

Network Programming with **UMIT** Project



Narendran Thangarajan

@naren_live

PyCon India 2011

Outline

- Why Network Programming
 - Network Scanning
- Umit Network Scanner
 - Nmap
- Packet Manipulator
 - Scapy
 - UMPA
 - PyPcap
 - Creating a new protocol
- Future Directions

”Network is the computer”

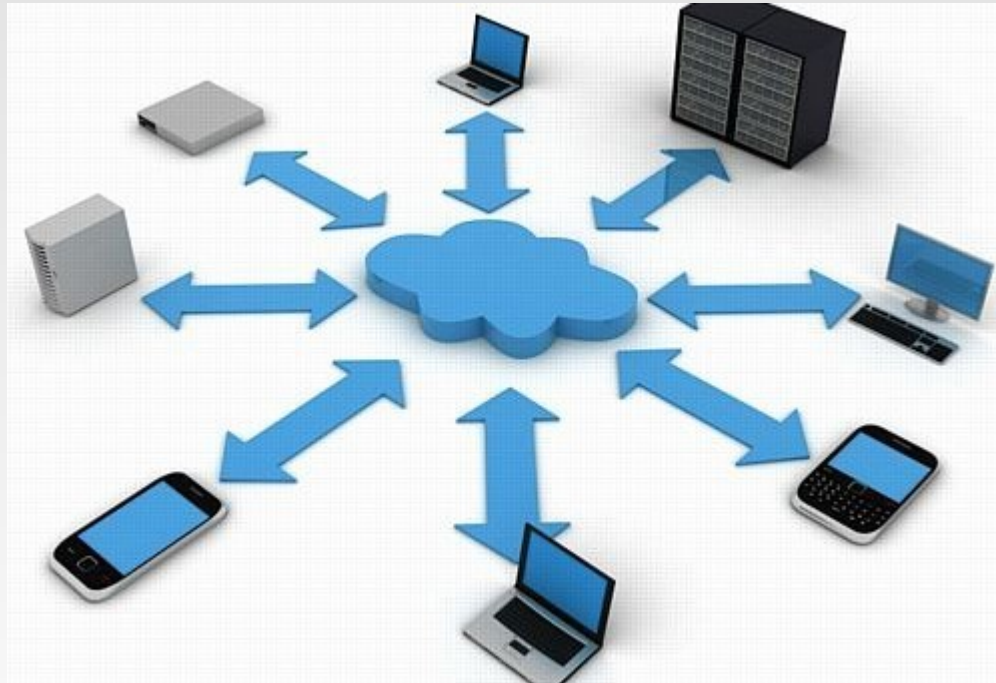
- Mitch Kapor

Why Network Programming?

- The future of computing is Mobile and Cloud Computing.
- With thinner clients and resources getting centralized, almost every file access is going to burden the network.
- In future, we might reach a point where the loss due to a one-minute network failure will cause a loss greater than earthquakes or cyclones.



We need data.. Enough data to predict a network failure



Network Scanning

- Second of the three data gathering steps.
- Footprinting – Scanning - Enumeration
- Procedure of finding active hosts on the network.
- Used for :
 - Network Security Assessment
 - Purpose of attacking
 - Research/Study

Nmap - Backend

- Terminal-based security scanner originally written by Gordon Lyon.
- Discovers hosts and services – Creates a "map"
- Basic Host scanning + determine OS + Names and versions of services running in the remote host + type of device.
- Examples

Umit Network Scanner – Frontend

- GUI based Network Scanner
- Began as a project for GSoC 2005
- Inspired other scanners like Zenmap
- What could we do?
 - Scanning
 - Schedule scans
 - View Network Topology
 - Create Profiles
 - Create our own Plugins

Packet Manipulator - Frontend

- Protocol Analyzer
- Can capture packets from any interface
- Decodes the packet based on the protocols supported by the backend

Scapy

- Python package for Send, sniff, dissect and forge network packets
- Whats so special?
 - Create ANY packet
 - Flexibility
 - Detailed decoding of the received packets
 - Fast Packet Design

Scapy - Demo

- Basic Packet construction
- Stacking Layers
- Sending Packets
- Receiving Packets
- Traceroute
- Graph the traces

UMPA – Backend L1

- Umit Manipulation of Packets Art
- Umit's Packet Generation and Manipulation Library
- Under Development
- Example : `sample.py`

Libpcap

- Father of Packet capture libraries
- Implemented in C
- Initially created for tcpdump
- Maintained by tcpdump organization
- Almost all the python packet libraries use libpcap as the backend

Future Directions

- Solve Connectivity problems – Internet shortages, ISP service blockages.
- A small disconnection could lead to huge losses in future.
- Internet Connectivity Monitor

Thus we have networked with Python

Thank You!!



Queries?

Email : narendran.thangarajan@gmail.com

Twitter : naren_live

Google : Narendran Thangarajan :P