Scapy: A Hands-On Review of Networking
What is Scapy?

- Network tool designed for packet crafting
- Built on Python
- Flexible, supports a variety of use cases
- Supports large number of protocols
- Extensible to support user-defined protocols
Why are we using Scapy

- Building/manipulating packets is the easiest way to learn about them
- Attacks often use specially crafted packets
- Gives us a quick way to play with packets
What is included?

• Building packets using any protocol
• Manipulating the fields
• Stacking protocols on a single packet
• Sending and receiving packets, traceroute, sniffing, fuzzing, custom routing tables, interfacing with visualization tools, interfacing with PCAP and Wireshark, and more!
How to use scapy

• From the command line, run “sudo scapy”

• Gives an interactive scapy shell

• Can also import using “from scapy.all import *”
Basic Commands

• IP() – creates an IP packet
• Ether()/IP()/TCP() – creates a packet with TCP stacked on IP stacked on Ethernet
• str(IP()) – string representation of a packet
• IP(dst="www.google.com/30") – creates 4 packets (netmask 255.255.255.252)
• send(IP(dst="1.2.3.4"]/ICMP()) – pings 1.2.3.4
Interactive Tutorial

• First go through http://www.secdev.org/projects/scapy/demo.html

• Then explore scapy however you see fit, some suggestions
  – Play with the fields in the protocols we discussed earlier this week and send the packets, to see how setting certain flags or changing fields affects things
  – Manipulate the scapy routing table and explore how that affects things (the routing table is at conf.route)
  – Build your own protocol (see http://www.secdev.org/projects/scapy/doc/build_dissect.html)