

Cybersecurity

Linde Nouwen

KdG Karel de Grote
Hogeschool

Alle teksten, afbeeldingen, tabellen en andere items in deze cursus vallen onder de bescherming van het auteursrecht. Het is daarom verboden (een gedeelte van) deze cursus te kopiëren, over te nemen of verder te verspreiden zonder voorafgaandelijk schriftelijke toestemming van de auteur. Dit geldt ook voor vertalingen, wijzigingen of bewerkingen ervan en ongeacht de manier waarop (elektronisch, papier, ...). Elke inbreuk hierop kan aanleiding geven tot een tuchtsanctie en vervolging voor een rechtbank.

CyberSecurity Intro

CyberSecurity Intro

General Introduction

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”

***“With Great Power
Comes Great
Responsibility”***

Spider-Man

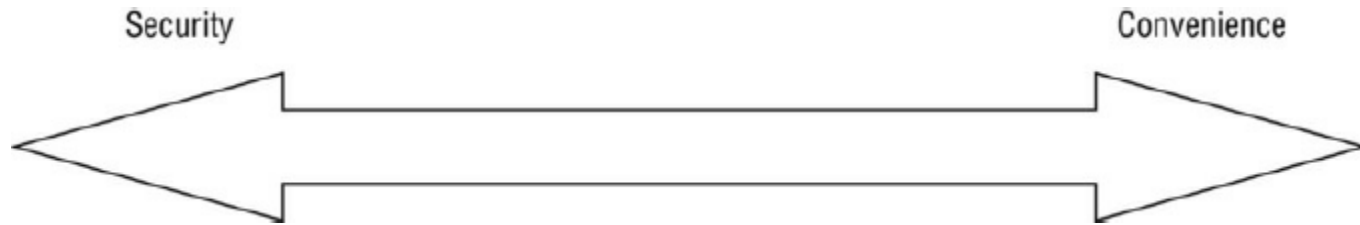
Saturday - Nov 10, 2012(2:00 am)

CyberSecurity Intro

Dilemmas

Intro

- The Security/Convenience dilemma



Intro

- System-Goals from Network Security point of view:



- CIA-Triangle
 - ❖ Confidentiality
 - ❖ Integrity
 - ❖ Availability

Intro

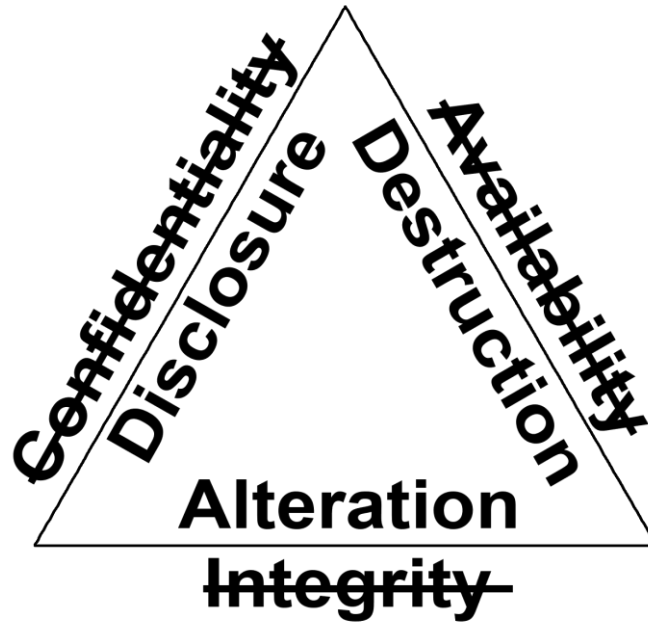
- System-Goals from Network Security point of view:



- 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

Intro

➤ Technological knowledge

❖ OSI model

❖ TCP/IP:

- Addressing
- Subnetting
- Sockets
- Protocols (DNS, ARP, HTTP, SMTP, DHCP, ...)

