Chapter 0x02 | Third Meetup

Computer Networks - Can we break them? Lets see!!!

About me

@MrMeterpreter

Security Enthusiast (Yes I test pens sometimes pencils too)

Sometimes builder but more into pulling things apart.

Working for [Redacted] Cyber Security company.

Not really the ‘hacker’ you would think of.

Host of the podcast ‘Nepal got Hacked’.

Agenda

The Network - what really makes it a network.

How systems communicate inside the network.

What’s exactly inside the communication.

Can we break the chain of communication.

Theoretically seems like we can - let’s do it (DEMO)

How do you protect yourself ?

Takeaway

The Network

Router

Switch

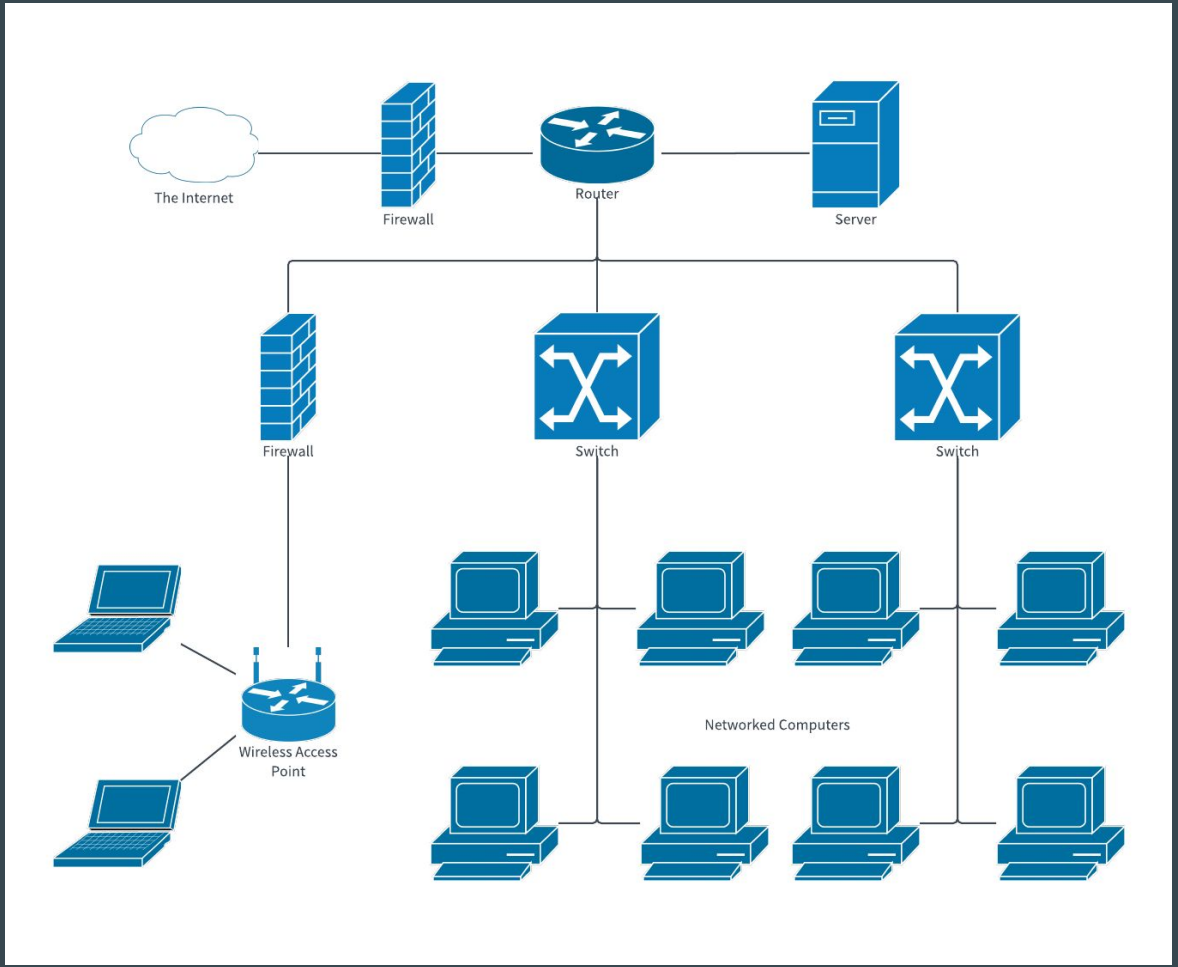
Server

Firewall

Computers

Phone

That's it???



Network - Is that it?

