DSCI 519 LAB-3 Report: CyberCIEGE User Identification

Rishit Saiya (rsaiya@usc.edu)

The CyberCIEGE User Identification of the lab has gone through several basic elemental user identification scenarios which help organizations to maintain their sanctity of security. Some of the scenarios explore the need to identify users to computers and the advantages of centralized authentication servers.

Phase - 1: Objective - 1: Users cannot login to workstations unless the workstations they know who they are. Somewhere there must be a list of authorized users.

While doing the Lollipop server configurations, I profiled the authentication server in a wrong manner by adding the marketing in authentication server profile which resulted in not achieving the authentication server settings (mistake). Post this, I configured the authentication server as instructed in the lab, by adding all users and this led to centralized authentication through Lollipop server.

Phase - 1: Objective - 2: Your boss's boss heard that computers are more secure if users are forced to use really long passwords. Configure the computers (or just the authentication server if used) to require long passwords. (And no, neither boss can explain the technical rationale for this mandate)

Post this, a popup showed up stating that the password policy was weak and this issue of password length was resolved by setting password length high. Post this, the Sugar Spinner Data needed to be protected by enforcing ACL mechanism. Primitively, I only assigned that ACL to public (mistake), which later was changed to individual users by assigning (Y, Y, Y, Y) permissions in the (Read, Write, Control, Execute) controls respectively.

Phase - 1: Objective - 3: Run secure for a few game hours while allowing all users to achieve their goals.

The scenario is made to run in the simulation for some time which later leads up to winning it and progressing to Phase-2.

Phase - 2: Objective - 1: Remote Access for Fiona - Fiona needs to access Sugar Spinner data from the hotel. Make sure she is known to the computer that contains that asset, or to the authentication server if one is used.

While assigning remote access to Fiona (new user), I assigned proper access in the authentication server. However while assigning the Access Controls, I purposely assigned wrong access control by assigning (Y, N, N, Y) permissions in the (Read, Write, Control, Execute) controls respectively (mistake). This threw an error where Fiona was not able to modify the data on Lollipop Server. Post this, I assigned correct accesses (Y, Y, Y, Y) permissions in the (Read, Write, Control, Execute) controls respectively. Also, there was a password policy pop-up and hence, I had to assign a OTP (One-Time Password) policy.

Phase - 2: Objective - 2: Once she has access, Fiona must work for a while from the public workstation in the hotel business office

The scenario is made to run in the simulation where Fiona is working for some time which later leads up to winning it and progressing to Phase-3.

Phase - 3: Objective - 1: Authorized Strangers - Visitors from a branch office are dropping in daily to meet with staff and access the Sugar Spinner data. You have no way to establish unique accounts for each visitor. However, the visitors have smart card badges that identify them as members of the company's marketing group. These smartcards also include complete biometric information about the user. Provide them with access to the Sugar Spinner Data. Consider the use of an authorization profile and an ID Device.

Initially, Blake (an outsider) wanted to access Sugar Spinner data through visitor workstation. Some certain settings were enabled wherein an outsider person can access requisite resources by adding visitor's workstation in Lollipop server to enable authentication. Meanwhile, I did not add the Marketing in a profile section of the visitor to the Marketing section (mistake). This led to an error showing: "Visitor's workstation lacks criteria for whom it should allow access". Thereafter, I was prompted to buy an ID Card reader & installed hence I installed it on the Visitor's workstation to verify an outsider user. Post this, the visitor automatically traveled to the visitor's workstation.

The above steps enabled me to get a gist of the User Identification in systems and organization secure as a whole. This lab helped to understand adding new user's information in an established user identification system with stronger ACL, Password and Hardware/Physical security and its importance through the CyberCIEGE game. Sequential executions of above objectives with the aid of prompts from the game, helped to achieve the necessary objectives.

Deliverable Answers:

Phase-1 Ans: If the network topology has to be changed, I will impose a network segregation method depending on the user's profile, activity history, criticality and functionality. The segregation of networks will compartmentalize the critical aspects of infrastructure and also enhance security. It is simple to implement network policy if just a few people need to utilize it. The network segregation must be tightly enforced in order to prevent access by outsiders to the critical components. Technologies like VLAN have the potential to be very instrumental for network system configuration. Systems should be given tasks only based on the operations and profile that need to be carried out for the system.

Phase-2 Ans: I have used One Time Password to increase security to prevent hackers from exploiting Fiona's password to access the business server. Additionally as directed, Card Readers were also installed for the Phase-3 in case of a new visitor. For existing/new users, the same techniques can be implemented.

CyberCiege Survey

Please mark the correct answer where the choices are provided.

1. List any difficulties you encountered during the CyberCiege lab exercises.
No. But some more resources could help in doing the lab more efficiently. Oftentimes, most errors we dealt with had no proper interaction with the user and hence only Trial-and-Error was the method to be used here.

2. The CyberCiege labs were helpful in reinforcing some of the concepts covered in class.
Strongly Agree
Please explain: Some of the concepts could be learned easily through this labs which provided unique blend of knowledge and
excitement.

3. The CyberCiege labs provided additional insights.
Strongly Agree.
Please Explain: I got to learn about Hardware/Physical Security which is often vital in infrastructures.

4. The CyberCiege labs helped me learn about the cost of implementing security and the importance of trade-offs.
Strongly Agree.

Please Explain: I understood how to manage budgets on different aspects of security constraints.

5. The CyberCiege labs helped me connect the concepts learned in class to the real world implementation.
Strongly Agree
Please Explain: I understood how state of the art industries work on a day to day basis and their problems.

6. Do you have any other comments about the CyberCiege learning tool?
Everything is very good but additionally resources and graphics of the game can be made better.