❖ OS

- Concepts
- Mgmt (Linux/Windows)

Intro

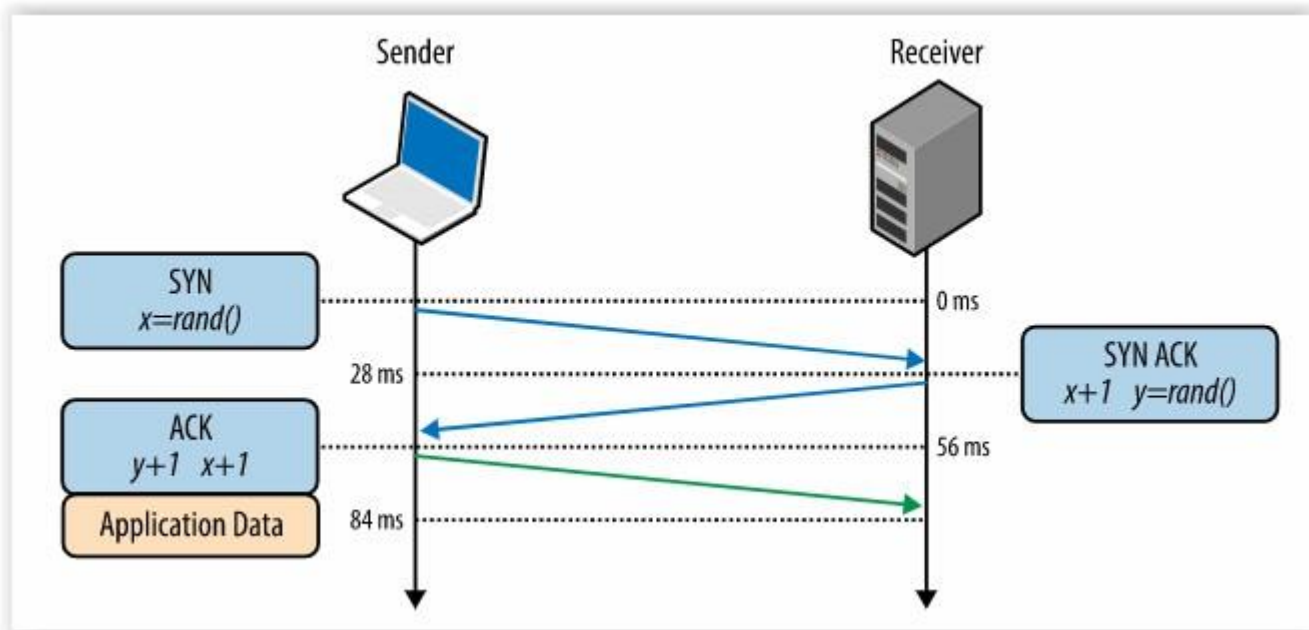
➤ Technical Knowledge

❖ OSI-Model:

| | |
|--------------------|-------------------------|
| Application Layer | Application Layer |
| Presentation Layer | |
| Session Layer | |
| Transport Layer | Host-to-Host Transport |
| Network Layer | Internet Layer |
| Data Link Layer | Network Interface Layer |
| Physical Layer | |

Intro

- Technical Knowledge
 - TCP Sequencing & 3-way handshake



Intro

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

36 3.549989000 74.125.236.82 192.168.0.84 TCP 60 https > 57452 [ACK] Seq=877777514 Ack=2605484855 Win...

Frame 16: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: AsustekC_24:1a:c1 (40:16:7e:24:1a:c1), Dst: Netgear_47:6c:06 (44:94:fc:47:6c:06)

Internet Protocol Version 4, Src: 192.168.0.84 (192.168.0.84), Dst: 74.125.236.82 (74.125.236.82)

Transmission Control Protocol, Src Port: 57452 (57452), Dst Port: https (443), Seq: 2605483508, Len: 0

Source port: 57452 (57452)

Destination port: https (443)

[Stream index: 1]

Sequence number: 2605483508

Header length: 32 bytes

Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (cWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...0 = Acknowledgment: Not set

....0 = Push: Not set

....0 = Reset: Not set

....1. = Syn: Set

....0 = Fin: Not set

Window size value: 8192

[Calculated window size: 8192]

Checksum: 0x53db [validation disabled]

OmniSecu.com

0000 44 94 fc 47 6c 06 40 16 7e 24 1a c1 08 00 45 00 D..G|.@. ~\$....E.

