IN2120 – Cybersikkerhet

Del 6: Pentesting og angrepsmetodikk

Nils Petter Wien



Høst 2026

Universitetet i Oslo

Penetrasjonstest /inntrengingstest

- Hvem/hva/hvorfor



Pentesting – best kjent som hacking

- En pentest skal etterligne uautoriserte hackere
  - **Bruker i størst mulig grad samme verktøy og metoder**

- Et **forebyggende** sikkerhetstiltak som skal:
  - **Utprøve** motstandskraften i informasjonssystemene
  - **Avdekke** svakheter som gjør informasjon og objekter sårbare

Pentesting – hvorfor?

«Den som kjenner seg selv og sine fiender,
trenger ikke å frykte resultatet av hundre slag»

– *Sun Tzu: (The Art of War, ca 450 fkr)*


Foto: Colorbox

Hacke en virksomhet for å få jobb?



- Du må nødvendigvis dokumentere det for virksomheten for å vise at du faktisk har klart det - noe som kalles SELVINKRIMINERING
  - Elden og Finstad (Store norske leksikon, 2022) definerer selvinkriminering som:
    - «*Bidra til sin egen domfellelse ved å avgi forklaring eller gi tilgang til andre bevis.*»

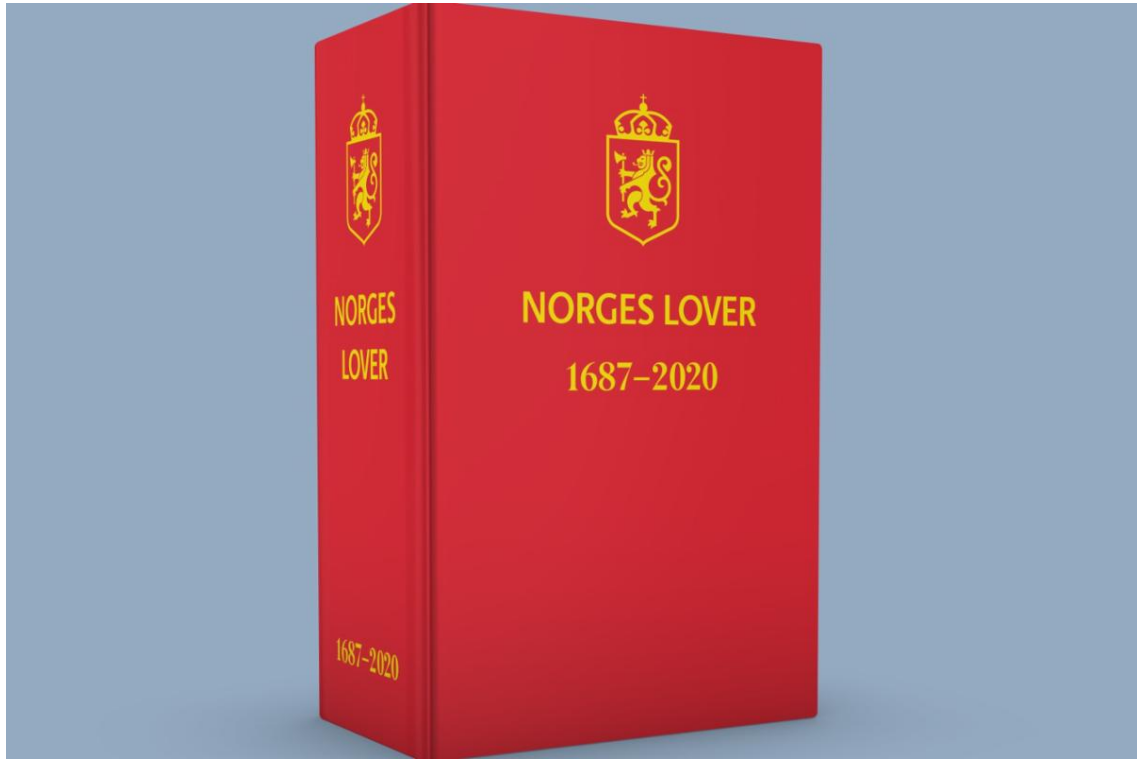
Straffelovens § 204 – *Innbrudd i datasystem*

«Med bot eller fengsel inntil 2 år straffes den som ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til datasystem eller del av det.»

- Datainnbrudd er ulovlig
  - Snakk med en jurist

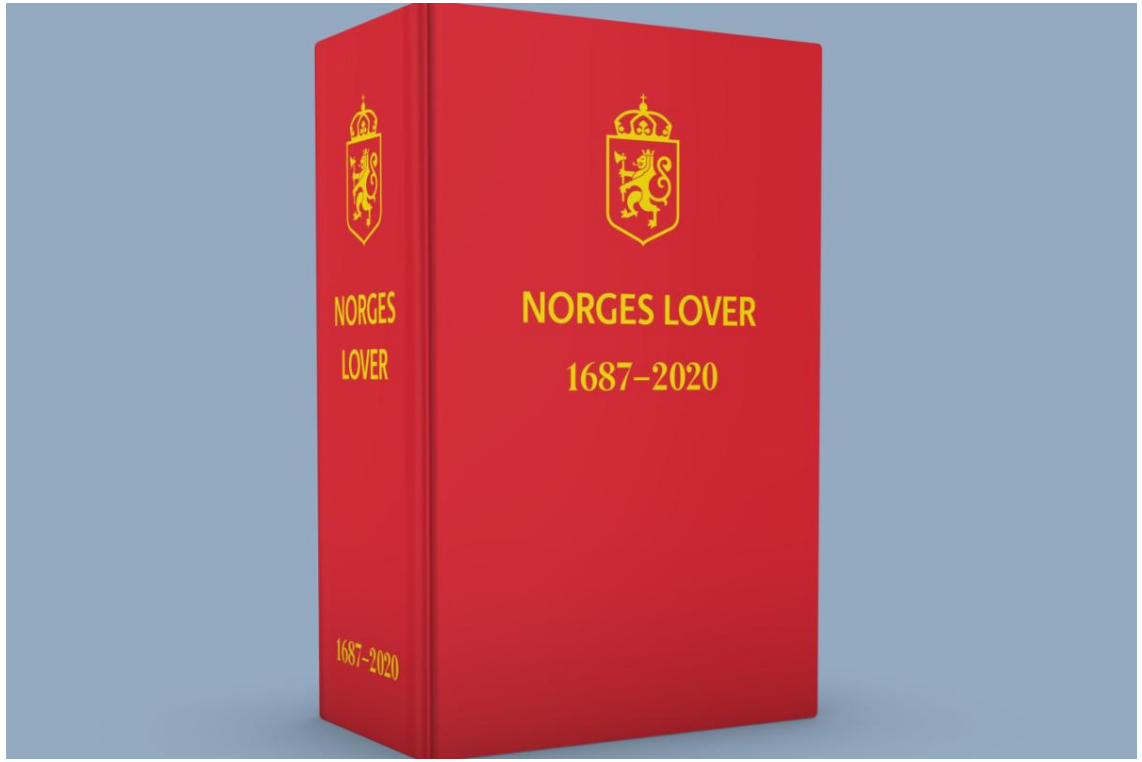
Nødvendig papirarbeid

- Få skriftlig tillatelse på FORHÅND
  - Sørg for at den som gir tillatelse faktisk har tilstrekkelig myndighet
  - Tillatelsen må ALLTID være skriftlig.
  - Dette kalles «Get out of jail free card»



Legalitetsprinsippet (forenklet)

- Som privatperson er alt lov – såfremt det ikke er forbudt.
- Som ansatt i forvaltningen er ALT ulovlig, såfremt det ikke er eksplisitt tillatt.



Hva skiller en pentest fra en ondsinnet hacker?

- Vanlig å definere hackere som hvite/grå/svarte hatter (white, grey, black hats)
  - White hats er typisk pentestere, analytikere eller akademikere som ønsker å gjøre godt (etisk)
  - Black hats er typisk kriminelle, eller andre som ønsker å gjøre uetisk, uautorisert hacking

- **Derfor gir UiO kurs i *etisk* hacking (IN5290)**

Hvit- og svartboks-testing

- Pentester deles ofte inn i hvit- eller svartbokstesting ut fra mengden informasjon pentesteren gis på forhånd
- I en **svartboks-test** (black box) gis pentesteren ingen informasjon om systemet før vedkommende begynner
- I en **hvitboks-test** (white box) gis pentesteren all relevant informasjon
- I tillegg har du en mellomting – ofte kalt **gråboks-testing** (grey box), hvor pentesteren får noe informasjon

Fordeler og ulemper med hvit- og svartboks-testing

Hvit	Svart
Kan være mer effektivt, spesielt på store nett	Enklere å selge inn
Kan planlegge bedre, noe som reduserer risiko	Starter med helt «nye øyne»
Du vet hva som skal være der, så finner ofte mer (enklere å se at «kart og terreng» ikke stemmer)	Kan aldri beskyldes for å ha for mye informasjon (enkelte virksomheter kontrer funnene dine med det)
MEN lett å se seg «blind» på informasjonen du får	Tar mer tid
Mange vil også si det er usannsynlig at en angriper sitter med så mye informasjon	Finner ofte færre ting

Motivasjon skiller pentestere fra ondsinnede hackere

- En ondsinnet hacker ønsker uautorisert tilgang til systemer for å
  - Lese informasjon (angrep på konfidensialitet)
  - Manipulere eller så tvil om informasjon (angrep på integritet)
  - Fjerne/kryptere informasjon (angrep på tilgjengelighet)
  - Utnytte systemressurser
    - Utvinne kryptovaluta
  - Kan være tilfeldige ofre (opportunistisk – prøver seg på alle)

