CSCD 330 – Computer Networks

scapy intro

Overview:

First thing you'll need to do is make sure `scapy` is installed on your system.

```
sudo apt-get install python3-scapy
```

`scapy` has its own interpreter **you will not use it**. Instead, we are going to interact with the `scapy` library via `python`.

- Open up `python` and import `scapy`
  - `from scapy.all import *`
- Create a packet on any layer by using its name.
  - E.g., to create a TCP packet:
  - `tcp = TCP()`
  - You can create other packets similarly.
  - `ip = IP()`
  - Remember, the left hand side is a variable and you can name it whatever you want.You can also set the fields of the packet during initialization.
  - E.g., `push_packet = TCP(flags='PA')`
- You can dump the contents of the packet with `ls()`
  - E.g., `ls(tcp)` or `ls(ip)`.
- Any of those fields can then be edited:
  - E.g., `tcp.dport = 8080` will set the destination port of the TCP packet to 8080.
  - You can also set the flags: `tcp.flags = "SA"`
  - Setting the TCP flags to be `SYN/ACK`.
- Join packets with encapsulation using the `/` symbol.
  - E.g., `ip/tcp`, will create a packet you can send.
  - You don't have to create an Ethernet packet. `scapy` will do that for you.
- Finally you can send with:
  - `send` or `sr1`
  - First just sends, second sends and receives 1 packet.
  - For `sr1`, don't forget to save the return packet!

As always, `tab` to autocomplete on the `python` interpreter is your friend.