Cybersecurity

Linde Nouwen

KdG Karel de Grote Hogeschool

CyberSecurity Intro

Karel de Grote Hogeschool

CyberSecurity Intro

General Introduction

Karel de Grote Hogeschool

Intro

- “The best defense is a good offense.”
- Learn to think & act like a hacker.

Intro

If you want to test your abilities on life machines:

- Rule1: get permission
- Rule2: get permission
- Rule3: …

Intro

If you want to test your abilities on live machines:

- Rule1: get permission
- Rule2: get permission
- Rule3: make sure you have permission (and keep things confidential and secret)

Intro

"With great power comes great responsibility"

Intro

"With great powers come great responsibilities"

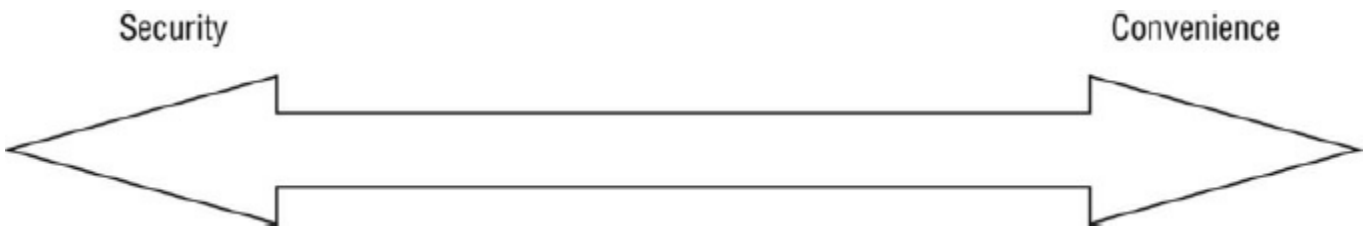
CyberSecurity Intro

Dilemmas

Karel de Grote Hogeschool

Intro

- The Security/Convenience dilemma



Intro

- System-Goals from Network Security point of view:

- CIA-Triangle
  - Confidentiality
  - Integrity
  - Availability

Intro

- System-Goals from Network Security point of view:

- Hacker tries to break the triangle
- System engineer tries to keep the triangle intact

Intro

- System-Goals from Network Security point of view:

When the triad fails the CIA triad becomes the DAD triad.

Intro

- More "complete" model: (Parkerian Hexad)

