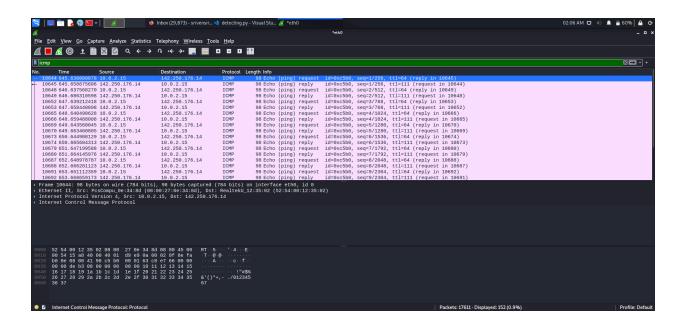
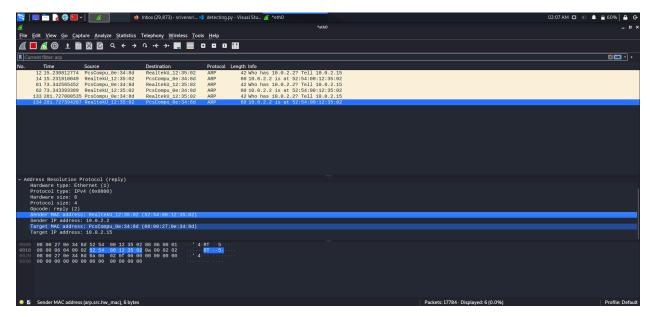
Detecting and Blocking Network Reconnaissance

```
minal Help
  ICMP.py
                                            🕏 t.py
                                                                                                detecting.py ×
                       udp.py
                                                                  tcppacketcreation.py
  home > kali > 🏓 detecting.py > ...
             from scapy.all import sniff, IP, ICMP, ARP
            def monitor_callback(pkt):
      4
                  # Detect ICMP (ping) requests which are often used in ping sweeps
                  if ICMP in pkt and pkt[ICMP].type == 8:
      5
      6
                       print(f"[!] Detected ICMP request from {pkt[IP].src} to {pkt[IP].dst}")
                  # Detect potential ARP scans which can be used for MAC address gathering and OS fingerprinting
      8
      9
                  if ARP in pkt and pkt[ARP].op == 1:
     10
                       print(f"[!] Detected ARP request from {pkt[ARP].psrc} asking about {pkt[ARP].pdst}")
     11
     12
                  # For port scans, you might want to look at raw TCP or UDP packet counts over time from specific IPs,
     13
                  # but it's more complex and beyond a simple script.
     14
     15
            def main():
                  print("[*] Starting network reconnaissance prevention tool ...")
     16
                  # Starting the sniffer. This will keep running until manually stopped.
     17
     18
                  sniff(prn=monitor_callback, store=0)
     19
     20
                   name
     21
                 main()
   PROBLEMS OUTPUT DEBUG CONSOLE
                                                  TERMINAL
                                                                PORTS
      —(kali⊕kali)-[~]
 o $ sudo python3 detecting.py
  sudo python3 detecting_py.
[sudo] password for kali:
[*] Starting network reconnaissance prevention tool ...
[!] Detected ARP request from 10.0.2.15 asking about 10.0.2.2
[!] Detected ARP request from 10.0.2.15 asking about 10.0.2.2
[!] Detected ARP request from 10.0.2.15 asking about 10.0.2.2
/bin/python3 /home/kali/ICMP.py
[!] Detected ICMP request from 10.0.2.15 to 142.250.176.14
[!] Detected ICMP request from 10.0.2.15 to 142.250.176.14
[!] Detected ICMP request from 10.0.2.15 to 142.250.176.14
         Detected ICMP request from 10.0.2.15 to 142.250.176.14

Detected ICMP request from 10.0.2.15 to 142.250.176.14

Detected ICMP request from 10.0.2.15 to 142.250.176.14
     [!] Detected ICMP request from 10.0.2.15 to 142.250.176.14
```





Possibly integrate with firewall rules to automatically block IPs that exceed certain thresholds.

1. You can write a custom shell or Python script to monitor logs and dynamically add rules to block IPs using iptables or nftables.

sudo iptables -A INPUT -s <malicious ip> -j DROP

2.Create a script that monitors /var/log/auth.log (for SSH) or any other log file.