Network Penetration Testing Using Python and Kali Linux

Before We Start

Author Gus Khawaja

Gus.Khawaja@guskhawaja.me

www.ethicalhackingblog.com

Why Choose Python?

Comparisons

- Business applications : C# / Java

- Hardware drivers: C/C++/Assembly

- Web applications: ASP.Net / PHP / Javascript

- Penetration testing :

    - Applications: Python / Perl

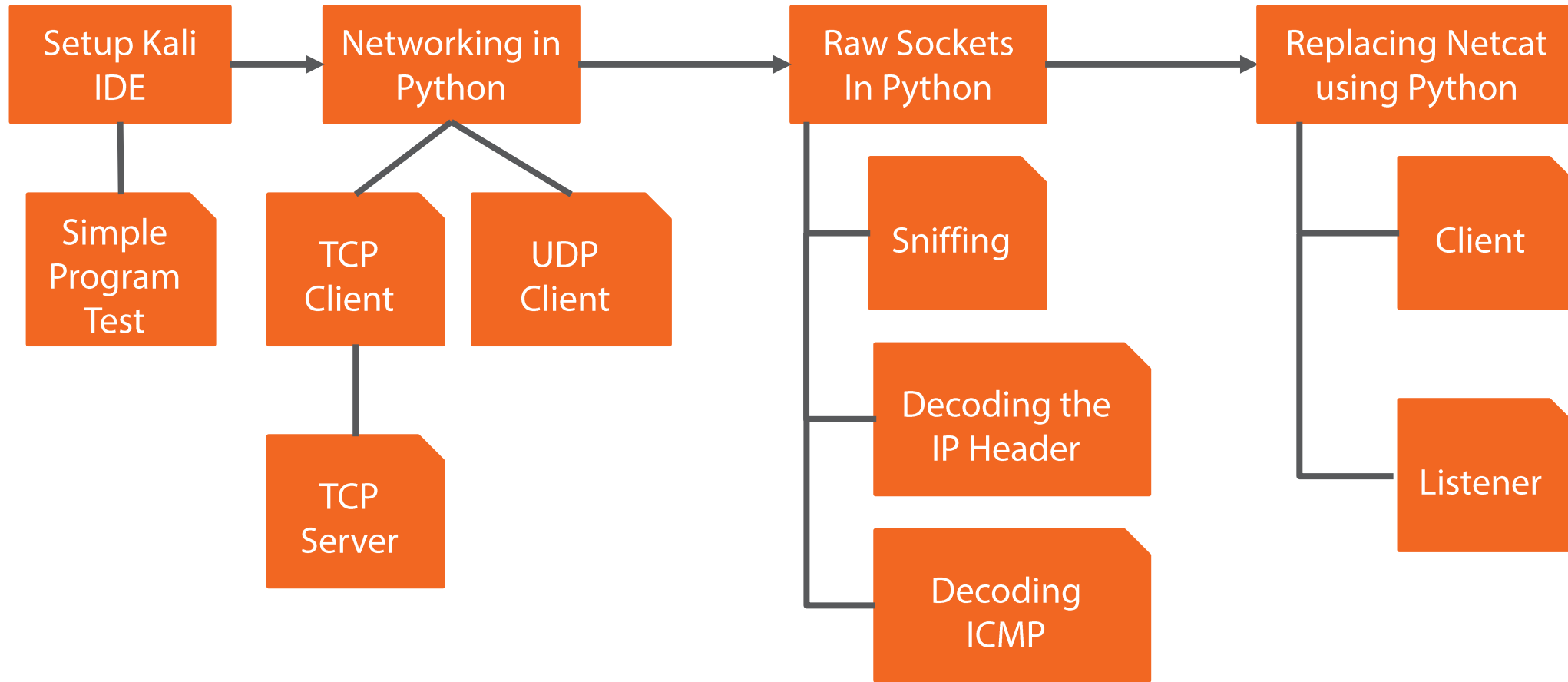   - Reverse engineering: C/C++/Assembly

Prerequisites

Ethical Hacking { http://www.pluralsight.com/courses/ethical-hacking-understanding

Penetration testing { 1 year +

Python language { http://www.pluralsight.com/courses/python-fundamentals

Course Workflow

Workflow

Setup Kali IDE → Networking in Python → Raw Sockets In Python → Replacing Netcat using Python

- Setup Kali IDE
  - Simple Program Test
- Networking in Python
  - TCP Client
    - TCP Server
  - UDP Client
- Raw Sockets In Python
  - Sniffing
  - Decoding the IP Header
  - Decoding ICMP
- Replacing Netcat using Python
  - Client
  - Listener

Summary

Summary

Python / C / C++ / Assembly

Workflow