CyberSecurity Intro

Technical Knowledge and Insight

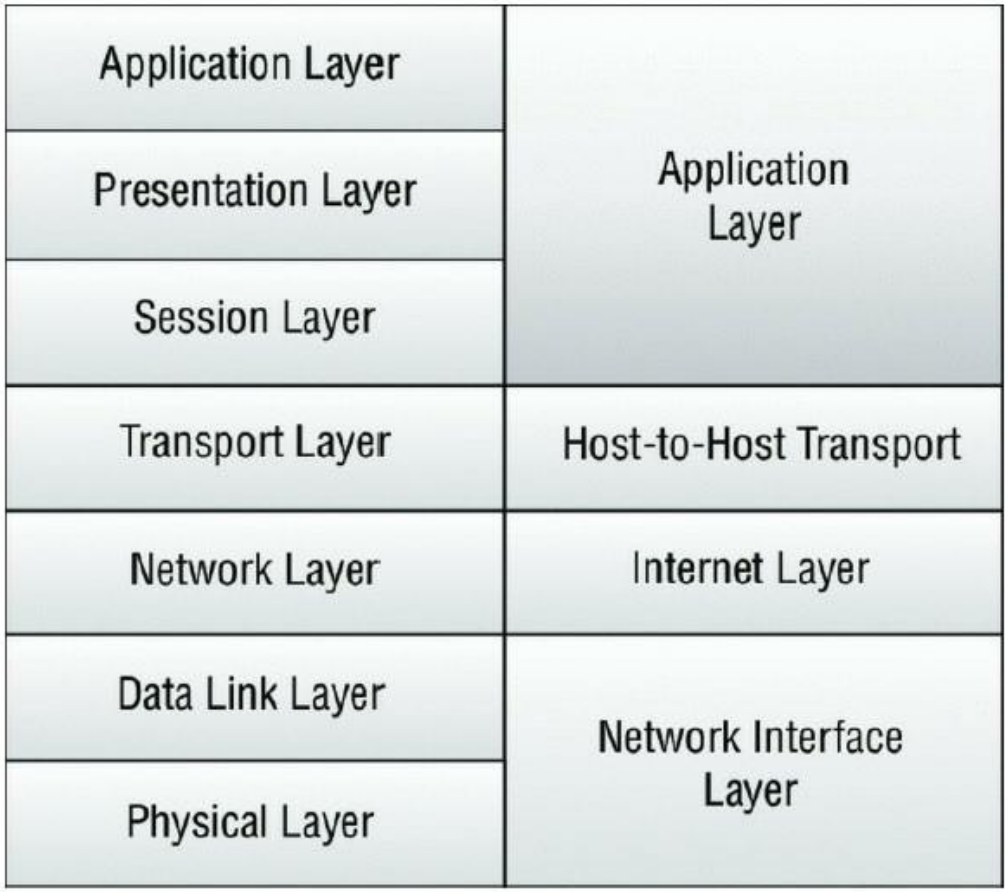
KdG Karel de Grote Hogeschool

Intro

- Technological knowledge
  - OSI model
  - TCP/IP:
    - Addressing
    - Subnetting
    - Sockets
    - Protocols (DNS, ARP, HTTP, SMTP, DHCP, …)
  - OS
    - Concepts
    - Mgmt (Linux/Windows)

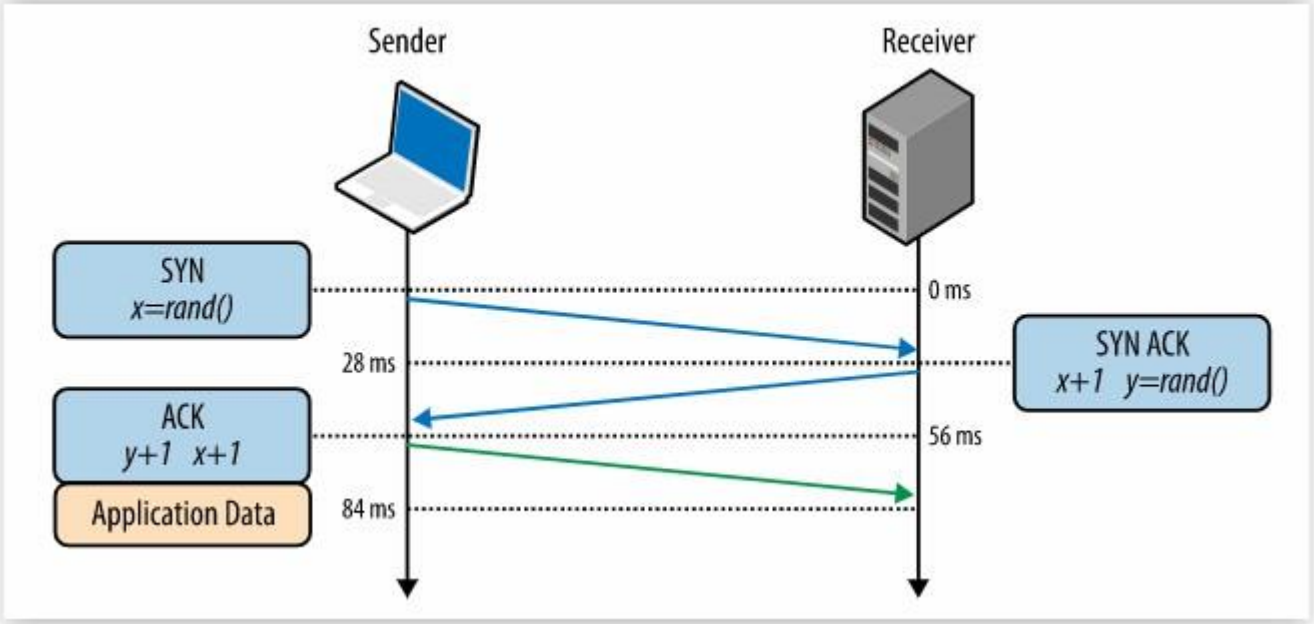
Intro

- Technical Knowledge
  - OSI-Model:



