De Danske Cybermesterskaber
Netværksscanning og overvågning

Jens Myrup Pedersen, Professor, AAU
Silas, Daniel, Zohra- studerende, AAU

INDUSTRIENS FOND

AALBORG UNIVERSITY
DENMARK

Hvem er vi?

Jens
Professor
Cybersikkerhed
Aalborg Universitet (Kbh)

Daniel
Studerende
Cybersikkerhed
Aalborg Universitet (Kbh)

Zohra
Studerende
Computerteknologi
Aalborg Universitet

Silas
Studerende
Computer Tekn.
Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

Dagens plan (vejledende)

- Noget om computernetværk og overvågning (17.00-17.45)
- Pause (17.45-17.55)
- Et par opgaver om overvågning (17.55-18.30)
- Scanning (18.30-18.50)
- Pause (18.50-19.00)
- Flere opgaver (19.00-19.45)
- Spørgsmål og fri leg (19.45-20.00)

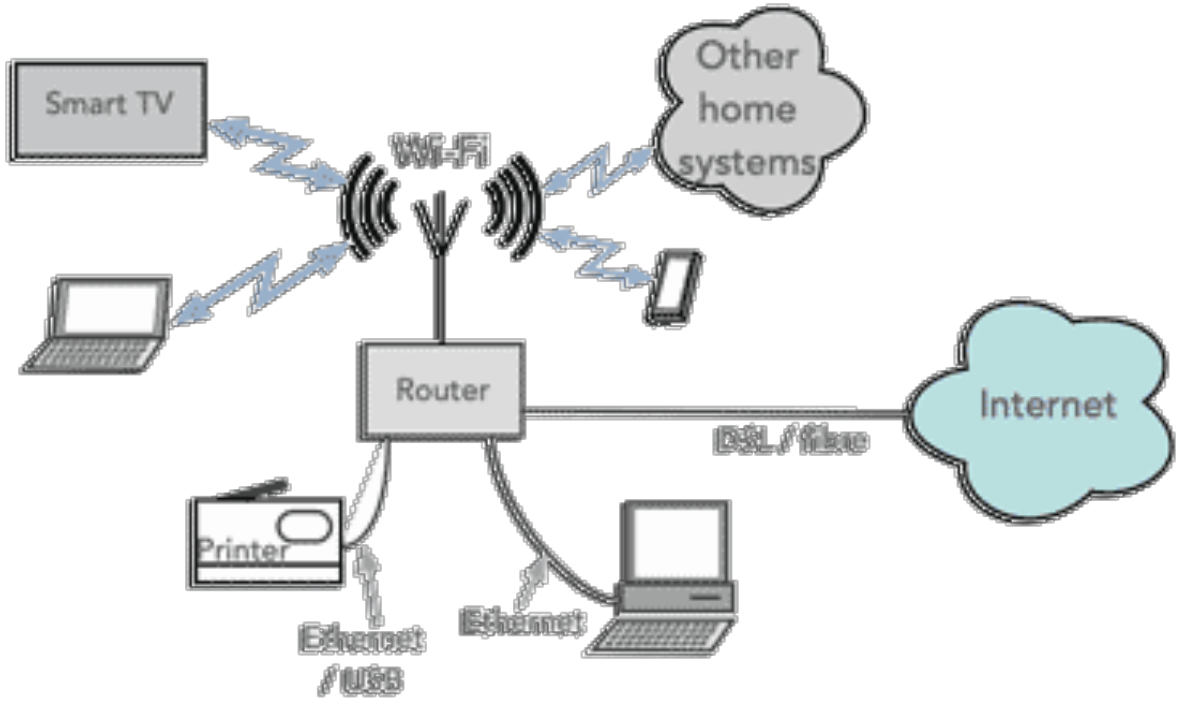
OBS1: Robert, Gustav og Michael er klar til at hjælpe i breakout-rooms og chat.

OBS2: Det er en fordel med nyeste version af Zoom (men ellers sig til…)

OBS3: Man må gerne arbejde hurtigere end jeg gør (evt. ”avanceret rum”)

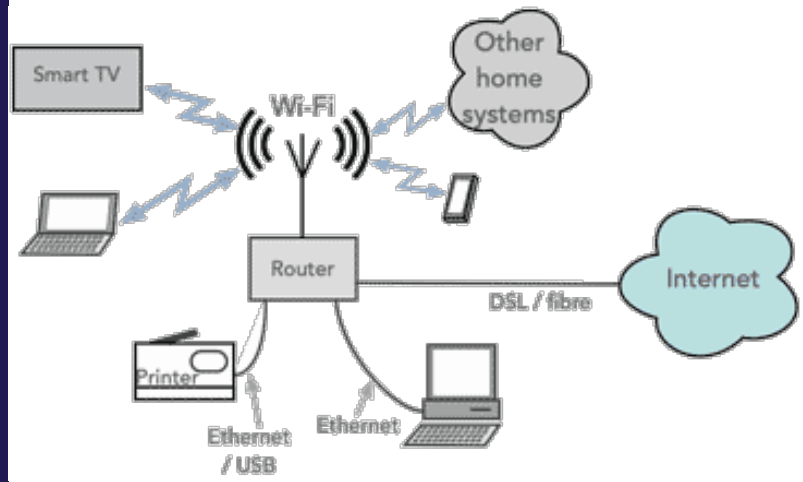
OBS4: Vi prøver at holde linket kørende til og med weekenden: dm.ntp-event.dk

Et kig på hjemme-netværket ☺



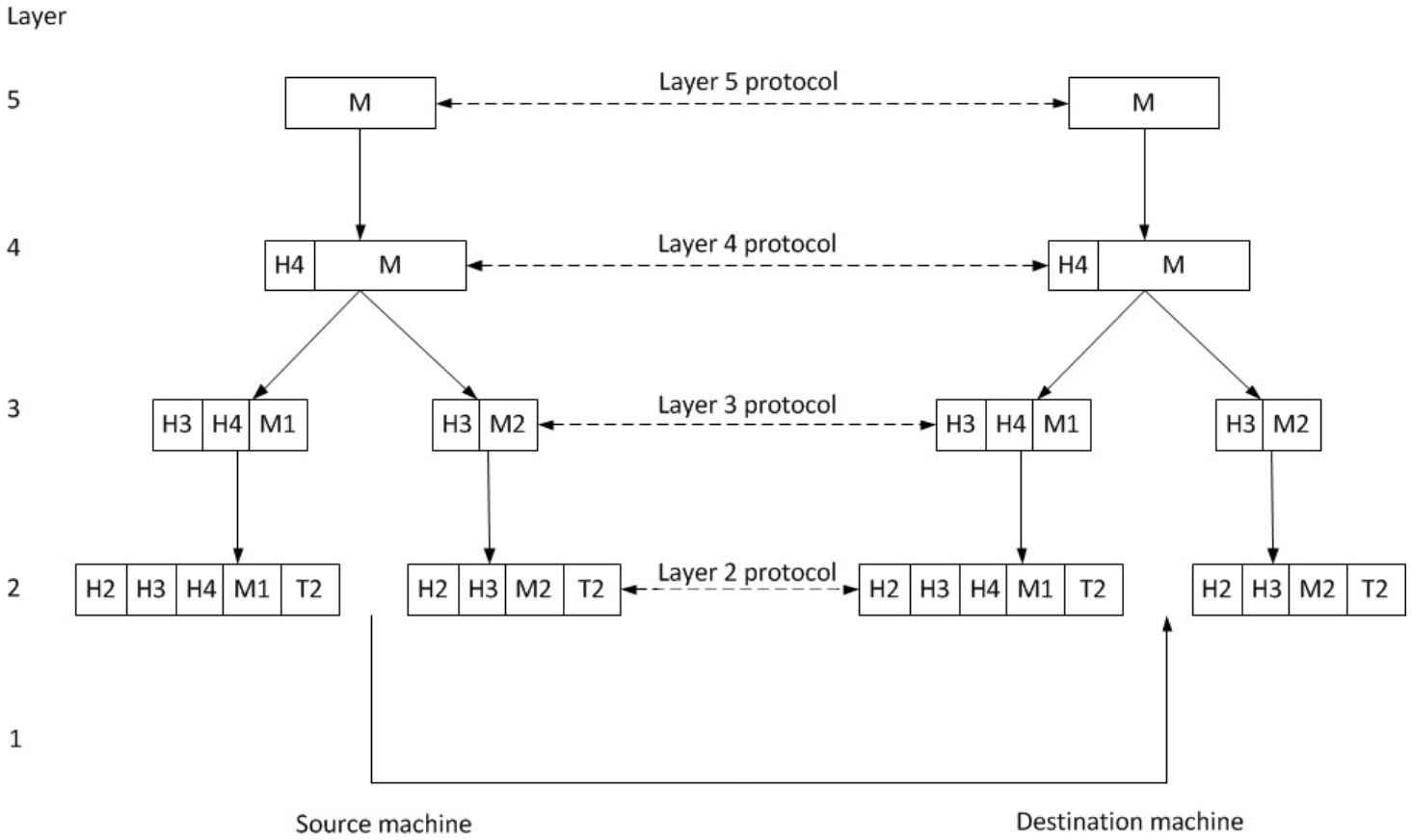
Det typiske trådløse hjemmenetværk

- I det typiske netværk er der en (eller flere) **gateways**, som skaber forbindelsen fra enheden til Internettet.
- Som udgangspunkt kan alle enheder (**klienter**) på det samme trådløse netværk kommunikere med hinanden, men gennem routeren – som både er gateway og **access point (AP)**.
- Hvert trådløst netværk har et **navn (SSID)**, som man kan se når man prøver at forbinde sig til det. Dette er som udgangspunkt ikke beskyttet.
- Vigtigt at skelne mellem **Internettet** og så det lokale **WiFi-netværk.**
- Internt netværk = **interne IP-adresser**. Internet = **globale IP-addresser**.
- 192.168.1.2

