MP5 Improvement Recommendations

Problem 5.2.1: Operating Systems

I would suggest, for the purposes of deeper understanding, asking students to further investigate the boot behavior and identify the specific file that causes the default boot behavior of erasing the hard drive. Specifically, they should identify the script that contains the following command `dd if=/dev/zero of=/dev/sda` in rc.d.

Rather than the relatively black-box understanding that the system erases itself, this will give students a better idea of how the system accomplishes this.

Problem 5.2.7: Extraction

There was a significant amount of confusion regarding this problem – specifically due to the differences between "recovery" and "extraction." Furthermore, for the Whiterose VM, the students identified "evilplan.doc" as the most suspicious file, but because that was not recoverable, they had to "extract" the toxic waste JPEG file instead. It has been very unclear for the students in terms of recovering versus extracting, as well as which file to zone in on. As is, the problem is not straightforward enough.

I would suggest making the file extraction for this similar to the LeetHaxor VM, where they recover the file in question by going to the victim's VM. This could be leaving the suspect's evilplan.doc in the victim's VM, etc.

Problem 5.2.8: Escape Plan (Part II)

This problem led to issues among students who were able to recover the image, but received incorrect coordinate information. Specifically, the operating system (in properties or details) of the file provides its version of the coordinates, and students who use this version get the answer wrong.

The idea was to use the metadata to find the coordinates, but the OS itself provides this information (which seems to be different than the expected answer). Suggestions to fix this include either removing this entirely or using the OS' provided coordinates as the final answer.