1. CyberCIEGE Patches

CyberCIEGE is an information assurance (IA) training tool that illustrates computer and network security principles through simulation and resource management trade-offs. CyberCIEGE players construct computer networks and make choices affecting the ability of these networks and the virtual users to protect valuable assets from attack by both vandals and well-motivated professionals.

The CyberCIEGE *patches* scenario explores the need to apply software patches to applications and operating systems.

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:

- Many applications and operating systems have flaws that can be exploited by attackers to compromise computers and/or assets stored on those computers;
- After specific flaws become publicly known, there are often a lot of attacks mounted against systems that contain those flaws.
- Sometimes an enterprise's use of unpatched software is visible from the Internet via a network "scan".
- Software patches that are only intended to address security flaws will sometimes have unexpected effects on the behavior of applications. It is advantageous to establish a regime to test new patches before applying them to operational systems.
- Procedures and responsibilities for managing patches must be consistent with available resources. In some environments, individual users must manage and apply patches to their own systems. In these environments, user training is often necessary.

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.

1.1 Preparation

The game is installed in the CS3600 lab and is available from the PC workstations.

From the CyberCEIGE folder on the desktop, open the CyberCIEGE icon. This will start the “Campaign Player” seen in Figure 1-1.

If you have not yet played a few introductory scenarios, you may wish to click the *Help* button and then select Help & *Getting Started*, which will open a browser to a page that will help familiarize you with CyberCIEGE, including a few brief movies.

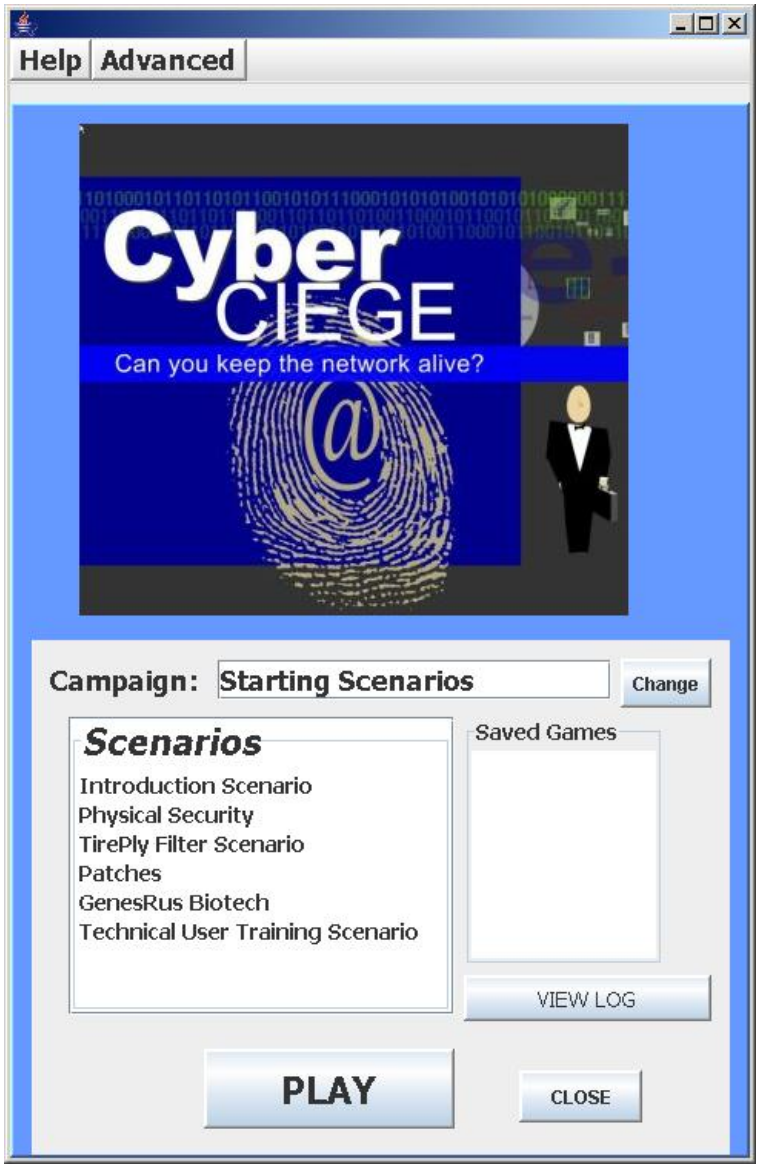

Figure 1-1. Select Patches and Click Play

Select “Patches” 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 state at any time and come back to that state later. Also, the game automatically saves your state at each transition to a new phase.

1.1 Play

1.1.1 Phase 1, First Objective: Instruct Edgar to Apply Patches

- Press the space bar (or click the play button) to start the scenario. The first time through you may wish to just watch until Edgar asks you: "What can you direct me to do to make it harder for those vandals to routinely trash our system?"
- Press F1 to learn about network scans. Then go to the NETWORK screen and right click on the Internet icon and select "Discover / Scan". Look at the patch information reported for the Logititan application.
- Double click on the server and select the appropriate configuration setting (note the different between configuration settings and procedural settings by hovering the mouse over each label.)

1.1.2 Phase 1, Second Objective: Direct Users to Apply Patches

- Let the game run until Edgar asks Arlo when was the last time he applied patches to his software.
- Double click on Arlo's computer and select the appropriate setting.
- Double click on Arlo and buy him some training so he better understands what he needs to do.

1.1.3 Phase 3 Patches are Breaking the Applications

In this phase, Edgar discovers that when he applies patches to the server, sometimes it breaks the application. Consider purchasing a second server upon which Edgar can test the patches before applying them.

1.2 Clean Up

The "View Log" button lets you view a log of what occurred during the game.

END OF LAB