NAME: Megan Leonard

TODAY’S DATE: 3/26/2023

# ISEC 375 Homework 8

Answer the following questions based on your reading of the textbook, the module key points, and the instructor’s presentation this week.

1. **[6 points]** Write down the basic steps when you’re conducting a forensic analysis of VMs.

We first want to make sure that the power to the system that is running the VM is secure as we do not want someone tripping over a cord and shutting it down. Now we determine which type of hypervisor we are working with which is determining if there is a separate OS it is using. Once we determine the type, we can better grasp how to handle it. If we are working with a type 2, we will begin with a forensic image of the host computer and the network logs. Then we see if the VM is located within the host computer or if it is a virtual network adapter. We need to check for usb drives and VMs within the VMs. We then export all files associated with the VM from the host machine and record the hash values of those files. Now we can open the VM in forensics software as an image file.

1. **[6 points]** Why should you make a live acquisition before powering off the VM under investigation?

You should make a live acquisition before powering off the VM because powering it off will change the state of the VM. We use snapshots and images to record the state of the VM at that moment and to keep record of it. There is the chance of programs running and temporary files within the VM that shutting it down will destroy. There is always the chance that the VM instance is temporary and the VM will reset to its original state upon shut down which would lead to a lot of trouble.

1. **[3 points]** Which one should be preferred during a live acquisition? GUI tools or command-line tools? Why?

I believe the command-line tools would be preferable as while the GUI tools are easier to use, if we are working with Windows OS we could get false readings with them and the system may not have enough resources for it to run. The command-line allows us to have more control over our work.

1. **[6 points]** Your company network is under cyber-attack. External attackers are scanning your publicly visible IP addresses continuously. There are some indications that hackers may compromise a few internal servers. You are performing network forensics to understand the intrusion details. What is the difference between the points of view of you and the server administrator? If the server administrator is reluctant to help you, what do you do for the administrator to collaborate more?

The network forensics view shows the external attacks with the scanning of the publicly visible IP addresses. The server administrator may not see the attack as there are indications they can compromise the internal servers. The best way to think of it is there is a wall between the network and the server which is where they interact. The network will look at one side of the wall and see the attackers and their scanning. The server is on the other side and can not see them at the time so the network would need to give the server the heads up. If the server administrator is reluctant to help, we can show them the indicators we spotted where the hackers could compromise the internal servers and we can talk with them about the benefit of attacking the problem now instead of waiting for them to access the internal servers.

1. **[9 points]** Please write down a challenge for network forensics. Explain why is it a challenge?

A challenge for network forensics is the data collection itself. The data that can be found can be a lot and having to determine what is useful can be time consuming. The size of the network affects the data as well as a network could be the size of a house, a company, a city, and even cover the world like the internet. So this will mean you have to take into account time zones when finding corresponding time and determine if the data needs to be real-time as that would be harder to collect than data already saved in the past. Data also covers a lot of different types and area so you would have to determine what type you need and the time frame.