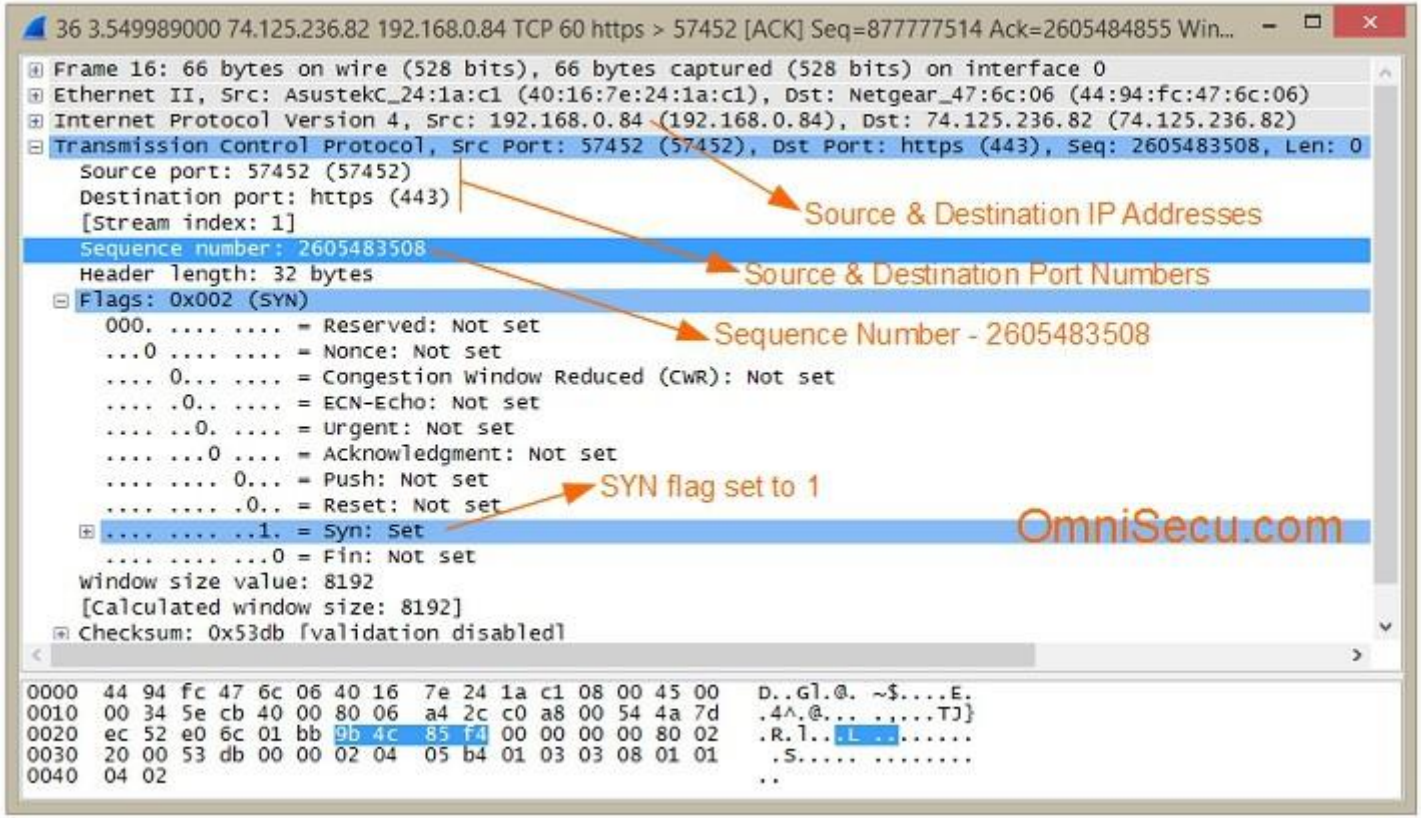
Intro

- Technical Knowledge
  - TCP Sequencing & 3-way handshake



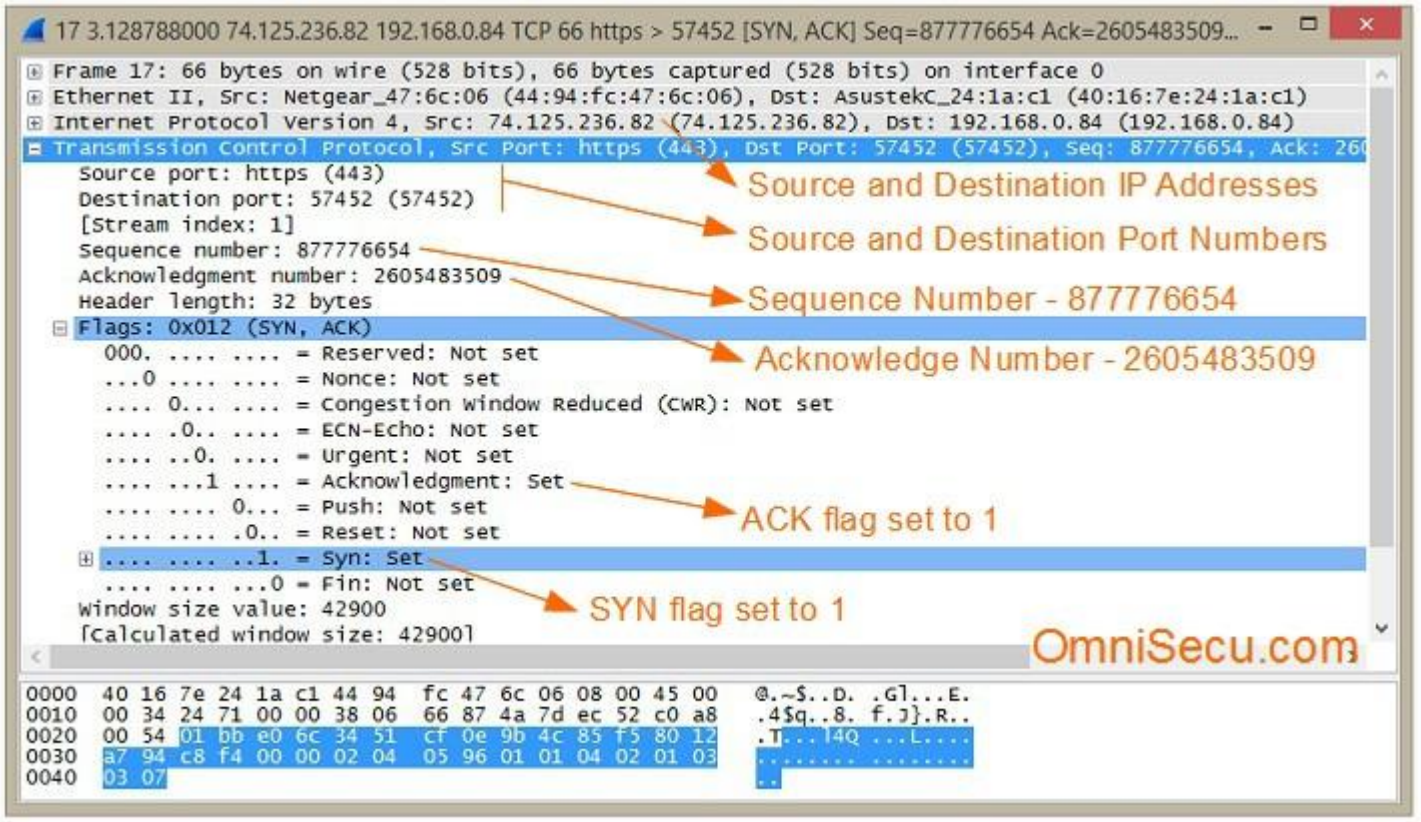
Intro

- Technical Knowledge
  - TCP Sequencing & 3-way handshake
