Weekly Report

Individual Contributions

Andy

Modified Xplico so each session can start collector (2 hours, 3/29)
HTTP Session now stores collector info on per-session basis
Info is accessed by prepending session ID to the requested piece of info

Modified deletion of case/session (2 hours, 3/29)
Cases and sessions now cannot be deleted if a collector is running
User must stop collectors and then delete case or session

Modified Xplico/Collectors so pcaps have unique ID number (8.5 hours, 3/30)

- Added command line argument that takes next ID number
- Collectors already increment ID when creating a new pcap
- Initially, tried adding field to Xplico's database (see below)
- Calculated from number of rows in inputs (pcaps) table for the sol (session)
- Inputs table stores pcaps uploaded to Xplico

Database schema changes (See above)

- Attempted to add field to sols (session) table with next available ID
- Very difficult to apply schema changes to database
- Needed to add code for inserting user types and default users

Modified Xplico so it detects when Collector error occurred (4 hours, 4/2)

- Fixed bugs in Collectors related to deleting collector_running
- Modified session page so it checks if collector_running exists
- Outputs error message if collector_running does not exist but should exist
- Deletes collector info from HTTP Session object

Total: 16.5 hours

Total-To-Date: 125 hours

Altay

Found/Modified ASN.1 (ber) and pcap format (1 hour, 3/30)

Modified error handling in both collectors (3 hours, 3/31)
Now, if exception is thrown, collector_running will be deleted
Xplico now has a way for detecting if collector is still running or not

Looked over several tutorials and learned about PHP (2 hours, 3/31)
Did not look at tutorials about CakePHP yet

Total: 6.5 hours

Total-To-Date: 77 hours

Tasks

Finish fixing documentation/presentation (Altay/Andy)

- Implementation details (Altay/Andy)
- Alternative designs (Altay)
- What you learned (All)
- Operation manual (Andy)

Work on PDF – better alternative? (Andy)

Install Xplico with Ubuntu instructions on non-Ubuntu (Abe)
(Try couple of OS – Kali and Redhat for sure)