Lab 9 CyberCIEGE Network Filters

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 *filters* scenario explores issues arising from connecting networks to the Internet and the use of filters to protect assets. Refer to the CS3600 course notes on firewalls for background.

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:

- Internal networks of workstations and servers are typically connected to the Internet via a router or firewall.
- Routers and firewalls typically can be configured to use filters to block or permit access to different applications via specified networks. In its most basic form, the filter blocks access to selected services. For example, a filter can block requests for FTP services destined for a particular network.
- Protection of assets requires knowledge of their value and of the requirements for legitimate access – i.e., knowledge of the information security policy.
- Router and firewall filters are not robust enough to protect some assets.
- Sometimes the best way to protect high value assets is to physically isolate them from external networks.

In this scenario you can largely ignore Zones and physical security issues. You can also largely ignore configuration settings and procedural settings (e.g., settings on the COMPONENTS screen). Also, don't worry about hiring or firing support staff or the trustworthiness of your virtual users.

9.1 Preparation

Access CyberCIEGE as described in "CyberCIEGE Information Assurance Training Tool Availability at NPS".

From the CyberCEIGE folder on the desktop, open the CyberCIEGE icon. This will start the "Campaign Player" seen in 0.

If you have not yet played the "Introduction" tutorial scenario in the "Starting Scenarios" campaign, you may wish to do that first. You may also want 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.

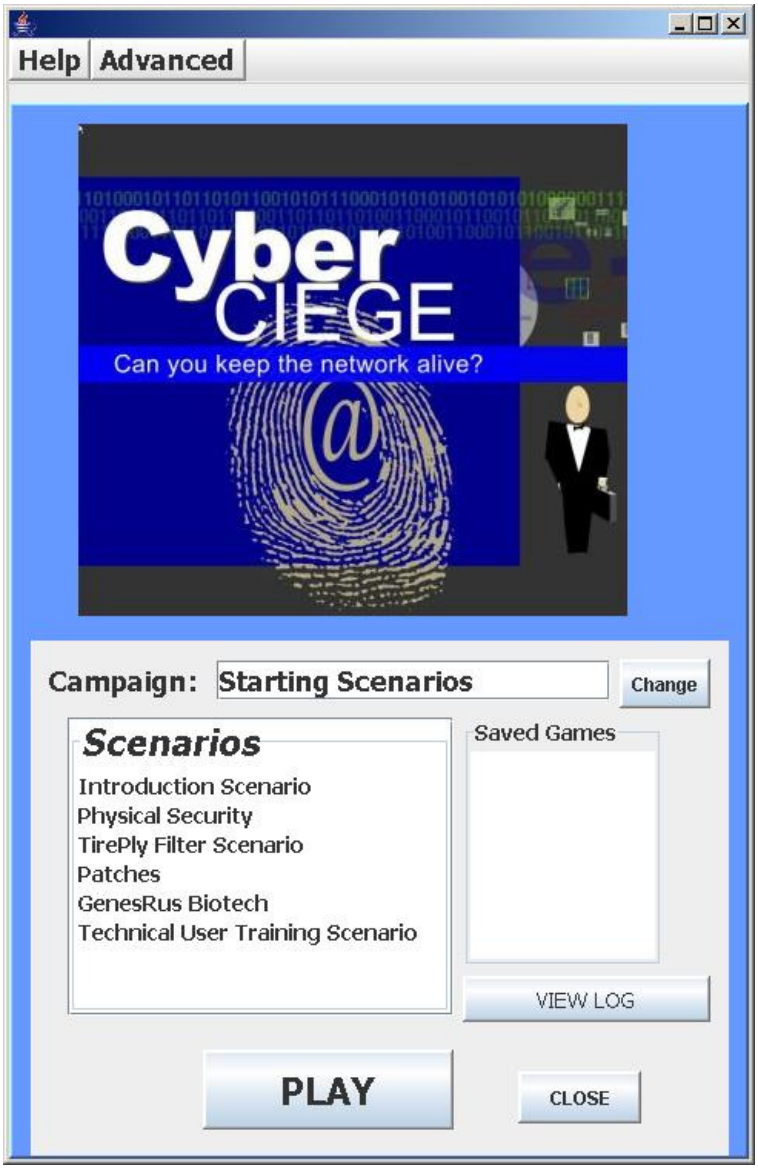

Figure 9-1 Select Tireply Filter Scenario and Click Play

If the selected campaign is not "Starting Scenarios" use the *Change* button to select the Starting Scenarios campaign. Then select the "TirePly Filters Scenario" from the scenario list. Then click the "Play" button.

