# Project #3. Ariel Taveras, Graduate Section

Main Part:

The main portion of the program works by checking to see if a certain combination and number of ports are seen from any single ip address in the list. If it notices that all ports are seen and they belong to the same ip address, then it will alert the user that a potential network scan has been detected.

Description of files:

* Most files have self-explanatory names.
* Log\_Exploit is the log of the payloads from the attacker VM gaining access to metasploitable through the vsftpd exploit.
* tcpdump\_no\_scan\_ALL is the log of different scans as well as a lot of web traffic mixed in.

Bonus:

1. The program is able to process the tcpdump information in real time by piping the output directly into the program.
2. The program can detect an F-scan and an sS-scan.

Sometimes -sV and –n scans as well.

1. Some research was done on how to detect the smiley face backdoor exploit on metasploitable. It has not been implemented however.

The idea was to try to examine the payload of the data from the attacker vm to the victim vm using the –X option for tcpdump. Within these payloads I would try to look for ftp/ssh access or logins and I would attempt to look for the smiley face input as a username.