**ARP Traffic Inspector – Kernel Module**

**1. Prepare the Environment**

**Install necessary tools:**

sudo apt update

sudo apt install build-essential linux-headers-$(uname -r)

**2. Create the Module Files**

**a. Create the folder:**

mkdir arp\_traffic\_inspector

cd arp\_traffic\_inspector

**b. Create arp\_traffic\_inspector.c:**

A computer screen shot of a computer code

AI-generated content may be incorrect.

**A computer screen shot of a computer code

AI-generated content may be incorrect.**

**A screenshot of a computer code

AI-generated content may be incorrect.**

**3. Create the Makefile**

**Create a Makefile:**

A computer code with black text

AI-generated content may be incorrect.

**4. Compile the Module**

Make

**5. Insert the Module**

Load the module into the kernel:

sudo insmod arp\_traffic\_inspector.ko

**Check kernel log:**

dmesg | tail

**6. Generate ARP Traffic**

**Ping gateway**

ping -c 1 192.168.1.1

**Then check kernel messages:**

dmesg | tail

**7. Remove the Module**

**unload the module:**

sudo rmmod arp\_traffic\_inspector

**GitHub Instructions**

1. Initialize Git:

git init

1. Stage and commit files:

git add .

git commit -m "Add ARP Traffic Inspector module"

1. Connect to your forked GitHub repo:

git branch -M master

git remote add origin <https://github.com/YOUR_USERNAME/kernel-playground.git>

1. Push to GitHub:

git push -u origin master

**What to Expect**

* ARP Traffic Inspector project will appear under projects/arp\_traffic\_inspector/ in your GitHub repository.
* You will see messages like "Received ARP packet" and "Sent ARP packet" in dmesg.

This project uses Netfilter to hook into incoming and outgoing packets.

To see logs

dmesg | tail -n 20