Development Plan: Frenemy

Intro: The goal is to develop a program in python which will leverage automated browsing and packet capture libraries to perform an ARP poisoning attack which will present a victim with a fake login page of the attacker’s choice.

Tools: The following are our toolkit for this project.

* Scapy – python packet analysis lib
* Apache – standard web-hosting framework
* Splinter – python automated browsing library

Modules: The following are a list of components that we will need to develop in order to implement Frenemy. Each of these can be viewed as an appropriate AGILE task for a weekly sprint.

* HTML scrape and PHP substitution: Given a URL, use an automated browsing tool (Splinter) to navigate to the requested site, scrape its HTML, and replace the login action with the name of a generic PHP script which grabs all text fields from the HTML and writes them to a local text file. The PHP should then redirect the user to the genuine webpage.
* Server configuration: Given the HTML for an index.html page and an accompanying PHP script, properly configure the attacker’s /var/www/html directory so that pointing a browser to the attacker’s IP brings up the desired page.
* Network diagnostic and target selection: Using the sample packet-sniffing code provided in the repo, monitor the network for some period of time to determine a list of potential targets. After this period of time has expired, prompt the user to select a target from a list.
* Wifijammer: Given the information for a target, temporarily jam the wifi of the target.
* ARP poisoning and packet forwarding with DNS spoof: poison the ARP cache of the victim and the router so that the router thinks you are the victim and the victim thinks you are the router. If the victim asks to see the webpage we are spoofing, give them the attacker’s IP – redirecting them to our phony page. **NOTE: This is conceptually the hardest piece of the puzzle, this will probably be something we have to team up for.**
* Cleanup: detect that we have successfully stolen information from the user, return the network to its normal state.