Lab 8
Two Goals

• **Implement** a simple traceroute
  • Get familiar with creating packets

• **Analyze** traffic *after* an incident
traceroute

Need to set both IP and ICMP headers

• Main IP fields
  • Dst IP address
  • TTL

• Main ICMP types:
  • Request
  • Reply
  • Time Exceeded

```
./traceroute <IP_ADDRESS>
```
traceroute

Build a path of routers from source to destination. How?

Echo Request
TTL = 1

Time Exceeded
traceroute

Build a path of routers from source to destination. How?

- Echo Request
  TTL = 2

- Time Exceeded
traceroute

Build a path of routers from source to destination. How?

Echo Request
TTL = 3

Echo Reply
scapy APIs

• Rich library (useful for spoofing, analysis, tooling, etc.)
• The scapy.all module:
  • Functions:
    • `sr`: send and receive multiple pkts
    • `sr1`: send pkts and receive the first one!
  • Classes:
    • IP and ICMP: corresponding protocol headers
• Basic library usage:
1. **Construct** a TCP packet:
   - IP and TCP headers
   - Payload

2. **Send** the packet using `sr1()`

3. **Print** a summary of the reply packet (if any)
Traffic Analysis

• A given harassment scenario

• You need to:
  • analyze the traffic
  • find the harasser
  • provide enough evidence
Questions?