important since important insights can be gleaned

from analyzing the timestamp of the actions. For instance, an FTP access time outside regular office hours might indicate unauthorized usage. The time information can be retrieved from the NetWitness Investigator report, which chronologically arranges events of a given service. In this particular case, the FTP service attempts were drilled and provided the timestamp of all FTP transmissions.

4. 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?

   The name of the “local user” account that was involved in the alleged actions is Administrator. The IP address of the alleged offender workstation was 172.16.177.132.

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

   During the packet capture analysis, I found two attempts to access the FTP server. This is important for my case since it indicates the attacker’s knowledge of the FTP account information. That is, a lower rate of attempts followed by a successful logon usually means the user has the password for the account, while several attempts could point towards a brute force attack.

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

   The password of the FTP client account used to perform the alleged action was you will never guess this !!

   I was able to obtain the password by analyzing the FTP packet capture in NetWitness Investigator. Once the FTP service type was drilled into, the FTP packet sessions were shown to have the associated password (mentioned above) that was involved in performing the FTP actions.

   The process was possible since passwords are visible in the FTP data as FTP traffic travels in clear text. This makes it easy to capture the information using a packet sniffer and analyze it using NetWitness.