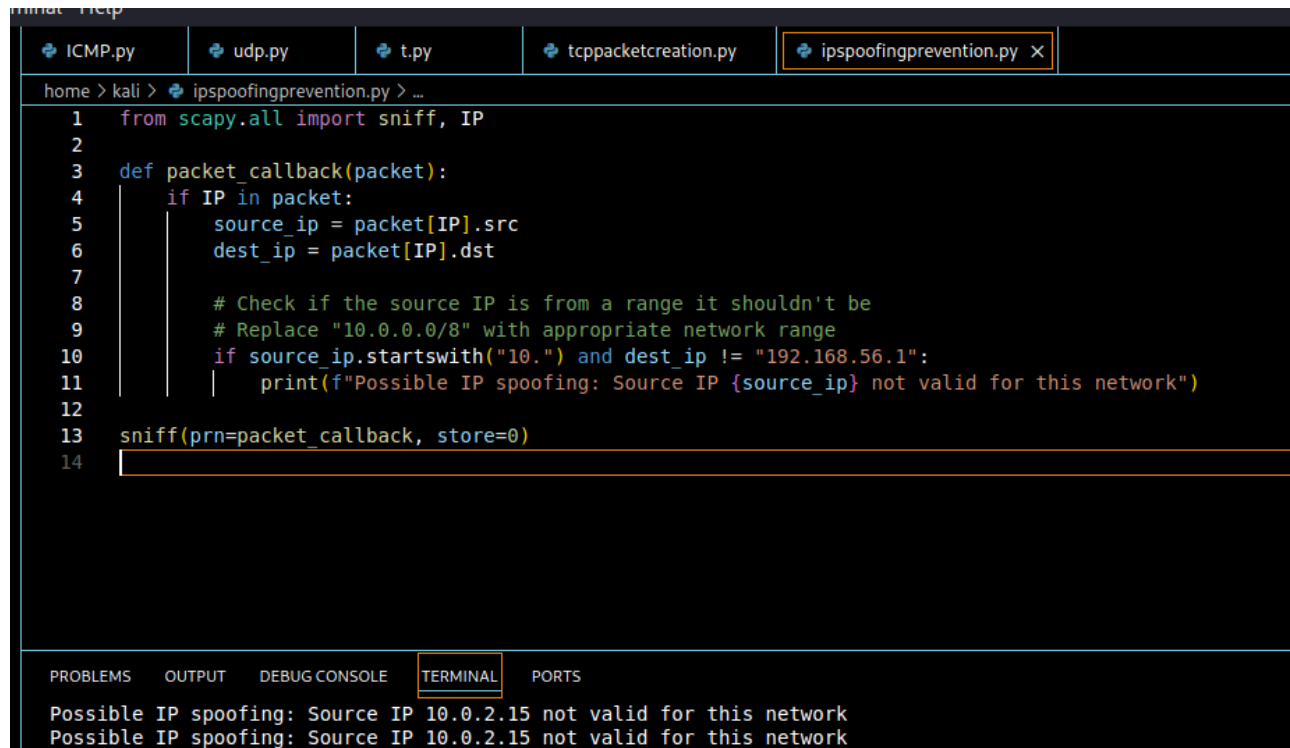


IP Spoofing Prevention



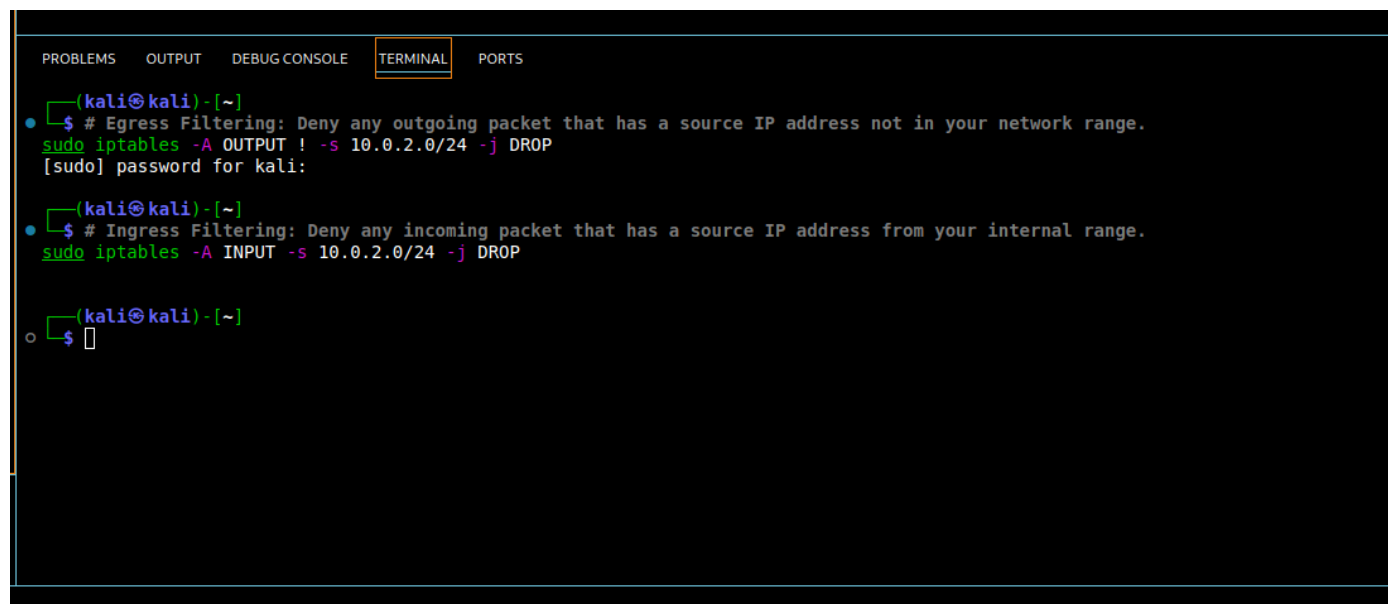
The screenshot shows a code editor with a file named `ipspoofingprevention.py` open. The script uses `scapy` to sniff network traffic and checks for IP spoofing. The terminal output shows two instances of a warning message for a source IP of 10.0.2.15.

```
1 from scapy.all import sniff, IP
2
3 def packet_callback(packet):
4     if IP in packet:
5         source_ip = packet[IP].src
6         dest_ip = packet[IP].dst
7
8         # Check if the source IP is from a range it shouldn't be
9         # Replace "10.0.0.0/8" with appropriate network range
10        if source_ip.startswith("10.") and dest_ip != "192.168.56.1":
11            print(f"Possible IP spoofing: Source IP {source_ip} not valid for this network")
12
13 sniff(prn=packet_callback, store=0)
14
```

PROBLEMS OUTPUT DEBUG CONSOLE **TERMINAL** PORTS

```
Possible IP spoofing: Source IP 10.0.2.15 not valid for this network
Possible IP spoofing: Source IP 10.0.2.15 not valid for this network
```

These can be implemented in practice using router configurations or firewall rules, for example:



The screenshot shows a terminal session where two iptables rules are added to the default chain to prevent IP spoofing. The first rule denies outgoing traffic from the 10.0.2.0/24 network. The second rule denies incoming traffic to the 10.0.2.0/24 network.

```
(kali㉿kali)-[~]
• $ # Egress Filtering: Deny any outgoing packet that has a source IP address not in your network range.
sudo iptables -A OUTPUT ! -s 10.0.2.0/24 -j DROP
[sudo] password for kali:

(kali㉿kali)-[~]
• $ # Ingress Filtering: Deny any incoming packet that has a source IP address from your internal range.
sudo iptables -A INPUT -s 10.0.2.0/24 -j DROP

(kali㉿kali)-[~]
o $
```

Ingress Filtering: This is applied by network routers or firewalls to check incoming traffic and block packets with source addresses that shouldn't come from outside the network.

Egress Filtering: This is used to inspect outgoing traffic from the network and prevent packets with forged source IP addresses from leaving the network. This ensures that no one inside your network is spoofing an IP address.