Weekly Report

Individual Contributions

Andy

Start Xplico daemon automatically when page is loaded (2.5 hours, 12/29)
- Xplico startup scripts needs to be run with sudo
- Apache cannot run commands using sudo for security reasons
- Possible workaround is to set SUDO_ASKPASS
- This variable is set to a program, which will prompt for password
- Not sure if this will be distribution-dependent

Set up SVN and add initial Xplico files (4.5 hours, 12/30)

Changed new case page - Prep for DeepSweep option (3 hours, 1/1)
- Database stored if a case was live capture or not
- Changed to track if a case is live capture or uploaded files
- Internally, cases are pols and sessions are sols

Added modified new case and session pages for Deep Sweep cases (7 hours, 1/5 + 1/12-13)
- New Case page has option for creating a Deep Sweep case
- Session page has button for starting/stopping collector/pusher
- Deep Sweep case will only permit output from collector/pusher

Read some of CakePHP documentation - http://book.cakephp.org (3 hours, 1/13)

Added form for setting Raw Collector parameters (3 hours, 1/15)
- User will set deep sweep port and interface
- Session page displays pcap-over-ip port and archive directory
- Archive directory = /opt/xplico/pol_ID/sol_ID
- ID is the case (pol) or session (sol) ID number

Started Raw Collector from Xplico's Session page (6 hours, 1/16)
- Tested with a couple of Xplico's sample pcaps
- Xplico's output is redirected to /dev/null currently
- GUI currently can't see error messages or stop Collector

Total-To-Date: 29 hours

Altay

Got examples of encapsulated raw from client (1/19, negligible time)

Discussed with client what encapsulated raw actually means (1/15- 1/21, 4 hours)
- It is not addition of extra TCP/IP headers to the raw traffic
- It is raw traffic wrapped with ASN.1 encoding (DER encoding used)
- Java DeepSweep libraries are called Cream apparently
- Cream can handle both encapsulated raw and ASN.1 the same way

Modified Raw Collector so DeepSweep can reconnect (1/20-1/21, 3 hours)
- When Deepsweep exits, collector wait for a new connection
- Xplico only accepts one session per connection and throws out the second session
- Collector closes and reopens Xplico's socket for each Deepsweep connection
- If any error occurs, collector closes everything and stops working

Total-To-Date: 7 hours

Abe

Researched/revisited decoding BER files (6 hours)
- JCollector outputs packet data in 2's complement
- Found library to help with decoding: http://www.snmp4j.org/doc/org/snmp4j/asn1/BER.html
- Found website to help with practice with this data: http://asn1-playground.oss.com/
- This data will be converted to packets, which JNetPcap can read

Researched creating PCAP files with JNetPcap (4 hours)
- RawFormatInputStream will take the packets created from decoding ASN.1
- PcapOutputStream will be used to create PCAP files from the packets
- Output from RawFormatInputStream will be read byte-by-byte to create PCAP file

Total-To-Date: 10 hours