# Forelæsningsnoter

Mikkel Boye Rasmussen

09.02.2023

# Introduktion

**Agenda:**

- Introduktion
- Introduktion af faget
- Øvelser
- Installation af Linux

**Alex:**

KEA, ITU

Reverse engineering malware (GIAC)
Python coder (GIAC)

**Dany:**

DTU, IHK og ITU

Certified pentester and ethical hacker (GWAPT)
Reverse engineering malware (GIAC)
Python coder (GIAC)

**Expectations**

5min brainstorm topics you want in this course

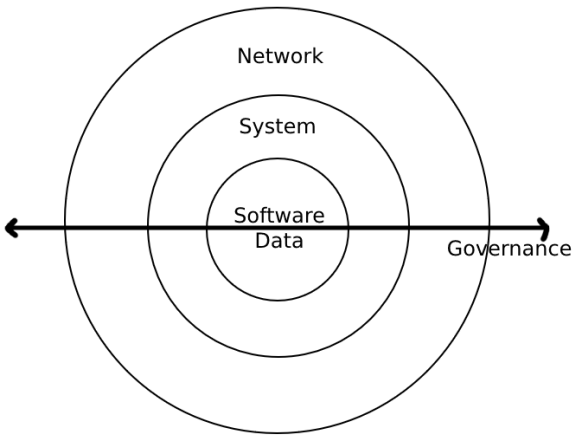
Use 5min agreeing on topics

1. Overvågning på netværk (nmap / netcat)
2. Network attacks og mitigations
3. Access management / privilege escalation
4. Fysisk sikkerhed
5. Authentication cookies og tokens - sikker opbevaring

**Udelukkende i Netværk og kommunikationssikkerhed**

- Kali linux til routing med henblik på hacking
- Hacking generelt
- Netflow (gammel cisco teknologi)
- VLAN (virtual local area network) Certifikater
- Firewall
- Netværksovervågning
- Angreb og forsvar af netværk
- Network layers - MEGET
- App layer
- IT tools

**Thoughs about the course**



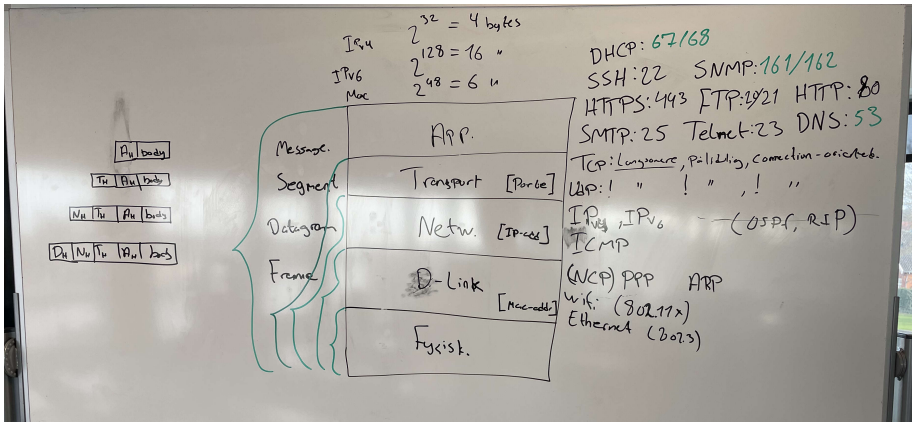

**Deliverables**
2 mandatory assignments
Mandatory 1 (2 exercises [scapy, sof-elk]) - ca 4 timer
Mandatory 2 (2 exercises [ids, net-mon]) - ca 4 timer
1 eksamensprojekt - startes om 2 uger, i grupper

**Exam**
30min incl votering
mundtlig baseret på eksamensprojekt og pensum
Graded
Mere om eksamenen senere

**Books**
ikke obligatoriske
Network security assessment
Applied Network Security Monitoring
yderligere optional books
Computer networking - kurose - ross
Computer networking a top down approach
computer networking - a top down approach
computer security principles and practice

TCP - IP model (5-lags modellen) i stedet for OSI (7-lags modellen)

- **App** - Header: $\boxed{A_H|\text{body}}$ (pakker her hedder message): Protokoller (port) - HTTPS (443), HTTP (80), FTP (20/21), SMTP (25), Telnet (23), DNS (53), SSH (22), SNMP (161/162), DHCP (67/68).
- **Transport** - Header : $\boxed{T_H|A_H|\text{body}}$ (pakker her hedder segmenter): Protokoller (egenskaber) - TCP (langsom, pålidelig, connection-oriented, altid client server - ikke flere personer)), UDP (hurtig, upålidelig, ingen connection)
- **Network** - Header: $\boxed{N_H|T_H|A_H|\text{body}}$ (pakker her hedder datagrammer): Protokoller - IPv4, IPv6, ICMP, OSPF, RIP
- **Data-link** - Header: $\boxed{D_H|N_H|T_H|A_H|\text{body}}$ (pakker her hedder frames): Protokoller - NCP, WiFi, Ethernet, PPP, Bluetooth, ARP
- **Fysisk**



IPv4 (network layer)- $2^{32}$ adresser - 4 bytes
IPv6 (network layer) - $2^{128}$ adresser - 16 bytes
MAC (datalink layer) - $2^{48}$ adresser - 6 bytes
*Kun SNMP, DHCP og DNS benytter UDP, resten benytter TCP*
*ICMP benyttes til at pinge*
VIGTIGT AT KUNNE PORTNAVNE!

**Forventet detaljeniveau**
TCP segment structure - se billede i slide
Wireshark
**Lidt om moodle rummet**