CySER Workshop

25 May 2022

Deborah Wells

Workshop Title: *Virtualization and Cybersecurity: Exposing the Dark Web*

Agenda:

1) **Introduction**
2) **Lecture:**
    a. Overview of Virtualization
    b. Understanding how virtualization fits into industry/Use Cases
    c. Introduction to CSI Linux
    d. Fundamentals of the Dark Web
    e. Using CSI Linux in a VM to conduct an investigation

3) **Lab:**
    a. Install this on your AWS workstation
        i. Virtual Box
        ii. CSI Linux
        iii. Add Rhino Hunt from https://cfreds.nist.gov/

    b. **Scenario:** *The city of New Orleans passed a law in 2004 making possession of nine or more unique rhinoceros images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB key seized from one of the University's labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the dd image is on the CD-ROM you've been given. In addition to the USB key drive image, three network traces are also available—these were provided by the network administrator and involve the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his Ph.D. at the University since 1972.*

    c. **Task:**

    Recover at least nine rhino pictures from the available evidence and include them in a brief report. In your report, provide answers to as many of the following questions as possible:

    - Who gave the accused a telnet/ftp account?
    - What's the username/password for the account?
    - What relevant file transfers appear in the network traces?
    - What happened to the hard drive in the computer? Where is it now?
    - What happened to the USB key?
    - What is recoverable from the dd image of the USB key?

- Is there any evidence that connects the USB key and the network traces?
  If so, what?
  When you're done, exclaim loudly and jump about the room.

Part II: Using CSI Linux go out to the Dark Web

a. Install this on your AWS workstation
   i. Virtual Box
   ii. CSI Linux

b. **Scenario:** *ACME University was faced with a large exfiltration of intellectual property (IP) from a new cyber education and research program that had just started this year – of all things, the program just so happened to be Cybersecurity (CySER)! The CySER directors call your forensics company, XXXXX, and wanted to hire you to go out and investigate where the IP was exfiltrated to and who did such a dastardly crime! During the initial intake from the CySER lead director, you have a fairly good suspicion that the data was being sold on the Dark Web.*

c. Task:
   i. You are tasked to go out to the Dark Web and using some of the tools in CSI Linux try and find out if indeed the data was sold to the Dark Web.
      1. If it was, then try to find out as much as you can about who might have stolen the credentials and who they are selling the information to.

         For exercise purposes you will need to search for higher education credentials from another university or college (not ACME University – that was a fictitious name).

      2. Provide a screenshot or 2 from what you found.