Instructor Notes for the Network Filters Scenario
June, 2011

These notes are for instructors and should not be shared with students. Students should be provided with the "CyberCIEGE Network Filters Scenario Lab Manual".

The filters scenario introduces the concept of connecting to the Internet via a router or firewall and using filters to block application traffic. The filtering mechanism is analogous to blocking TCP "open" requests for selected ports, which are abstracted to their corresponding applications, e.g., "Web Server". The scenario also illustrates the inability of filters to block high motive attacks. The scenario is divided into four phases that explore different concepts:

- Phase 1: Local area networks of workstations and servers are typically connected to the Internet via a local router or firewall. The student must purchase a router or firewall and connect it to both the Internet and the local LAN. The game prevents connection of the Internet directly to a workstation or server.
- Phase 2: A basic router and firewall protection mechanism is the filtering of application service requests. This simple mechanism blocks or permits the opening of communications with an application service such as a web server or a POP email service. These protection mechanisms are typically associated with traffic flowing between two specified networks in a specified direction. In the second phase, students must deny application service requests originating from the Internet. If the student also blocks web requests heading out of the enterprise, the objective won't be met because the user can't get to the web.
- Phase 3: Protection of assets requires knowledge of the information security policy. In the third phase of the game, the student must learn the value of the steel formula asset so that it can be properly protected. And the student must understand who needs to access the steel formula, and what other assets need to be accessed as part of that goal. Once the value of the steel formula is understood, the student should conclude that a firewall is unable to protect it from a Trojan horse on Mary's workstation. And given the actual user goals, the simplest protection is to simply isolate Mary's computer from the rest of the network.
- Phase 4: Sometimes filters must be configured to permit application service requests to enter the enterprise. The student must open an SSH port to permit an external user to gain access to specific data.

Solution steps:

1) Buy router and connect to lan and Internet
2) Configure router/firewall filter to block traffic "from" the Internet.

3) Disconnect Mary's workstation from the LAN (several warnings are given prior to the asset being compromised.)
4) Open a filter to permit SSH from the Internet to allow the regulator to access the database.

Suggested solution demonstration flow:

- view objectives
- start game and wait for complaint
- buy router and connect to lan and internet
- press e to "see how he feels" when prompted
- run until the mac truck rumbles through your filter
- go to filter and "set all" on internet connection, then open Web Server "in" to internet.
- run until warning that mary will start working on steel formula
- save game, give it a name you'll remember
- continue until steel formula stolen
- restart game and load what you saved
- disconnect mary's workstation from lan
- continue
- when offsite regulator needs access, open filter for SSH from internet

Getting Student's Started

Students should be provided with a copy of the "CyberCIEGE Network Filters Lab Manual". Some students are challenged by the game's mechanics, so it may be helpful if the instructor spends about 10 minutes demonstrating some of the mechanics of the game. The "Introduction" scenario can be used to illustrate how to purchase computers and hook them to networks, and how to navigate around the office. Also show how to view objectives, user goals and descriptions of assets. The introductory scenario includes items that are not needed for the Filters scenario. These include configuring components, physical security and hiring support staff. Make a note of that to the students. Highlight the encyclopedia, especially the "How To" section.

Student Assessment

Student progress and results can be assessed using the Campaign Analyzer. From the CyberCIEGE desktop folder, select the "ccse" directory and then start the "Campaign Analyzer". It defaults to the "Starting Scenarios" campaign, which is the desired campaign. Select the "TirePly Filters Scenario". Each student that has played the game will appear in the list, along with summary status. If the student did not "win" the game, the status identifies the most advanced phase the student had reached. To view details of a student's play, select that student entry and press the "View Log" button.