- En pentester ønsker
  - Fjerne, eller redusere sårbarheter
  - Sikre systemer

Praktisk forskjell mellom pentestere og ondsinnede hackere

- En ondsinnet hacker ønsker
  - Persistens (vedvarende tilgang, typisk gjennom bakdører)
  - Ikke å bli oppdaget
    - Ønsker følgelig å finne EN, maks to veier inn
- En pentester
  - Trenger ikke nødvendigvis å være stille
    - noen ganger ønskes det selvsagt for å teste deteksjon og respons!
  - Leter videre etter flere feil
    - Ønsker å finne alle

Forskjeller i tidsbruk

- En ondsinnet hacker kan bruke lang tid
  - Måneder og år
  - Stillhet tar tid
- Pentestere bruker alt fra dager til et par uker
  - Kostnader

Stadiene i en pentest / angrep

- Planlegge med virksomheten

- Rekognosering
- Innledende tilgang
- Utvide tilgang
- Sikre fotfeste
- Gevinst

- Skrive rapport

Planleggingsfasen

- En pentest bør ha et mål om å «ramme» den, eller de kjerneverdiene virksomheten setter høyest
  - Økonomi
  - Sensitive data
  - Tilgjengelighet
  - Mulighet til å manipulere data
  - Mulighet til å hente ut (eksfiltrere) data

Rekognosering i åpne kilder
OSINT (Open source intelligence)

- Finn ut mest mulig om virksom
  - Søkemotorer
  - Virksomhetens egne nettsider
  - Doffin
  - Stillingsannonser
  - Linkedin
  - Facebook
  - Instagram
  - Nettaviser



Foto: Colorbox

Rekognosering i åpne kilder forts.

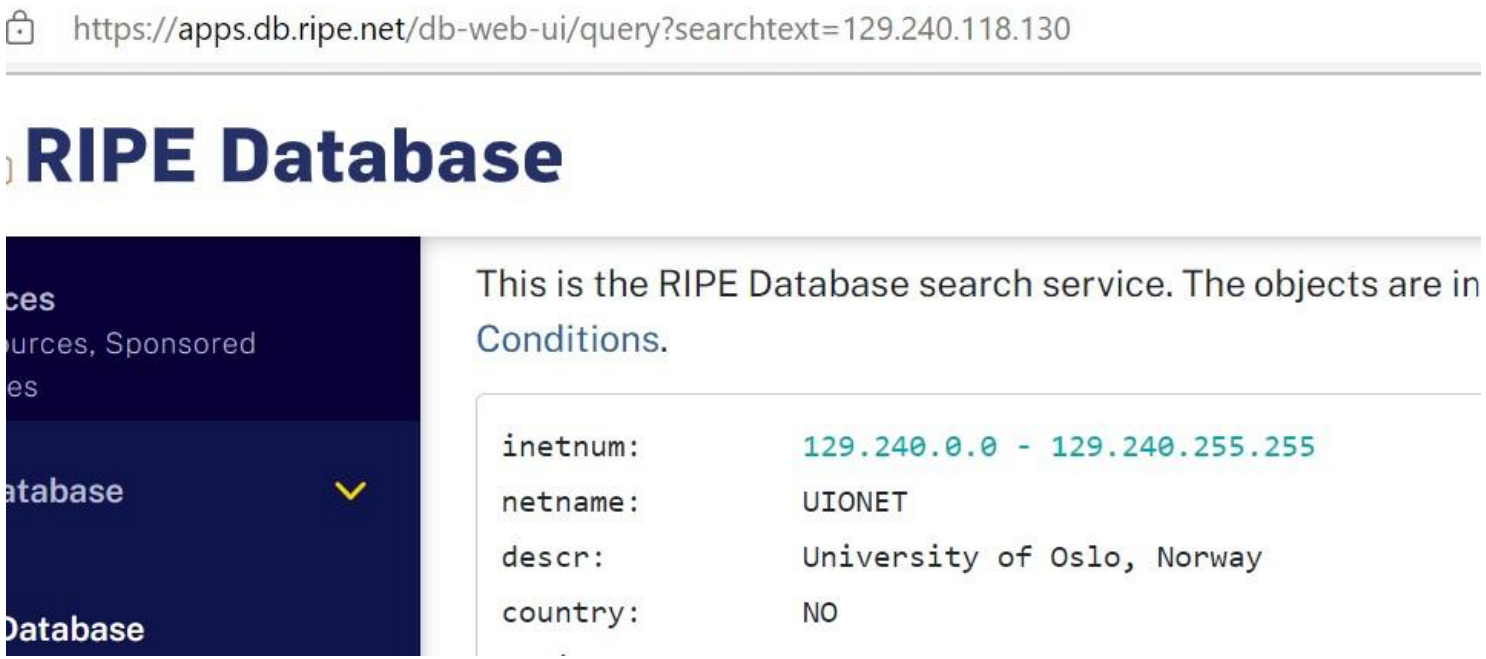
- Finn ut mest mulig om virksomheten
  - Google maps
  - Kart
  - Området rundt
    - Mulig å speide?
    - Overvåke?



Foto: Google maps

Finn ip-adresseområdet

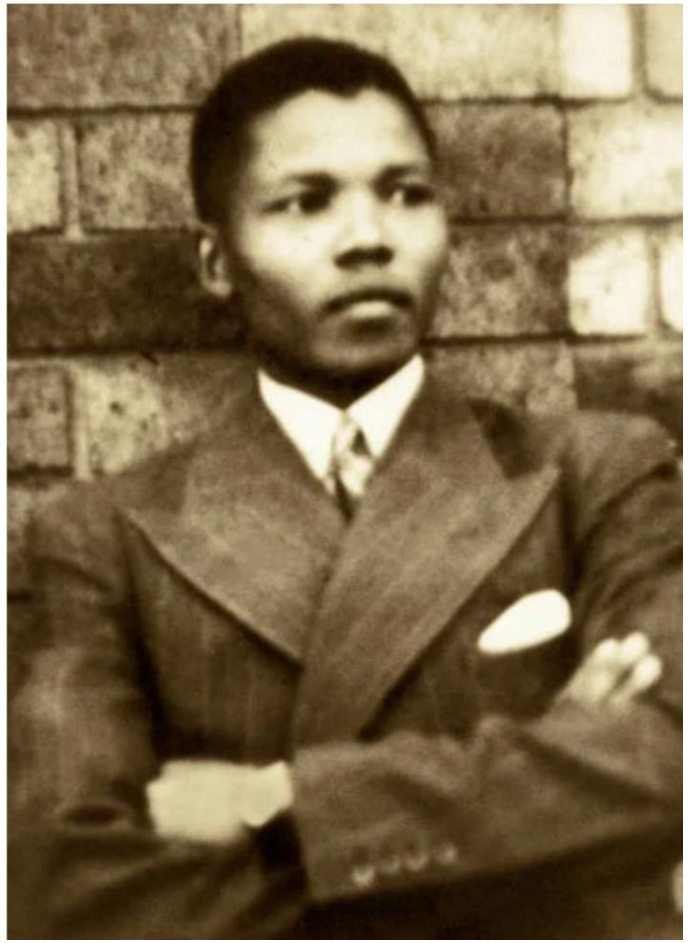
- Nslookup uio.no – gir 129.240.118.130



Boot-angrep

- Gitt fysisk tilgang til en maskin:
  - Boot den i et alternativt OS som du kontrollerer
  - Enkel måte å omgå passord og lignende og få admintilgang

- Dette kan forhindres med sikker oppstart (UEFI) og full diskkryptering (eksempelvis Bitlocker til Windows eller LUKS til Linux)





Initial tilgang via phishing

- Spyd- eller masse-phishing via epost
  - Kjøre scripts
  - Innlogging, hente passord
  - Gir ofte brukertilgang

En effektiv phish er gjerne

- Noe man vil vite
- Noe man vil ha
- Noe man *IKKE* vil ha
- Stressende
  - Stressede folk gjør oftere feil

- Forsvaret er sikkerhetskultur og opplæring
  - Husk å skap en kultur hvor folk *IKKE* er redde for å si ifra!

Hvilke tilganger bør en pentester få

- Hvis man ikke finner brukere raskt, bør de gis
  - Med vanlige rettigheter
  - Utfør mesteparten av testen med vanlig brukertilgang
    - Finner flere feil
    - Sparer tid

