Student's name: Matheus Henrique Schaly

Professor's name: Carlisle Adams

Course: CSI 4139 Design of Secure Computer Systems

Due date: 2nd December, 2019

Report #5

a) There are many conflicting objectives within a security environment. For example:

1. You, as a security person, have a limited budget. You need to keep your environment safe, but at the same time you must ensure that you will not be spending more than the necessary. So, if you are having problems letting unauthorized users come into your company, you'll need to think about having either a low cost and low security method or a high cost and high security method to let people in. These are conflicting objectives.
2. You may want to have a secure environment by using passwords. Then, you'd have the conflicting objective. On one hand, if you want a really secure environment, you'd ask for your employees to make strong and long password, change it often, use two factor authentications… On the other hand, if you want a convenient and easy to use environment, you'd allow your employees to have weak, short passwords, or not using any password at all. The security person would need to consider these two extremes and create something in between that would work for his own company.
3. Choosing the way to store permissions of a person to an object. The security person could decide to go with an ACL (access-control list) or a CL (capability list). In an ACL, each object has a list of users. Whereas in a CL each user has a list of objects. A CL is better suited to delegate permissions to other users; it's easier to completely

remove permissions from a user; it's easier to find all the objects that one single user has access to, etc. Whereas in a ACL, we would have quite the opposite of an CL. Therefore, it's the security person duty to choose the best list of permissions of his own company.

b) Yes, especially Because it's based on real life example scenarios. In its interactive environment, CyberCIEGE covers significant aspects of computer and network security and defense. Players of this video game purchase and configure workstations, servers, operating systems, applications, and network devices. The players have to make trade offs as they struggle to maintain a balance between budget, productivity, and security.

   The game includes configurable firewalls, VPNs, link encryptors and access control mechanisms. It includes identity management components such as biometric scanners and authentication servers. Attack types include corrupt insiders, trap doors, Trojan horses, viruses, denial of service, and exploitation of weakly configured systems. Attacker motives to compromise assets differ by asset and scenario, thereby supporting scenarios ranging from e-mail attachment awareness to cyber warfare.

   The effectiveness of CyberCIEGE has been demonstrated in several studies. [1]

   Therefore, as it can be seen, CyberCIEGE has a wide spectrum of real life example scenarios that a security person may have to face.

c) CyberCIEGE actually already has a pretty good job on realistically portraying day-to-day security officer's tasks. I believe that the people aspect should be improved. For example, it's too easy to only ask an employee to follow "certain rules", or to simply click a button saying "train this employee". Whereas in real life, your employee may be hard to deal with, he may not simply follow "your instructions". Also, "training an employee" may involve making contact with a company that does training, or may involve asking for some of your other employees to train his colleague.

Therefore, having such an easy interface where you can simply click things does not really realistically portray the reality. However, it may be a hard task to find a way to implement those types of improvements into an educational computer game.

d) *Stop Worms*: This scenario was too simple and its tasks were common sense. For example, it's obvious that we shouldn't open suspicious e-mail attachments. So, I haven't learned anything from this scenario except for how the game works.

Life With Macros: I've learned that Macro virus are contained within documents types such as Word or Excel.

Identity Theft: Same as Stop Worms, too obvious, nothing new to be learned. For example, it's obvious that you need to be cautious when receiving an email from your bank requesting that you provide personal information. As email addresses and websites can be easy spoofed.

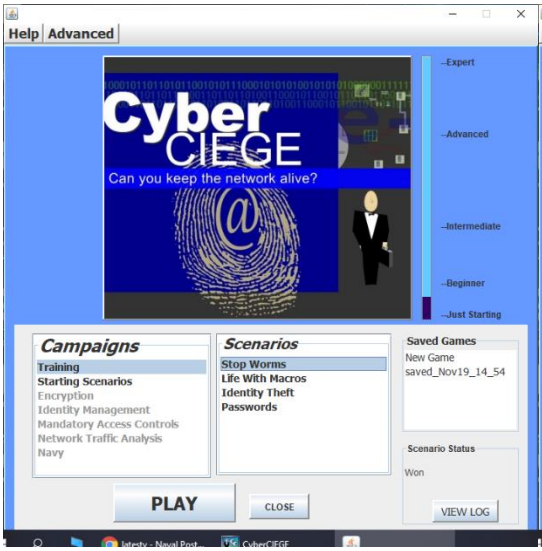
Passwords: I've learned that people may actually save their passwords in a post-it below their keyboard, and that the security officer has to enforce a policy to not allow employees to do that.