  - SYN



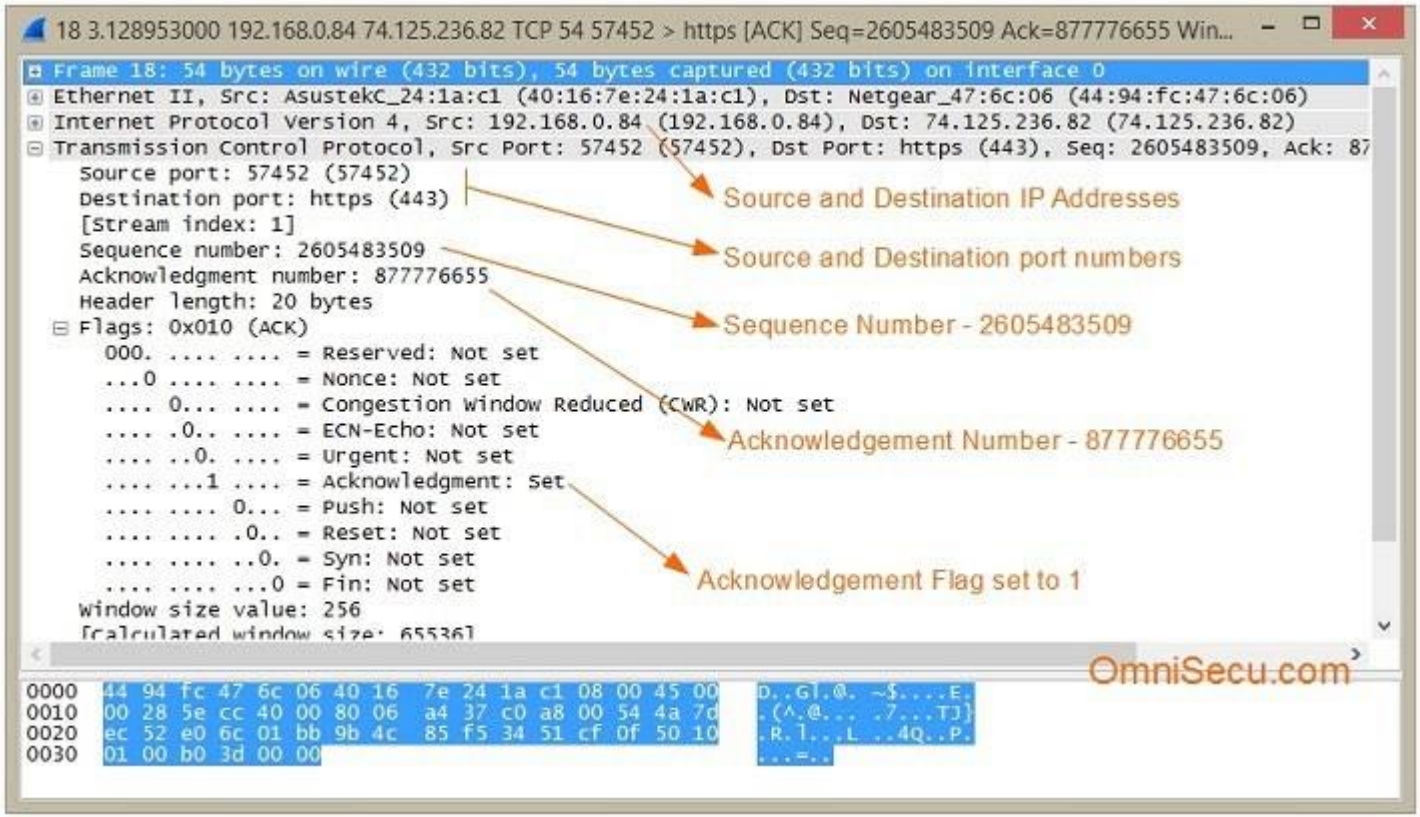
Intro

- Technical Knowledge
  - TCP Sequencing & 3-way handshake
  - SYN + ACK



Intro

- Technical Knowledge
  - TCP Sequencing & 3-way handshake