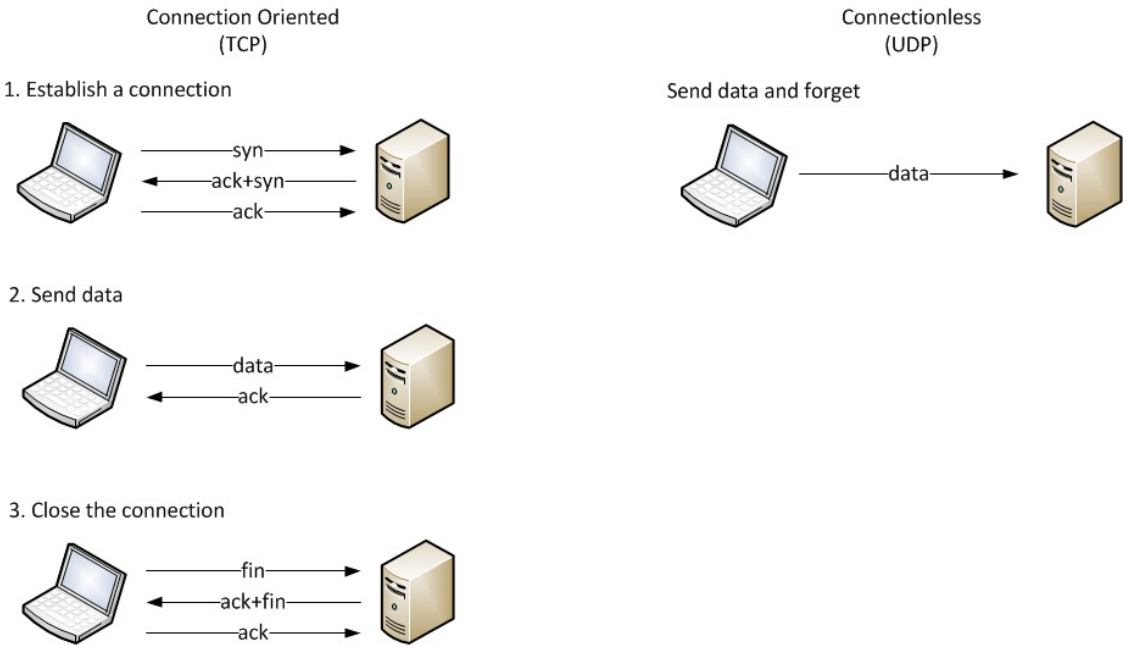


Hvordan fungerer et netværk? (tegn)

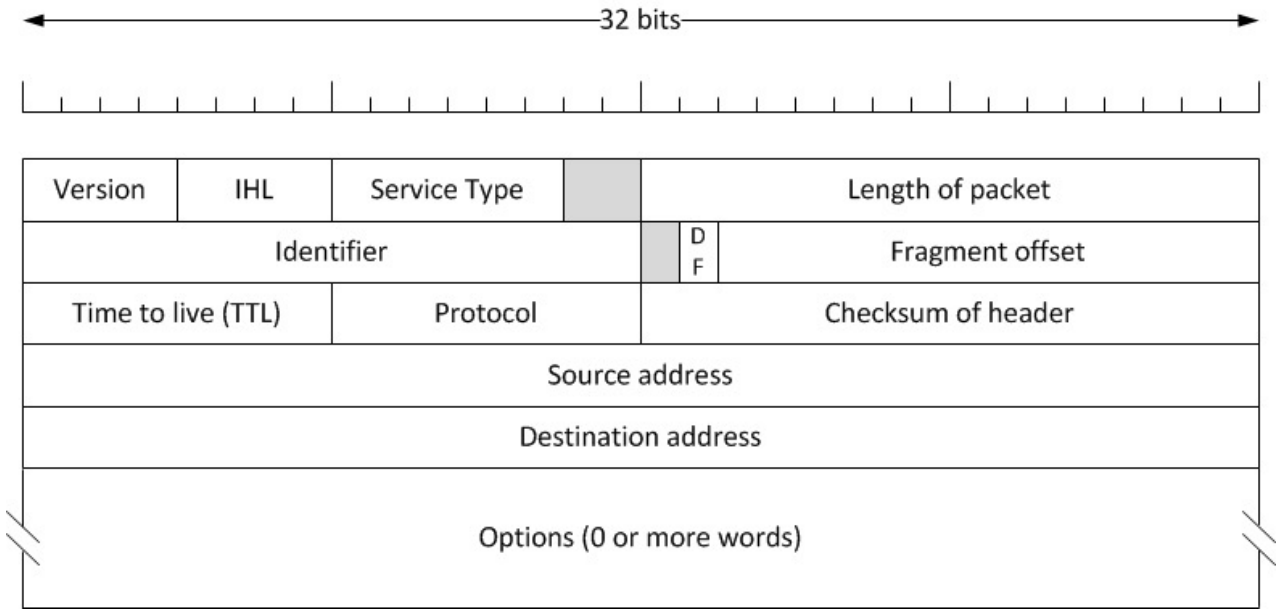
Princippet med protokoller/headers/tails



Protokoller: TCP/IP og UDP



IP Header


32 bits
Version
IHL
Service Type
Length of packet
Identifier
D
F
Fragment offset
Time to live (TTL)
Protocol
Checksum of header
Source address
Destination address
Options (0 or more words)

Netværksovervågning – hvorfor?

- Fejlsøgning
- Undersøge sikkerhedproblemer
- Debugge protokoller (implementationer)
- Lære om netværksprotokoller
- Og meget mere…

Network Monitoring

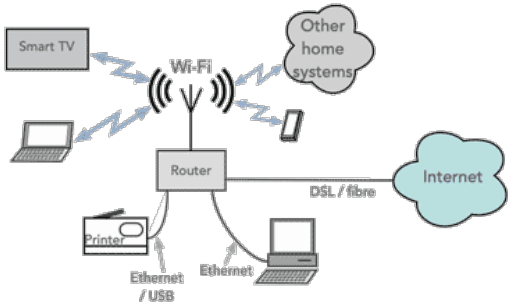
Wireshark – gratis, open source

- Måler al trafik, der går ind og ud af eget interface
- Promiscous mode: Også pakker til/fra andre maskiner
- Monitor mode: Lytter på alle SSID'er uden at joine

- Lad os kigge på hvilke typer af information vi kan indsamle… på bowling! (only do this at home)

De åbne trådløse netværk er simple!

- Klienten sender en **authentication request** til access pointet. Hver enhed har en **MAC-adresse**.
- Og får en **authentication response** tilbage om forbindelsen er lykkedes eller ej.
- Typsik er det også i forbindelse med denne proces at klienten får tildelt en **IP-adresse** på det lokale netværk.
- Og så er man ellers ”på nettet”.
  - Den trafik man sender kan også ses og læses af alle andre på det lokale netværk.
  - Det hele kan ses af den gateway man kommunikerer med, og som er ansvarlig for at sende alting ud på Internettet.
  - Ingen kontrol af identiteter (**spoofing** er muligt).
- **VPN** – giver end-to-end kryptering af beskeder!
- **HTTPS** og andre krypterings-protokoller hjælper!
- Vær OBS på at **DNS-opslag** ofte sendes i cleartext!



Kryptering

- Kryptering gør kommunikationen “hemmelig”
- Kryptering kan ske på forskellige lag (f.eks. HTTPS over et ukrypteret trådløst netværk)
- Kan være let, svært eller umuligt at bryde afhængig af hvilken type kryptering der anvendes
- Men i dag kigger vi ”kun” på ukrypteret trafik

