Lab SSL

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 SSL scenario illustrates the use of SSL to authenticate the identity of web servers and protect data in transit. The scenario also illustrates the use of Transport Layer Security (TLS) to authenticate clients to servers.

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:

- SSL is a means of authenticating a server (e.g., a web server) to a client (e.g., a browser).
- SSL provides a means of protecting the secrecy and integrity information in transit.
- Browsers come pre-loaded with a set of installed roots from public pay-per-cert certification authorities. Offering SSL services to the general public generally requires that you obtain a certificate from one of these services because users are reluctant to perform the steps necessary to install a new root certificate.
- SSL alone does not authenticate a client to a server.
- TLS is similar to SSL, but it does require the client to have a certificate (and its corresponding private key).
- When using TLS, the CA that signs the server certificate may be independent of the CA that signs the client certificate.

10.1 Preparation

From the "Campaign Player", select the "Encryption" campaign as seen in figure 10-1.

The player is expected to have first completed the "Encryption Key Types" scenario prior to playing this scenario.

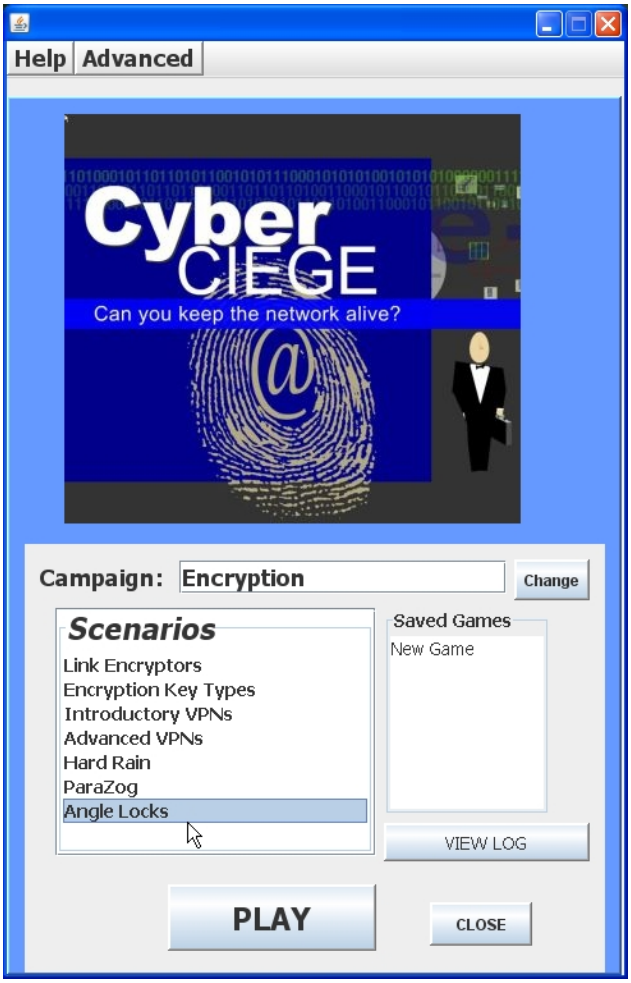

Figure 10-1: Select Angle Locks and Click Play

Select "Angle Locks" 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.

10.2 Play

10.2.1 Phase 1: Customer Access

In this phase you must allow a customer to rely on SSL to give her confidence that she is entering her credit card information into a legitimate web site..

- Click the Objectives tab to learn about your first objective.
- Review the network topology via the NETWORK tab
- Press F1 to learn about the use of SSL in CyberCIEGE

- Right click on the customer's computer and select "Applications" / "Configure Browser Application". Notice how she will insist on using SSL to achieve this goal. Look at her installed roots to see which CA's certificates can be validated by her browser. Note how you cannot add roots because she is reluctant to do that.
- Right click on the web server (e.g., in the NETWORK screen) and select "Applications" / "Configure Web Server Application".
- Revisit the F1 help as needed to configure the server to provide SSL when accessing the Product Order Catalogue.
- Run the simulation until you get to phase two.

10.2.2 Phase 2: Vendor Access

- Check your objectives
- Use F1 to learn about the use of TLS
- Notice how you cannot add vendor to your list of authorized users?
- Right click on the web server and require SSL/TLS when accessing the schematics.
- Figure out a way to let your server validate Bill's certificate

10.2.3 Phase 3: Buyer Access

- Check your objectives
- Bill is now highly motivated to get the pricing data.
- Figure out a way to have your buyer use TLS to reliably authenticate herself to your web server without giving Bill a chance to get his hands on the keys.

10.3 Clean Up

The "View Log" button lets you view a log of what occurred during the game. Use the "Advanced / Collect Logs" choice in the Campaign Player to collect your logs into a zip folder that can be emailed or dropped into the CyberCIEGE-logs folder if running on a CS-3600 VM.

10.4 Additional Questions

END OF LAB