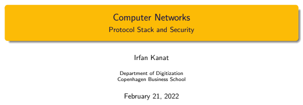
Computer Networks

Protocol Stack and Security

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022



Computer Networks
Protocol Stack and Security

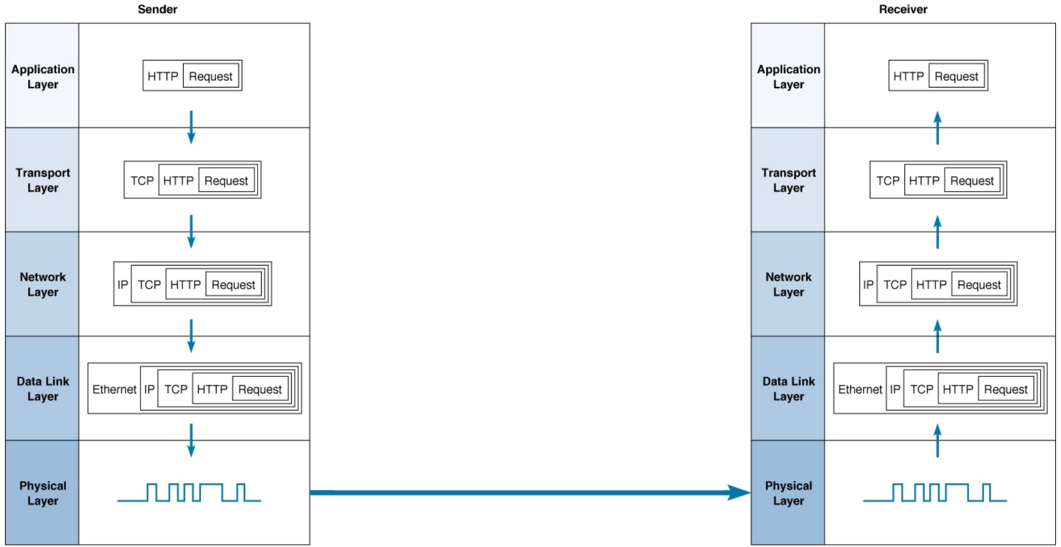
Irfan Kanat

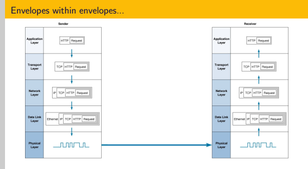
Department of Digitization
Copenhagen Business School

February 21, 2022

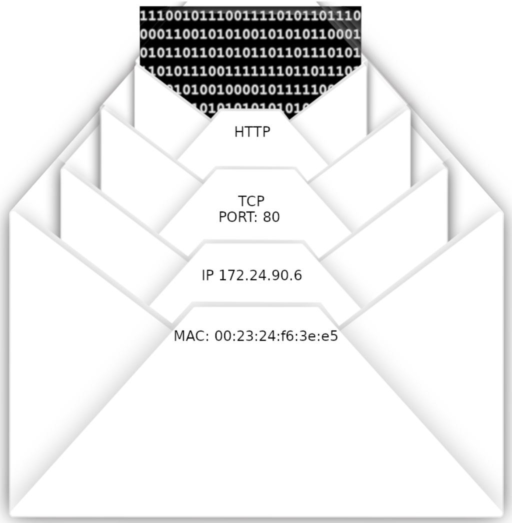
In this video we will talk about how the protocol stack effects security.

Envelopes within envelopes...

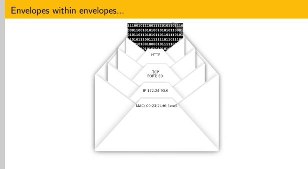




Envelopes within envelopes...



└Envelopes within envelopes...



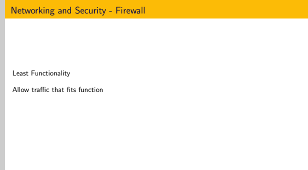
We learned in the previous video that there was this protocol stack with different types of addressing in each layer.

This can be used both for attack and for defense.

Networking and Security - Firewall

Least Functionality

Allow traffic that fits function



Networking and Security - Firewall

Least Functionality

Allow traffic that fits function

Most attacks that come over the network work by exploiting an unpatched vulnerability in the server.

One way to minimize this impact is to minimize the attack surface. Don't give access to services you don't absolutely need. This ties in with the "Least functionality" principle.