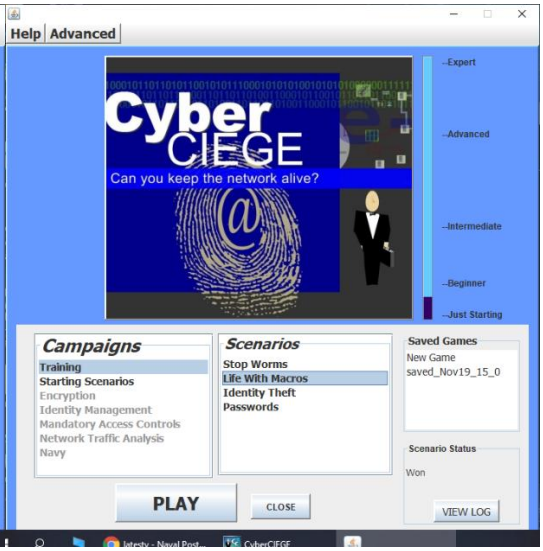
Introduction Scenario: I've learned that the security officer also has to deal with physical zone security. For example, by including a guard at the door, key lock, or some kind of scanner.

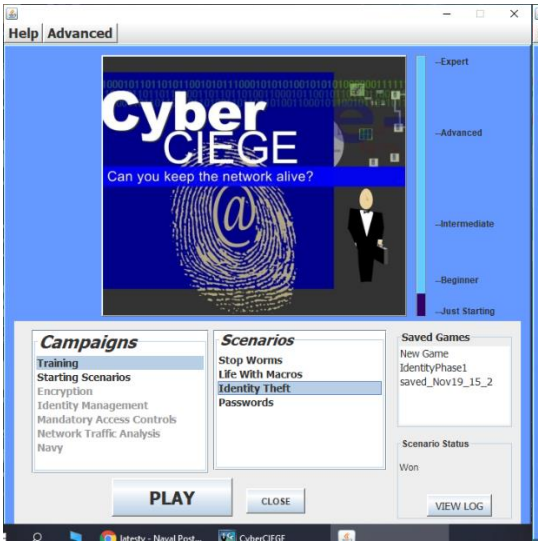
Physical Security: I've learned that the security officer also has the responsibility to give access permit access to people that actually have access to that specific part of the company and to deny that access to people that are unauthorized.

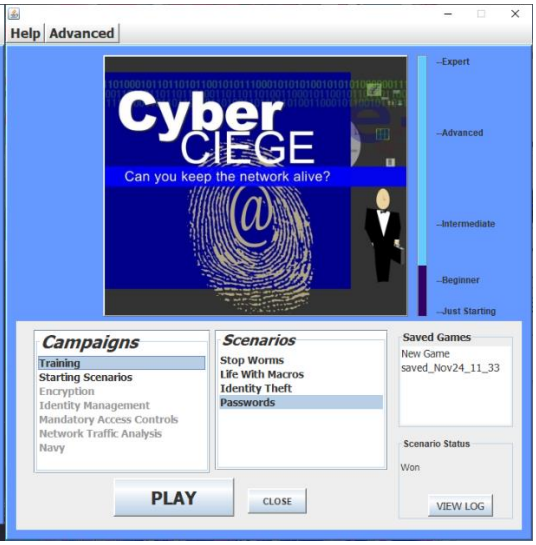
Patches: I've learned that if the IT guy updates patches as released then the web application server is less likely to be compromised. So, it's important to patching frequently and correctly.

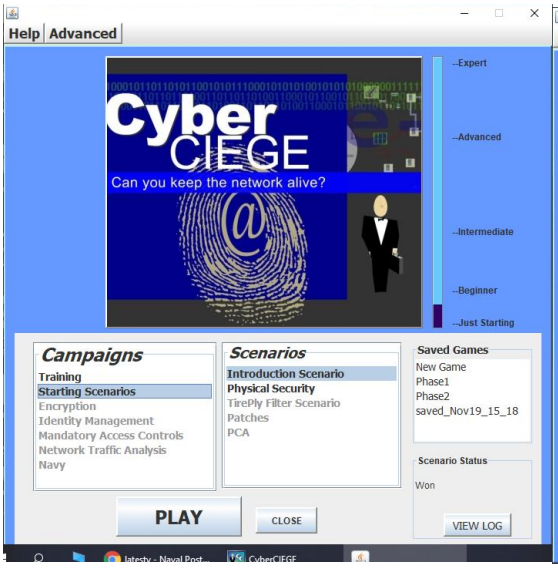
Won's scenarios screenshots:

