CNA473 Final Project Proposal

Dustin Watson

**A method of detecting and blocking Steganography traversing through a network.**

Required tools:

* 2 VM running a Linux computer
  + One with squid installed
  + Another with webserver installed

Various stenography tools:

* OutGuess
* Steghide

Methods:

Proxy firewall squid allows for writing custom external scripts that are used as rules in ACL.

By creating a set off squid proxy rule scripts files of matching MIMO types can be checked against one or more steganography tools to check for covert communications passing through a network.

Many steganography command line tools exist for the detection, embedding, and extraction of hidden messages from various other file formats. As described in “Steganalysis: Detecting hidden information with computer forensic analysis” (<https://www.sans.org/reading-room/whitepapers/stenganography/steganalysis-detecting-hidden-information-computer-forensic-analysis-1014>)

These rules are called external ACLs with squid proxy.

Test results of detection:

Create files with steganography inside them and pass them through the network for the proxy to try to detect them using the custom external ACL rules.

Benefits:

Implementing these existing tools with the squid proxy creates a new method which was not found on several internet searches regarding the squid proxy and steganography. Squid can provide an extra layer against covert challenges using images and sound files. Blocking or acting as a silent intermitted bump in the wire proxy copying questionable files for further inspection.

As more tools or methods are created for detecting steganography these set of proxy rules could be updated to block or copy files for later inspection. Creating new tools would be beyond the scope and time frame of this project.

Testing:

Use steghide and other common tools to copy