Andrew Li

Project Description:

My project will be to write a homework scavenger hunt that combines the use of volatility and wireshark, in the style of a cybersecurity CTF.

Milestone Goals:

1. Write a “virus” that is downloaded through a site (the site does not have to be anything),
    a. The virus will hopefully be fileless and open a file and send it to an IP
        i. If not fileless, we can make it install a miscellaneous driver or become a keylogger
2. Create a empty linux VM with a file that has the contains a super secret password
3. Make a server through a raspberry pi or another computer, if not a server, a website that simply downloads the virus
4. Generate a pcap for the virus download, the PCAP shall contain the file of the virus
5. Generate memory dump when the virus starts running
6. Generate a wireshark pcap for when the virus sends the super secret password back to another IP
7. Create the files for download
8. Create question to ask:
    a. The point of these questions is to lead the person using the tools to discover the virus and what it is doing

For more plausibility it the assignment could just be a malicious actor that runs a small script that sends information to another IP. This could also be simply a virus downloaded as part of a program that is appended to that program that is then run.

Final project goal:

Write a homework assignment in the 565 style that utilizes both wireshark and volatility to discover a virus.