- Den vanskeligste delen av en test er å få initial tilgang

  - *«Jo mer tilgang du har, jo enklere er det å få mer»*
    - Wien

Bli kjent med systemet

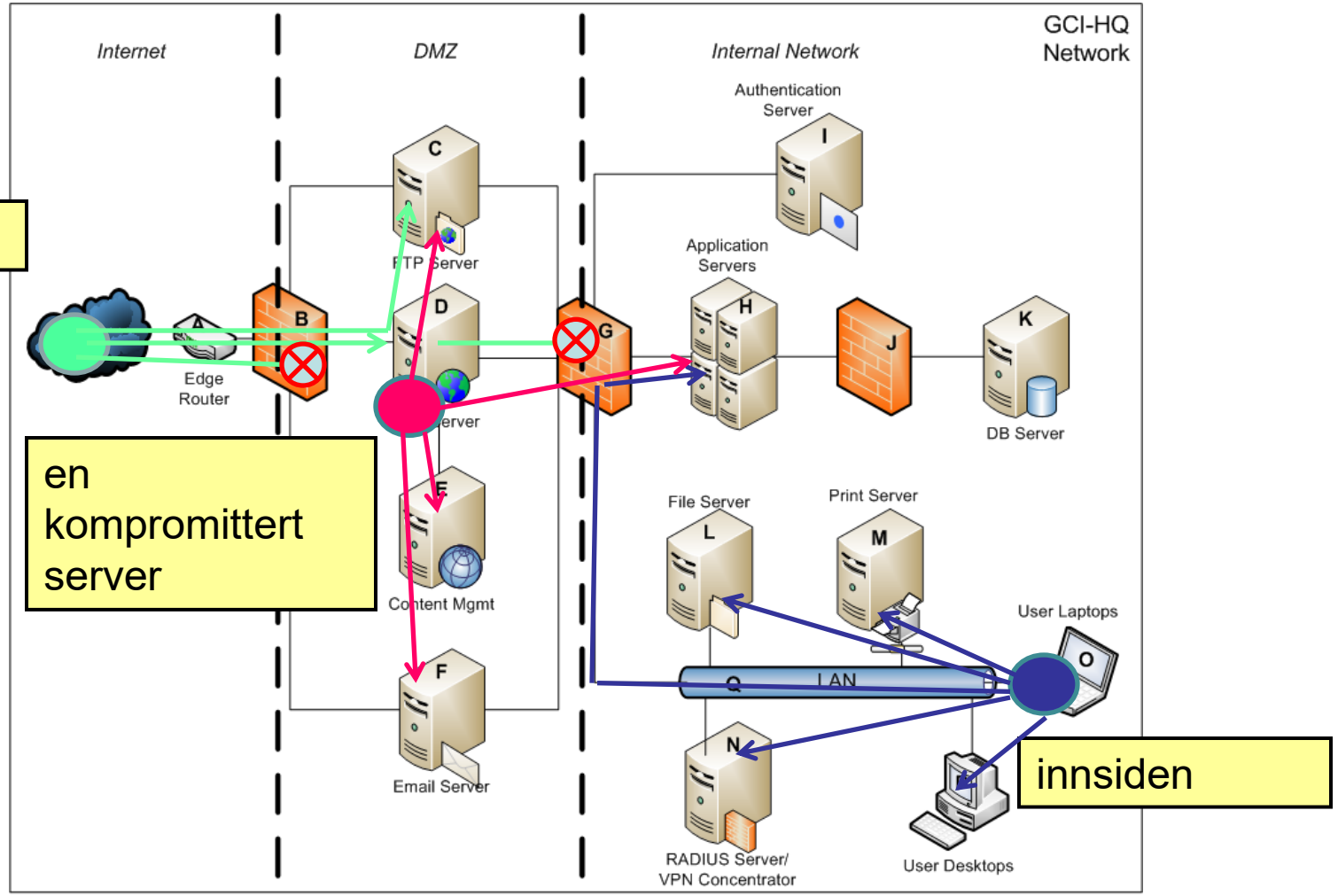
- Kartlegg nettet ved hjelp av portscanner
  - nmap «Network Mapper»
  - Kan gjøres i powershell eller andre språk

- Hvilke maskiner og enheter finnes på hvilke ipadresser
  - Og hvilke tjenester kjører på hvilke porter
    - Husk at portnummer kan «lyve»
      - Man kan kjøre tjenester på ikke-standard porter

Hvor bør man kartlegge fra?

utsiden

en kompromittert server



innsiden

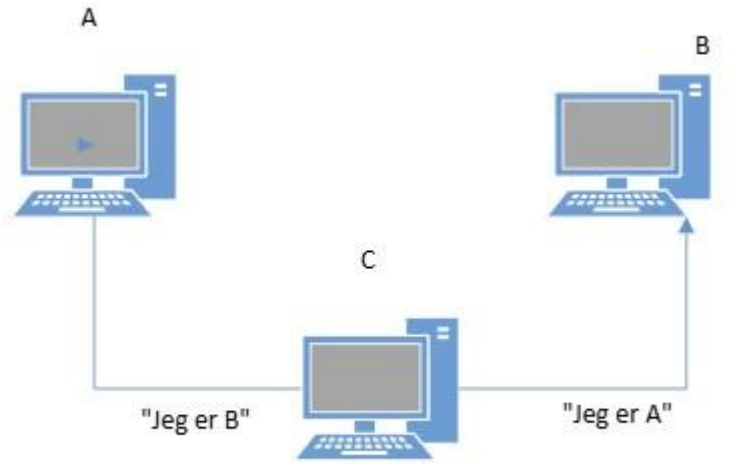
Bli kjent med systemet

- Lytte etter trafikk på nettet
  - Kan gi mye kjennskap til nettverket
  - Tcpdump
  - Wireshark

- *«The quieter you become, the more you are able to hear”*
  - Baba Ram Dass

“Man in the middle” (MiTM)

- Angriper setter seg mellom maskiner
  - Avlytter trafikk
  - Downgradeangrep

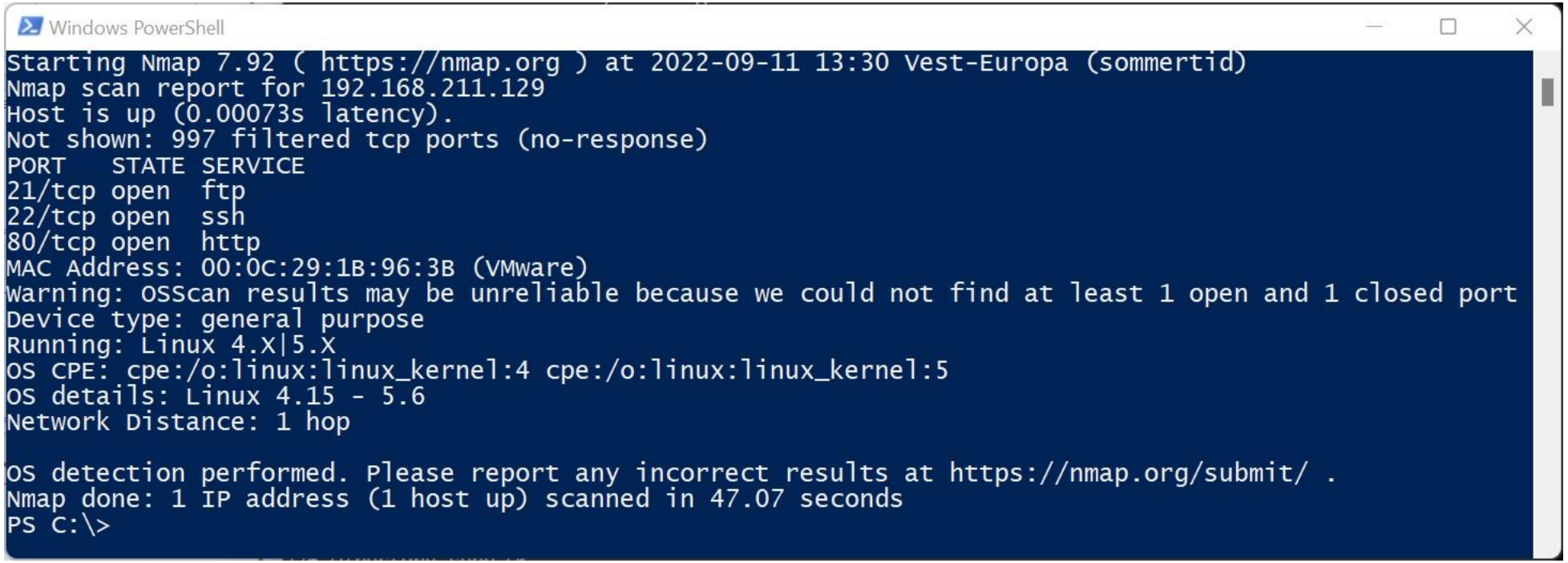


Direkte angrep

- Direkte angrep mot usikrede IoT-enheter (Internet of Things)

