Christopher Calvani
Homework #4 – Red Team Tool

Instructions:

1. Plant the script on the target machine.
2. Run the script.
3. Watch as Blue Team's confidence suddenly crumbles!

What is the goal of this tool? What purpose does it bring to the competition?

The goal of this tool is to be very distracting as well as partially destructive. This script targets Windows boxes that leverage GUI usage, such as Windows Server machines (AD). When this script runs, three things will happen: (1) Two firewall rules are added to block incoming and outgoing traffic to port 22. This will ensure that the script cannot be shut down easily. (2) The mouse will become very erratic as well as inverted to distract the Blue Team user. And finally, (3) to further distract the user, the screen will rotate 90 degrees, 180 degrees, and 270 degrees every 10 seconds to make it very difficult to adapt to the inverted mouse.

Did other tools influence your tool? If so, what are they? If not what was your inspiration for the tool?

While other tools did not influence the script that I created, I did draw inspiration from multiple web articles detailing how to create a virus in python. I combined multiple articles I read to create a bombshell of a script that will most definitely distract Blue Team users for a good while.

What is the feasibility of another team member quickly learning to use or contribute to your tool? What makes it easy or difficult to learn?

Another team member can very easily learn to use the script, as it is just that, a script that you simply load onto the target machine and run. As for contributing to the tool, there is definitely room for improvement, and team members would mostly definitely be able to append what ideas they might have before the *while True:* loop to add onto the script.