**DSCI 519**

**Lab 2: CyberCIEGE Mandatory Access Control**

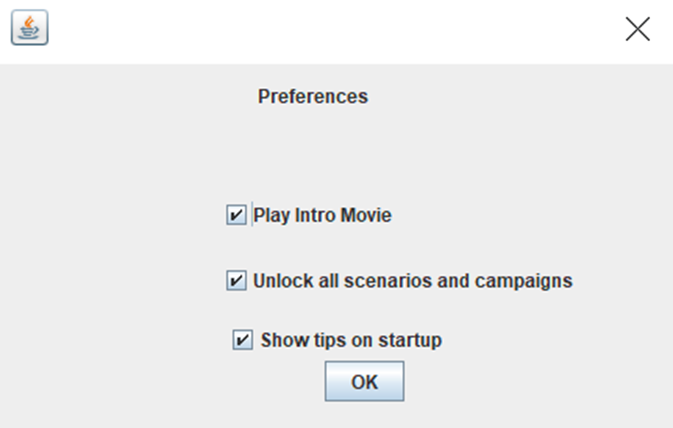
**100 points**

This lab has two parts.

**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.**

NOTE:

Campaigns grayed out. To unlock the MAC scenario. Go to Advanced then Preferences and check Unlock all scenarios and Campaigns.



There is a bug that causes two configurations for security and integrity levels lead to successfully completing the scenario.

**Part 1. Assign Security Labels to Network**

The CyberCIEGE MAC scenario is a simple example of mandatory access control (MAC) policy enforcement using security labels and a server that enforces the MAC policy.

The MAC scenario explores the following concepts:

* Real-time sharing of information across security levels may require reliance on a computer to enforce a MAC policy. Such computers are sometimes referred to as “multilevel”.
* Connecting physical networks to a MAC enforcement mechanism requires that you provide the MAC mechanism with a security label for the connection.
* Networks that contain other computers that lack suitable MAC enforcement mechanisms are typically treated by MAC enforcing computers as “single level” networks, i.e., the networks may handle information of different security levels, but all of the information on the network is treated at a single security level by the MAC mechanism.

**Play Scenario**

From the “Campaign Player”, select the “Mandatory Access Controls” campaign. Select the “Mandatory Access Control” scenario from the scenario list. Then click the “Play” button.

Read the briefing and the objectives screens, and explore the encyclopedia (via the “F1” key). From the Multilevel Components entry in the “Tutorials and Movies” content page of the online help, view the movie. As you play the scenario, remember you can save the game at any time and come back to that state later.

Assign Security Labels to Network:

* Read the briefing in the GAME tab and check your objectives in the OBJECTIVES tab.
* Look at the labels of the assets via the ASSET tab. Look at the user clearances via the USER tab. Also look at the user goals and notice how they need to share the asset that is on the server.
* In the OFFICE screen, start the simulation and notice how both users are failing a goal because of their inability to share the “Open Source Reports” asset.
* Go to the NETWORK tab. Notice Joe’s workstation is already connected to the LAN1 network and Jill’s workstation is connected to the LAN2 network.
* Connect each network to Server by first selecting the server (click on it) and then click the LAN1 and the LAN2 buttons in the upper right.
* Right click on the server, select Networks and “Label Single Level Network” and then assign labels to each of the two networks.

**Finish scenario**

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

**Part 2. MAC Integrity**

The MAC Integrity scenario builds on the concepts covered in the MAC scenario, which covered a secrecy policy. This scenario is very similar to that previous MAC scenario, but this scenario includes an integrity policy. This scenario explores the following concepts:

* Real-time sharing of information across integrity levels may require reliance on a computer to enforce a MAC policy. Such computers are sometimes referred to as providing “multilevel integrity”.
* Connecting physical networks to a MAC enforcement mechanism requires that you provide the MAC mechanism with a security label for the connection. Some environments may require both secrecy labels and integrity labels.
* Malicious software on a network can corrupt the integrity of information, and thus the integrity label associated with networks should account for the potential for low integrity or malicious software.

Students are expected to have complete the CyberCIEGE Mandatory Access Controls scenario.

**Play Scenario**

From the “Campaign Player”, select the “Mandatory Access Controls” campaign Select the “MAC Integrity” scenario from the scenario list. 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 game at any time and come back to that state later.

Assign Security Labels to Network:

* Read the briefing in the GAME tab and check your objectives in the OBJECTIVES tab.
* Look at the labels of the assets via the ASSET tab. Look at the user clearances via the USER tab. Also look at the user goals and notice how they need to share the asset that is on the server.
* In the OFFICE screen, start the simulation and notice how both users are failing a goal because of their inability to share the “Critical Logistics Database” asset.
* Go to the NETWORK tab. Notice Grace’s workstation is already connected to the LAN1 network and Sean’s workstation is connected to the LAN2 network.
* Connect each network to Server by first selecting the server (click on it) and then click the LAN1 and the LAN2 buttons in the upper right.
* Right click on the server, select Networks and “Label Single Level Network” and then assign labels to each of the two networks.
* Start the simulation and see if you are successful by winning the scenario.
* Play the scenario again and this time assign the wrong label to Grace’s network. Start the simulation. What happens? Click the “Attack Log” button to see a description of the attack. Replay the game, trying to counter each attack while keeping the wrong label on Grace’s network. Why do you ultimately fail?

**Finish scenario**

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

**Deliverables**

Prepare a report in PDF format with a font size of 10 points, single-spaced, single column and upload it to D2L “Lab2” 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 part 1, answer the following questions:
  + Question 1. What label did you assign to the network connected to Jill’s workstation?
  + Question 2. What would you expect to happen if you assigned the other label to Jill’s workstation? Give it a try.
* For part 2, answer the following questions:
  + Question 1. What label did you assign to the network connected to Grace’s workstation?
  + Question 2. What would you expect to happen if you assigned the other integrity label to Grace’s workstation? After all, she is cleared to “CRITICAL OPERATIONS” integrity. Give it a try.
* 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 “Mandatory Access Controls” scenarios (collect all files in “logs” directory and create a zipped folder for submission).

**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.**