Vlad Synnes
Sam Decanio
Philip Porter
COMP 429

UDP Flood Tool - Initial Description

We are going to create a UDP packet flood tool. This tool will work by accepting an initial request (via UDP) that contains the target IP address, target port, and amount of packets to send. From this point our program will fork as many processes as the computer has cpu cores. Each process is responsible for sending amount_to_send / cpu_cores UDP packets. The server will reply to the requester specifying that the request was received. The server then executes the request. Upon completion of the UDP flood we send another message to the requester informing them the attack was complete, as well as detail the amount of time it took to carry out the attack.

In our project, the user will interact with our program by sending the requests that determine who the UDP flood will be directed at. The user gets to specify who to send the flood to as well as how many packets to flood the target with.

We will implement this as two separate programs:

1. flood.py
   This program will be the one to send the UDP flood. It is considered the server. Our program will wait for requests to arrive on its specified port and then handle them by dispatching the UDP flood request.

2. flood_client.py
   This program will be responsible for handling the user interaction portion of our project. Running this program will ask for parameters of who you want to target as well as the amount of packets you wish to send them. This program is then responsible for forming the UDP packet that will be sent to flood.py (the server) as the request. It will also be responsible for receiving the response UDP packets from flood.py and displaying the information in them to the user. Lastly, this program implements a method of detecting packet loss by having a timer that will resend the flood request after having not received a confirmation from flood.py after 2 seconds.