Traffic light systems

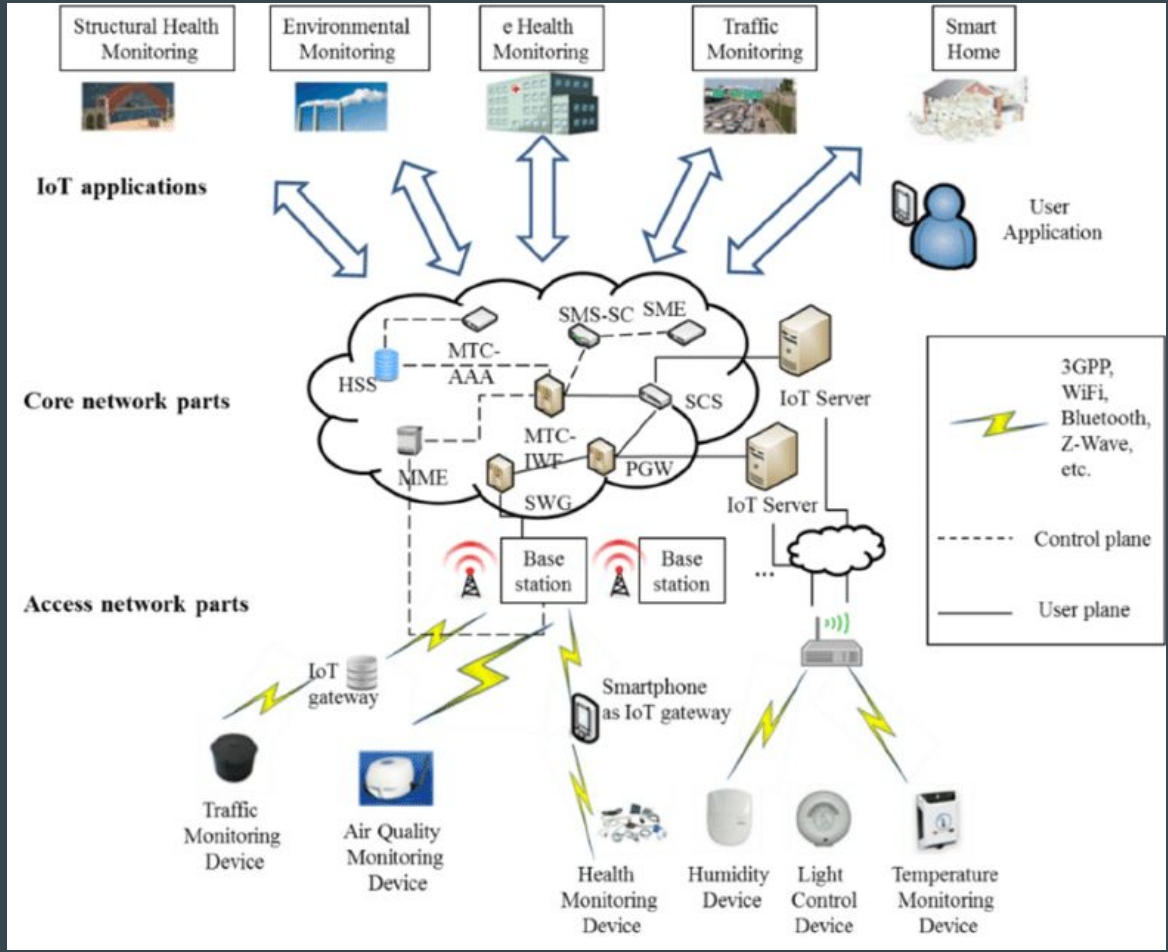
Weather monitoring stations

Smart home appliances

Pacemakers

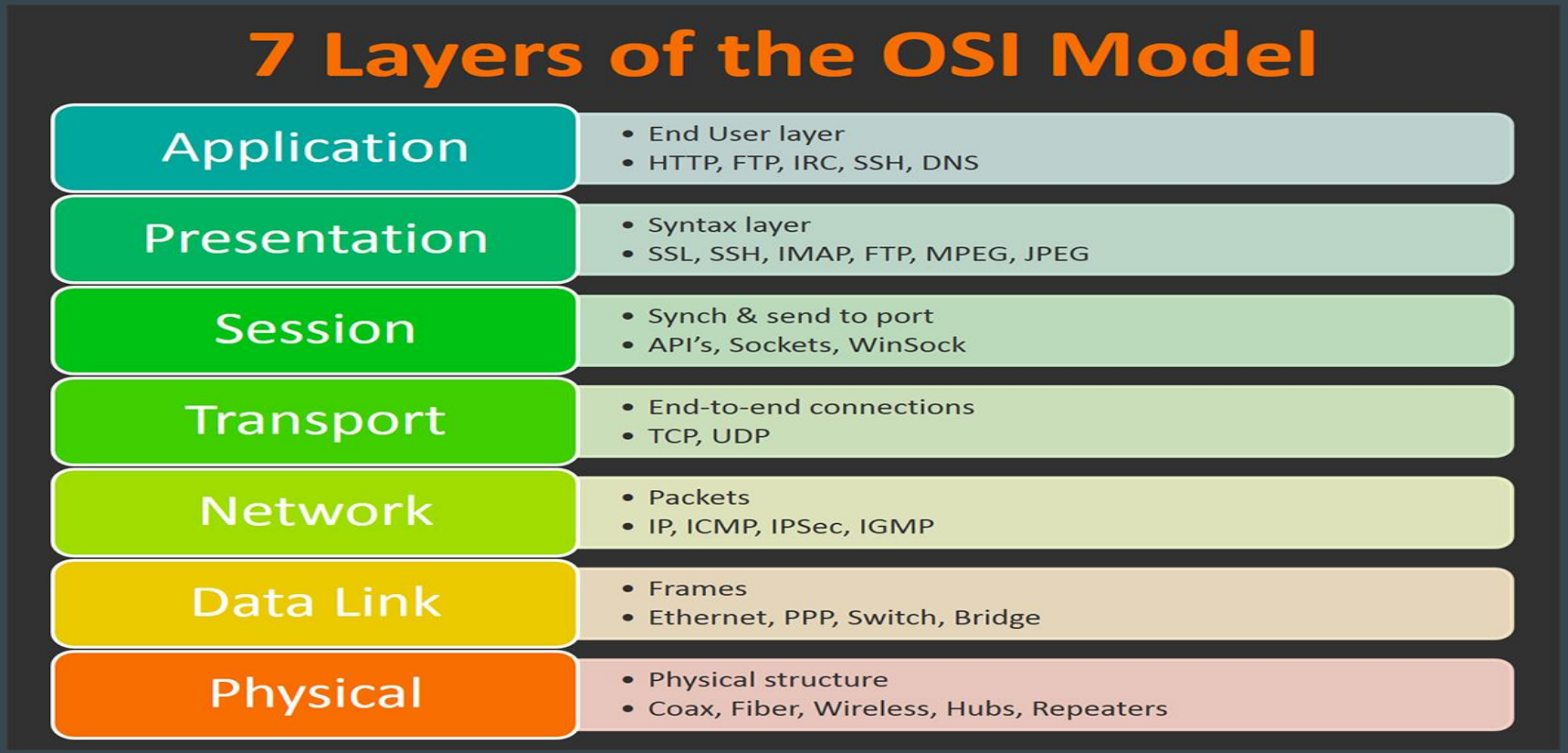
3G, 4G, 5G

yada yada yada - - - - -



Tl;dr - Perhaps anything/everything