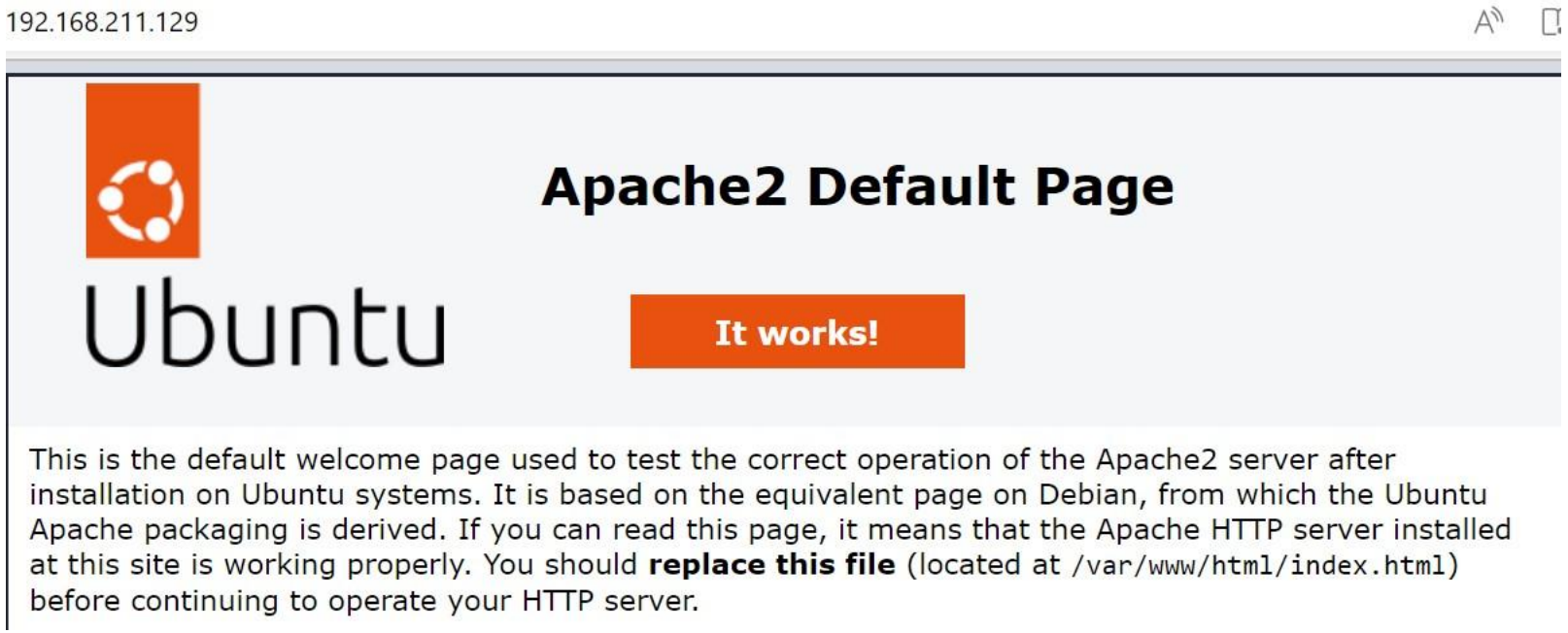
- SQL-injection
- Command injection

Let etter muligheter i tilgjengelige tjenester



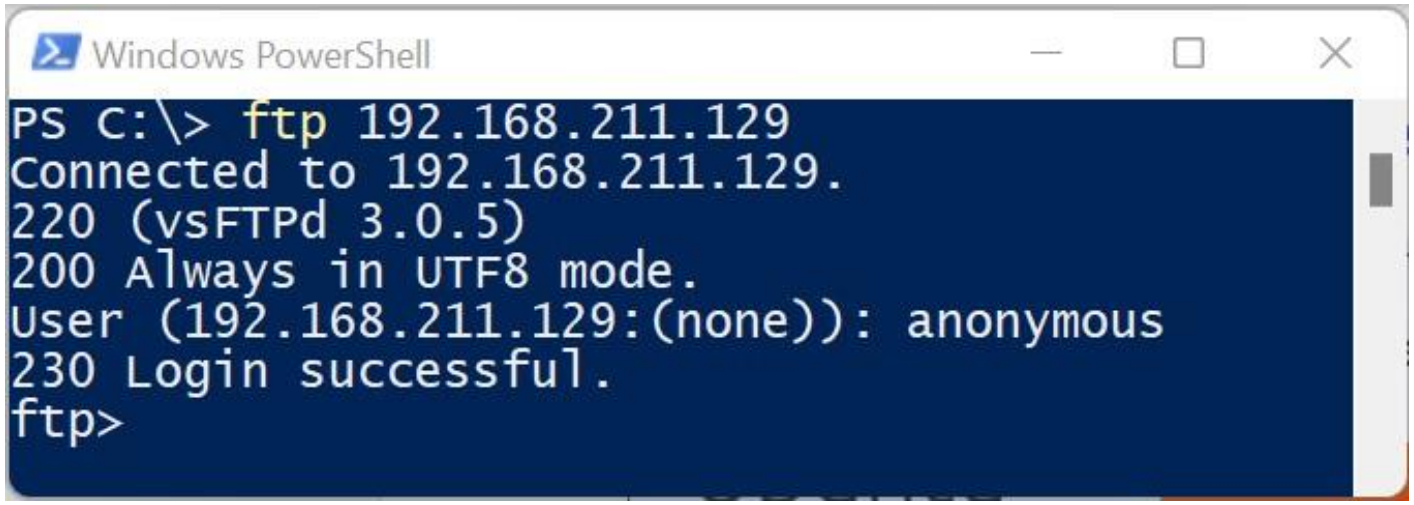
- Besøk tjenester
  - Se hva de tilbyr

Let etter muligheter i tilgjengelige tjenester



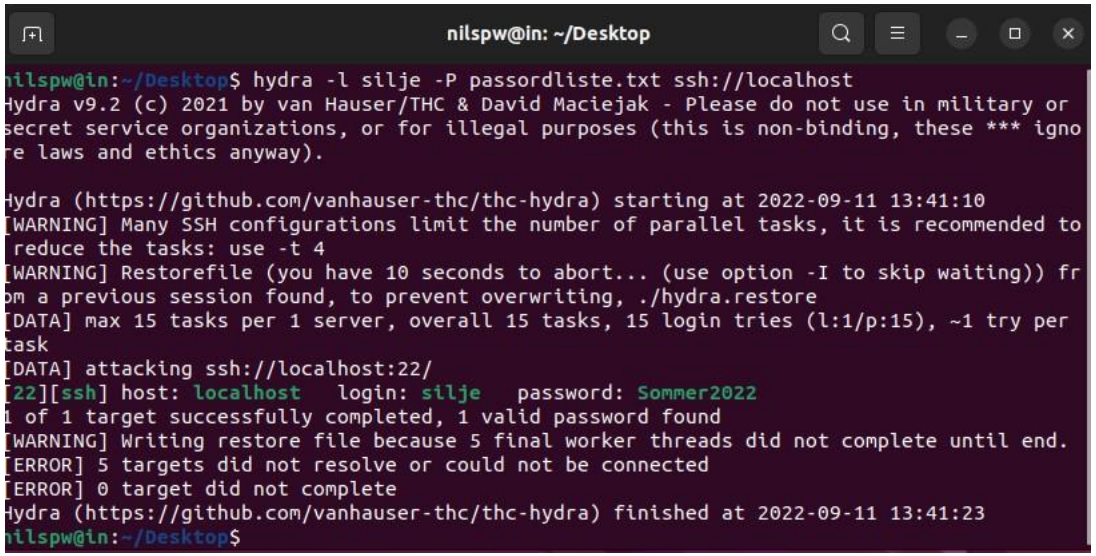
- Standard installasjonsside
  - Maskinen er antakelig ikke ferdig oppsatt

Let etter muligheter i tilgjengelige tjenester



- Kan logge inn på ftp
  - Anonymous pålogging til ftp krever ikke passord
  - Kan finne interessante filer

Let etter muligheter i tilgjengelige tjenester



- Prøver en ordliste med vanlige passord med programmet Hydra
  - (Kan også bruteforce oss frem til brukernavn)
  - Får innlogging
  - Dette kan også gjøres i vanlig AD (Active Directory) i Windows

Passordspraying

- Prøver enkeltpassord mot alle, eller utvalgte brukere
  - Net user /domain (for Windows)
  - Sjekk /etc/passwd (Linux – lesbar for alle)

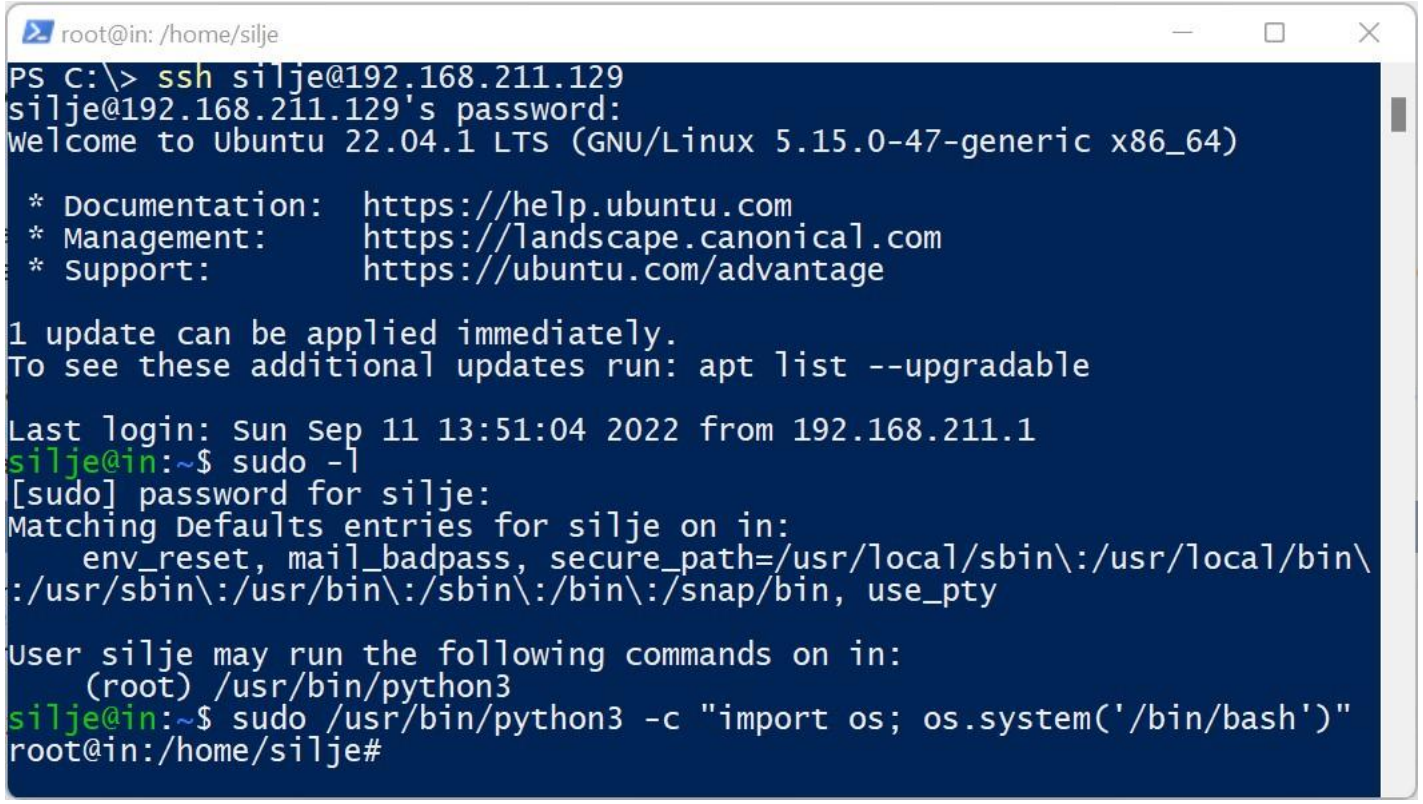
- Prøver å logge på med samme passordet mot alle brukere
  - NB: Dette kan veldig fort låse brukere ute!
    - SJEKK passordpolicy før du gjør dette
    - SJEKK med egen bruker først! (og ligg alltid minst ett gjett før med egen bruker)
  - Brukes til å finne svake passord