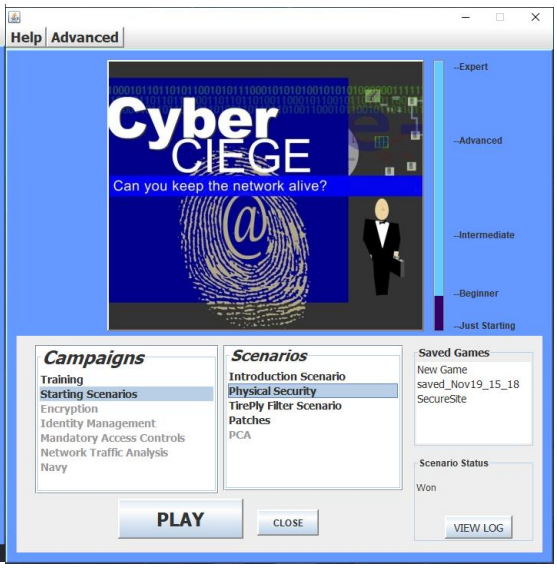


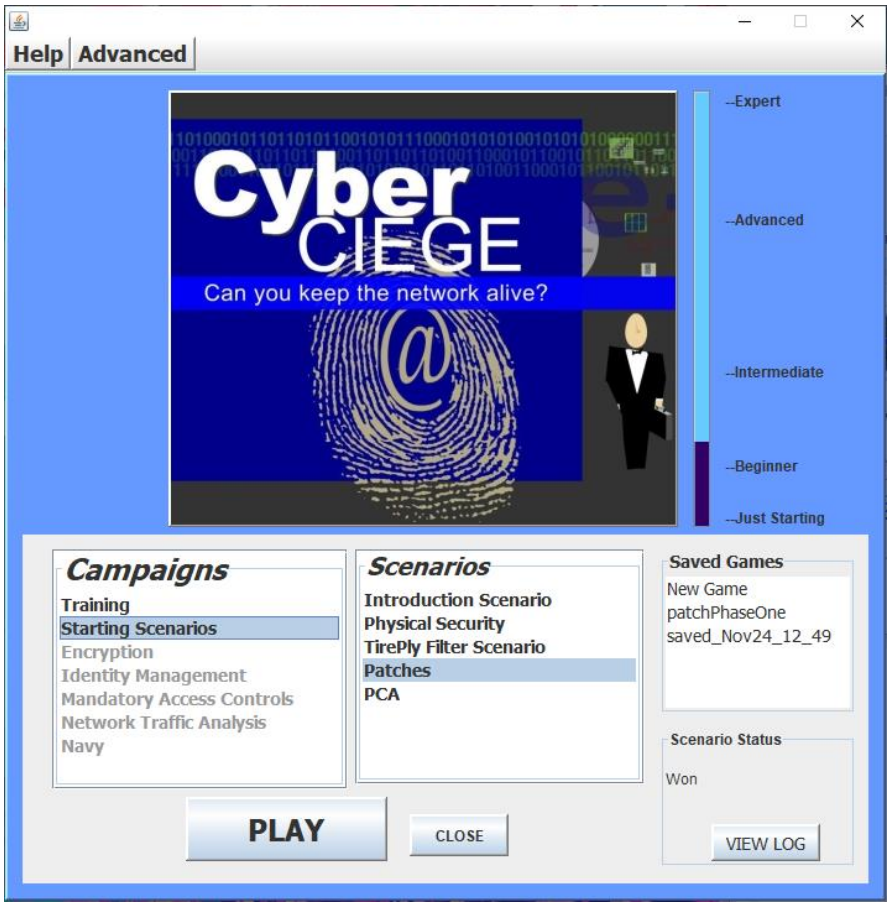












Reference

[1] My.nps.edu. (2019). *CyberCIEGE - Naval Postgraduate School*. [online] Available at: https://my.nps.edu/web/c3o/cyberciege [Accessed 24 Nov. 2019].