What I Will Need for My Professional Toolkit

Alexei Hooks – anh5653@psu.edu

The role that I plan on working in when entering the workforce should be a position that deals with security and practices within the company that I work for. I will create an example company called "Money Capital" that is an investment banking group that has over 600 billion in customer assets. My role within Money Capital is to oversee all security alerts and move potential threats into a secure location to be analyzed. From there, I will need to analyze this potentially malicious threat to better learn about what kind of attack might be used against the company. This job will require multiple pieces of hardware and software to be most effective in protecting the company's image and client's privacy.

Software:

- Wireshark
    - Wireshark is used to monitor network traffic within the company's mainframe network in an attempt better alert analysts of possible malicious content trying to breach Money Capital. Any threat alerts that come from Wireshark will be moved to be more deeply analyzed by other software and personnel.
- IDA Pro
    - IDA Pro is a software that will allow me to better analyze possible malware after being extracted from the alerts in Wireshark. This process can tell the security team what type of attack is trying to breach the network, and lead the team to move to take the necessary security steps.
- Windows PowerShell
    - Windows PowerShell is another opportunity to take a potentially corrupt file and analyze it in a safe space. Although less options are within the program compared to IDA Pro, the ability to analyze strings and other basic items about the file could prove valuable for the security of the company.
- Secure Virtual Machine with Kali Linux
    - Within my work desk, I am expecting access to a computer that has capabilities to hold and use a virtual machine that I can move and tamper with the malicious files that Wireshark alerts the security team. Having an operating system such as Kali Linux would provide me with an array of tools that could be used for both defensive and offensive measures to better secure the network of Money Capital.

Hardware:

- Computer Hardwired to the Main Network of Money Capital
    - For each piece of software mentioned above, I need to be able to have a secure connection to the company's network to make sure that I can get an up-to-minute stream of data to allow my software to alert me as potentially malicious packets come through the network.
- Dual or Tri-monitor Setup
    - Having access to multiple monitors on a single computer allows the user to have visually access to more programs at once, so that I would not miss any alerts and could use the screens for real-time comparisons of programs.
- Physical 2FA Key Fob

    - It is important to have two factor authentication at the company's disposal, as it both useful for security and memory. With this key fob, the connection will ask for a password that is randomly generated and must be entering within a certain time limit. This allows for a secure connection that eliminates potential malicious attacks against the Money Capital's employee's saved passwords.

Resources:

- NIST Guideline Booklet
    - Having the NIST Guideline within reach is important for me as it allows for quick reference in planning and controlling the security of Money Capital. The booklet will give insight into key plans in safe and secure methods to better Money Capital's security programs.
- Company HR Manual and Cybersecurity Policies
    - Having the company's most recent compilation of Cybersecurity policies will allow the employees of Money Capital to best approach a situation throughout the business day so that everyone can be prepared in the fight against malicious threats. If there is ever a dispute or a situation that I would need to analyze the situation within the business day, having the reference of a human resources manual would be helpful. This would provide help or a contact that I would be able to use as a reference to resolve interpersonal issues that could arise within the company.
- Emergency Phone Number Contacts of Co-workers
    - Having a contact sheet within my work space in case of an emergency, either within the network or a physical emergency, as it will give me a quick reference to use in order to gain help or spread news of a crisis situation. Along with having these numbers, they should be used appropriately as certain people could be best to call over others in different situations.