- Men vi kan godt tage et hurtigt kig på en PineApple

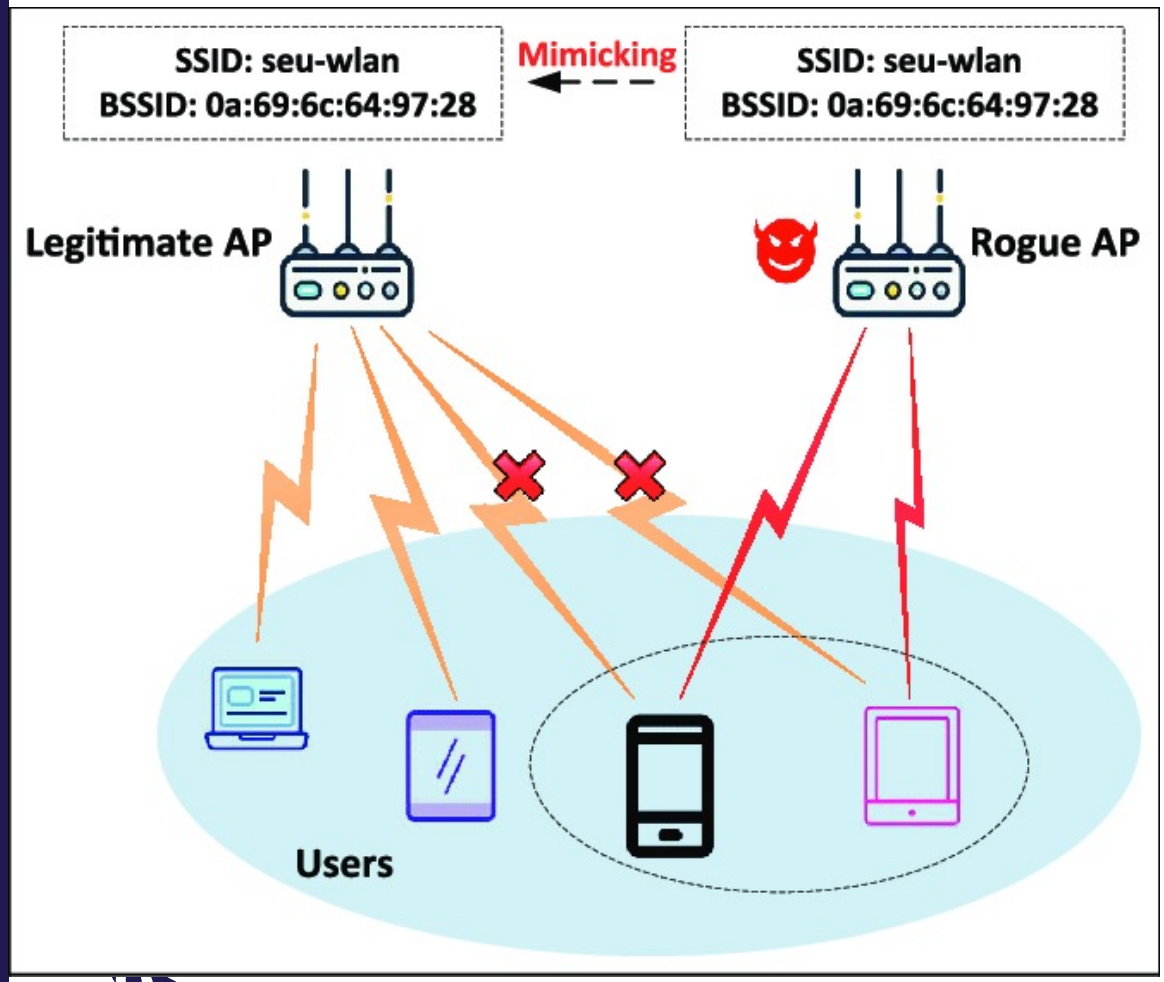
Authentication

- Din telefon spørger om de sidste kendte wifi-SSID'er er i Nærheden.
- SSID'er kan spoofes…
- Og **de-authentication** requests kan normalt også **spoofes** (!!)

- Er din telefon sat til automatisk at forbinde til kendte wifi?
- Men: Kryptering gør det væsentligt mere tricky!

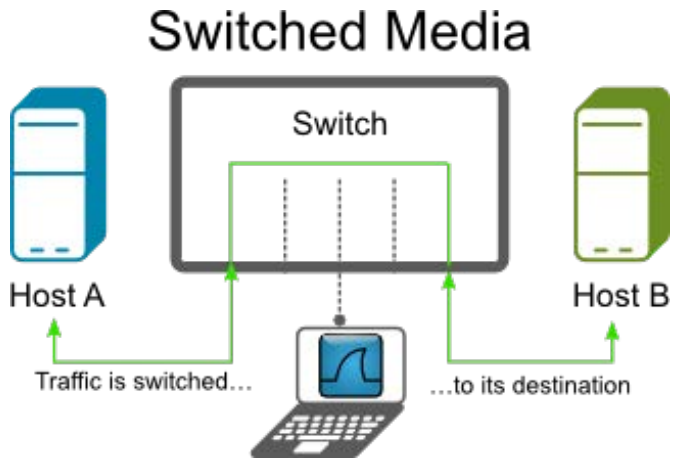
Og så den onde tvilling

- Den klassiske – **Rogue access point**.
- I dette tilfælde også kombineret med en **evil twin**.
- Hvad kan man mon bruge sådan et **Man-in-the-middle angreb** til?

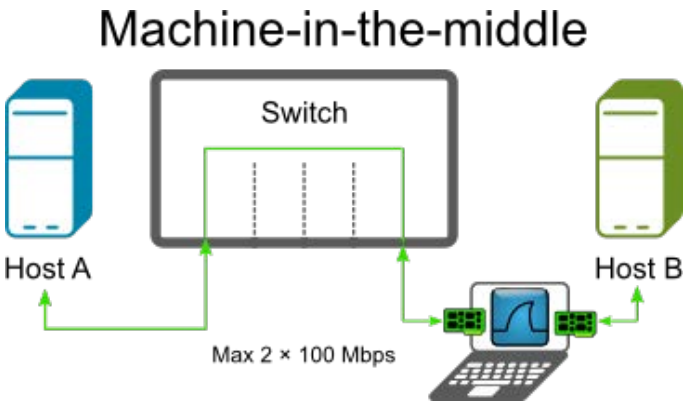


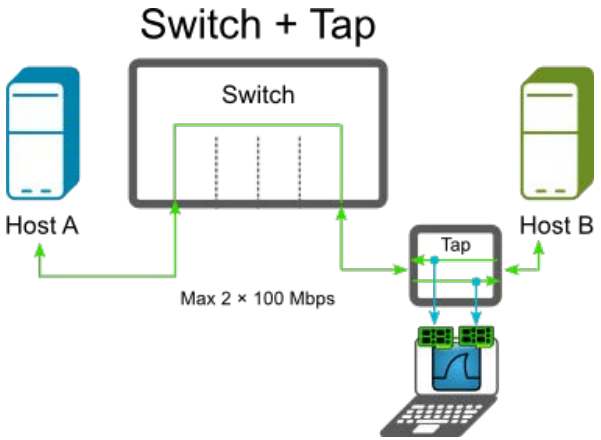
Hvad med kablede netværk?

- Med en switch hører man sædvanligvis kun sig selv…



Så man skal overveje sin opsætning



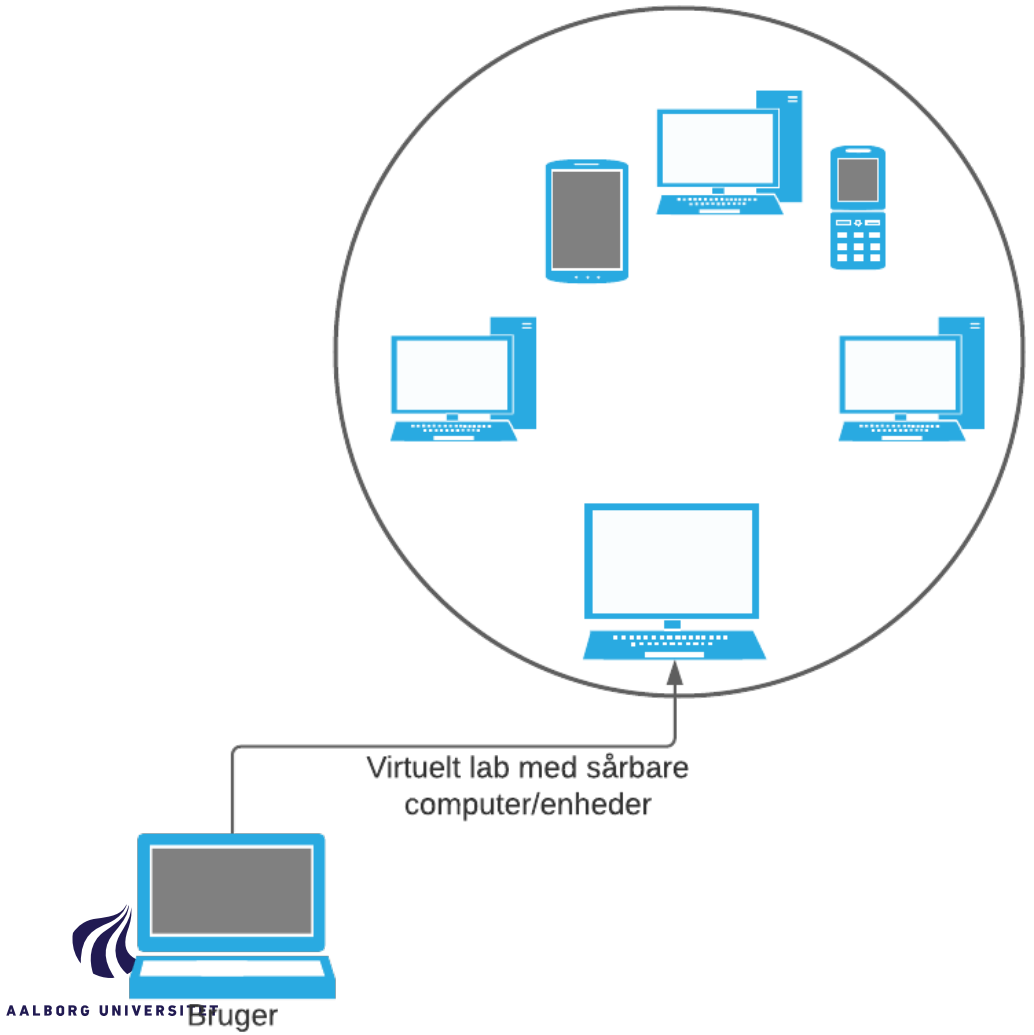


Tid til en kort pause

- Spørgsmål?
- Vi starter igen 17.65
- dm.ntp-event.dk

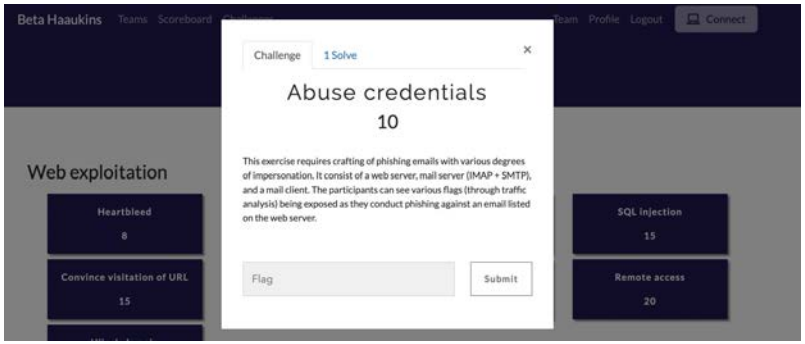
Praktiske opgaver med Haaukins!

