INF 528
Case 3: Suspicious Portscanning

Background

You have been hired by the IT staff at the local college. Upon demonstrating a new security appliance, the appliance started reporting portscanning activity originating from a particular computer system. Upon investigation and cross-correlating the registered MAC address, it was determined that the computer system belongs to Alicia Houston. This student has a system on loan from the college for independent research. The college security policy states that any portscanning or other malicious activity must be fully investigated. The IT staff hired you to investigate this system.

The target of the portscanning appears to be a system belonging to Professor Biff Tannen of the Philosophy department. It appears as though Ms. Houston was a student of Prof. Tannen's in the Fall of 2015 in PHIL 230.

Both systems have been forensically imaged and provided to you for analysis. Professor Tannen's system is indicated as 02USC01 and Ms. Houston's system is 02USC02. Additionally, prior to shutdown, Professor Tannen's system had the RAM imaged using FTK imager to a network share, Y:\. You will be given this memory image at a later point for analysis.

Task

Determine if any suspicious activity was conducted by Ms. Houston. You have been given both systems to analyze, 02USC01 and 02USC02. Be sure to conduct a thorough investigation of both systems and be sure to indicate whichever artifacts and analysis involve one or both systems.

Deadline

A final report is due by 10:30 AM on 4/26/2018. The report must be a hard copy with any and all investigative notes.