# Proposal Document – TCP Hijack Attack Vector

### Introduction

A tool and walkthrough to attempt to hijack TCP traffic between 2 systems. It is designed to hijack a Telnet connection however can be modified to attempt to hijack other forms of TCP traffic

### Functionality

This attack requires an ongoing Man-In-the-Middle attack to function. This has been provided in the toolkit and functions in unison. The user will need to input the IP of both of the systems it wants to intercept traffic between. The script will then anticipate the next packet number and insert a packet with a Telnet command of the users choice into the traffic.

### How (Product) relates to our project

This tool can be used in a variety of ways. It can be used offensively by the user in active penetration testing scenarios as it is a viable attack to try and pop a shell. It can also be used for education purposes as it is a good insight into the workings of TCP and Telnet.

### What needs to be done to implement it and alternative methods

This attack would be well served by pairing it with other tools and attacks in the toolkit that establish a man in the middle attack.

### Additional information (if applicable)

### References