that has IP address and can communicate. (IOE)

Let's get the fundamentals



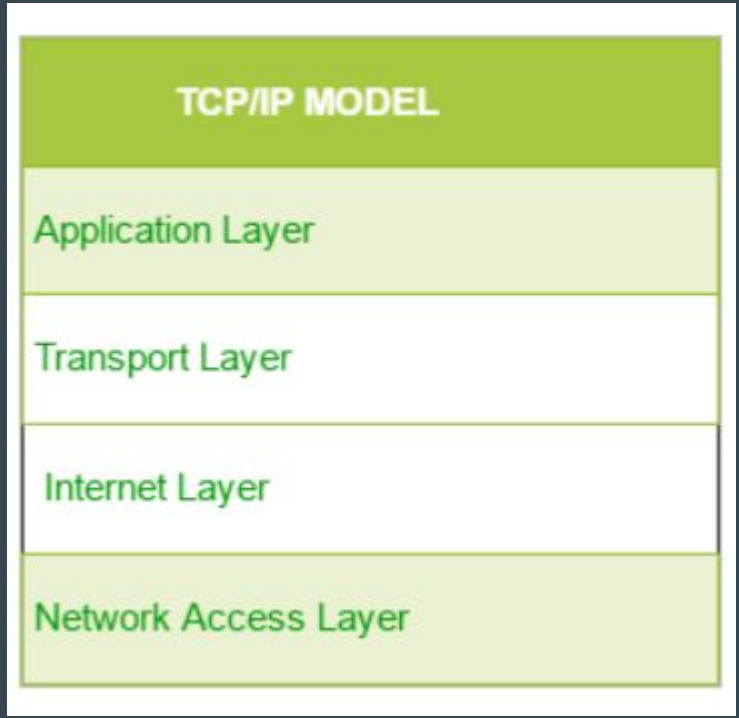
OSI was the reference model - TCP is the standard

Came somewhere in 1983.

Initially designed for research.

Came before OSI.

