**DSCI 519 LAB-1 Report: CyberCIEGE Introduction**

**Rishit Saiya (rsaiya@usc.edu)**

The CyberCIEGE Introduction Part of the lab has gone through several basic elemental scenarios which help an organization to maintain its sanctity of security. Some of the scenarios which were divided in phases included objectives like Buying systems, securing perimeters, training, automation, etc.

***PHASE - 1: Objective - 1: Buy Moe and Curly workstations***

Instead of buying a workstation computer, a "Bit Flipper Border – Network Firewall" (mistake) was bought to test out the level of risk involved in such scenario. With these configurations, the objectives of Phase-1 aren't achieved. So, from that point onwards, Curly and Moe were assigned a workstation computer each.

***PHASE - 1: Objective - 2: Connect the workstations to LAN1***

While doing the network configurations, LAN2 (mistake) was connected instead of LAN1. Trivially, this led to another attack then workstation systems were connected using LAN1 to the network.

***PHASE - 1: Objective - 3: Hire the Support Staff***

Since, there was no liberty of exploring options for hiring IT Manager, no false choices here were implemented in hiring IT Management - **Larry**.

***PHASE - 2: Objective - 1: Select "Beware Email Attachments" and "No External Software" for both workstations***

In this scenario where an external software/malware (Aladinz) was installed, the module instructed to check on "Beware of Email Attachments". But instead, in order to endure the simulation, the option of "Lock or Logoff if unattended" (mistake) was checked. With these configurations, the objectives of Phase-2 weren't achieved. In the next step, the trivial instructions were followed.

Despite the above configurations, there came a pop-up of another attack. Post analyzing the attack report, it was conclusive that "No external software" had to be configured on both workstations.

***PHASE - 2: Objective - 2: Buying Training for employees***

Post this, there was another attack, wherein the prompt asked to give training to the employees. In order to conserve on economic front, "Low Training" option (mistake) was chosen. The system still was vulnerable and later "Medium Training" option was selected.

***PHASE - 3: Objective - 1: Physical Security for the Office Area***

Since random people were entering the office, the objective was to protect the office zone. It was deduced that some physical security for the doors "Key Lock" (cheapest) be selected (mistake). But this didn't give clearance to the objective and hence, the public access to the Entire Office had to be constrained limited to the COMPANY field.

***PHASE - 3: Objective - 2: Automated Configurations on Office systems***

Above configurations led to the final left objective of accountability to the vulnerabilities. A pop-up informed that the work-station which was left logged as quoted by the Janitor, there had been a malicious activity resulting in loss of $550 (mistake). This was a mistake as the configurations made earlier didn't account for the holistic approach to the security. Clearly, after the configuration of "Automated Locks/Log-Off if left Unattended" made in the workstations cleared this objective as well.

The above steps enabled to get a gist of basic necessity of security to maintain systems and organization secure as a whole. This lab helped to understand the primitive knowledge and hands-on experience on the CyberCIEGE game. Sequential executions of above objectives with the aid of prompts from the game, helped to achieve the necessary objectives in securing Borsoft's assets.