```
# Kernel Module - TCP Packet Logger

## Overview

This kernel module is designed to log information about incoming TCP packets in the
Linux kernel. It uses Netfilter hooks to intercept TCP packets and prints details
such as the source port.

## Table of Contents

- [Prerequisites](#prerequisites)
- [Building the Module](#building-the-module)
- [Loading and Unloading the Module](#loading-and-unloading-the-module)
- [Usage](#usage)
- [Troubleshooting](#troubleshooting)
- [Further Development](#further-development)
- [License](#license)

## Prerequisites

Before building and using this kernel module, make sure you have the following
prerequisites installed on your system:

- Linux kernel headers
- GCC compiler

## Building the Module

To build the kernel module, use the following commands:

make
```

Loading and Unloading the Module

To load the kernel module, use the following command:

```
sudo insmod kernelMod.ko
```

To unload the kernel module, use the following command:

```
sudo rmmod kernelMod
```

Usage

Once the module is loaded, it will start monitoring incoming TCP packets. You can check the kernel logs using:

```
dmesg | tail
```

Troubleshooting

- If you encounter issues loading the module, ensure that you have the necessary permissions (use `sudo`). - I have had to do this a few times

- Check the kernel logs for error messages or additional information.

Further Development

- I modeled this project for my Operating Systems course at Fordham University utilizing skills from that course and my Network Essentials course
- Further on, I would love to add an intrusion detection function to it, I did not get to it this time, but I am taking an intrusion detection course next semester, which should give me the knowledge to filter out faulty packets

License

This project was made by Tatum Allen on December 12, 2023