ML for Cyber Security
LAB 2

Name: Rakshit Lodha
netID: rl4563

This is a graph of Accuracy and Attack Success Rate vs fraction of pruned channels:

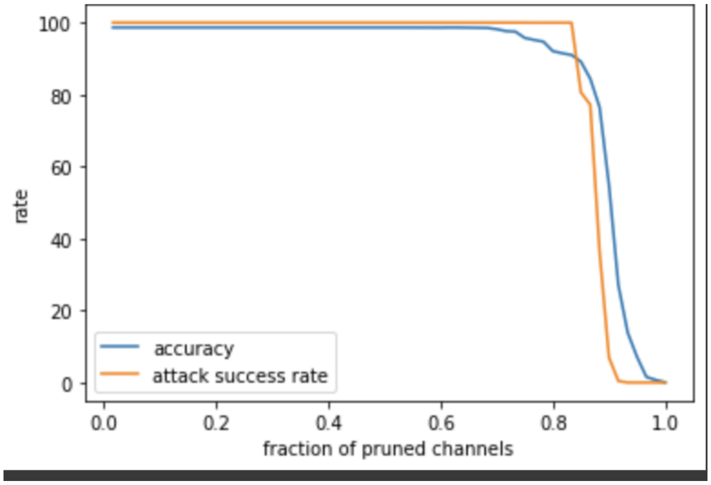

Table with the accuracy on clean test data and the attack success rate (on backdoored test data) as a function of the fraction of channels pruned (X) :

	B Prime Model			Retrained Net			B model
X	2%	4%	10%	2%	4%	10%	
Clean Accuracy	95.90023382696803	92.2915042868277 5	84.5440374123148 9	95.7443491816056 1	92.127825409197 2	84.3335931410756	98.6204208885424 8
Attack Success rate	100.0	99.9844115354637 6	77.2096648480124 7	100.0	99.9844115354637 6	77.20966484801247	100.0

GitHub link:
https://github.com/rakshit24/Rl4563_Lab2_MLCyber.git