Cybersecurity BootCamp
week 2

ZERNA Lesly

October 2017

1 Introduction

Cybersecurity BootCamp by CyberWayFinder SPRL consists in a four week training in topics to be introduced into the cybersecurity field. This training is mainly focused on women inclusion into this field.

This document contains my personal notes and extra info about the topics involved during the 4 weeks.

2 Class 4 - Risk management

Asset * Threat = Risk mitigation Risk can be possible in three dimensions:

- **Confidentiality** (what will happen if this is lost?)
- **Integrity** (mitigation with CRC "Cyclic redundancy check" ?)
- **Availability**

Risk management is about mitigation. Sometimes we need to "guess" the value of assets.
Example, assets for a company:

- Strategy (business model?)
- People and processes
- Application
- Hardware

It is recommendable to start with a list of threats and to define the risks and impact in case of attack.

- Risk identification
- Risk impact

- Risk treatment

In case of mitigation:

- Detection (when do you detect the threat)
- Reaction
- Resilience

Governance Important: Remember its 5 pillars.

- Governance
- Risks
- Strategy
- Maintenance
- Incidence

3 Class 5 - Networking and Telecommunications security

Recommended book: "The phoenix project".
Availability is super important.

Basic Definitions in **Networking**

- **LAN** -> Local Area Network
- **MAN** -> Metropolitan Area Network
- **WAN** -> Wide Area Network
- **Internet**
- **Extranet**
- **WWW** -> World Wide Web

Network is a stack of protocols. We focused on working in switch layer 2 and routers layer 3 (layers of OSI Model).

OSI Model "The OSI model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers.

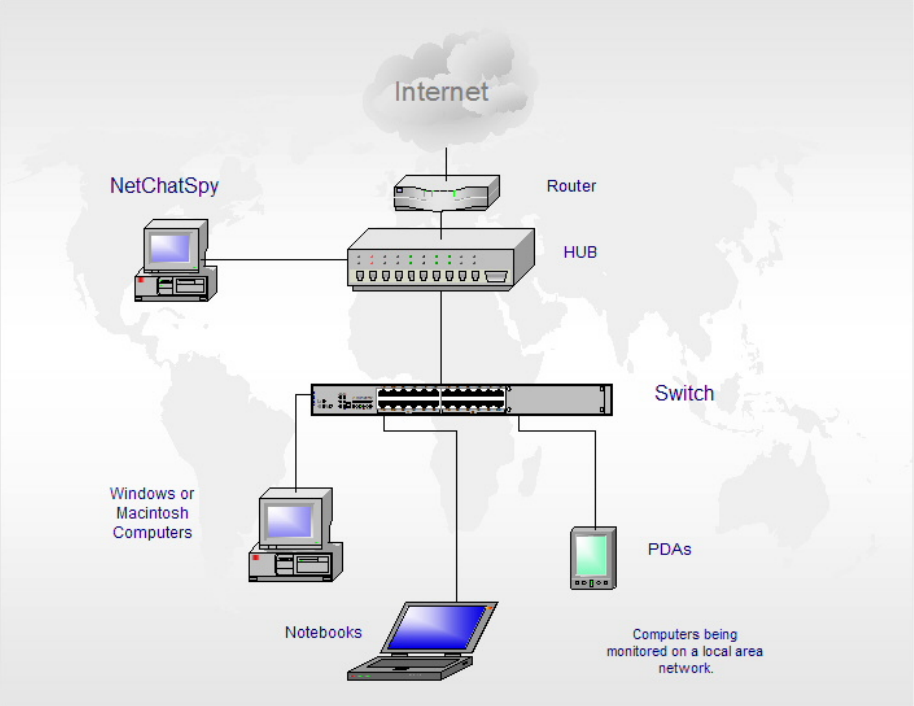

Figure 1: Basic Network

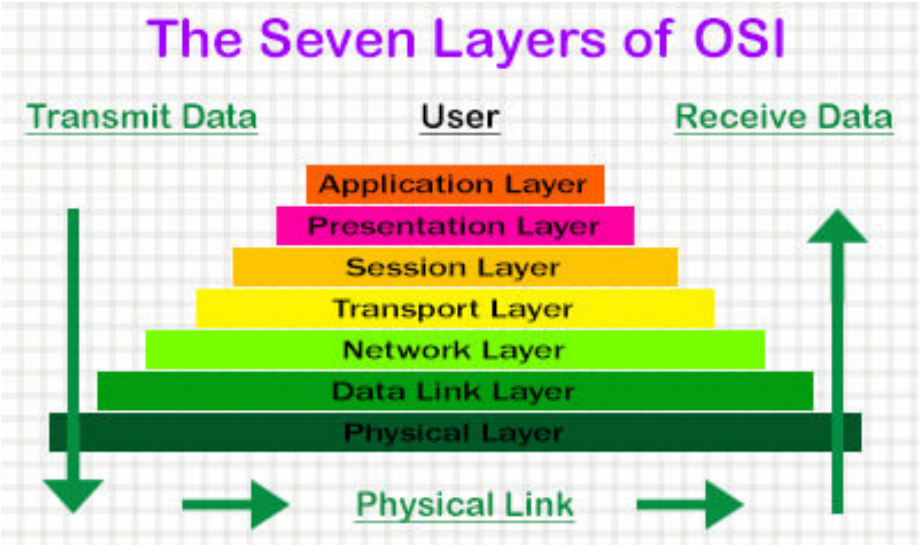

Figure 2: OSI model

The original version of the model defined seven layers."[wikipedia]

Subnetting
Examples of **Public IP** and **Private IP**
Design of an application

- Front-end: WAF
- Back-end
- Data

Possible attacks

- Sniffer
- SQL Injection
- PostScripting

4 Class 6 - Law, regulation and incidents

<missing session>

Acronyms

- **LAN** -> Local Area Network
- **MAN** -> Metropolitan Area Network
- **WAN** -> Wide Area Network
- **WWW** -> World Wide Web
- **DMZ** -> Demilitarized Zone
- **OSI** -> Open Systems Interconnection
- **IP** -> Internet Protocol
- **DNS** -> Domain Name System
- **NAT** -> Network Address Translation
- **WAF** -> Web Application Firewall
- **OWASP** -> Open Web Application Security Project
- **SIEM** -> Security Information and Event Management
- **SQL** -> Structured Query Language
- **VPN** -> Virtual Private Network

References

OSI model, https://en.wikipedia.org/wiki/OSI_model [cited November 2017].