0010 00 34 5e cb 40 00 80 06 a4 2c c0 a8 00 54 4a 7d .4^.@... ..TJ}

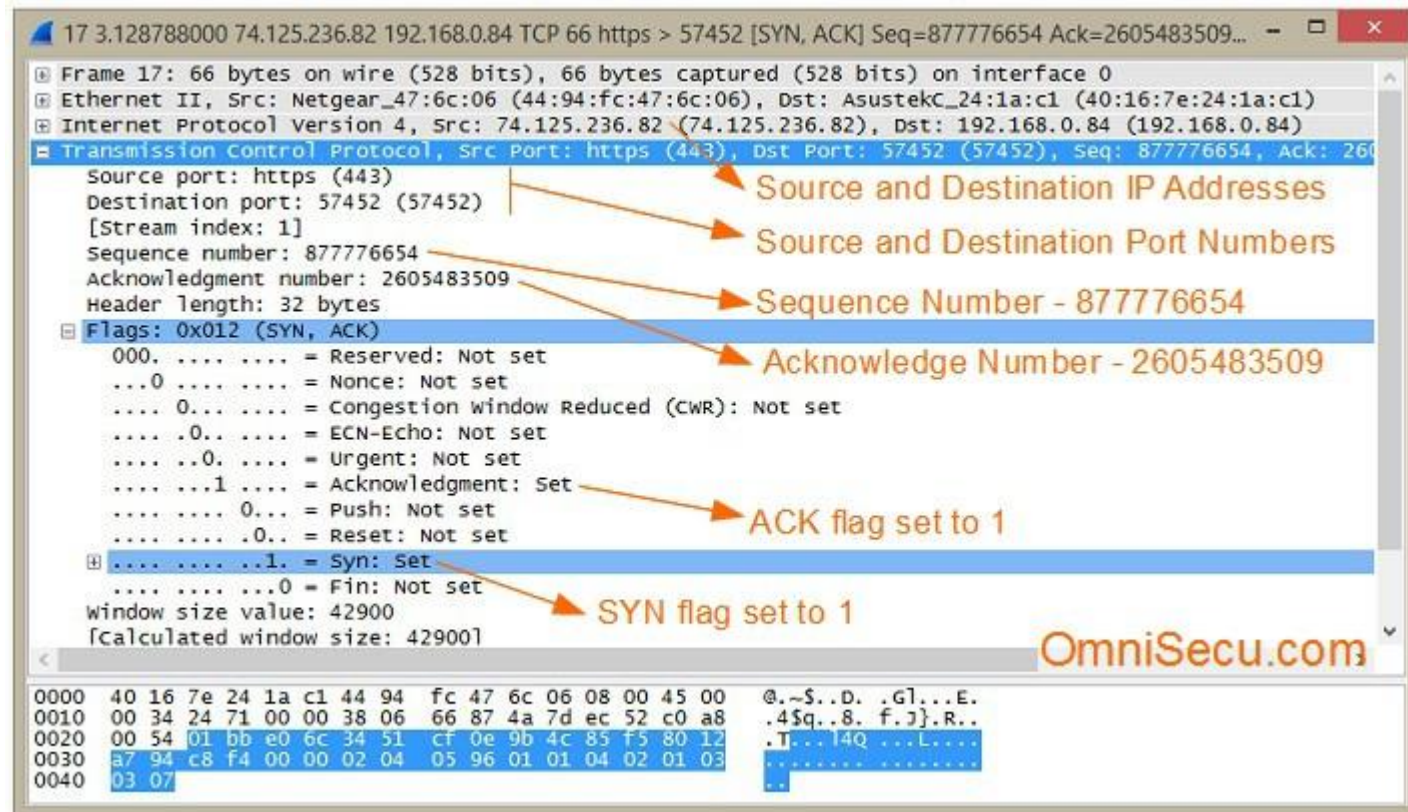
0020 ec 52 e0 6c 01 bb 9b 4c 85 f4 00 00 00 00 80 02 .R.l..[L.. ..

