**DSCI519**

**Lab 3: CyberCIEGE User Identification**

The CyberCIEGE User Identification scenario explores the need to identify users to computers and the advantages of centralized authentication servers. The scenario also includes the challenge of authenticating remote users on hostile networks and computers. Finally, the scenario introduces the use of identity peripheral devices as a way of identifying authorized strangers and determining their authorizations.

***As with all CyberCIEGE scenarios, students are encouraged to explore the effects of “wrong” choices as well as trying to select the correct choices. Plan on playing the scenario several times before finally going through it making what you believe are the correct choices.***

This scenario explores the following concepts:

* Computers require information about the identity of users. This information may be used to control who can access (e.g., login to) a workstation or who can remotely access a server.
* Verification of user identity is necessary to achieve individual accountability.
* Verification of user identity is necessary to provide access control and implementation of least privilege.
* Use of *authentication servers* can simplify the management of multiple users and multiple computers. When deployed, only the authentication server must manage information that is used to identify users. “Client computers” then use the authentication server to establish the identity of users.
* Sometimes circumstances demand that users access enterprise servers from remote computers that may be hostile (e.g., computers in a Hotel’s business center). Identifying users from these computers can be risky unless suitable counter measures are deployed.
* Some situations require a means to authenticate “authorized strangers”, i.e., people who are authorized to access a system, but are not explicitly known to the system. Examples are facilities that host many authorized visitors where it is not practical to establish individual user accounts for each visitor. Use of smart cards that contain user authorizations enable systems in which the computers are configured to recognize the authorization (e.g., all members of a specific group) rather than recognizing specific individuals.

In this scenario you can largely ignore Zones and physical security issues. Also, don’t worry about hiring or firing support staff or the trustworthiness of your virtual users.

**Play Scenario**

To reach the User Identification scenario, you must unlock all scenarios using the “Advanced/Preferences” menu selection.

To play the User Identification scenario, select the “Identity Management” campaign and the “User Identification” scenario and then click the “PLAY” button.

Read the briefing and the objectives screens, and explore the encyclopedia (via the “F1” key). As you play the scenario, remember you can save the state at any time and come back to that state later.

**Phase 1, First Identify Users to the Computers**

* Press the space bar (or click the play button) to start the scenario. Observe the users are unhappy because they can’t login to their workstations. When the ticker at the bottom of the screen suggests it, press F1 to learn how about user identification in CyberCIEGE.
* As per the instructions in the encyclopedia, configure the computers to identify users. Note you can do this either by configuring each individual computer (i.e., using the “LOCAL” button), or by defining an authentication server. If you configure an authentication server, you can also easily assign it client computers as seen in the encyclopedia “Authentication Server” heading. To configure an Authentication server, review the instructions per the encyclopedia – pick a server from the list in the upper left of the COMPONENT screen and then click the “Authentication Server” button on the lower middle of the screen.
* To configure local authentication, go to the component tab, select a user’s workstation, click on “LOCAL” under “User and Group Identity” and add the corresponding user. You will need to do this for each of the 4 employees.
* To configure an authentication server, go to the component tab, select one of the servers, click on “Authentication Server” under “User and Group Identity”. Add each of the 4 users and then click on “Clients” and add each of their workstations.
* After you provide the computers with user identification information, you will be directed to change a password policy. If you’ve defined an authentication server, this can be accomplished by changing a configuration setting on that one computer. Password policies are set by selecting the computer from the list in the upper left of the COMPONENT screen and making selections on the upper right of the COMPONENT screen. If you chose local authentication you will need to make this change in each user workstation.
* Access to server-based resources should include individual accountability, and this requires that the server that contains the asset only permit remote access to authenticated users. This is configured via the “Remote Authentication” checkbox in the computer’s “Configuration Settings” (middle of the COMPONENT screen). First select the component in the upper left of that screen, then make the configuration change.
* If you chose local authentication then you need to add users to the local group on the server hosting the Sugar Spinner data.
* If you chose an authentication server then the server with Sugar Spinner data needs to be added as a client in the authentication server.
* The Sugar Spinner data needs protection. It is on a server that also includes an outward facing web server – and you don’t have the resources to move the web server to a separate computer (e.g., to create a DMZ.) Thus, you need to consider access control mechanisms (e.g., ACLs). Select the Lollipop Server (in the upper left list of computers in the COMPONENT screen) then select the “Sugar Spinner Data” in the asset list (lower right) and click the ACL button. Who should be able to access this data?

