Nick Alexander

April 29, 2015

NAPALM

The purpose of the assignment was to properly parse and extract data from a hundreds-of-thousands entry TCP dump. When working in the networking field, network logs can become extraordinarily large and requires the work of a computer to easily parse to find interesting information. The program, written in Python, is capable of determining how many protocols were used and their respective amounts, all IP address communications, all FTP server IP addresses, all FTP usernames and passwords, and all MAC addresses. The program shows each output in a formatted manner and is capable of writing to both standard output and to file.

In order to count the total number of packets, the number of lines in the TCP dump were counted since each line in the dump was equivalent to one packet. From each line, the protocol was extracted and stored in a dictionary with the usage count. Once all the packets were counted, the number of usages was divided by the number of packets to yield a percentage of protocol usage. These values were then sorted by ascending values and displayed.

In order to track IP address communications, all IP addresses were found by analyzing every packet for the sender IP. Once the sender IP was specified, the program finds every packet with the same sender IP and extracts the receiver IP. Once the search has exhausted, all IP addresses that received a packet from the sender are displayed to the user.

In order to handle FTP, all packets that used the FTP protocol were extracted first. Searching through each FTP packet, it was simple to check the sender IP of response messages that clearly came from the server-side to accrue all FTP server addresses. Once that was completed, all user login prompts were tracked. Examples of login prompts include the server Response 331 which is a request for a password. Since FTP is unencrypted, the username and passwords could be extracted directly from the packet and stored. Afterwards all FTP server IP addresses and FTP credentials were displayed.

Finally, in order to determine the mapping between IP addresses and MAC addresses, the ARP protocol packets were analyzed. In each ARP protocol, there is an ARP request and an ARP response. In the ARP response, the protocol directly tells an IP address to MAC address mapping. Extracting all ARP and Who Has packets resulted in building a simple ARP table that is presented to the user.