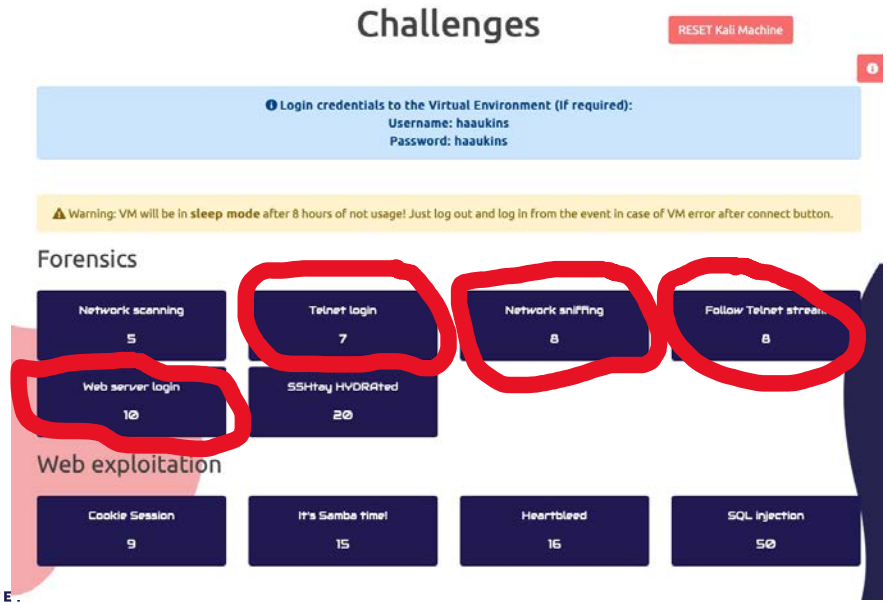
- Findes på dm.ntp-event.dk
- Register dig som et hold (en person = et hold)
- Hver person har sig eget virtuelle **laboratorium**, med sine egne **enheder/computere**.
- Al trafik går gennem vores virtuelle Kali-maskine ☺
- 192.168.1.4 IP addressen
- Subnet mask: 255.255.255.0
- IP adresser i lab: 192.168.1.0-255
- IP adresse 32 bit
- 11111111.11111111.11111111.00000000



Praktiske opgaver med Haaukins!

- Hver **opgave** indeholder en **beskrivelse**. Man skal finde et flag, dvs. en kode, der giver point. Flag ser ud som HKN{123ABC}, hvor 123ABC skifter fra flag til flag.
- Flag indsættes så i ”flag”-feltet, og man får sine **point** ☺
- At kopiere fra det virtuelle miljø kan være en udfordring. Hint: **Kopier ind i en browser**, og så derfra ud.
- OBS: Når du er i det virtuelle miljø har du et **Linux-tastatur**!





AALBORG UNIVERSITET

Opgaver til Haaukins

- Lad os tage et kig på Wireshark:
  - Find login til en webserver ved at kigge i http-trafik (network sniffing)
  - Brug det fundne login til at logge ind (web server login)
  - Kan I finde en Telnet stream, og følge den (check Wireshark's funktionalitet!)
- Der er tid til at løse opgaver til 18.50, og så går vi i gang med at se på Scanning!

- dm.haaukins.com

Netværksscaning: Lidt om jura!

Hvad siger straffeloven?

§263, stk. 1

Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem.

Note: Sædvanligvis kan politiet kun undersøge en sag, hvis offeret anmelder angrebet (§275, stk. 2)

Hvornår tager man fat i døren for at mærke om den er låst - og hvornår går man ind?

(De næste slides er lånt fra Lene Wacher Lentz, Adjunkt i jura, Aalborg Universitet)

Case 1: Hacket Facebook-profil

- En kvinde skaffer sig uberettiget adgang til sin ekskærestes Facebook-konto
- Ændrer brugernavn, adgangskode, sletter telefonnumre, ændrer profilbillede.
- Hun forklarer, at han havde givet hende password til sin Facebook-profil.
- Efter forholdet var gået forbi, havde hun fundet ud af, at han havde været hende utro. Hun benyttede adgangen til hans Facebook-profil til at drille ham.
- Sagen blev afgjort som tilståelsessag, idet hun erkendte det faktiske hændelsesforløb. Ifølge referatet forklarede hun, at det er helt almindeligt at ændre på profiler på Facebook, fx hvis en person ikke har logget af. Hun havde ikke fået noget ud af det uden at drille ham, og ”det ville tage ingen tid at genoprette en ændret konto”.

Hacking eller ej?

Case 1: Hacket Facebook-profil

- En kvinde skaffer sig uberettiget adgang til sin ekskærestes Facebook-konto
- Ændrer brugernavn, adgangskode, sletter telefonnumre, ændrer profilbillede.
- Hun forklarer, at han havde givet hende password til sin Facebook-profil.
- Efter forholdet var gået forbi, havde hun fundet ud af, at han havde været hende utro. Hun benyttede adgangen til hans Facebook-profil til at drille ham.
- Sagen blev afgjort som tilståelsessag, idet hun erkendte det faktiske hændelsesforløb. Ifølge referatet forklarede hun, at det er helt almindeligt at ændre på profiler på Facebook, fx hvis en person ikke har logget af. Hun havde ikke fået noget ud af det uden at drille ham, og ”det ville tage ingen tid at genoprette en ændret konto”.

Hacking eller ej?

Byretten: 20 dagbøder á 100 kr.

Landsretten: Stadfæstet

Case 2:
Software-udvikler tiltalt for hacking...

Softwareudvikler er tiltalt for hacking og hærværk mod it-system i søns børnehave

En bekymret far, der valgte at tage sagen i egen hånd og fandt sårbarheder i en børnehaves it-system, er nu blevet tiltalt for på ulovlig vis at have tiltvunget sig adgang til systemet. Retssagen kan danne præcedens ifølge professor.

Elías Christian Lundström @TekkyViking Tirsdag, 22. december 2015 - 6:29 71

Case 2:
Software-udvikler tiltalt for hacking...

Softwareudvikler er tiltalt for hacking og hærværk mod it-system i søns børnehave

En bekymret far, der valgte at tage sagen i egen hånd og fandt sårbarheder i en børnehaves it-system, er nu blevet tiltalt for på ulovlig vis at have tiltvunget sig adgang til systemet. Retssagen kan danne præcedens ifølge professor.

Elías Christian Lundström @TekkyViking Tirsdag, 22. december 2015 - 6:29 71

- Byret: Dømt for hacking. 10 dagbøder á 500 kr.
- Landsret: Ikke skyldig.

Netværks-scanning

- Baseret på Bou-Harb, Elias & Debbabi, Mourad & Assi, Chadi. (2014). Cyber Scanning: A Comprehensive Survey. Communications Surveys & Tutorials, IEEE. 16. 1496-1519. 10.1109/SURV.2013.102913.00020.
- Det er fedt at scanne, men det er vigtigt at vide hvad man laver…

☆ **Peter Dissing** archive 11 September 2017 at 15.13

STOP Sikkerheds scanning omgående Details

To: Nicolaj Kjettrup, Cc: Jens Myrup Pedersen, Mads Peter Bach

Hej Nikolaj

Vil i OMGÅENDE stoppe med at scanne vores maskiner

I ligger vores systemer ned.

Mvh
Peter Dissing
Infrastruktur Linux

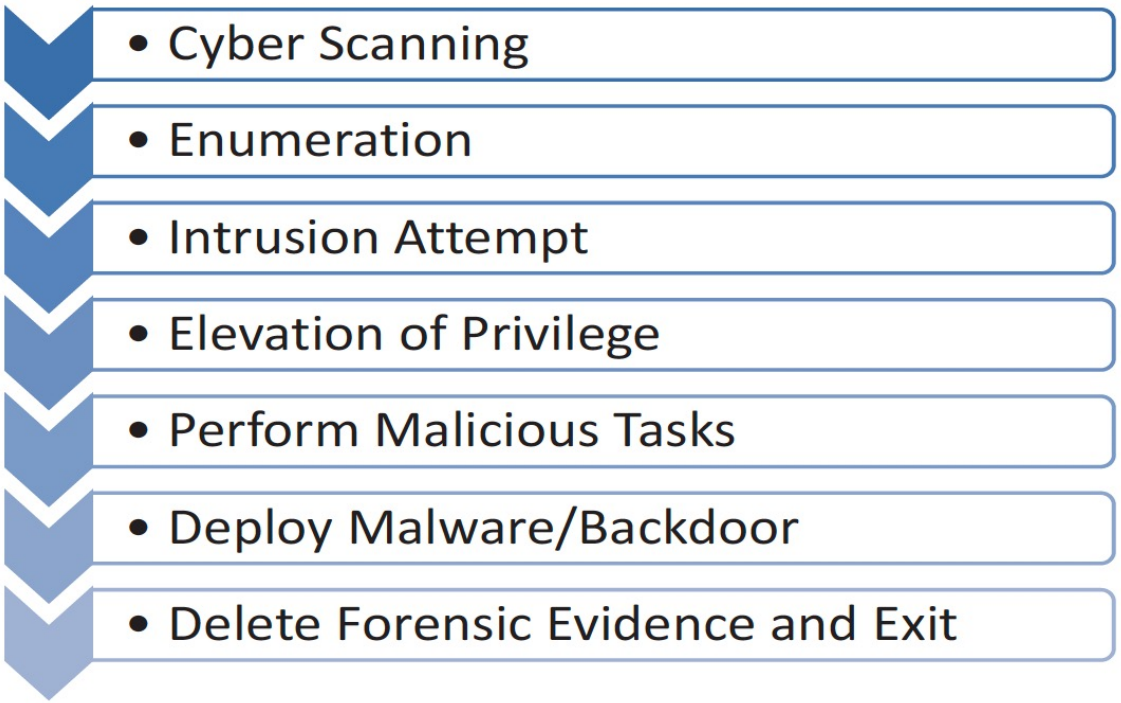
Netværks-scanning

- Nmap er et super værktøj
- Send pakker til andre maskiner, og se hvordan de svarer…
- Hvordan kan man vide hvilke maskiner der ellers eksisterer?

