Weekly Report

Individual Contributions

Andy

Changed Raw collector to accept any interface (3 hours, 2/19)
- Removed loop for checking interface
- Set socket address to INADDR_ANY
- Updated View and Controller to reflect these changes

Added option for selecting DeepSweep's input type (4 hours, 2/19)
- Had trouble aligning the labels after their buttons
- CSS file was setting the float property on the label tag
- Added radio buttons to session page for Raw/ASN.1
- Looked into how jar files are run on command line
- Did not add code for actually starting ASN.1 collector yet

Total: 7 hours

Total-To-Date: 58.5 hours

Altay

Removed case/session creation from ASN.1 and retested (1 hrs, 2/16)
- Now it only requires the session directory

Figured out how to run Cream in Bash (3 hrs, 2/17)
- Assembled custom library class folder consisting of .class files

Modified ASN.1 code to work with piping (4 hrs, 2/17)
- Now it runs forever and waits for input to come so real-time
- If input won't come for 50 iterations, then it sends what it has (flushes)

Total: 8 hours

Total-To-Date: 39 hours

Abe

Worked on separating pcaps in DeepSweep raw traffic
- Scans n bytes at a time and searches for magic number
- Given offset of n bytes, it splits pcap files

Total: 2 hours

Total-To-Date: 22 hours

Tasks

- Modify Xplico to start ASN.1 Collector and Cream (Andy)
  (Figure out better way of including jar files when running Cream)

- Update documentation to reflect diagram/UI changes (Andy)
  (Alternative: Look into PDF library for PHP)

- Change C collector to use separate pcaps function (Altay)

- Convert Raw Collector from C to Java (Altay)

- Look into how to install project, possibly with Docker (Abe)
  (Alternative: Begin learning basics of PHP)