Charles Richards
cer1713@rit.edu
Delta Team

Repo: https://github.com/Dr-N0/RedTeamSupportingFiles
DuckyText is designed to add an alias to the bashrc file for a given command. The alias will add random letters to the command and execute, this will lead to an error message. This script is designed to annoy the blue team. This tool was influenced by another tool that would move the mouse of a user to be annoying. This tool is tricky to use as it might have unintended consequences on the system and the tool in some cases doesn't work. For example, the kill command can't be aliased this way. This tool has a learning curve.

TouchNoise is designed to touch all the files in a directory to mask the modification history, this prevents the blue team from quickly finding a malicious file modification quickly. This was inspired by a noise machine Beckett and I were talking about to make it harder for wireshark users to sniff us out. This tool is not hard to use, it should most likely be used as ./touchnoise / to get all files. Although this tool has not been tested with hidden directories, but adjustments can be made

Hashfind is designed to search a given directory for a file with a matching hash, this will allow us to find renamed binaries and binary backups. This tool was not inspired by anything else, during the second competition I renamed a file to prevent the red team from using find on my computer if they had a similar script to this they could find the binary and use it to find the cheese. This tool is easy to use especially since we will have our own binary files to get the hashes for, if the given file hash is unknown and the file is renamed then it will not be able to be used in that context.