External Pen-testing

Author Gus Khawaja
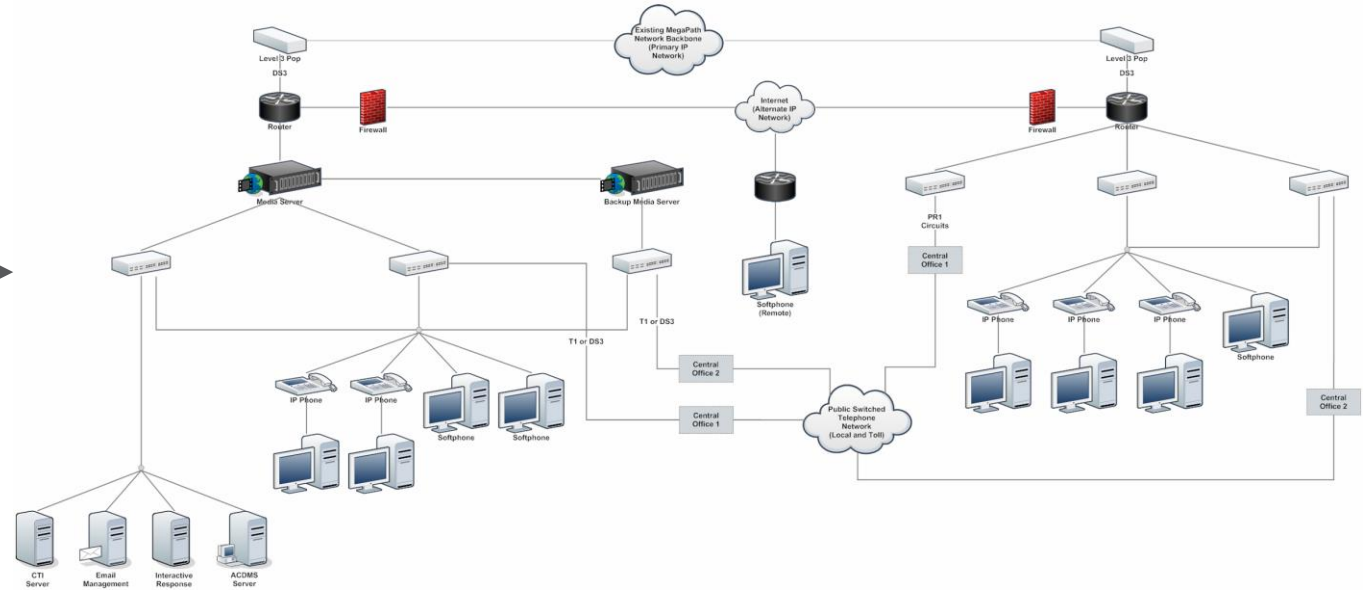
Gus.Khawaja@guskhawaja.me

www.ethicalhackingblog.com
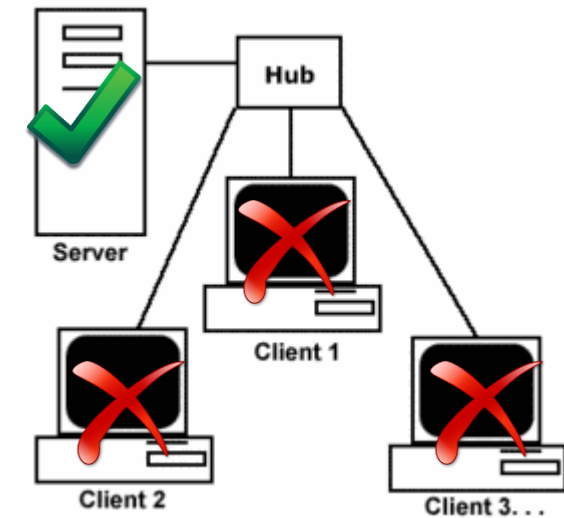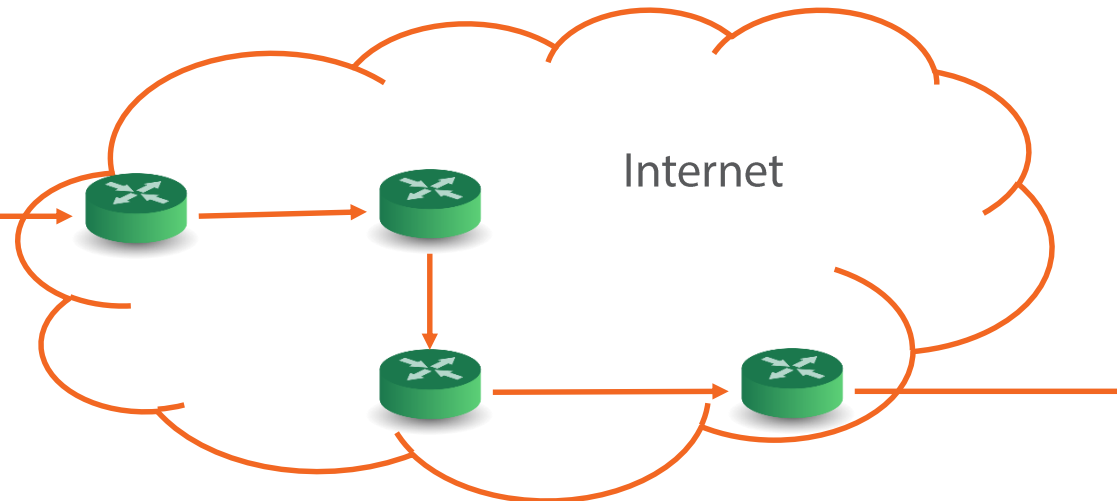
External Pen-test Workflow

