Networking Refresher

Iker M. Canut

June 10, 2020

1 IP Addresses

ifconfig bring up networking information.

- inet: IPv4 Address in Decimal notation. Made up of 32 bits.
- inet6: IPv6 Address in Hexa notation. Made up of 128 bits.

How is it possible that we're using IPv4 but we're out of address space? It's all about NAT: Network Address Translation. What we're doing is assigning private addresses, so we're not taking space from the 4 billion IPv4 addresses. All private addresses are not going to be out in the interweb, it's an IP address that is only known to you. So because we use these private IP addresses we can pass them out through what is called a public IP address.

Network Class	Network Numbers	Network Mask	#Networks	#Hosts per Network
CLASS A	10.0.0.0	255.0.0.0	126	16.646.144
CLASS B	172.16.0.0 to 172.31.0.0	255.255.0.0	16.383	65024
CLASS C	192.168.0.0 to 192.168.255.255	255.255.255.0	2.097.151	254
LOOPBACK	127.0.0.0 to 127.0.0.7	255.255.255.0	-	-

So you probably got all your devices on a class C network, and all of them are talking out of one IP address: your public IP address. You rent it from your ISP, and all this network traffic goes out through this IP.

2 MAC Addresses

This is layer 2. MAC stands for Media Access Control and that is identified in our *ifconfig* as **ether**. This is our physical address and a way that we communicate when we are using switches. This is how switches know what device is what.

Suppose that you have a computer and you're installing a Network Interface Card. You plug that in and you're going to have a MAC Address for that NIC. Anything that's using a NIC is going to have a MAC Address.

If we take the first 3 pairs of a MAC Address, we can identify the manufacturer. E.g. $b0 : c0 : 90$, is from Chicony Electronics Co. Ltd. That way we can identify what we're up against.

3 TCP

TCP stands for Transmission Control Protocol and that is a connection oriented protocol. This one is used when we need high reliability. E.g, websites (HTTP/HTTPS), SSH, FTP.

3.1 The Three-Way Handshake

1. SYN: *You say Hello!*
2. SYN/ACK: *Ey SYN, I Acknowledge you, hello!*
3. ACK: *Cool, let's start the conversation.*

This logic could be extrapolated to ports (an item that we can open in order to communicate with certain protocols, e.g HTTP is port 80, HTTPS is port 443). So, if for example you want to connect to port 80 on a website, first you're going to send a SYN (*Ey, I want to connect to port 80!*). If that port is open and can start a conversation, the reply will be a SYN/ACK (*You can go ahead, connect to me*). Then, if you want to actually establish a connection, you send an ACK packet back.

```
19 1.178137205   192.168.0.165    216.58.202.35    TCP    74 51916 → 80 [SYN] Seq=0 Win
20 1.204127977   216.58.202.35    192.168.0.165    TCP    76 80 → 51916 [SYN, ACK] Seq=
21 1.204151354   192.168.0.165    216.58.202.35    TCP    66 51916 → 80 [ACK] Seq=1 Ack
```

In this example we can see the three way handshake between the port 51916 from the computer on 192.168.0.165 and the port 80 from the server on 216.58.202.35.

4 UDP

UDP stands for User Datagram Protocol and that is a connection-less protocol. This one is used for example in streaming services, DNS, Voice over IP.

5 Common Ports and Protocols

- **TCP**
  - **FTP (21)**: File transfer protocol. You can log in and put a file or get a file off the server.
  - **SSH (22)**: Log into a machine remotely (encrypted).
  - **Telnet (23)**: Log into a machine remotely (plain text).
  - **SMTP (25)**: Mail.
  - **DNS (53)**: Domain Name System: Resolve IP addresses to names.
  - **HTTP (80) / HTTPS(443)**: Web sites.
  - **POP3 (110)**: Mail.
  - **SMB (139 + 445)**: The most common port for pentesters. File shares: think about all the crazy exploits: Wannacry, Eternal Blue, MS17.0.1.0. SMB is open so frequently on networks.
  - **IMAP (143)**: Mail
- **UDP**
  - **DNS (53)**: Domain Name System: Resolve IP addresses to names.
  - **DHCP (67, 68)**: Associates you with an IP address, kinda random (from a range). The opposite is static IP address.
  - **TFTP (69)**: Trivial FTP.
  - **SNMP (161)**: Simple Network Management Protocol. When we encounter it there may be information to be gathered. Especially if there are strings being used that are public.