0030 20 00 53 db 00 00 02 04 05 b4 01 03 03 08 01 01 .S.....

0040 04 02 ..

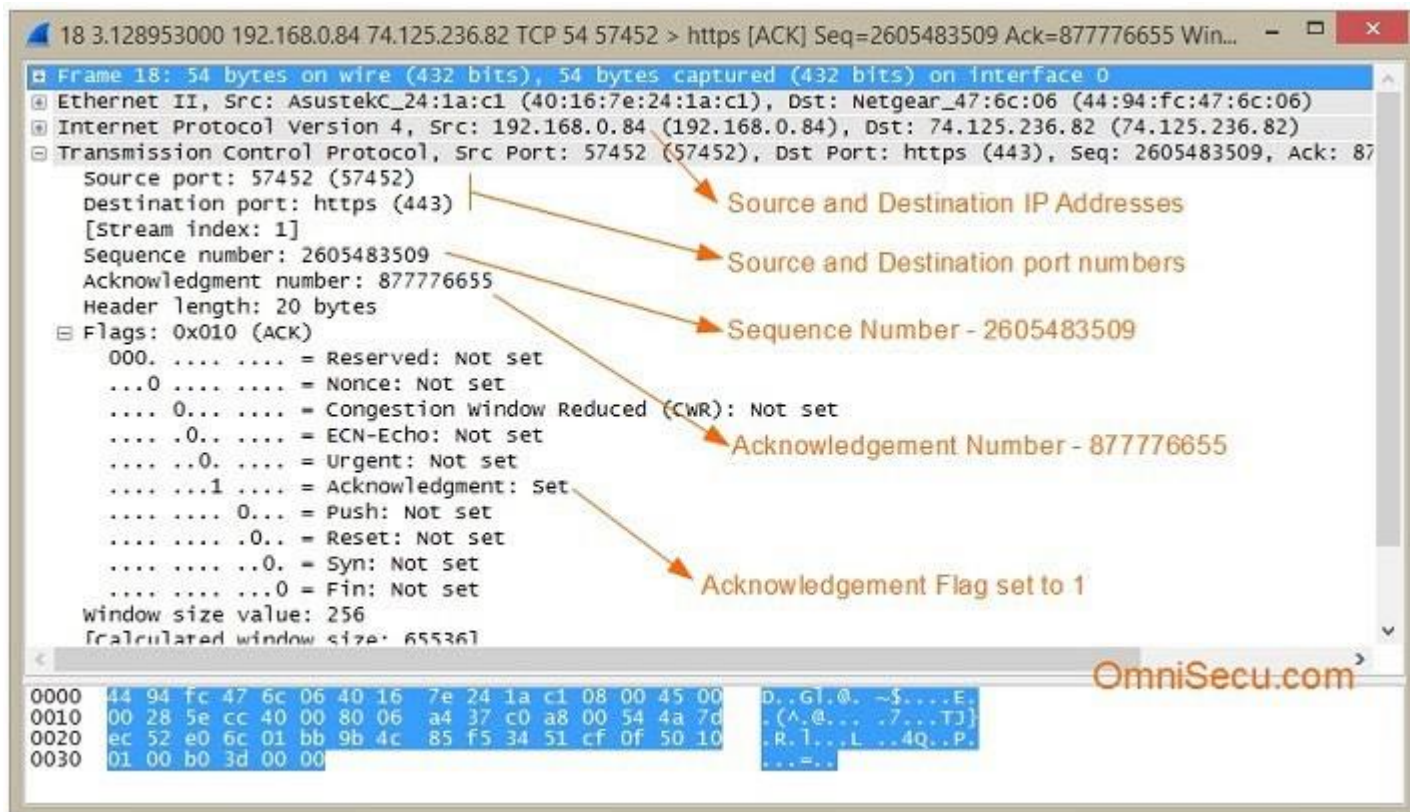
Intro

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



Intro

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