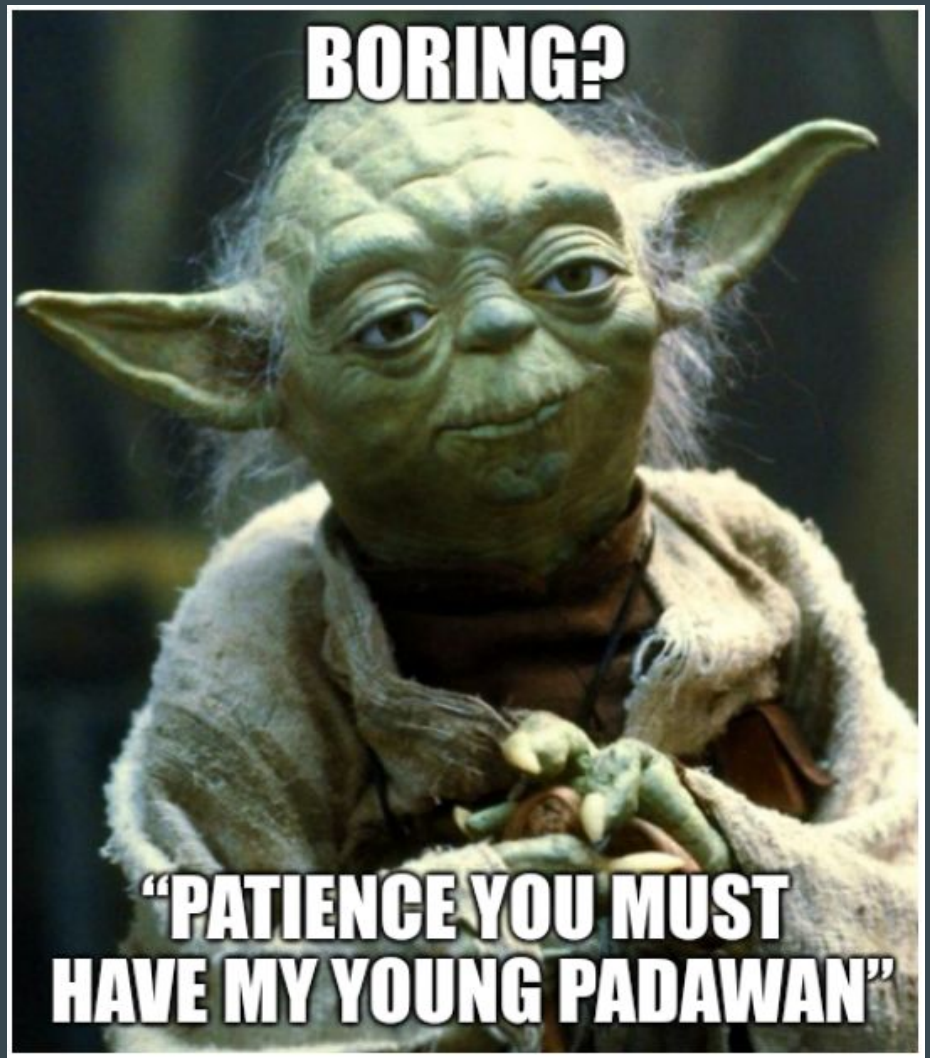
Developed by DARPA or ARPA.



All these designed by amazing minds..

So where could this go wrong!

Right?



So, what could go wrong?

Physical Layer - Physical destruction, obstruction, manipulation, or malfunction of physical assets.

Data Link - MAC flooding - overload the network switch with data packets.

Network Layer - ICMP Flooding - A Layer 3 infrastructure D/DoS attack method that uses ICMP messages to overload the targeted network's bandwidth.

Transport Layer - SYN Flood, Smurf Attack (the handshake thing)

And still more - (contd...)

Session Layer - Session hijacking, Person/thing in the middle attack (aka MITM) etc.

Presentation Layer - Malformed SSL Requests - SSL hijacking, SSL Striping etc.

Application Layer - GET, POST, OPTIONS request and/or/also etc. etc. and all the OWASP thing.

And still more - (contd...)

No just kidding

No but seriously, that's not just it.

They were just an insight, there's a lot more.

Time to play the game....

What we did today?

TCP and OSI thing.

Inside the 7 layers thing.

Attack surface and types of attacks in different layers.

ARP/MAC flooding thing. (in the game session)

DNS attack/hijacking thing (in the game session)

All the DOS stuff (SYN, FIN - basically the handshake thing)

Takeaway - Yoda wisdoms

“Control, control, you must learn control!” i.e. Only hack what you own.

“Your weapons, you will not need them.” i.e. Installing Kali does not make you hacker.

“Much to learn you still have…my old padawan.” … “This is just the beginning!” i.e. Be curious, be passionate

“Always pass on what you have learned.” - You know what I mean.