- Fungerer overaskende bra

Bruk det du har

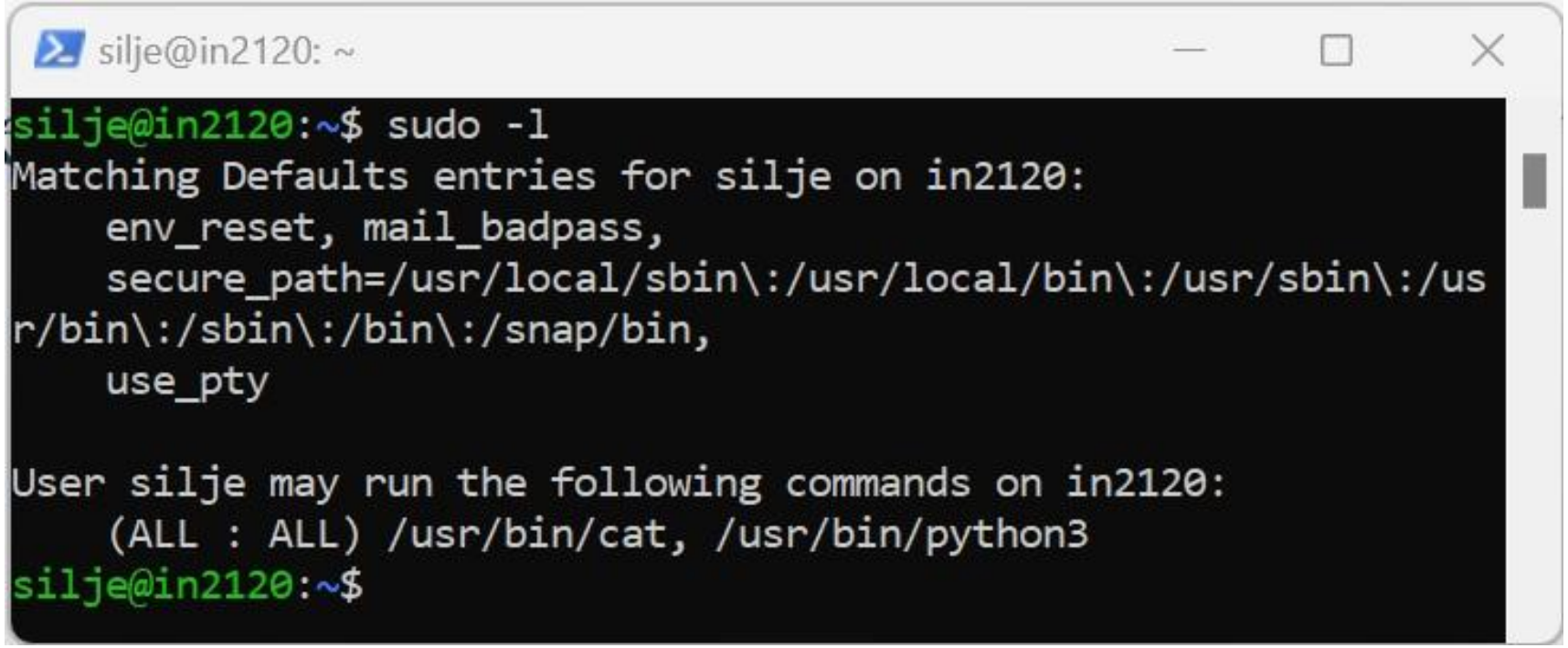
- «Live off the land»
  - Bruk det som er tilgjengelig i systemet
  - Powershell
  - Python
  - Driftsverktøy

Bruk det du har - Sudo



- Logg inn med ssh
  - Sjekk rettigheter
  - Få root

Bruk det du har del to

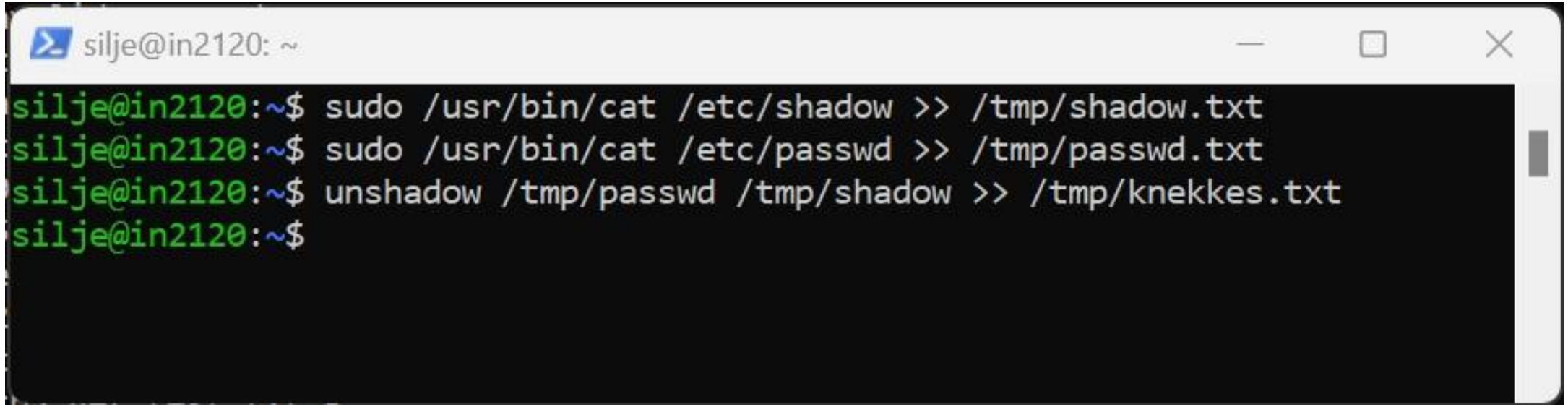


- cat
  - /usr/bin/cat .. <- Verktøy for å lese filer

Hva kan bruke cat til som root?

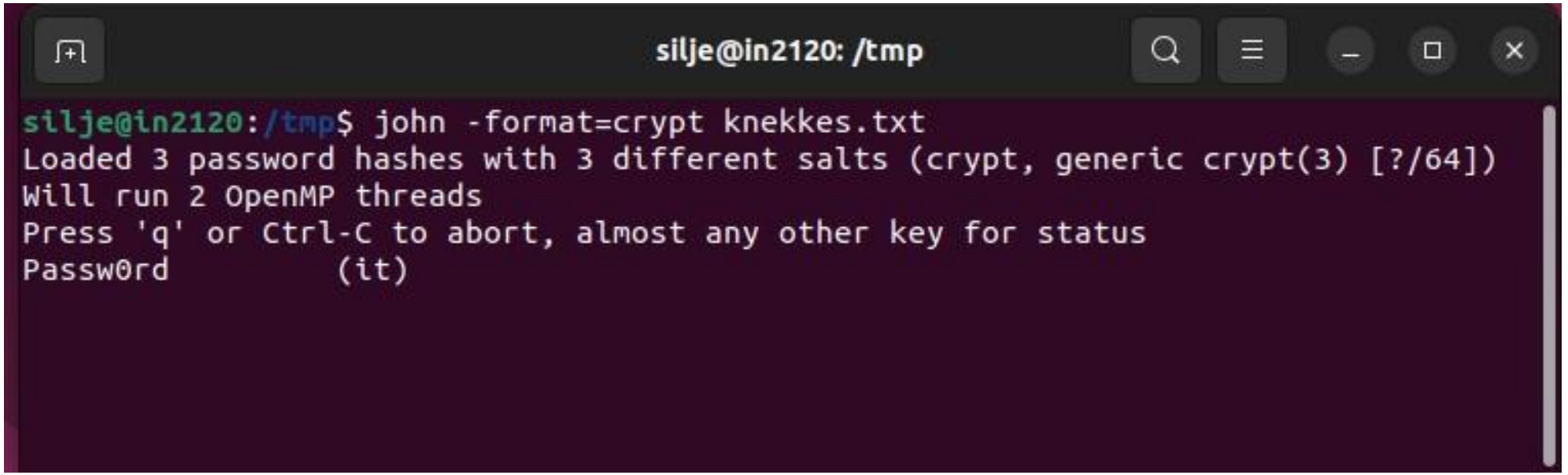
- Man kan lese alle filer
  - Let etter sensitive filer
    - Passord
    - SSH-nøkler
    - Konfigurasjonsfiler

Privesc med cat



- Hente ut passordhashene
  - Shadow krever root, passwd er lesbar for alle
- Forberede passordknekking

Knekk passord



- Forskjellige brukere kan ha ulike tilganger
  - Logg inn og sjekk hvilke tilganger brukeren har

Passordknekking - programmer

- John the ripper
  - Raskest på uttømmende søk
  - Enklest å bruke
- Hashcat
  - Klart best på regelbasert passordknekking
    - Eksempelvis maskeangrep (slide 55)
  - Mer komplisert, men gir større kontroll

Hva er et godt passord?