**Phase 2, Remote Authentication**

* Let the game run until prompted to check your new objectives.
* Configure the system so that the Sugar Spinner Server can identify Fiona as directed by the objectives. This will require you to make changes to local groups on the server with Sugar Spinner data or to the authentication server depending on which you chose in earlier phase.
* Let the game run until something bad happens. After three attacks, you will be prompted to press F1 to see how to prevent these attacks.

Authorized Strangers:

* Check your new objectives
* Look at the visitor’s workstation and consider the use of peripheral devices that would let you recognize authorized visitors. Note you cannot add user accounts for visitors.
* Configure a validation profile on the visitor’s workstation to permit access by the appropriate group of users. This will require you to make changes to local groups on the server with Sugar Spinner data or to the authentication server depending on which you chose in earlier phase.

**Finish scenario**

* Exit the scenario by clicking the “Quit” button in the GAME screen.

**CyberCiege Survey (mandatory but not graded on the content)**

Please mark the correct answer where the choices are provided.

1. **List any difficulties you encountered during the CyberCiege lab exercises.**
2. **The CyberCiege labs were helpful in reinforcing some of the concepts covered in class.**

* Strongly disagree
* Disagree
* Agree
* Strongly agree

**Please explain:**

1. **The CyberCiege labs provided additional insights.**

* Strongly disagree
* Disagree
* Agree
* Strongly agree

**Please explain:**

1. **The CyberCiege labs helped me learn about the cost of implementing security and the importance of trade-offs.**

* Strongly disagree
* Disagree
* Agree
* Strongly agree

**Please explain:**

1. **The CyberCiege labs helped me connect the concepts learned in class to the real world implementation.**

* Strongly disagree
* Disagree
* Agree
* Strongly agree

**Please explain:**

1. **Do you have any other comments about the CyberCiege learning tool?**

**Deliverables**: Prepare a report in PDF format with a font size of 10 points, single-spaced, single column and upload it to D2L “Lab3” folder:

* A one-page summary about what you had to do to successfully complete this scenario including a discussion of what did not work and why.
* For phase 1, answer the following question:
  + If you were allowed to change the network topology and the allocation of functions to computers, what might you do differently?
* For phase 2, answer the following question:
  + What did you do to keep attackers from accessing the enterprise server using Fiona’s password?
* Game logs in a zipped folder.
  + Click the “Advanced” menu button and select “Collect Logs”. This will create a zipped folder containing information about your ALL played scenarios.
  + Extract logs related to the “Identity management” scenarios (collect all files in “logs” directory and create a zipped folder for submission).
* Answer the CyberCiege survey questions (mandatory but not graded).

**Grading Rubric**

**Part 1:**

* Step 1: Configure computers to identify users:

Report correct Solution: 5 points, Explore Incorrect Solution: 5 points.

* Step 2: Change and set password policy correctly:

Report correct Solution: 5 points, Explore Incorrect Solution: 5 points.

* Step 3: Correct remote authentication configuration:

Report correct Solution: 5 points, Explore Incorrect Solution: 5 points.

* Step 4: Configurations to protect Sugar Spinner data:

Report correct Solution: 5 points, Explore Incorrect Solution: 5 points.

**Part 2:**

* Step 1: Configure Sugar Spinner to identify Fiona:

Report correct Solution: 5 points, Explore Incorrect Solution: 5 points.

* Step 2: Prevent attacks:

Report correct Solution: 5 points, Explore Incorrect Solution: 5 points.

* Step 3: Configure a validation profile for visitors:

Report correct Solution: 5 points, Explore Incorrect Solution: 5 points

**Concluding part:**

* Correctly answering 2 questions at the end: 5 points
* Submission of correct logs: 10 points.
* Overall understanding reflected in summary: 5 points.

**Survey:** 10 points

**NOTE: to get full credit you need to explore the effects of “wrong” choices as well as select the correct choices. Even if you made correct choices on your first try, you need to experiment with other choices to explore various consequences. If you only report the correct choices, you will NOT get full credit.**