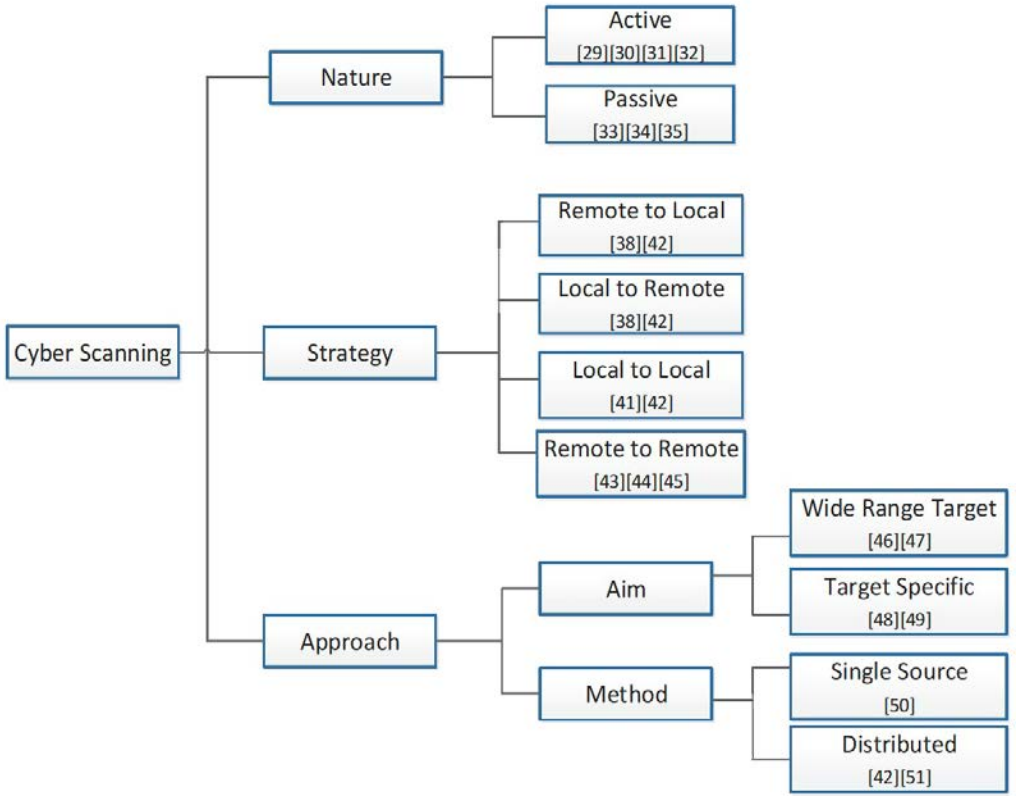
Netværks-scanning

- Nmap er et super værktøj
- Send pakker til andre maskiner, og se hvordan de svarer…
- Hvordan kan man vide hvilke maskiner der ellers eksisterer?
- Simpleste form for scanning: Ping!

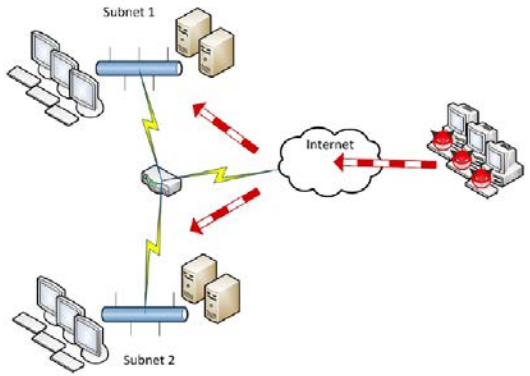
Netværks-scanning



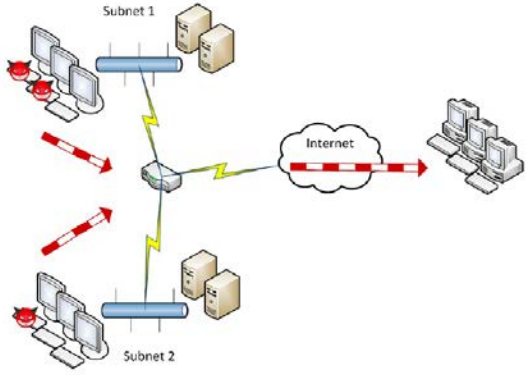
Simpelt, men...


Cyber Scanning
Nature
Active
[29][30][31][32]
Passive
[33][34][35]
Strategy
Remote to Local
[38][42]
Local to Remote
[38][42]
Local to Local
[41][42]
Remote to Remote
[43][44][45]
Approach
Aim
Wide Range Target
[46][47]
Target Specific
[48][49]
Method
Single Source
[50]
Distributed
[42][51]

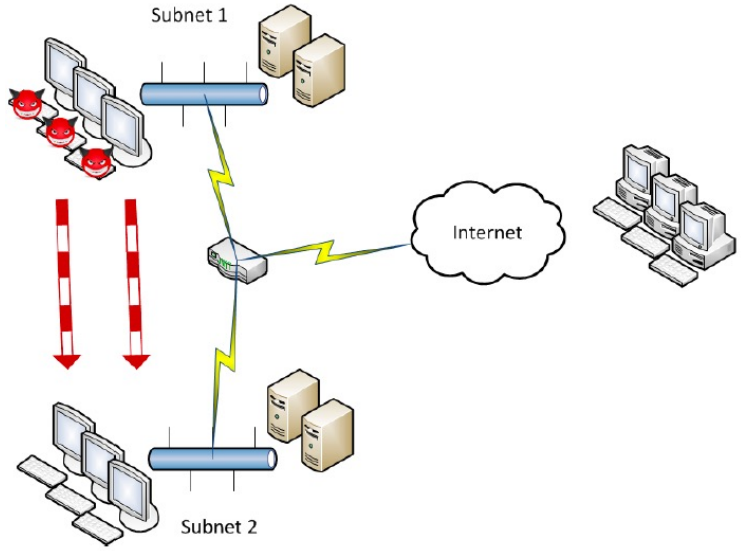
Scanning fra forskellige steder



(a) Remote to Local



(b) Local to Remote



(c) Local to Local

Hvilke typer scanning skal man vælge?

- Hvilke informationer har man brug for?
- Hvor meget tid har man?
- Hvilke ressourcer har man?
- Vil man gerne undgå at støje?

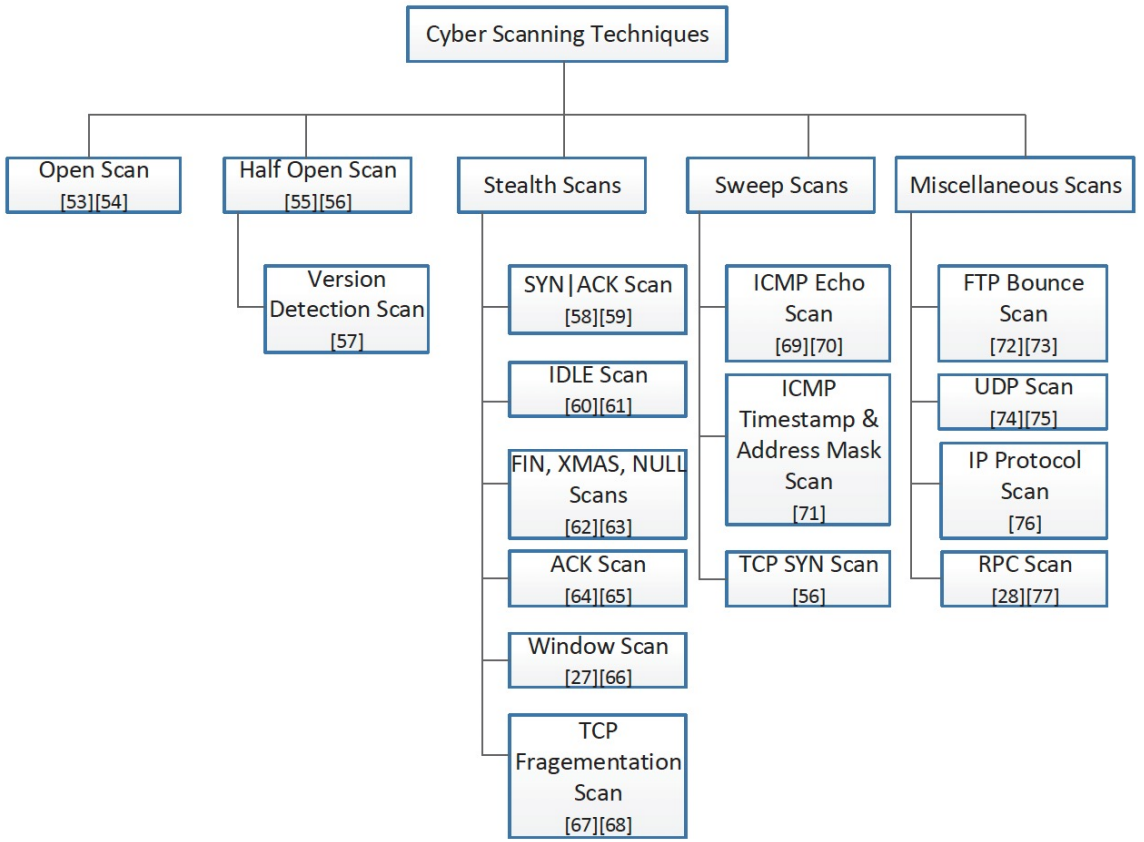
Hvilke typer scanning skal man vælge?

