EXPERIENCING SECURITY:
Hands On with CyberCIEGE

Ayush Dhoot

Developing the Industrial Internet of Things

Background:

Security is an important aspect of any organization as there are loads and loads of data available. Any individual can misuse that data for many purposes. Now that we are in Industry Revolution 4.0 where there is advancement in Cyber and Physical Networks, we need to have network security and information assurance more than ever before. There is increasing threats of hackers who try to infect computers or devices having an internet connection. There are rival companies who try to steal assets or secrets from each other. Having a data breach in a company which has all your bank credentials is a nightmare for a person. Hence, security is very important for any system. Nowadays, companies have huge budgets set aside for maintaining the security of their systems as even a small loss of data can have long lasting effect on the company as well the user.

What I did:

I chose to go with the second option of playing the game called CyberCIEGE. It is an innovative videogame and tool to learn more about computers and networks security concepts. The game is based upon the basis of SimCity where users must make choices and run the city. [3] Here, the user has money to operate and defend their systems by making choices and run the simulation according to the choices made. I first downloaded the game from the website and installed it on my Windows 10 laptop. There was an introductory video which gave the details about the game and how to play. The video mentions that the user is the chief of managing information security and how each decision made by the user defines the output of the game. Then I was taken to a window where the main menu was displayed as shown in figure below.

Figure 1 : Main Menu

I selected the help menu where there was a tutorial video showing how to play the game and walkthrough the scenarios. [4] I then started with the first campaign module 'Training'. The first scenario was 'Stop Worms' where I had to buy a router and connect a new employee to the internet. The main objective of the scenario was to highlight the risk involved with downloading stuff from the internet without any antivirus protection. The scenario was designed to make the user understand that they should not open any attachments which is not from a verified source. There were also few multiple-choice questions which gave the above concept a proper understanding. This scenario had help and tips along the whole process so that a user can get the feel of the interfaces.