  - ACK

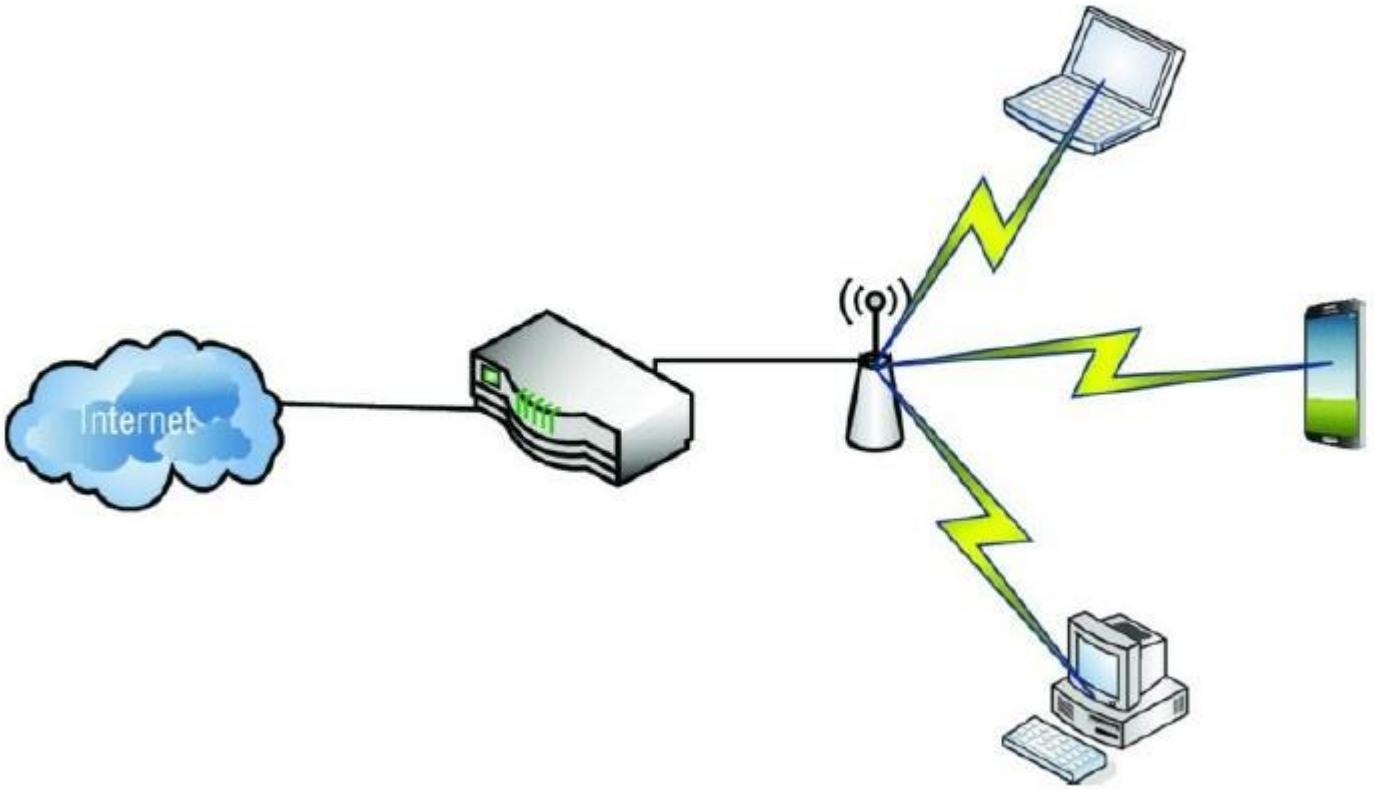


Intro

- Technical Knowledge
  - Subnetting
  - IP & Port = Socket
  - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
  - Switch vs Router