Network Diagram: Telecommunications Network Architecture

Traceroute

Ping: Live hosts ?

Nmap: Port Scanning
Knock Knock Port 21
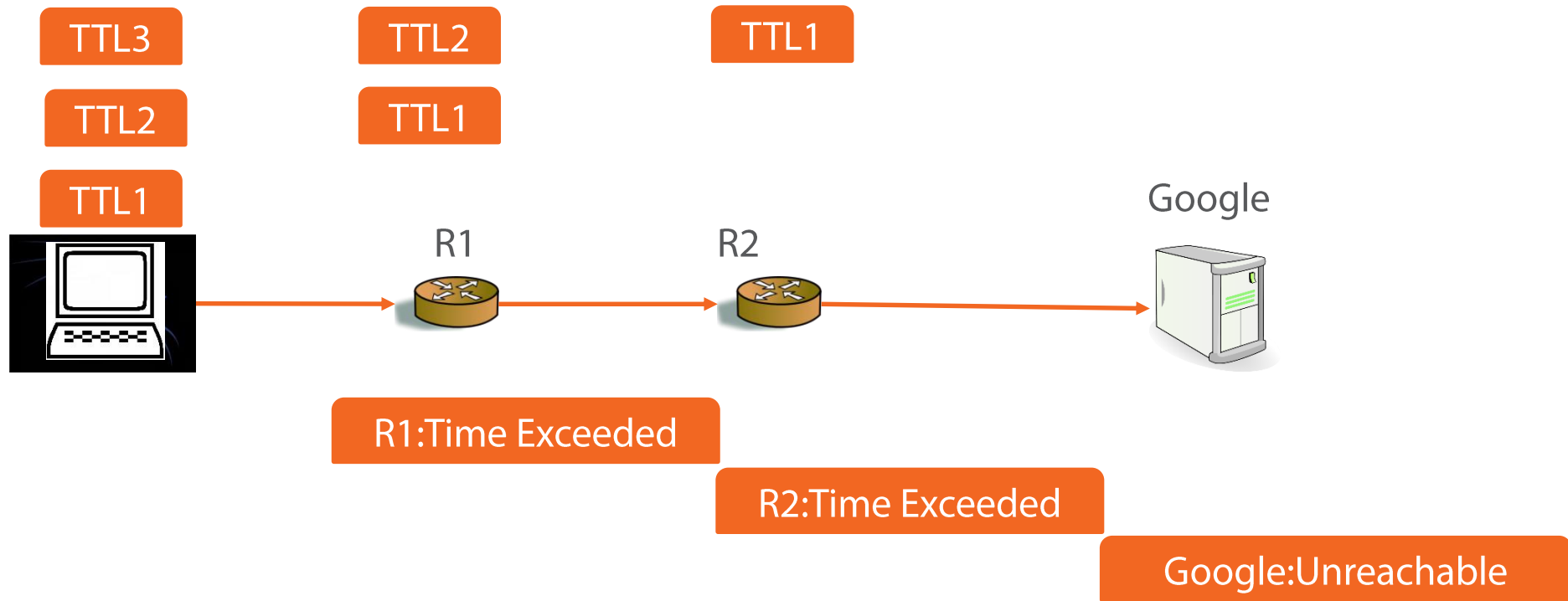**Knock Knock Port 25**
Knock Knock Port 80
Knock Knock Port ?

KALI LINUX

Internet

Hub

Server

Client 1

Client 2

Client 3. . .

Traceroute

Traceroute

Live Host Discovery (Ping)

Tools

Ping scanners on Kali
- Nmap
- Hping3

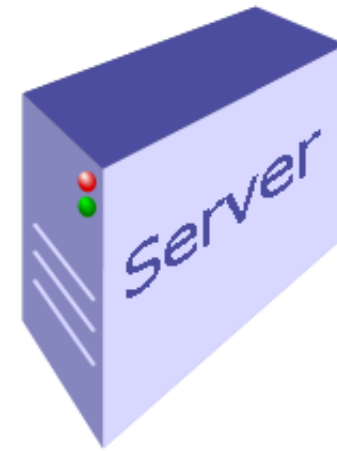**TCP PING**

Port Scan

Nmap

Nmap
Network Mapper

TCP SYN
:80

SYN-ACK:
80 opened

Server

Output: Port 80 opened → Web Server

Summary