Press the "F1 key and watch the two movies in the "Firewall Functions and Limitations" entry under "Tutorials and Movies" section.

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.

9.2 Play

9.2.1 Phase 1 Connect Larry to the Internet

Use the encyclopedia "How To" section to learn how to connect a network to the Internet. Start with "Connect to the Internet". This will point you to how to buy a router or firewall and how to connect components to networks.

- From the OFFICE screen click the buy button
- Select the "Network Devices" tab
- Select the first router and click "Buy"
- Press the Tab key repeatedly to get a good view of where you might want to place the router
- Click the location where you'd like to place the router
- Click the Network tab
- Click the router that you just bought
- Click the Internet button on the upper right
- Click the Lan1 Button
- Select the OFFICE tab

Press the green arrow to start the simulation. Is Larry now achieving his goal of getting onto the Internet? Let it run for a while as it is. What do you expect to happen?

9.2.2 Phase 2 Configure Filter

- Double click on the router, or click the "FILTER" button after selecting the router.
- For this phase, you need to restrict traffic coming *from* the Internet.
- As noted in the movie (or the encyclopedia "How To" section), if the "From Internet" network connection is selected, clicking the "Deny All" button will block all unsolicited traffic originating from the Internet.

- Note the above step has no effect on Larry's ability to send traffic to the Internet. And for this scenario, it is fine to permit all traffic from the Internal LAN to the Internet.

9.2.3 Phase 3 New Asset Introduced into the Enterprise

In this phase, Mary begins work on a new asset called the "Steel Formula". You cannot know how to appropriately protect this new asset unless you know its value to the enterprise and to potential attackers.

Click the Objectives button in the OFFICE screen to see how to learn about the value of this asset.

Be sure to view the encyclopedia tutorial movie on Firewall Limitations after exploring this phase if you have not already watched it.

9.2.4 Phase 4 Remote Access Into the Server

You are required to open a hole into the system to support offsite access to the server. Previously, you clicked "Deny All" to deny all traffic originating from the Internet.

Find the desired application service in the list of applications, select it and click "permit".

9.3 Clean Up

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

Collect the game logs into a zipped folder by clicking the "**Advanced**" menu button and selecting "**Collect Logs**". Feel free to provide comments on the game within the provided space. Enter your NPS User ID as the user name in the field. Then click "**OK**" to create the zipped file on the desktop.

If you are running the exercise in the NPS Lab:
- copy the `logCollection.zip` file from the VM's desktop
- Minimize the VM (click on the "_" in the grey bar at the top of the screen)
- paste it into the workstation host's desktop "CyberCIEGE-Logs" folder.
- if prompted to overwrite the file, click **Yes**.

If you are running the exercise outside of the NPS Lab:
- please email the `logCollection.zip` file to CyberCIEGELogs@nps.edu.

Click on the minimized VMware Workstation session to resume it (and press **<Ctrl>-<Alt>-<Enter>** if it doesn't return to full-screen).

Click the **CLOSE** button to exit CyberCIEGE.

Shutdown or suspend the VM and logoff the workstation if you are finished in the lab.

9.4 Additional Questions

Question 1. *Were you reluctant to disconnect Mary's computer from the Network? If so, why?*

Question 2. *Did you take time to experiment with alternate network filter configurations? If so, were the results what you expected?*

Question 3. *In the Firewall Security Basics movie, how did malicious software get past the intrusion detection system?*

END OF LAB