- Eksempel: OS fingerprinting

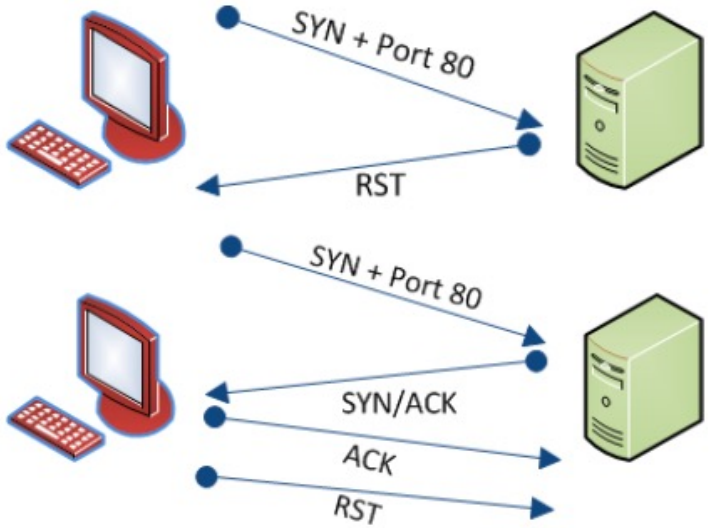
	linux 2.4	linux 2.6	openbsd	windows 9x	windows 200	windows xp
ttl	64	64	64	32	128	128
packet length	60	60	64	48	48	48
initial windows	5840	5840	16384	9000	16384	16384
mss	512	512	1460	1460	1460	1460
ip id	0	random	random	Increment	increment	increment
enabled tcp opt	MNNTNW	MNNTNW	M	M	MNNT	MNW
timestamp inc.	100hz	1000hz	unsupported	unsupported	unsupported	unsupported
sack	OK	OK	OK	OK	OK	OK
SYN attempts	5	5	4	3	3	3

Forskellige typer af scanninger

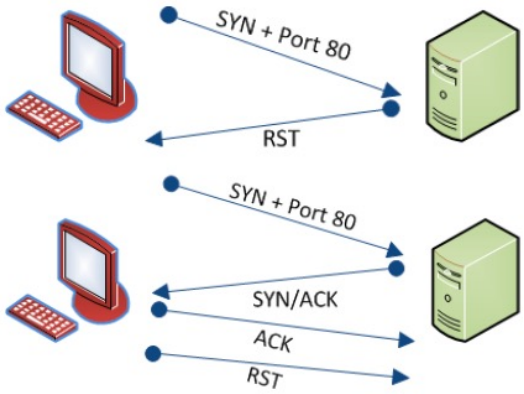
- Lad os se nærmere på nogle af dem
- Husk et nævne sårbarheds-scans

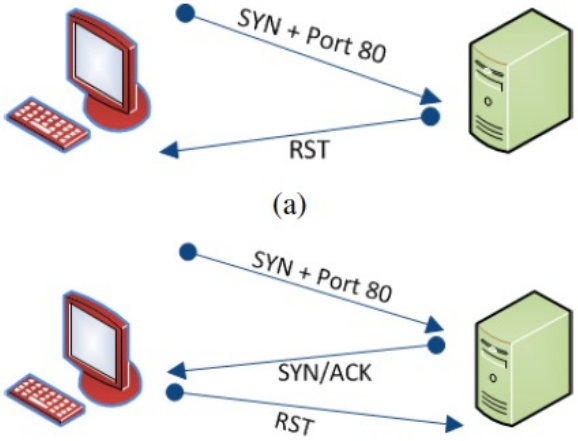


Open Scan

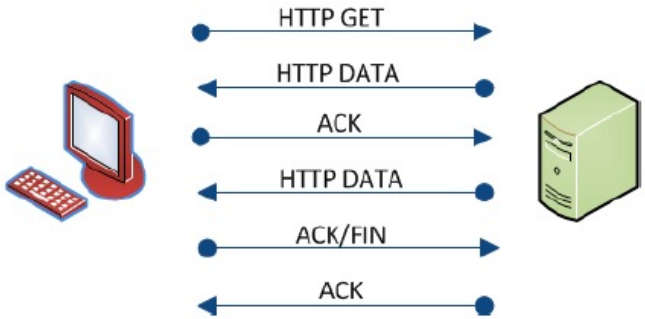


Open Scan – og Half-open Scan

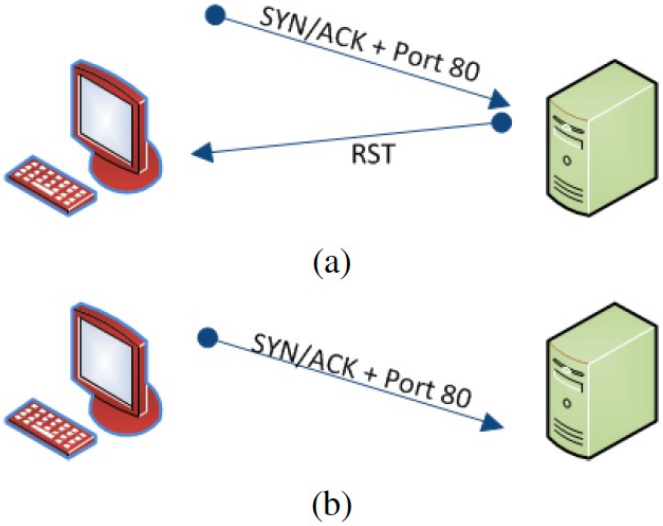




Vi kan gå dybere med en versions-scanning

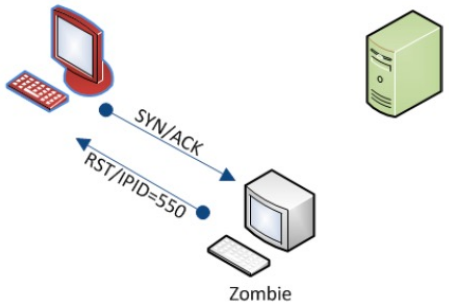


SYN/ACK scan er også et alternativ...

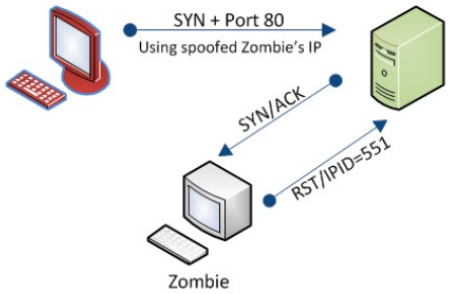


Eller et Idle Scan

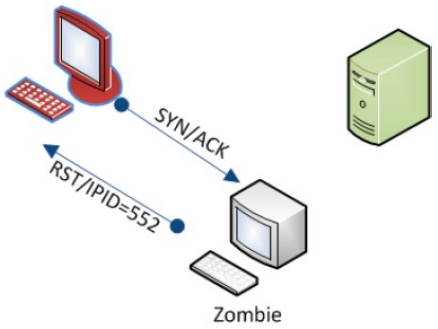
(1)



(2)



(3)



Eller et Idle Scan

```
# nmap -Pn -p- -sI kiosk.adobe.com www.riaa.com

Starting Nmap ( http://nmap.org )
Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental
Nmap scan report for 208.225.90.120
(The 65522 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
135/tcp    open        loc-srv
443/tcp    open        https
1027/tcp   open        IIS
1030/tcp   open        iad1
2306/tcp   open        unknown
5631/tcp   open        pcanywheredata
7937/tcp   open        unknown
7938/tcp   open        unknown
36890/tcp  open        unknown

Nmap done: 1 IP address (1 host up) scanned in 2594.47 seconds
```

Nmap er et super værktøj

- De-facto mest brugte netværksscanner
- nmap → Kommandolinie
- zenmap → Nmap gui
- nmap/zenmap kan håndtere:
  - Avancerede teknikker: port scanning, OS detection, version detection, ping sweeps, etc.
  - Store netværk.
  - Virker på de fleste platforme.
  - Gratis.
  - Veldokumenteret, og masser af support til rådighed.

