



Denne forelesningsøkten vil bli tatt opp og lagt ut i emnet i etterkant.

Hvis du ikke vil være med på opptaket:

 Start Video	La være å delta med webkameraet ditt.
 Unmute	La være å delta med mikrofonen din.
To: <span>Marianne Sundby</span> (Privately) Type message here...	Still spørsmål i Chat i stedet for som lyd. Hvis du ønsker kan spørsmålet også sendes privat til foreleser.



Høyskolen  
Kristiania

# TK2100: Informasjonsikkerhet

Åttende forelesning:  
Modeller, standarder, lover  
og  
penetrasjonstesting

## Pensum:

Forelesningen

Nätt & Heide, kapittel 1

Nätt & Heide, kapittel 9

Nätt & Heide, kapittel 14

- CIA
- Kryptering
  - Symmetrisk (AES) vs Public Key (RSA)
  - Blokk (AES) vs strøm (RC4)
- Operativsystem
  - Sikring av prosess, minne, filsystem
  - Autentisering og autorisering + ACL
  - Bufferoverflows og «zero day attacks»
- Malware
  - Bakdører, logikkbomber; Virus, ormer og trojanere
  - Zero-day angrep; Rootkit; Botnet
  - Antivirus

- Browseren («nettleseren») og sikkerhet på WWW
  - (dynamisk) HTML, HTTP, HTTP over TLS (https)
  - Sesjoner og cookies
- Angrep på klient
  - Sesjonskidnapping
  - Phishing, klick-hijacking
  - Media, addons og plugins
  - XSS og CSRF
- Angrep på tjener
  - Scripting og svakheter
  - SQL injisering
- Forsvar

- Trusler på Link- & nettverks-  
laget
  - ARP-spoofing og –cache-  
poisoning
  - IP: IP-spoofing
  - ICMP: Smurfe-angrep
- Trusler på Transportlaget
  - TCP: SYN-flood, optimistisk ACK  
angrep («metningskontroll»-  
basert); sesjons-kidnapping
- Hovedsakelig ulike former for  
DoS
- Applikasjonslaget
  - DNS, DNS-spoofing, DNSSEC
- Brannmurer
  - Typer og tekniker (policies/regler)
- Tunneling
  - IPSec og VPN
- Intrusion Detection  
(«innbruddsalarmer»)
- Nmap og portscanning

- Stoff som er mest aktuelt for bedrifter og utviklere
  - Vi må kjenne til det, men de fleste kommer ikke til å ha «nytte av det i det daglige»
  - Alle som skal jobbe med sikkerhet vil ha et forhold til dette 😊
- Wireshark og sniffing
- Rammeverk og retningslinjer for systemer
- Formelle tilgangskontroll-modeller
- Standarder og revisjon
- Teknikker for sårbarhetsvurdering (etisk hacking)
- *(Internet of Things er flyttet til forelesning 9)*

# WIRESHARK

**HVA ER LOVLIG?  
HVA ER STRAFFBART?  
HVOR STRENGE ER STRAFFENE?**



# Datakriminalitet

- I følge Kripos så er de typiske formene for datakriminalitet:
  - datainnbrudd
  - databedrageri
  - informasjonssheleri
  - skadeverk
  - dokumentfalsk
  - piratkopiering
  - beskyttelsesbrudd (TV- og radiosignaler)
- **Straffeloven av 2005** er strengere og har erstattet den gamle fra 1902, den er mer konkret om flere typer «dataforbrytelser»

# Straffeloven § 145

§ 145. Den som uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer, straffes med bøter eller med fengsel inntil 6 måneder eller begge deler.

Det samme gjelder den som **uberettiget skaffer seg adgang til data eller programutrustning** som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler.

Voldes skade ved erverv eller bruk av slik uberettiget kunnskap, eller er forbrytelsen forøvet i hensikt å skaffe noen en uberettiget vinning, kan fengsel inntil 2 år anvendes.

Medvirkning straffes på samme måte.

Offentlig påtale finner bare sted når allmenne hensyn krever det.

Endret ved lover 16 feb 1979 nr. 3, 12 juni 1987 nr. 54, 8 apr 2005 nr. 16.

# Straffeloven § 145b

§ 145b. Den som uberettiget gjør tilgjengelig for andre **passord** eller andre data som kan gi **tilgang til et datasystem**, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler.

Grov spredning av tilgangsdata straffes med fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, skal det særlig legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade.

Medvirkning straffes på samme måte.

Tilføyd ved lov 8 apr 2005 nr. 16.

# Ulovlig bruk av datakraft ( § 261)

- Ikke eksplisitt nevnt datamaskiner men det er denne paragrafen som benyttes

**§ 261.** Den som rettsstridig bruker eller forføyer over en løsøregegenstand som tilhører en annen, og derved skaffer seg eller andre betydelig vinning eller påfører den berettigede betydelig tap, straffes med fengsel inntil 3 år. Medvirkning straffes på samme måte. Under særdeles formildende omstendigheter kan bøter anvendes.