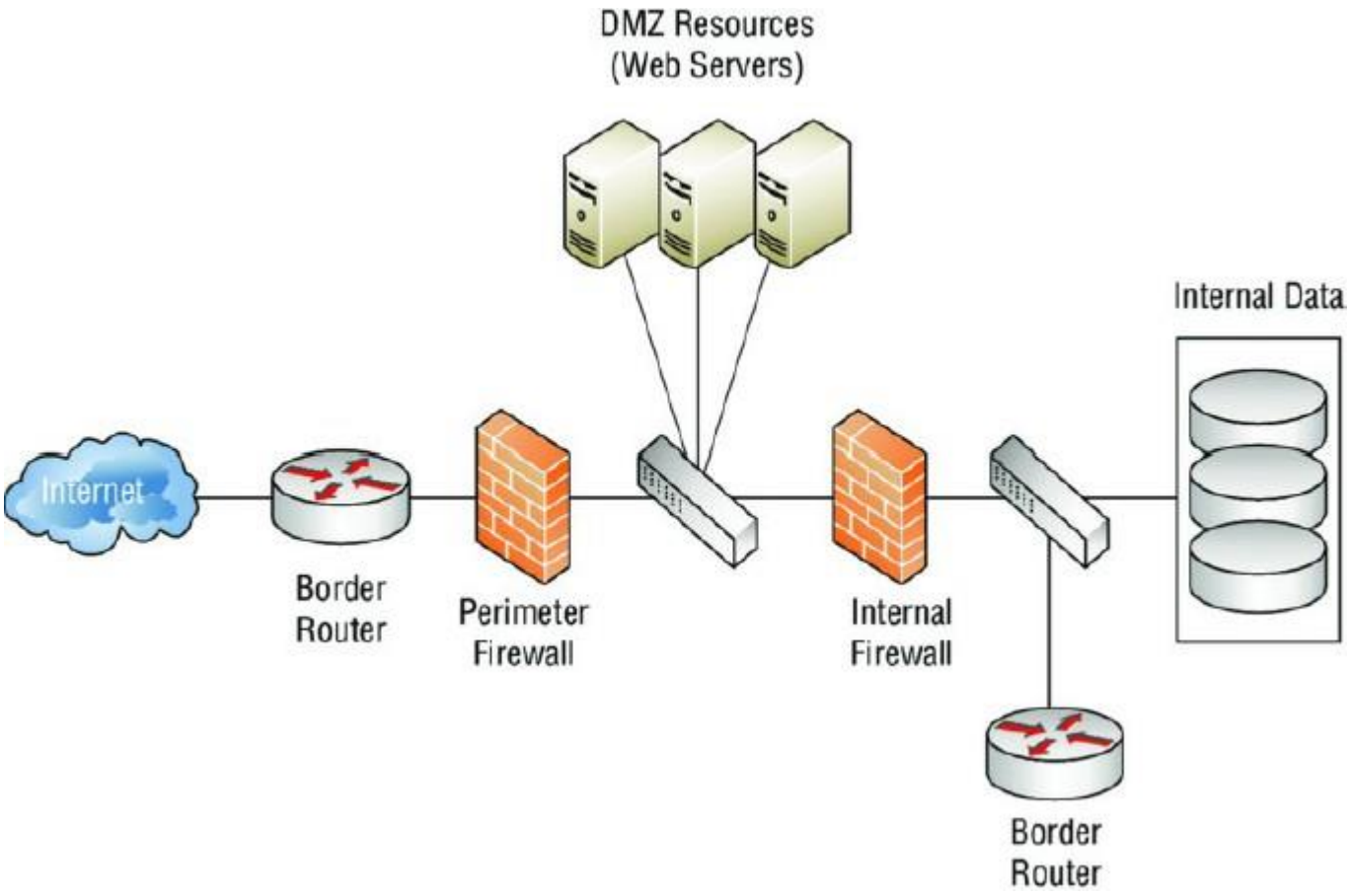
Intro

- Technical Knowledge
  - Diagrams: home network



Intro

- Technical Knowledge
  - Diagrams: company network



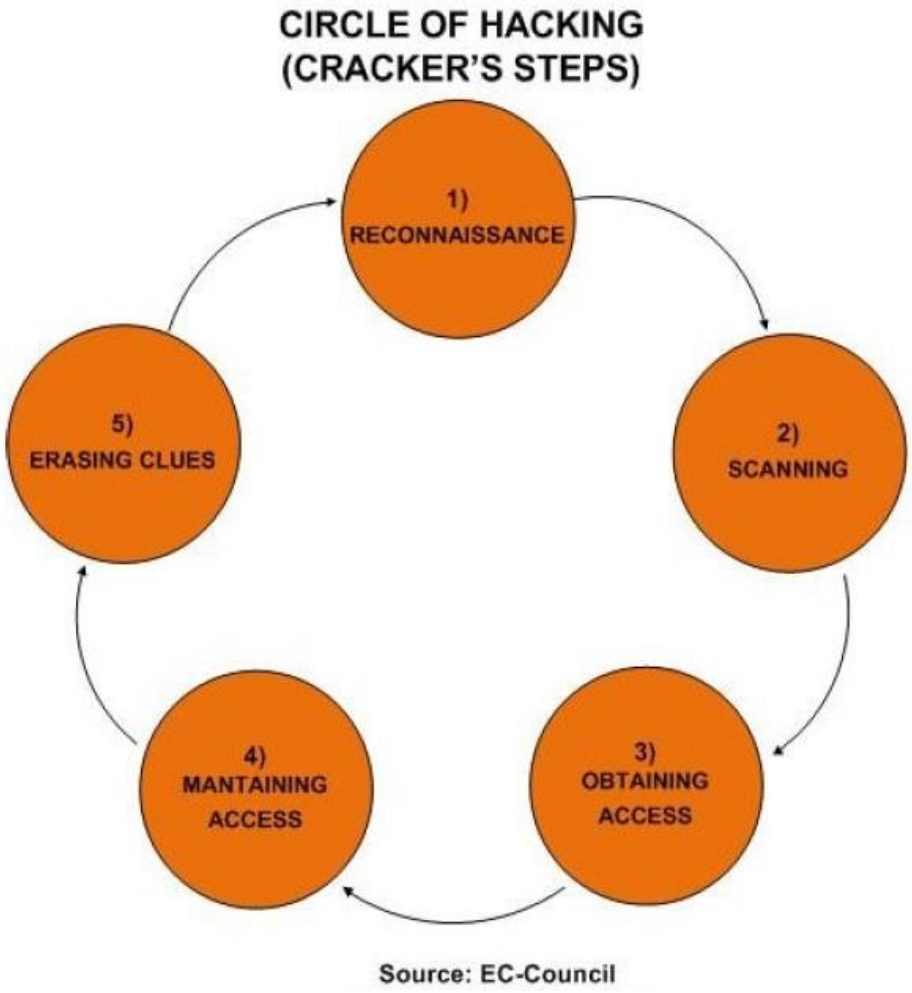
CyberSecurity Intro

Methodology

Karel de Grote Hogeschool

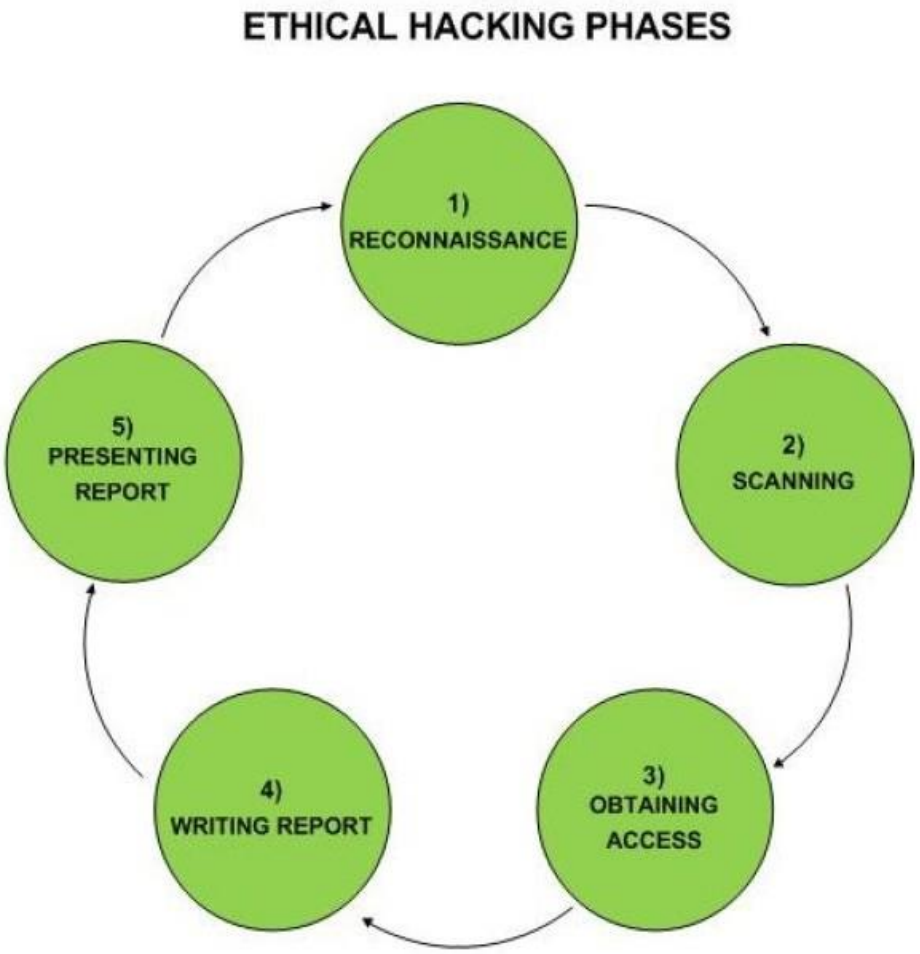
Intro

- Cracker/Hacker



Intro

- Security Advisor or Ethical Hacker



CyberSecurity Intro

Terminology

Karel de Grote Hogeschool

Intro

- Terminology
  - To discuss with clients, peers, authorities, etc…
  - Mode in which to operate
  - Services to be provided

Intro

- Terminology
  - Hacking Types:
    - Red teaming
    - Purple teaming
    - External Pentesting
    - Internal Pentesting
    - Physical Pentesting
    - …

Intro

- Terminology
  - Hacking Modes:

- Black Box