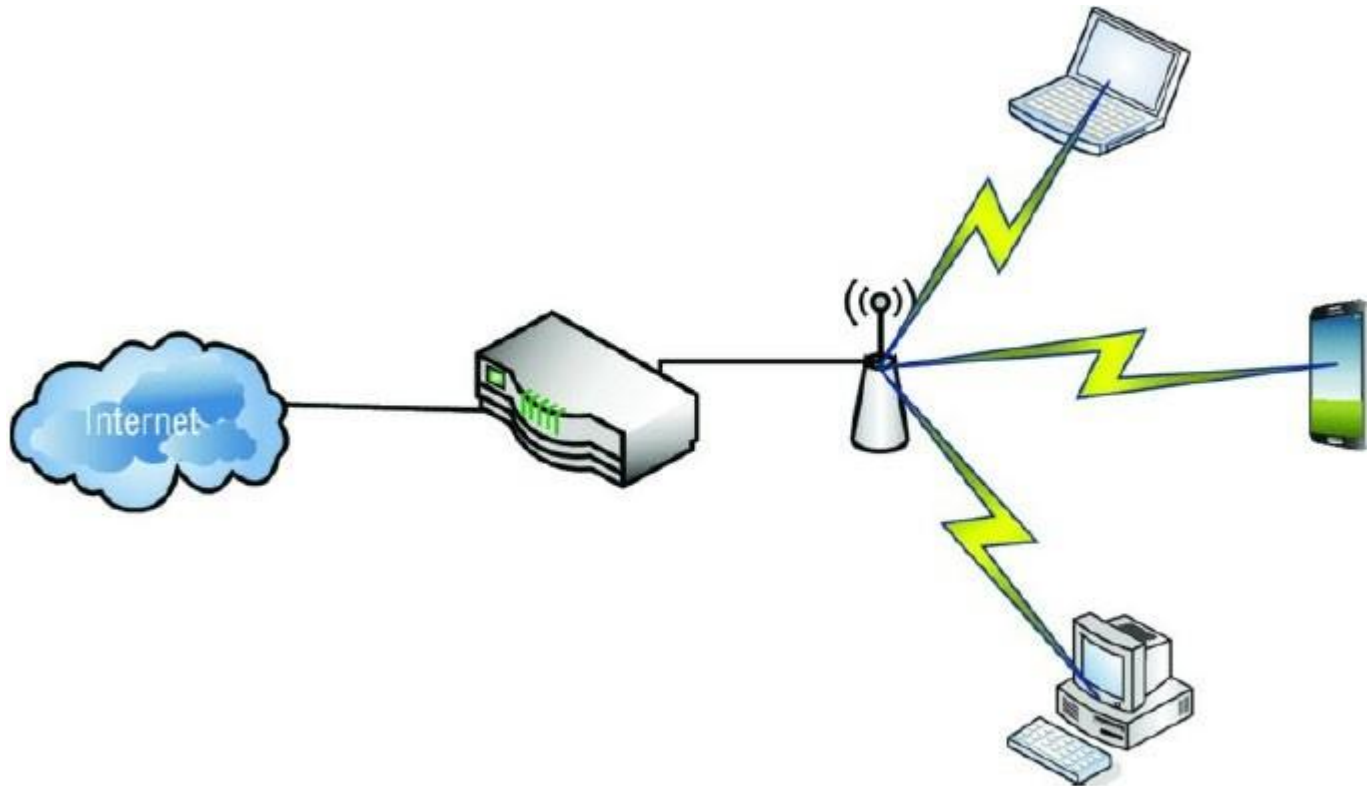
Intro

➤ Technical Knowledge

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

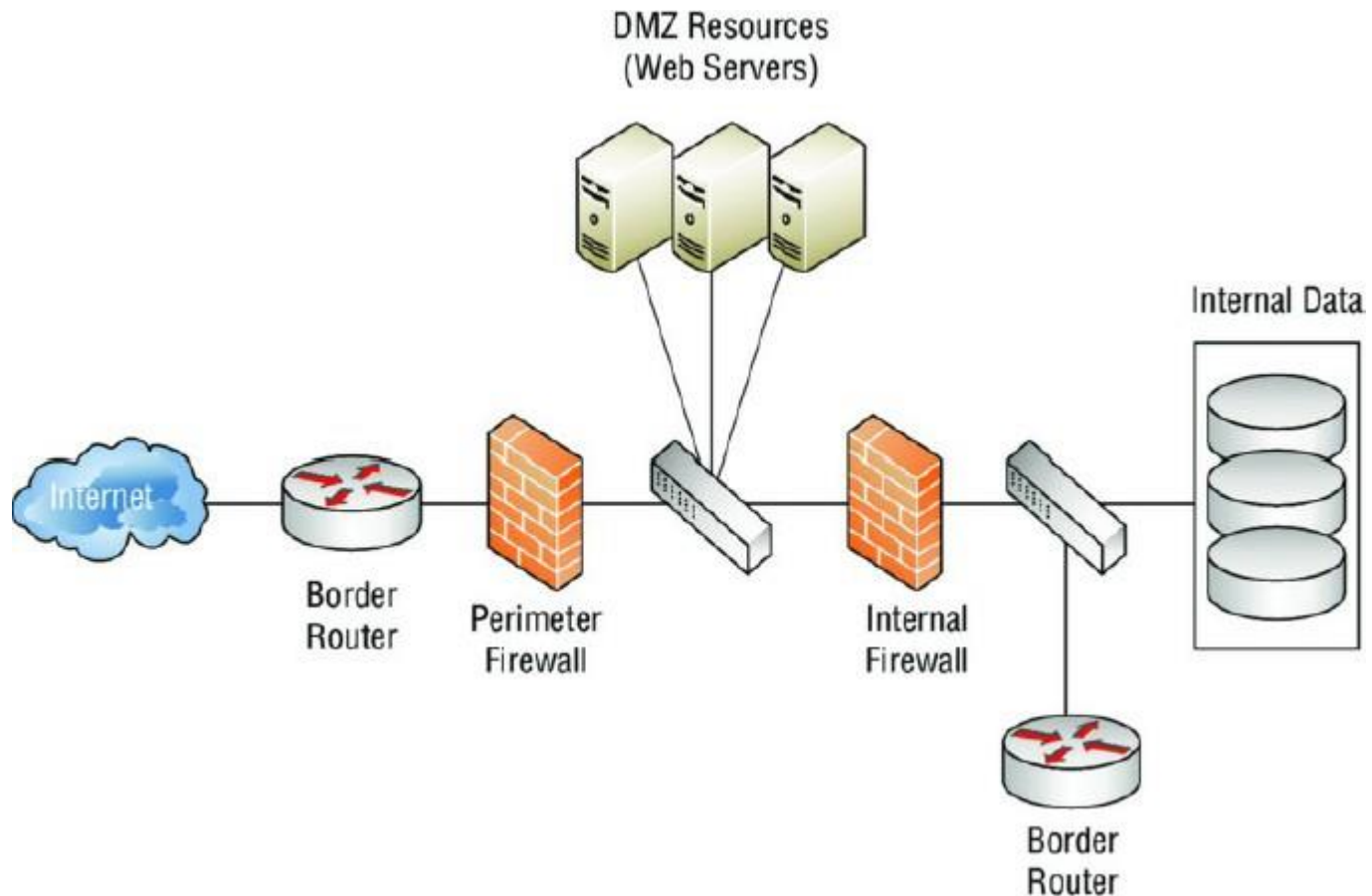
Intro

- Technical Knowledge
 - ❖ Diagrams: home network



Intro

- Technical Knowledge
 - ❖ Diagrams: company network