Forskellige nmap-scanninger

- **Port Division:** open, closed, filtered, unfiltered, open|filtered and closed|filtered

Scanning techniques:

-sS (TCP SYN scan)

-sT (TCP connect() scan)

-sU (UDP scans)

-sA (TCP ACK scan)

-sW (TCP Window scan)

-sM (TCP Maimon scan)

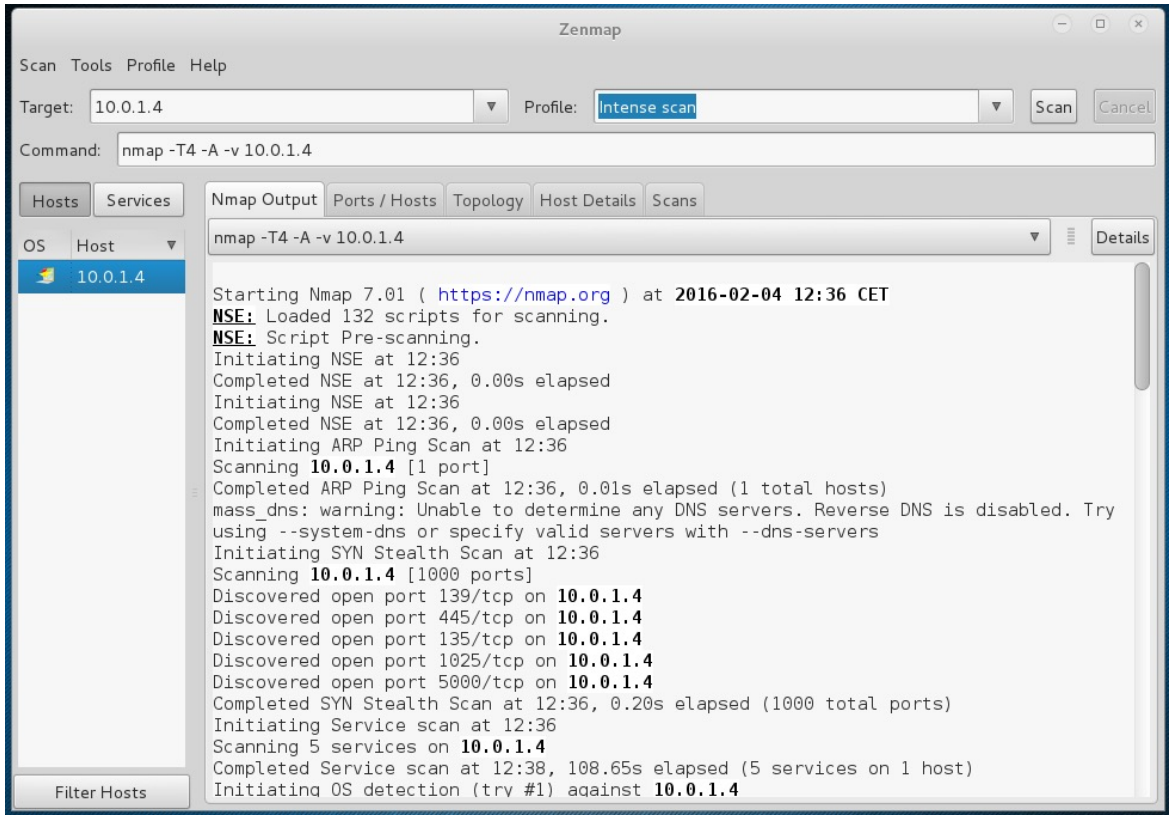
Nogle få eksempler

- Ping sweep
  - nmap -v -sP 192.168.100.0/24
  - -sP ping scan.

- Port scanning for at finde aktive hosts og åbne porte
  - nmap -v -sT 192.168.100.0/24
  - -sT normal scan
  - -sS stealth scan
  - -A OS and Services

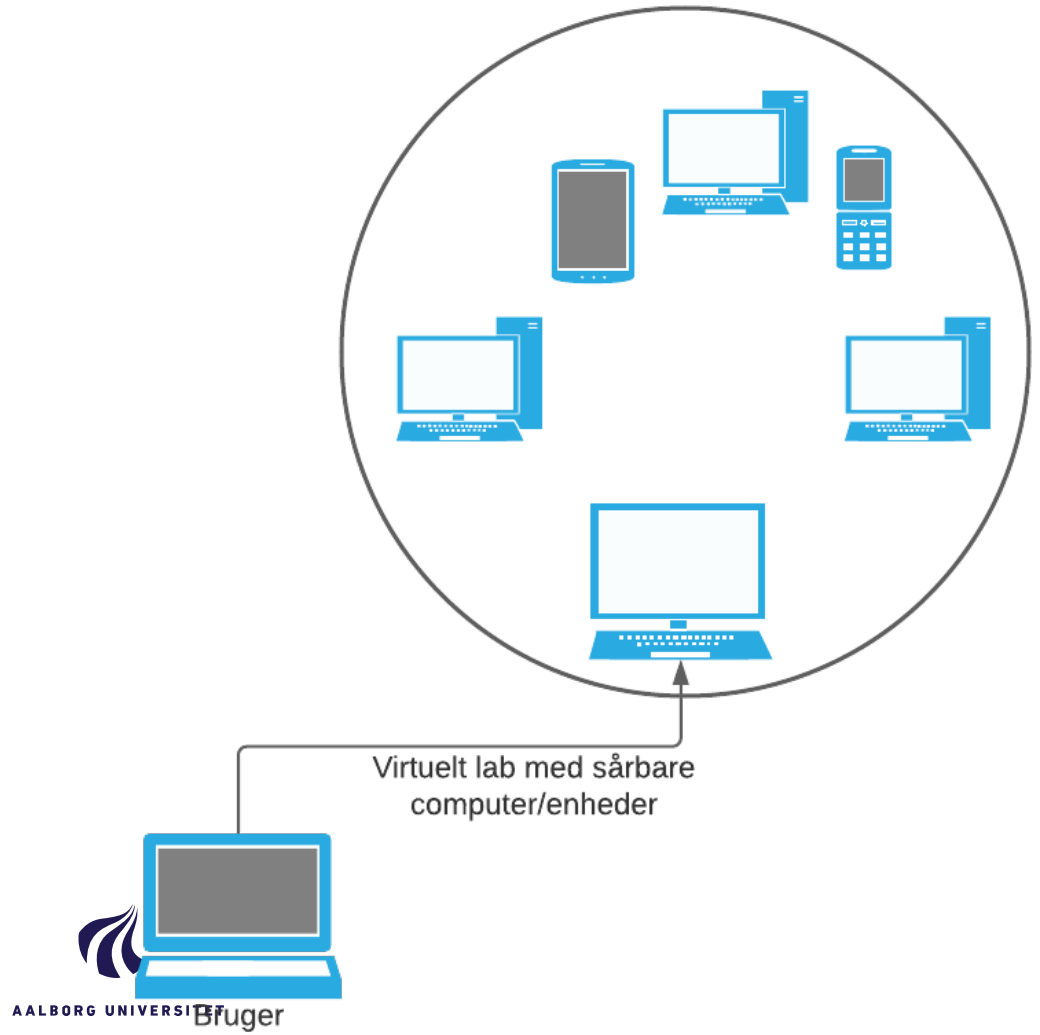
- OS scanning for at fingerprinte operativsystemer
  - nmap –O 192.168.100.0/24

Zenmap hvis man gerne vil have GUI



Praktiske opgaver med Haaukins!

- Findes på dm.haaukins.com
- Samme registrering som før
- Hver person har sig eget virtuelle **laboratorium**, med sine egne **enheder/computere**.
- Bemærk randomized IP-adresser for hvert lab!
- Hvis vore Kali-maskine har adressen 192.168.1.4 og subnet mask er 255.255.255.0, så er de mulige adresser 192.168.1-255.
- Brug *ifconfig* først til at finde ud af vores adresse og netværk.
- Simpel kommando:
- nmap 192.168.1.1-255.
- Eller nmap 192.168.1.0/24



Opgave 1: Network Scanning
Find en webserver (der kun kører på port 80)

- Åben en terminal
- Skriv *ifconfig* for at finde ud af hvad netværk og subnet du er på, og hvad din egen adresse er.
- Brug *nmap xx.xx.xx.1-255* (eller *nmap xx.xx.xx.00/24*, gør det samme)
- Prøv også *nmap –sP* og *nmap -O*. Hvad er forskellen?
- Leg gerne med lidt forskellige nmap-kommandoer
- Og så løser vi lige scanning-opgaven ved at finde en webserver der kun kører på port 80.

AALBORG UNIVERSITY
DENMARK

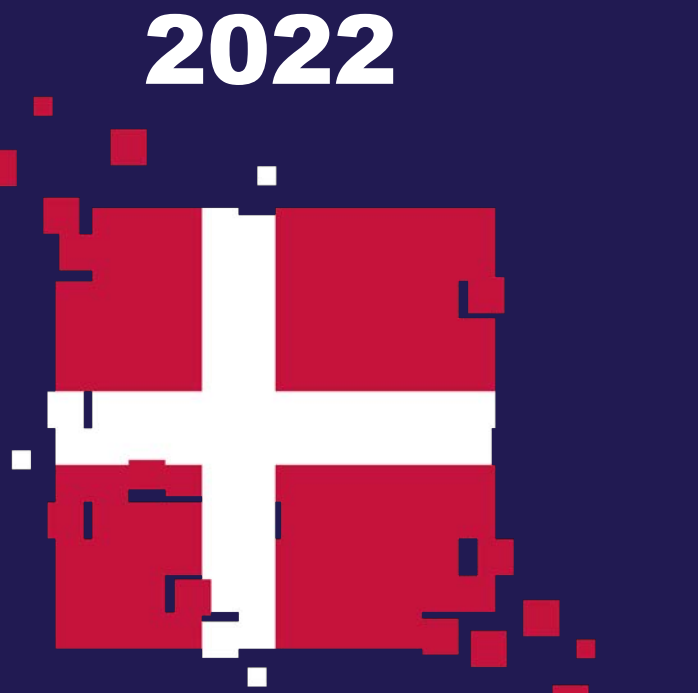
Opgave 2: Heartbleed

Find en maskine, der er sårbar overfor “heartbleed”

- Nmap kan også bruges til at køre scripts til at finde specifikke sårbarheder
- Google er vores ven ☺
- Spørg, og efter 10 minutter viser vi løsningen!

AALBORG UNIVERSITY
DENMARK

De Danske Cybermesterskaber 2022



DE DANSKE
CYBERMESTERSKABER

Hvad er De Danske Cybermesterskaber (DDC)?