- Har tilstrekkelig entropi (uorden)
- Tilstrekkelig lengde
- Noe som betyr noe for DEG
- Noe du kan huske

- J,vedlsdsf,fvovmd1000h.

«J,vedlsdsf,fvovmd1000h.»???

- Ja, vi elsker dette landet som det stiger frem, furet værbitt over vannet med de 1000 hjem.



Passorddumping

- Hente ut klartekst- og passordhasher
  fra alle maskiner

- Verktøy:
  - Mimikatz
  - Kiwi (Metasploit)

- Krever debug /adminrettigheter

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
...
```

Pass the hash

- Passordhasher kan gjenbrukes
  - ‘Pass the hash’ – logge på med selve hashen, ikke passord
    - Derfor man ikke skal gjenbruke selv gode passord!
- Kan bla. gjøres med
  - Impacket
  - psexec

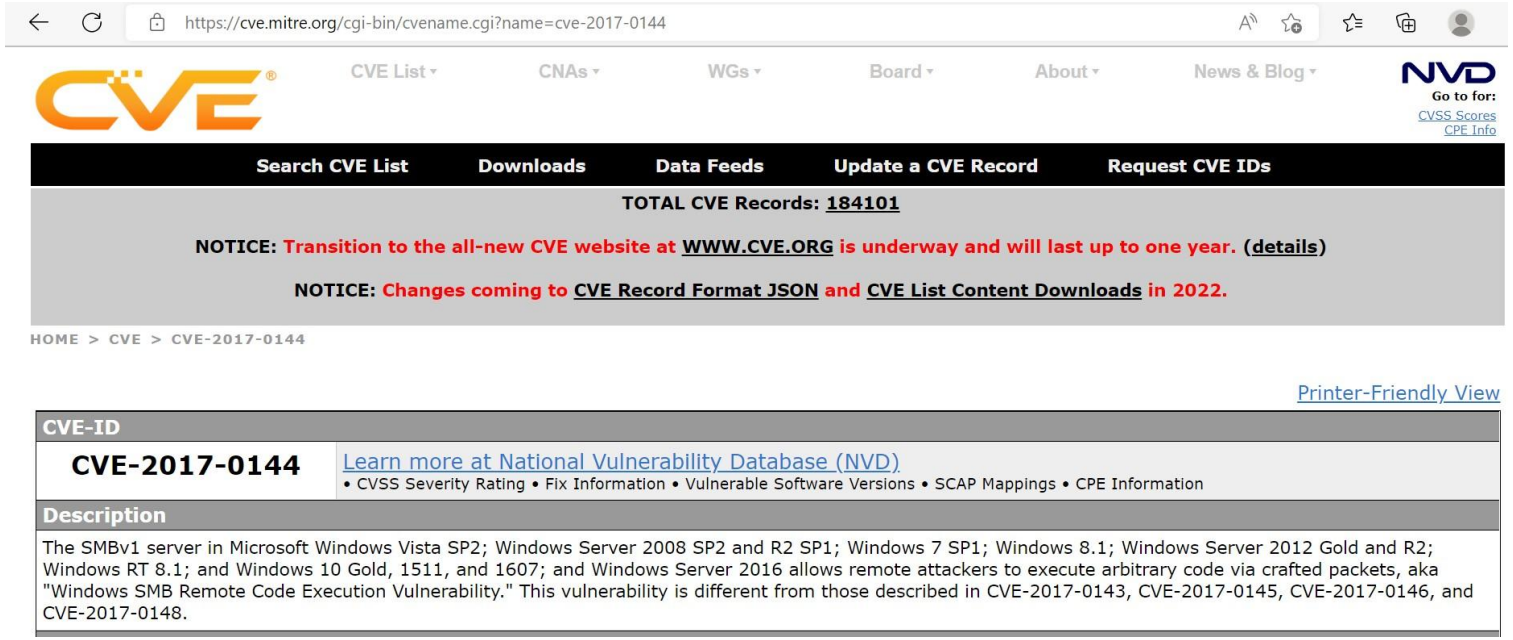
Lateral movement (sideveis bevegelse)

- Utnyttelse av sårbarheter gir økt sannsynlighet for driftsforstyrrelser
  - Man ønsker følgelig ikke å kjøre flere exploits enn nødvendig

- I stedet beveger man seg rundt i nettet fra maskin til maskin
  - Gjenbruker brukernavn og passord eller tilganger i AD (Active Directory) eller gruppemedlemskap i linux

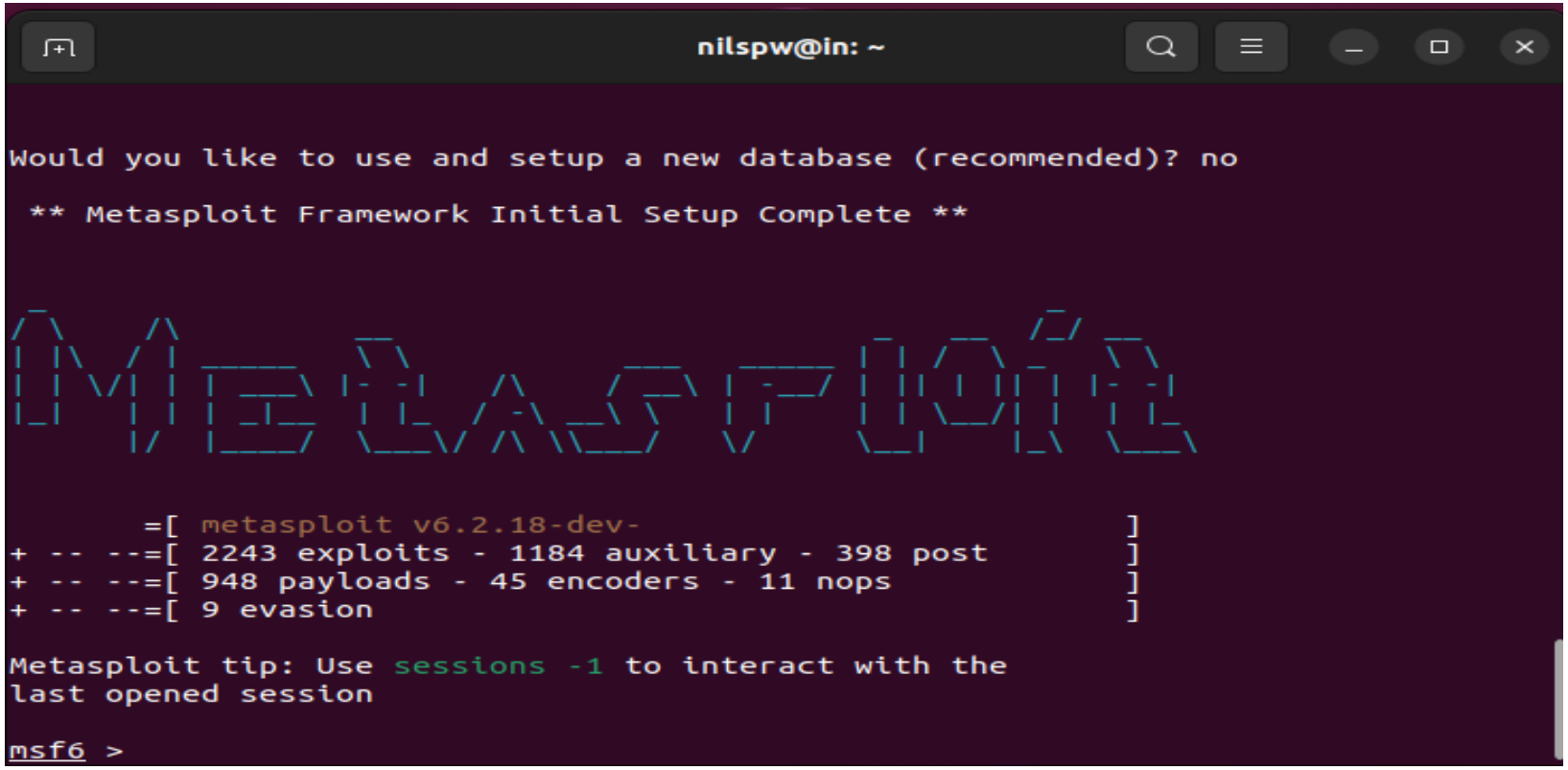
Let etter sårbarheter

- Kartlegge sårbarheter
  - I kurset benytter man sårbarhetskartleggeren OpenVAS (men nessus er mest kjent)
  - Hente ut versjonsnummer
    - Let på nettet etter sårbarheter i den aktuelle versjonen



Utnytt sårbarheter

- Rammeverk for utnyttelse av sårbarheter - metasploit
- Finnes flere, men dette er mest kjent (og gratis)



“What if”

- En systemutvikler tenker: «Hva vil jeg få til, hva vil kunden?»
- Pentesteren tenker: «Jaha, dette er hva DE vil, men.. What if»
  - Finnes det alternative veier?
  - Hva skjer hvis…

Hva skjer hvis…

- Adgangskontroll slipper alle ut uten kort?



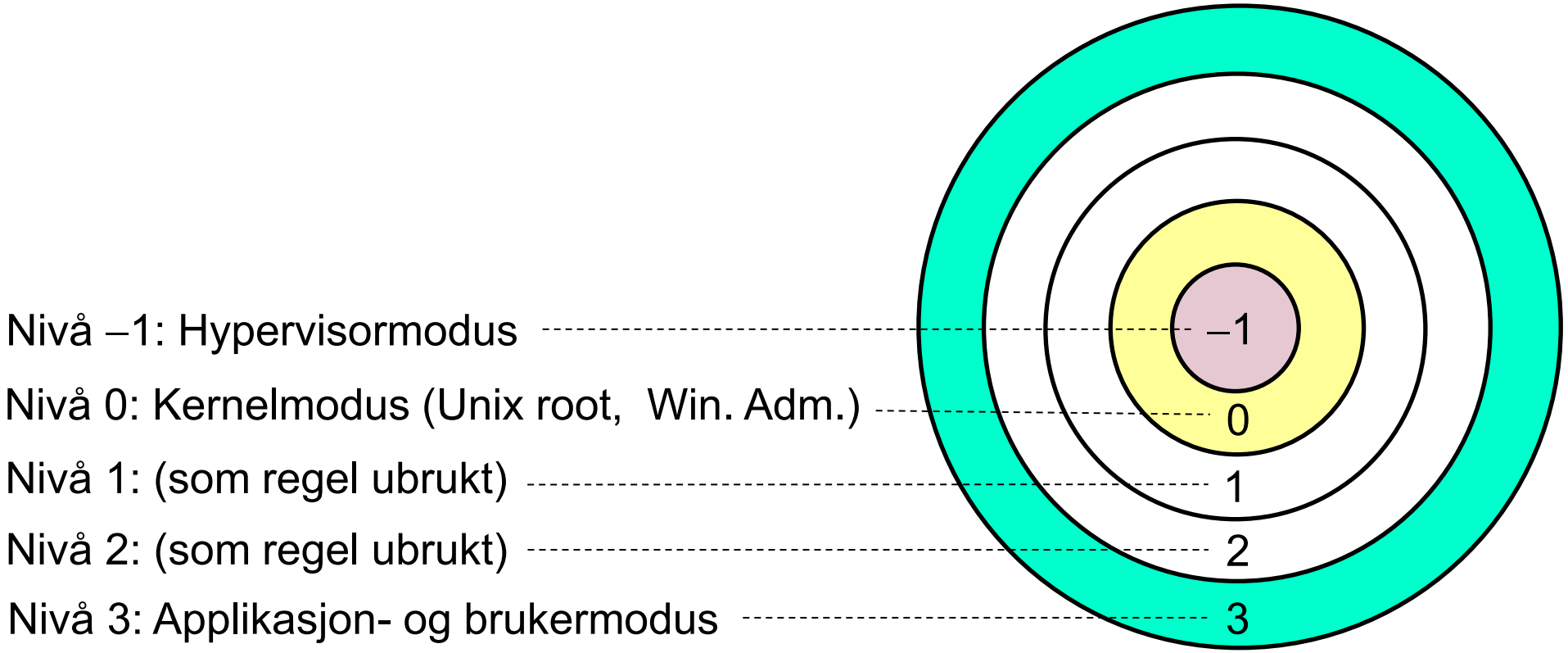
Fuzzing

