EE576 HW 1

Matt Ruffner

January 19, 2019

1 Cybersecurity Implementation

To start with, UC places much more emphasis on information protection processes than the Intel implementation does. Intel places significant emphasis on protection practices, however their emphasis on the detection aspect of security is much higher than that of UC. Intel has outlined a much more detailed and in-depth plan, with specific aspects of their implementation of what they deem to be adequate cybersecurity. This is logical since Intel is a large corporation with much at stake but also many resources to plan with. Intel explicitly explains how their implemented solutions will utilize less than the equivalent of 175 employee hours.

Both adoptions of the framework include the idea of 'continuous improvement', with the UC implementation stating that "cybersecurity is a journey, not a destination." I agree with this, as does Intel's plan. As technology evolves, alongside normal use cases, protection and detection policies and methodologies must adapt in lock step. Intel also plans to "Communicate an aligned cybersecurity risk picture to senior leadership." This aligns with UC's goal to create a tool which fascilitates periodic self-assessment on a deptartment by department basis. This leads into a key difference between the two adoptions of this framework. It is a matter of principle, however still relevant. UC is adopting this framework on behalf of its researchers and as an academic institution. Intel is doing this adoptions as a company and for a more profit and security of its customers based approach.

2 Ethics

2.1

The student's action in searching for the loophole was ethical, he may or may have not found one. In searching for one he was exploring the integrity of the system in which he trusted his own private information. The student's action in continuing to access the file was very unethical, once he had explored enough to determine the loophole was indeed what he suspected, he should have stop accessing the files.

The sys admin's failure to fix it sooner was unethical. I discovered a flaw in the unnofficial transcript system and UK took at a least week to fix, and offered no thanks for finding the fix.

2.2

The programmers position in this situation is unethical since it sounds like they are pushing the limits of acceptable actions in the given situation.

The engineers position in this situation was also unethical since they were also pushing the limits of acceptable behavior.

2.3

The student's action of infecting hundreds of computers was very unethical. No matter the circumstance, disseminating code of this type should be considered unethical.

If the output of the program was cheery and benign, the situation would have still have been unethical. This simple benign message represents security flaws in the system and should be considered a serious breech.

If the student's virus breeched and deleted files it would have been equally as unethical.

3 Deterlab

3.1 File Hunt

`/.hidden/asdf136Kentucky-5kqlw.jpeg`
`/dev/136Kentucky-2jjaj.JPEG`
`/var/log/136kentucky-3.jpg`
`/etc/wuer136kentucky-4.JPG`
`/usr/share/pixmaps/xbzf136KENTUCKY-1.jpg`

3.2 Information Hunt

`/var` is a directory where the OS writes data during the course of its operation, such as log files, log files and other computer specific information. `/dev` is the directory where device files are stored, representing an interface by which data can be sent to physical hardware.

`df -h` info in `diskfree.txt`

`cat /proc/cpuinfo` in `vendor.txt` - "Genuine Intel"