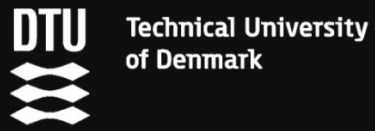
De Danske Cybermesterskaber 2022 er for alle **mellem 15-25 år.**
Du kan vælge at starte i **virtuel træningslejr (som denne træning)** med undervisning, hands-on og udfordringer, hvor du bliver coachet og undervist af førende danske og udenlandske cyberspecialister.

Eller du kan gå direkte til online kvalifikationen, hvor du kæmper om en adgangsbillet til **De Regionale Cybermesterskaber** og derfra videre til **De Danske Cybermesterskaber.** Der er også begynder opgaver, dog skal du løse 6 ud af 15 for at gå videre.

Og hvem ved, måske går du hele vejen til **Det Danske Cyberlandshold**, der drager til Østrig i efteråret!

DE DANSKE CYBERMESTERSKABER

Hvem står bag DDC?



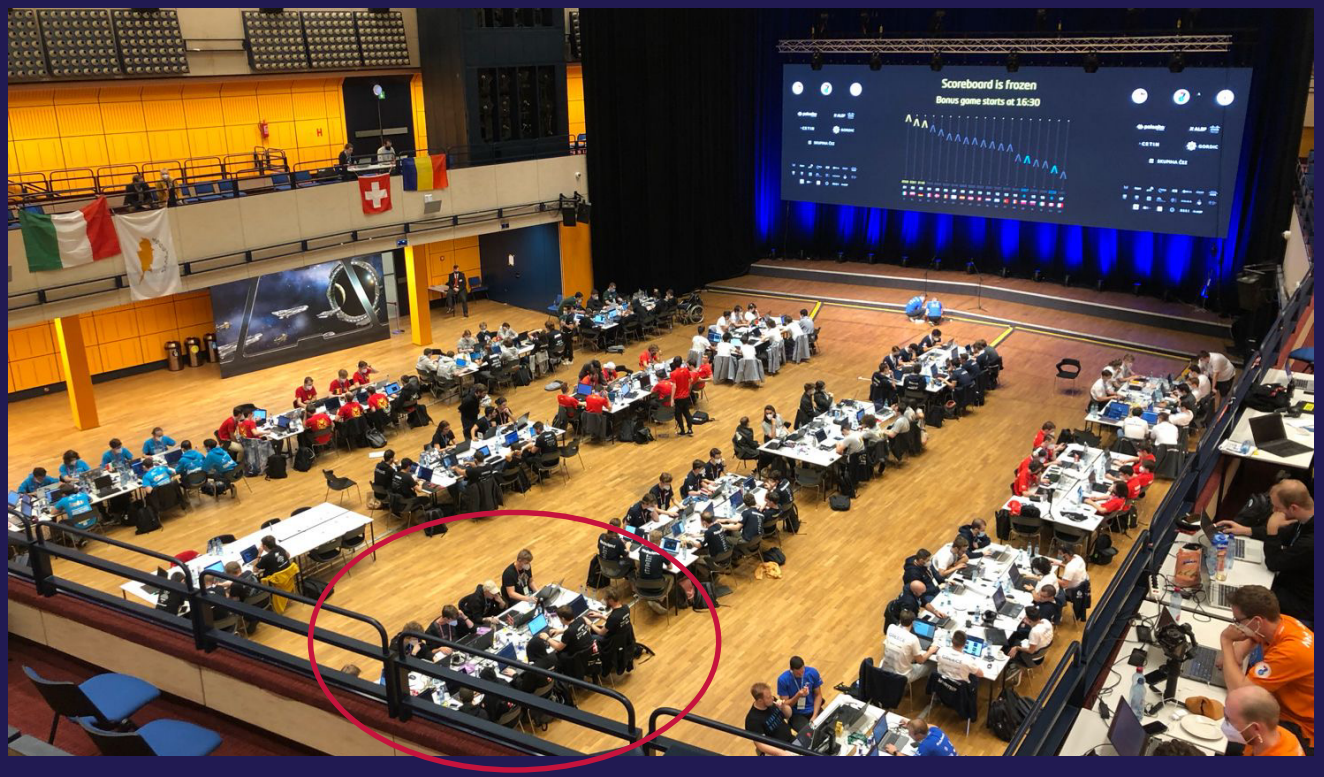
Hvor mange var med i 2021?

+1700 unge til online træning
+450 unge til online kvalifikation
+200 unge til de Regionale Mesterskaber
100 unge til det Nationale Mesterskab
25 unge til Bootcamp
10 blev udvalgt til det danske landshold

Landsholdet anno 2021

DE DANSKE CYBERMESTERSKABER

Danmark fik en 5. plads i 2021!



DE DANSKE CYBERMESTERSKABER

Så hvornår starter det i 2022?

ONLINE TRÆNINGSDAGE

UGE 7-10

ONLINE KVALIFIKATION

UGE 9-12

REGIONALE MESTERSKABER

9. APRIL

DE DANSKE CYBERMESTER-SKABER

7. MAJ

DE DANSKE CYBERMESTERSKABER

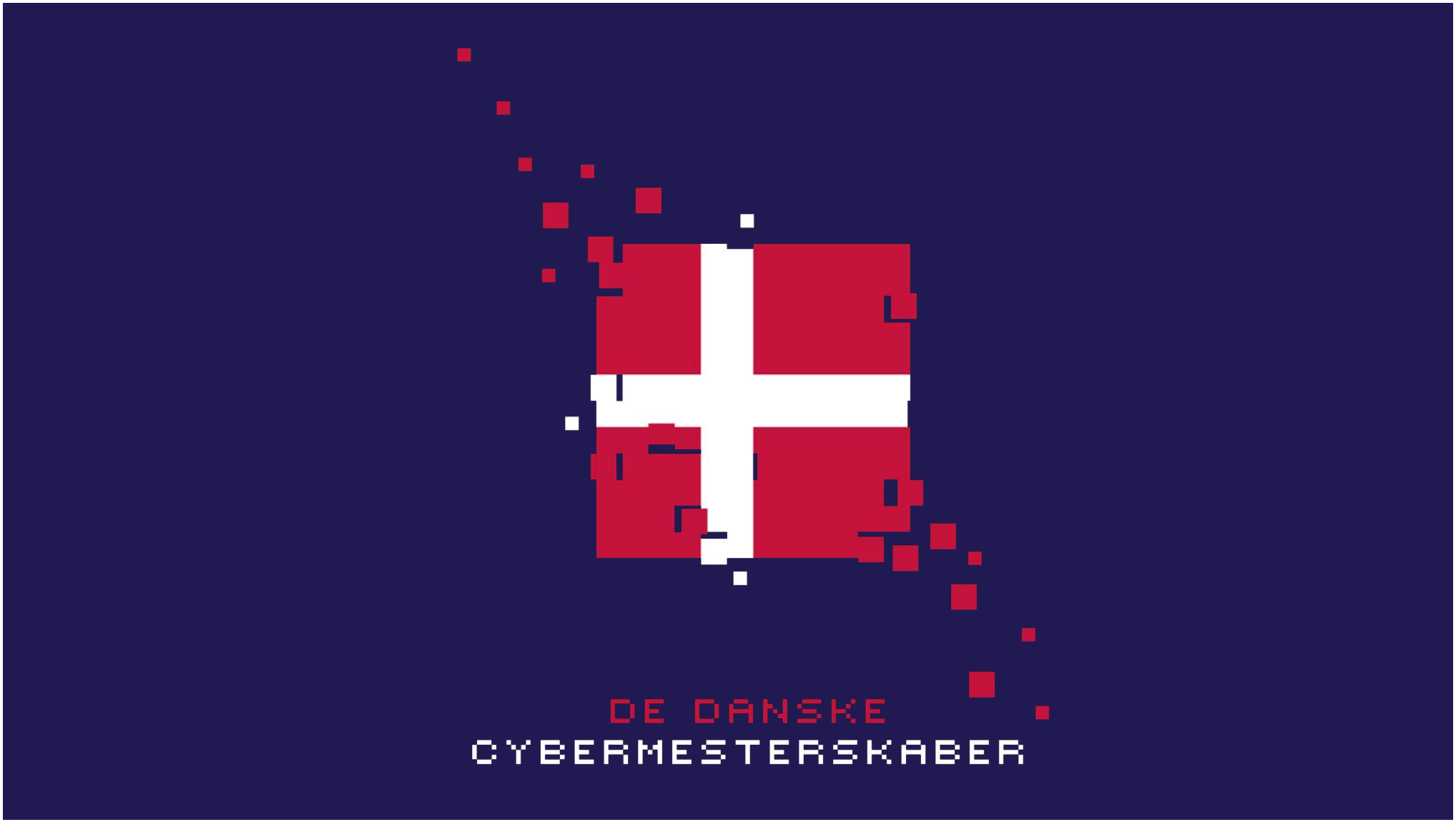
Join CyberSkills fællesskabet på Discord!

https://discord.gg/2tTwMvbSXu

DE DANSKE CYBERMESTERSKABER

CYBER SKILLS

DE DANSKE CYBERMESTERSKABER


DE DANSKE
CYBERMESTERSKABER

Tak for i dag!

Vi har normalt altid https://general.haaukins.com åben, med lidt blandede udfordringer i alle sværhedsgrader.

Der er links til masser af e-læring på https://www.cyberskills.dk.

CyberSkills: Aarhus - https://www.facebook.com/groups/1923727471100826
CyberSkills: København - https://www.facebook.com/groups/500963300882448
CyberSkills: Aalborg - https://www.facebook.com/groups/957517617737780

Husk at tilmelde jer på https://cybermesterskaberne.dk

Og spørg endeligt, hvis du vil høre mere om vores uddannelser! :)

AALBORG UNIVERSITY
DENMARK