Knowing the functionality of a computer, you can create rules for acceptable network traffic.

Firewall

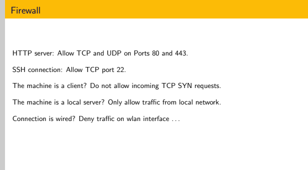
HTTP server: Allow TCP and UDP on Ports 80 and 443.

SSH connection: Allow TCP port 22.

The machine is a client? Do not allow incoming TCP SYN requests.

The machine is a local server? Only allow traffic from local network.

Connection is wired? Deny traffic on wlan interface . . .



Firewall

HTTP server: Allow TCP and UDP on Ports 80 and 443.

SSH connection: Allow TCP port 22.

The machine is a client? Do not allow incoming TCP SYN requests.

The machine is a local server? Only allow traffic from local network.

Connection is wired? Deny traffic on wlan interface . . .

UFW Firewall

Computer Networks

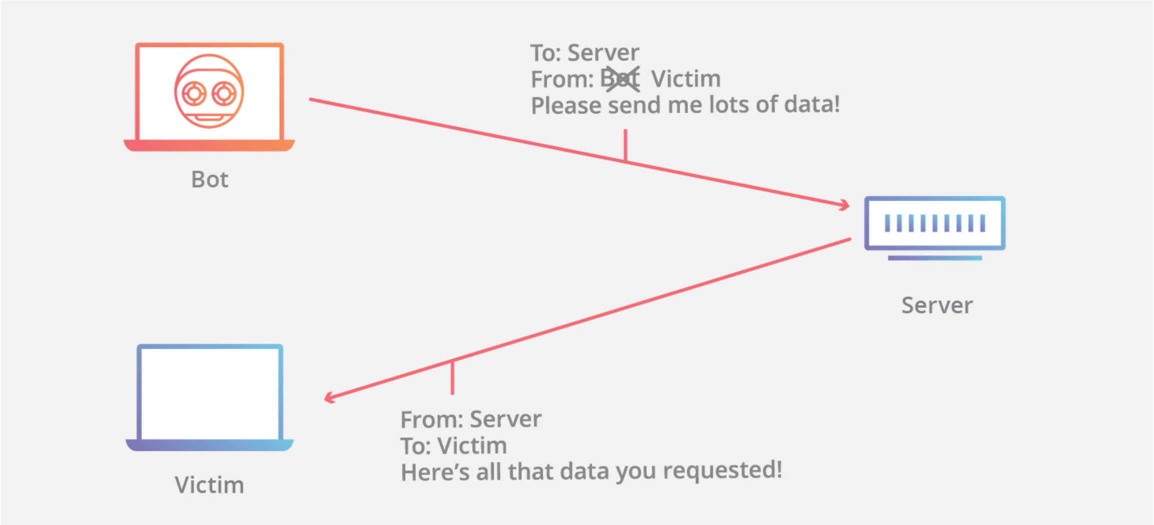
2022-02-21

└UFW Firewall

UFW Firewall

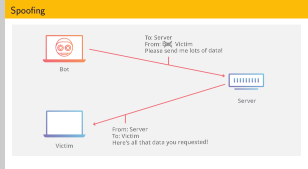
I set up an AWS instance for this demo. Look up its IP address before you begin.
1 - Show which ports are open on a computer with nmap
2 - Try to feed ip into a browser and get no result
3 - Log into the server.
4 - Change firewall settings to allow HTTP traffic
sudo ufw status
sudo ufw enable 80
5 - Get back to your own machine and do another port scan show 80 now open for business
6 - Show in browser the hello friend page.
Other rules for purposes.
Deny certain networks
sudo ufw deny from 15.15.15.0/24
Allow SSH?
sudo ufw allow ssh
A series of rules carried out in order
sudo ufw status numbered

Spoofing



To: Server
From: ~~Bot~~ Victim
Please send me lots of data!

From: Server
To: Victim
Here's all that data you requested!



Many different kinds of spoofing exist.
Mail spoofing, MAC address spoofing, IP spoofing.
It essentially means pretending to be someone you are not.
In case of IP spoofing, it is very useful in multiplying your DDoS capability.

Make a small request to a server with a large return package. Plug victim IP as source IP. Now for every small package you sent, victim will receive a large package. Used in DNS amplification attacks.