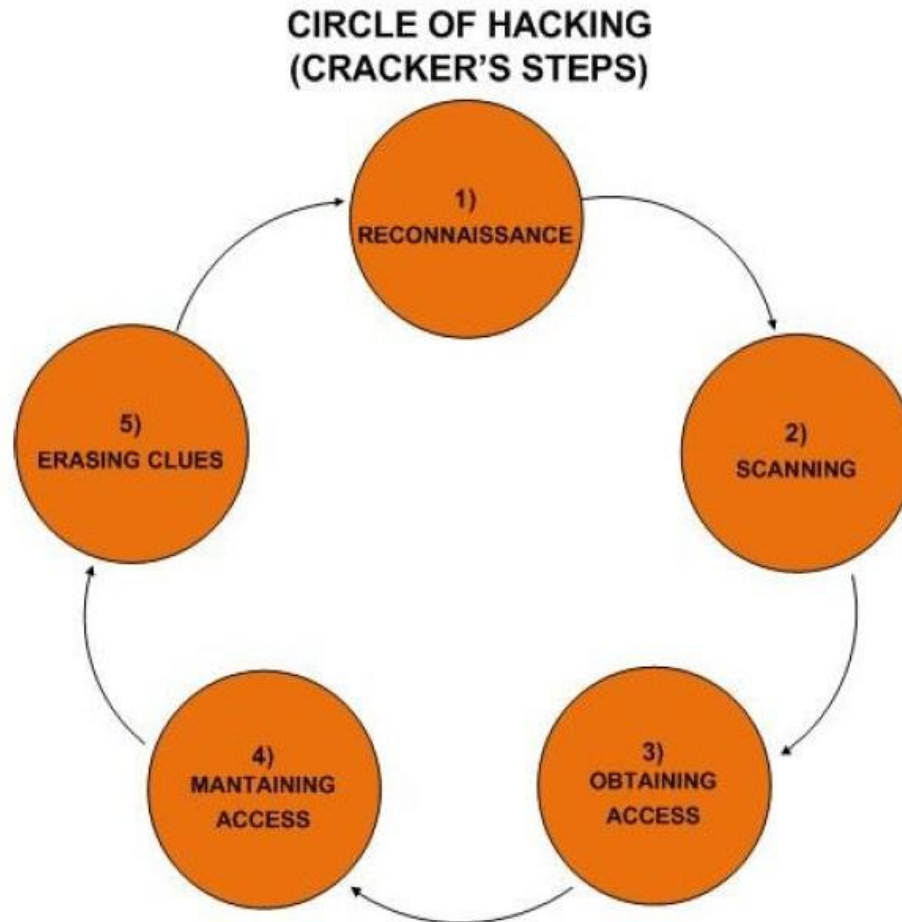


CyberSecurity Intro

Methodology

Intro

➤ Cracker/Hacker



Source: EC-Council

Intro

➤ Security Advisor or Ethical Hacker



CyberSecurity Intro

Terminology

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

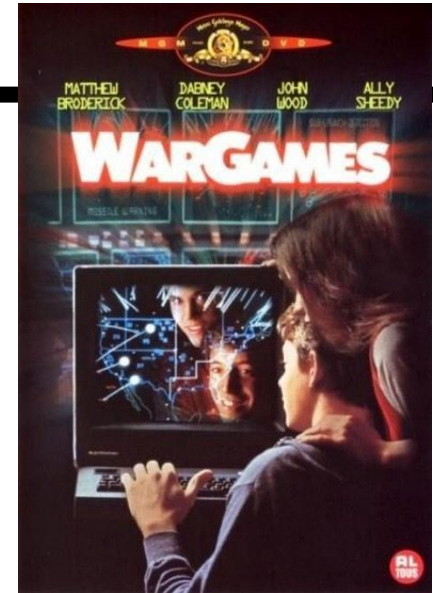
➤ Social Engineering

❖ 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...

Intro

➤ First step...

❖ Proposal creation:

- Scope & Deliverables
- Time
- Cost

➤ Last step...

❖ Reporting

- Documentation
- Presentation