  - External
  - Organisation name & let's go…
- White Box
  - Internal (connection and/or access)
  - Lots of internal information: schematics, addresses, … (from client)
- Grey Box
  - In between
  - Client provides some information
  - Some form of access: e.g. employee-like access
- + Script Kiddies & Suicide Hackers & Hacktivists & …

Intro

- Terminology
  - Hacking Services:
    - Social Engineering
    - Wardialing
    - Wardriving
    - Stolen equipment simulation
    - Physical security

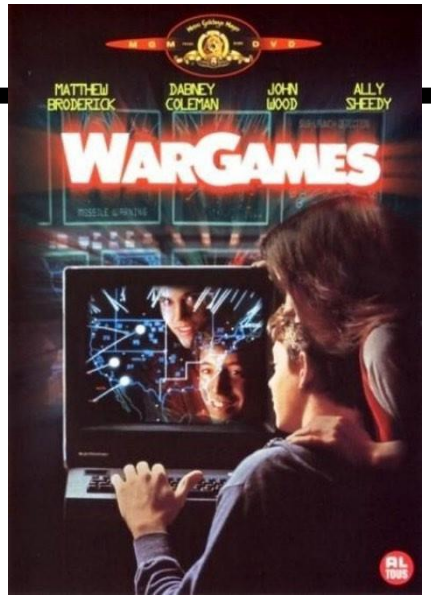
Intro

- Social Engineering
  - Six key principles of human influence
    1. Reciprocity
    2. Commitment and consistency
    3. Social proof
    4. Authority
    5. Liking
    6. Scarcity

Intro

- Social Engineering
  - Four methods:
    1. Phishing
    2. Vishing
    3. Smishing
    4. Impersonation

Intro



- Wardialing
  - For reference only?
  - Old = from modem-times
  - But sometimes “modems” still used as backup strategy

Intro

- Wardriving
  - Off-premise wireless network scans or attacks
  - E.g. car + laptop + signal booster
  - More information: https://www.wigle.net/

Intro

- Stolen equipment simulation
  - Confidential information on mobile devices
  - Check safety/encryption
  - Backup OK?

Intro

- Physical security
  - From simple inspection
  - To infiltration & placement of spy-devices

CyberSecurity Intro

Beyond the technical…

Karel de Grote Hogeschool

Intro

- First step…
  - Proposal creation:
    - Scope & Deliverables
    - Time
    - Cost
- Last step…
  - Reporting
    - Documentation
    - Presentation