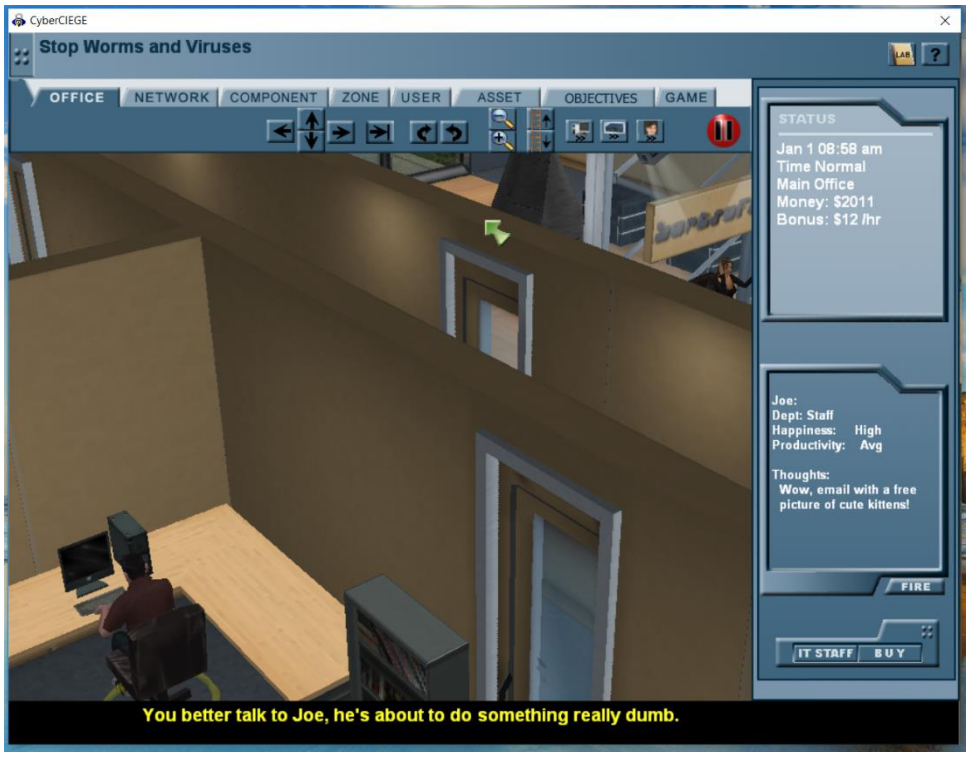

Figure 2 : “Stop Worms” scenario start

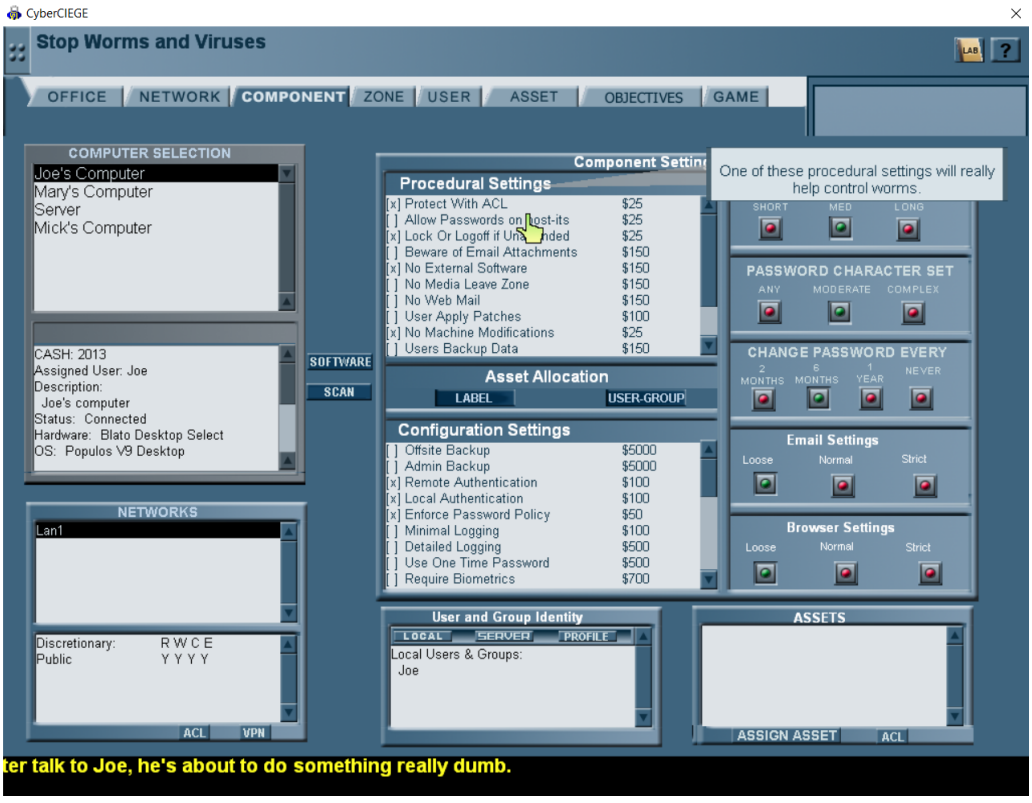

Figure 3 : “Stop Worms” scenario solution

The second one was called ‘Life with Macros’ where we introduced to the very basic, yet drastic threat caused by macro viruses. They are usually placed on top of the software which are used daily and cannot be ignored like Word, Excel. The only solution to this scenario was to install an antivirus software and regularly update and scan the computer, so that the macro viruses are destroyed by the software and cannot harm the files of the user.

The third scenario of the ‘Tutorial’ module was considering ‘Identity Theft’. This scenario presents us with an employee who has just joined the company. I had to connect her computer with an internet connection so that she can surf and browse the internet. Then I had to have some procedural settings changed so that there are no worms, trojan invasion occurring. Finally, I had to secure the connection so that there is no identity theft. There was a question which tells that we should not put our credentials in webpages which do not have ‘https:/’ as the ‘s’ stands for secure shell which will keep the credentials safe.

The next scenario was ‘Passwords’ where an employee was using the password of another employee to create entries and glitches in the app. Here, I had to make few changes where the password had to be changed every 6 months and the complexity was also increased. Even I had to train the employee that they should not keep their password written on post-its and have the computer shut down automatically after a period of inactivity. The new policies regarding the passwords helped the company as there was no more data being changed or modified.

After completing the ‘Training’ campaign, I learnt a lot about the risks involved with having no security in the software and internet. Then I moved to the next campaign called ‘Starting Scenarios’. The first one was ‘Introduction’ where I was introduced to the more complex options of the game. I had to setup computers for two new employees and train them according to the security level clearance they had. I had to staff an IT guy to maintain my network system and also had few changes made to the procedural system so that there are no alterations of data or data breach happening.

The next scenario was ‘Physical Security’ where I was introduced to the concept of having security levels and having mechanisms in place to enforce that the user cleared for that level is only allowed to enter or use those resources. I had to create

a zone where the security level was ‘Secret’ by purchasing physical security like guards, ID cards, Cypher lock to reach the total of 400. The next phase was to create a similar zone where the security level was ‘Top Secret’ and required a physical security level of 700.

After this, ‘Network filters’ scenario explored the problems occurring from the internet and make use of the component network filter to avoid them. The second phase was to have a firewall setup so that there is no leak in the data regarding a secret formula file. The network filter was configured to deny all incoming connections so that there is no change in the outgoing messages but block unwelcoming data from the internet. The asset was protected using a network filter along with a firewall connected to an internal server as it reduces the risk of trojans to destroy the assets.

The next scenario was ‘Patches’ where the network was vulnerable to external threats and could cause harm to the computers and assets stored on it. I had to scan the whole network to find the flaws to identify the origin of the attacks. Then, I had to place software patches to the system so that the flaws are rectified, and the security is restored once again. There can be a possibility that the new patches can break the system, so it is better to first apply the patches to a test system before uploading it to the main system.

The last scenario is the ‘PCA’ where I had to help the Professional Croquette Association protect their secrets using a DMZ. I had to purchase a secondary email server and use it as a proxy for the original email server. Also, I could have made exceptions for the incoming mail in the network filter configuration which could serve the purpose, but it could be taken down using DoS attacks.

What I learnt:

The game ‘CyberCIEGE’ gives hands on experience with tasks which teaches more about security of any system and the risks involved with it. The game properly creates environments where there are real life security issues which simplifies the learning of security and the consequences of any decision made for it. [2] This was a different type of an assignment where I didn’t know where to start but after each scenario, I learnt more about security than what I would have learnt by reading some papers or books. I did learn about how security is important in any organization or individual work and how a simple mistake can have disastrous

effect on the overall process. As per the game, the scenarios are made so that it can cover modules like Network Security, Information Assurances and Security Policies, Identification and Authentication, Cryptography. [1] The game deals with Cybersecurity and Information security concepts whose objective is to raise awareness among the user about security without the conventional notion of studying it from a book but rather actively simulate it through a game. I learned about the strategies I need to apply to maintain security and assurance in networks and computers.

References:

[1] https://my.nps.edu/web/c3o/syllabus

[2] https://www.usenix.org/legacy/events/cset11/tech/final_files/Thompson.pdf

[3] https://my.nps.edu/web/c3o/cyberciege

[4] https://my.nps.edu/web/c3o/scenarios