Homework 2: Ethan Davis

Our assignment was to write a perl program that took in a log of pings to a UNH server and output the IPs of the most frequent pingers, then do research on who or what they might be.

-With 720 occurrences, the most frequent IP address is 27.118.21.217. However, when we check the log, we find that this is not an IP address of someone accessing the site, but is the subject of someone’s query (or they are using it for some purpose). Research tells me this IP address belongs to a data center/web hosting institution in Vietnam (the output says this occurs 1440 time, however if you check the log it occurs twice in each line as a result of how the log took inputs).

-Also with 720 occurrences is 221.193.214.36, the IP address that keeps inputting 27.118.21.217. Research notes that this IP is unlisted and is from Shijiazhuang, Hebei, China. Interestingly enough, googling “Shijiazhuang, Hebei, China hackers” results in a lot of IP addresses reported as trying a variety of attacks including port scanning or searching for vulnerable web pages. Sketchy folks.

-In a distant third at 48 occurrences is 185.40.4.130 which comes courtesy of Russia. This IP address has already been reported multiple times before for web attacks (looking for ports, etc.).

-Way off in fourth with 8 instances is 122.200.65.30 which calls Beijing, China home. Yet another instance of attempted hackings. This IP address has been reported more than any other so far, for a host of sins.

-In fifth at 6 instances is our new champion of being reported. 183.129.160.229, straight out of Hangzou China, has been reported to the AbuseIPDB database 820 times. For comparison, the previous IP 122.200… had been reported 15 times. Curiously enough, there is a prestigious Chinese science and technology school in Hangzou. Perhaps some students are up to no good.

As we can see, the top 5 acessers are out of country hackers looking for vulnerabilities to exploit.