- Nettside ber om fullt ellevesifferet personnummer
  - Hva med 0?
  - Hva med ett tegn?
  - Hva med en million tegn?
  - Dette kalles fuzzing

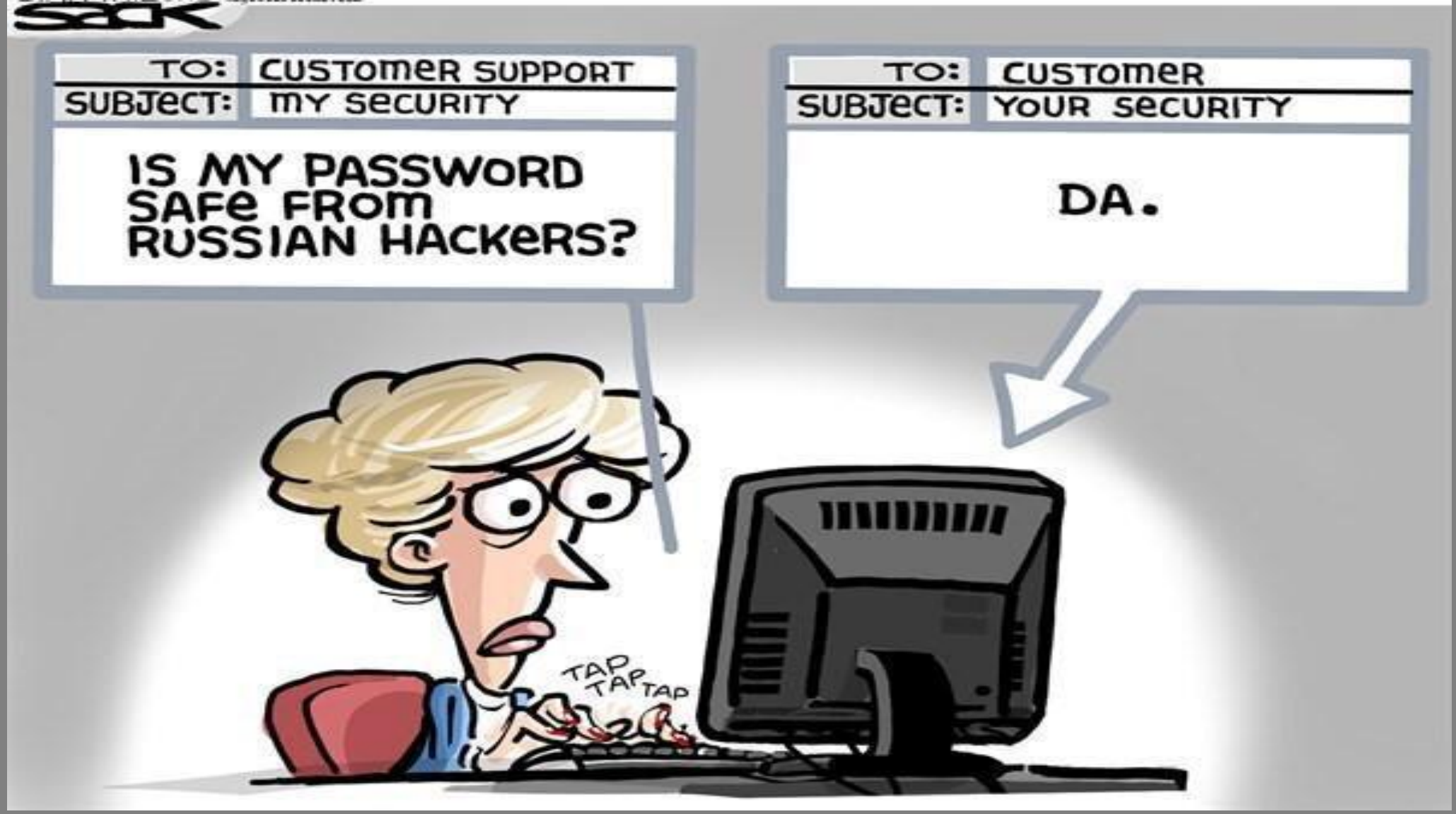
- Fuzzing kan beskrives som jakt på feilmeldinger
  - Fuzzing er enkleste, og eneste praktiske måten å finne buffer overflow-feil
  - For lokale programmer brukes en debugger
    - Ønsker å få en gitt tekst inn i returpekeren (EIP)

Angrep på virtualisert infrastruktur

- «Den som kommer lavest i stacken vinner alltid» - Dave Shackleford
- Stol med andre ord aldri mer på en vm enn hostmaskinen den kjører på



Passord


TO: CUSTOMER SUPPORT
SUBJECT: MY SECURITY
IS MY PASSWORD SAFE FROM RUSSIAN HACKERS?
TO: CUSTOMER
SUBJECT: YOUR SECURITY
DA.
TAP TAP TAP

Passordknekking

26 store bokstaver (engelsk), 26 små, 10 tall, 33 spesialtegn -> 95

Dette gir en teoretisk kompleksitet på 95^antallTegn

10 tegn: 95^10 / (28*10^9 * 60sek*60min*24timer*365,25) = ca 68 år

Så da bør vel 10 tegn være mer enn nok?

(NB dette er uttømmende søk – gjennomsnittlig tid er halvparten ((1+N)/2))

Passordsikkerhet

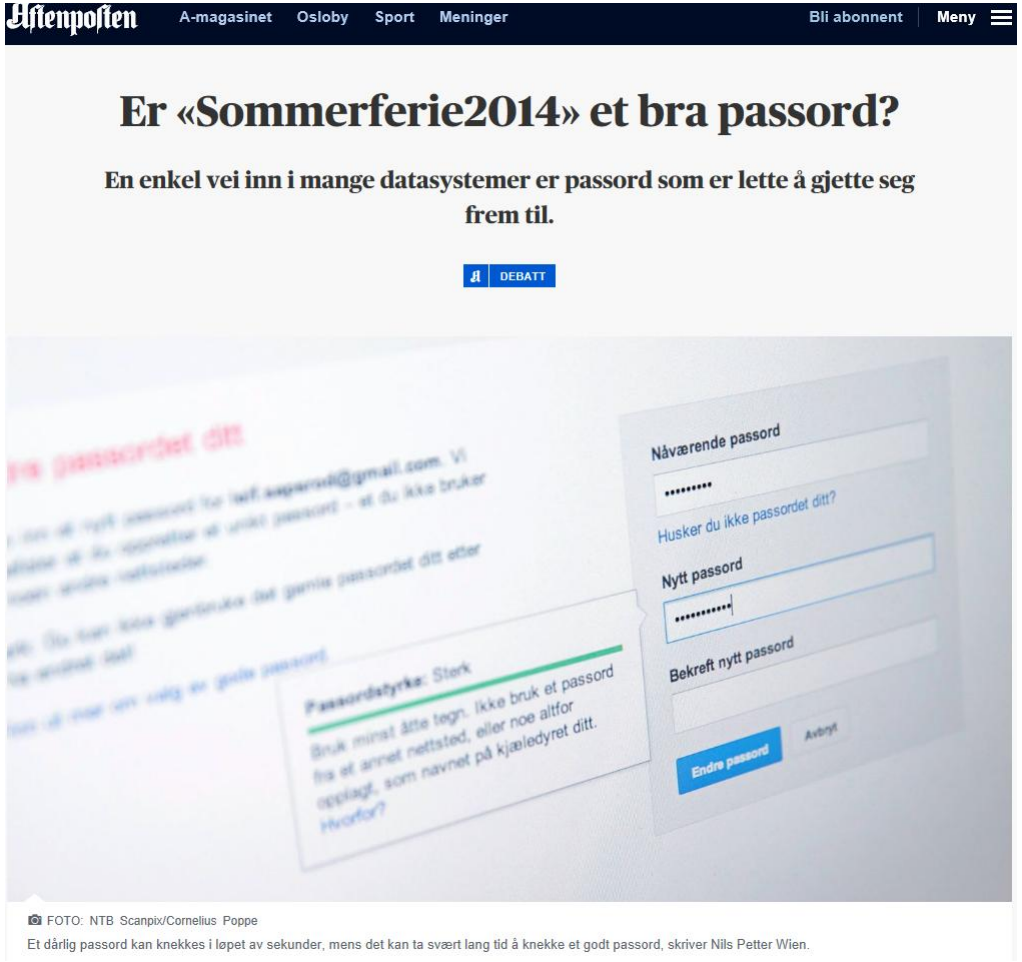
- 10 tegn: 95^10 / (14*10^9 * 60sek*60min*24timer*365,25) = ca 68 år
  - Så da bør vel 10 tegn være mer enn nok?

- Folk er enkle
  - Passord begynner med stor forbokstav, inneholder 6 små bokstaver, 2 tall og så ett spesialtegn (typisk !)
  - Så i praksis..
  - (26^7*10^2*1) / (28*10^9) = ca 29 sekunder..

Og det er med vilkårlige tegn

- I praksis brukes hybride angrep (kombinasjoner av et fast ord)
  - Eksempelvis SommerXXXX

- Og hvorfor maser jeg sånn om sommer?

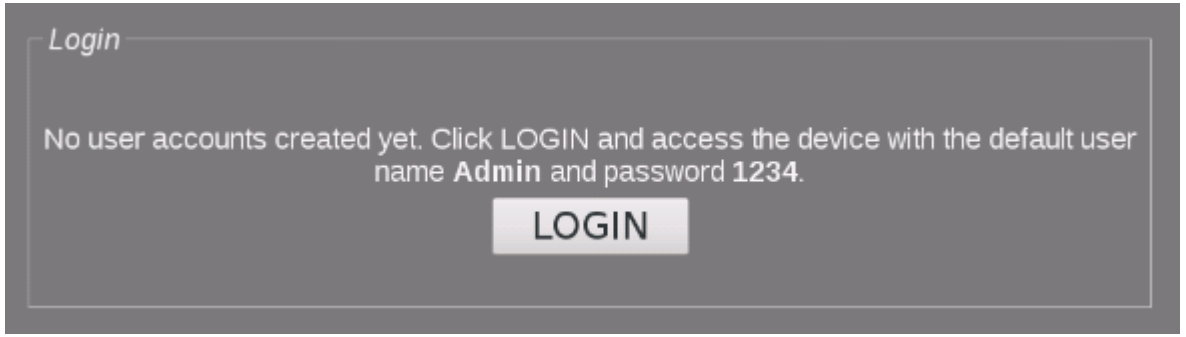


Passordsikkerhet

- Folk er enkle
  - «NavnPåBarnAlder»
  - «VirksomhetsnavnÅr»
  - «Hvavirksomhetenjobbermed»
  - «ÅrstidÅr»
  - «StedDeHarHytteÅR»
