Instructor Notes for the CyberCIEGE Network Traffic Analysis Scenario

May 2013

Students should have run the Filters scenario and perhaps the DMZ scenario. Also, the student should have run the SSL scenario (Angle Locks).

Not the simulated traffic that appears in the packet logs is notional. The fidelity of the traffic is not accurate, i.e., you cannot reliably see traffic from workstations to servers, though samples of such representative traffic do appear in the logs. Similarly, in order to keep the logs relatively small, the DoS traffic rates are quite low relative to a real DoS attack. The purpose is present reasonable representations of the content of such traffic, and not to accurately represent the volume of traffic.

Phase I :

Buy Sam a workstation and a router. Connect the router to the Internet and to Lan1, and connect the workstation to Lan1. Run until attacked. Configure the Web Server application (right click / Applications / Configure Web Server Application) to require SSL for the "SyberSIEGE Launch Page"; and configure Sam's workstation browser application to "Accept any roots & self-signed certificates".

Find Sam's clear-text password: Right-click on the web server, select "View packet log". Enter "credential" into the "Search Payload" field and click "Apply". Expand the "Hypertext Transfer Protocol" and then expand the "Authorization". (Or "Expand All"). Look for the value of the "Credentials" field.

Run the scenario and answer the questions.

Phase II:

Single source attack:

Run the scenario until a DoS attack occurs. View the packet log and select the "Syn Flag" filter and click Apply. Note the syn packets coming from "SpaceInvader1.BlueBird". The "host name" is "SpaceInvader1". Configure the Router's network filter. Permit Web Server and Web Server (SSL) traffic, but click the "Exceptions" column for each and add the host "SpaceInvader1" to the exception list. Run the scenario and answer the questions.

Single domain, multiple hosts attack:

Run the scenario until the next DoS attack occurs. View the packet log, filter on syn packets and note the domain from which the various hosts are participating in the attack. Reconfigure the Router filter exceptions for Web Server and SSL to block that domain.

Multiple domain, multiple hosts:

Run the scenario until the next DoS attack occurs. View the packet log, filter on syn packets and note that many different domains and many different hosts are participating in the attack. Reconfigure the Router filter by clearing the exceptions, blocking all traffic from the Internet to Web Server and SSL, and then adding exceptions for Sam's workstation.

IP Spoofing attack:

Run the scenario until the next DoS attack occurs. View the packet log, filter on the syn packets and note that the latest attack appears to be coming from Sam's workstation. The IP address is being spoofed. Run the scenario until Tina observes that her time is worth a lot more than Sam's time. Then disconnect the Internet.