- Stadig passord på avveie
  - Rockyou – mest kjent
  - Passordbreach 2017

Passordsikkerhet

- Utstrakt bruk av utstyr med standard brukernavn og passord
  - Nettverksutstyr
  - Printere
  - Tjenester
  - IP-kameraer



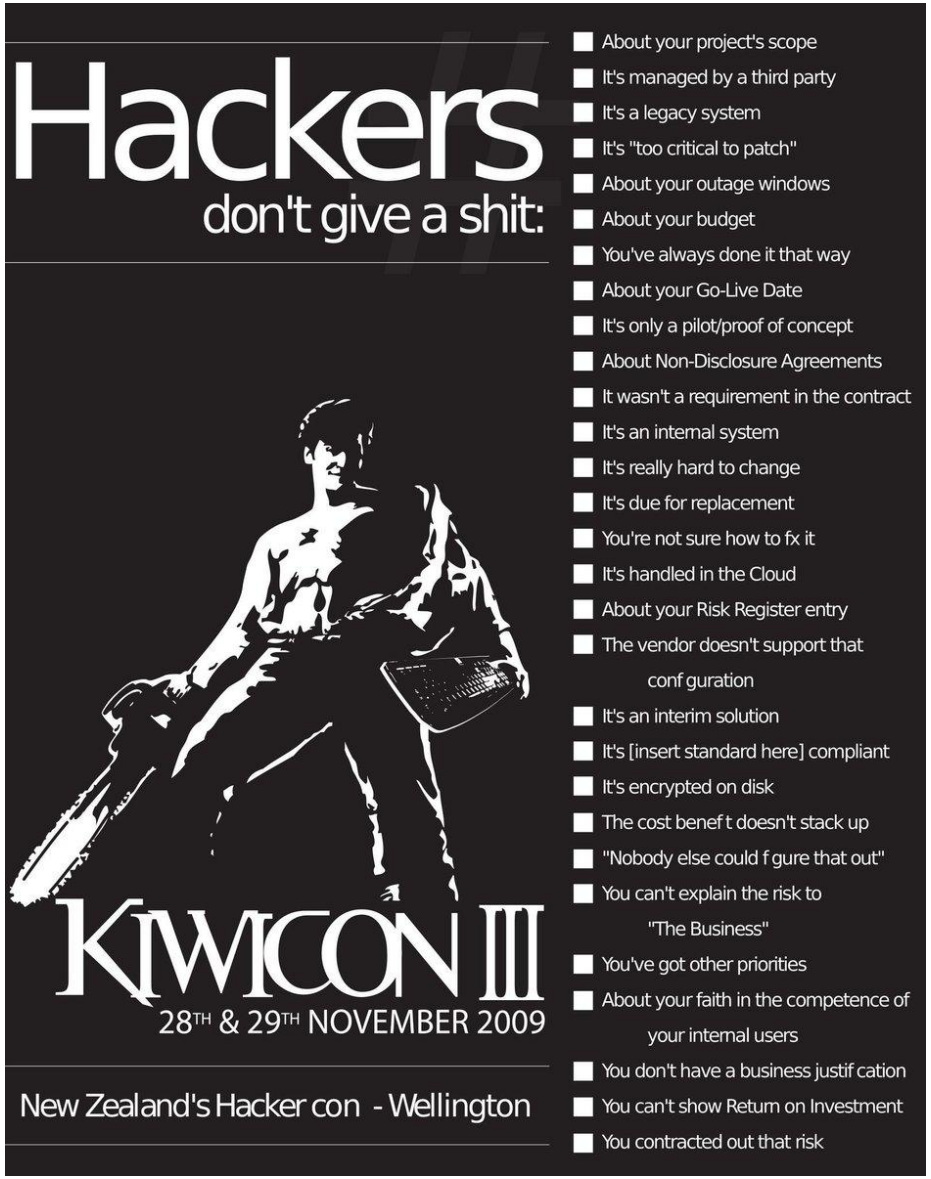
- Passord som kan googles/binges er alltid bra…
  - Som regel har disse også høye rettigheter
- Mange ellers godt sikre systemer faller på dårlig passordsikkerhet

Gevinst

- Vis hvilke kjerneverdier du har klart å ramme:
  - Uautorisert tilgang?
    - Vis eller endre filer
  - Hvis virksomheten er redd for at du får data ut
    - Vis at du får (usensitive) data ut
    - Sideveiskanaler
      - DNS-oppslag
      - Blinkende lys
      - Viftestøy

Test systemene deres




Hackers
don't give a shit:
About your project's scope
It's managed by a third party
It's a legacy system
It's "too critical to patch"
About your outage windows
About your budget
You've always done it that way
About your Go-Live Date
It's only a pilot/proof of concept
About Non-Disclosure Agreements
It wasn't a requirement in the contract
It's an internal system
It's really hard to change
It's due for replacement
You're not sure how to fx it
It's handled in the Cloud
About your Risk Register entry
The vendor doesn't support that conf guration
It's an interim solution
It's [insert standard here] compliant
It's encrypted on disk
The cost benef t doesn't stack up
"Nobody else could f gure that out"
You can't explain the risk to "The Business"
You've got other priorities
About your faith in the competence of your internal users
You don't have a business justif cation
You can't show Return on Investment
You contracted out that risk
KIWICON III
28TH & 29TH NOVEMBER 2009
New Zealand's Hacker con - Wellington

Avsluttende visdomsord



Bilde: Gudmund Grov