Offentlig påtale finner ikke sted uten fornærmedes begjæring med mindre allmenne hensyn krever påtale.

Opphevet ved lov 11 mai 1951 nr. 2, tilføyd ved lov 12 juni 1987 nr. 54.

# Beskyttelsesbrudd

§ 262. Den som

- a) i vinnings hensikt framstiller, innfører, distribuerer, selger, leier ut, besitter, installerer, vedlikeholder eller skifter ut **dekodingsinnretning**,
  - b) i vinnings hensikt annonserer eller på annen måte reklamerer for dekodingsinnretning, eller
  - c) søker å utbre dekodingsinnretning
- når hensikten er å skaffe noen uautorisert tilgang til en vernet tjeneste, eller medvirker til dette, straffes med bøter eller fengsel inntil 1 år.

Den som ved bruk av dekodingsinnretning påfører den berettigede et tap eller skaffer seg selv eller andre en vinning ved å få uautorisert tilgang til en vernet tjeneste, straffes med bøter eller fengsel inntil 6 måneder.

Med dekodingsinnretning menes i denne paragraf ethvert hjelpemiddel, enten dette er teknisk utstyr eller programvare, som er utformet eller tilpasset, alene eller sammen med andre hjelpemidler, for å gi tilgang i forståelig form til en vernet tjeneste.

Med vernet tjeneste menes i denne paragraf

- a) fjernsyns- og radiosignaler, og
- b) **tjenester som teleformidles elektronisk på forespørsel fra den enkelte tjenestemottaker, når tilgang i forståelig form er avhengig av tillatelse fra tjenesteyter og ytes mot betaling, eller selve tilgangskontrollen til tjenestene nevnt i a og b, når den må regnes som en egen tjeneste.**

Offentlig påtale finner ikke sted uten fornærmedes begjæring med mindre allmenne hensyn krever påtale. Som fornærmet regnes også den som yter tilgangskontroll når denne må regnes som en egen tjeneste.

# Virus, trojanere m.m.

§ 291. For skadeverk straffes den som rettstridig ødelegger, skader, gjør ubrukelig eller forspiller en gjenstand som helt eller delvis tilhører en annen.

Straffen for skadeverk er bøter eller fengsel inntil 1 år. Medvirkning straffes på samme måte.

Offentlig påtale finner ikke sted uten fornærmedes begjæring, medmindre almene hensyn krever påtale.

Endret ved lov 11 mai 1951 nr. 2.

§ 292. Grovt skadeverk straffes med bøter eller med fengsel inntil 6 år. Medvirkning straffes på samme måte.

Ved avgjørelsen av om skadeverket er grovt skal det særlig legges vekt på om skaden er betydelig, om den skyldige vitende har voldt velferdstap eller fare for noens liv eller helbred, om handlingen er rasistisk motivert, om det er voldt avbrekk i den offentlige samferdsel, om skaden er øvd på grenseskjel mot naborike eller mot offentlig minnesmerke, samlinger eller andre gjenstander som er bestemt til alminnelig nytte eller pryð eller som for almenheten eller en større krets har historisk, nasjonal eller religiøs verdi.

Endret ved lover 11 mai 1951 nr. 2, 7 apr 1995 nr. 15, 23 jan 1998 nr. 9 (ikr. 1 feb 1998 iflg. res. 23 jan 1998 nr. 72).

§ 201. Med bot eller fengsel inntil 1 år straffes den som (...) uten forsett om å begå en straffbar handling besitter et selvspredende dataprogram, og besittelsen skyldes uberettiget fremstilling eller anskaffelse av programmet

Tilføyd ved lov 19 juni 2009 nr. 74.

# Offentlige anlegg

§ 151b. Den som ved å ødelegge, skade eller sette ut av virksomhet **informasjonssamling** eller anlegg for energiforsyning, kringkasting, elektronisk kommunikasjon eller samferdsel volder omfattende forstyrrelse i den offentlige forvaltning eller i samfunnslivet for øvrig, straffes med fengsel inntil 10 år.

Uaktsomme handlinger som nevnt i første ledd straffes med bøter eller med fengsel inntil 1 år.

Medvirkning straffes på samme måte.

Tilføyd ved lov 12 juni 1987 nr. 54, endret ved lov 4 juli 2003 nr. 83 (ikr. 25 juli 2003 iflg. res. 4 juli 2003 nr. 879).

- Hvorfor bruker man wireshark?
  - Lese nettverksdata til andre maskiner
  - Passord som er sendt i klartekst
  - Oppdage svakheter i kommunikasjonsprotokoller som kan gi angriperen tilgang (uten å vite passordet til tjenesten)
  - **Straffeloven §145 og §262**
- Portscanning med nmap?
  - Oppdage svakheter i utdatert programvare
  - Potensiell tilgang til «ubeskyttede data»
  - **Straffeloven §145**
- Bruke kali linux?
  - «med forsett om å begå en straffbar handling (...) besitter (...) dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem»
  - **Straffeloven §201**



# Wireshark, nmap, og hacker verktøy

---

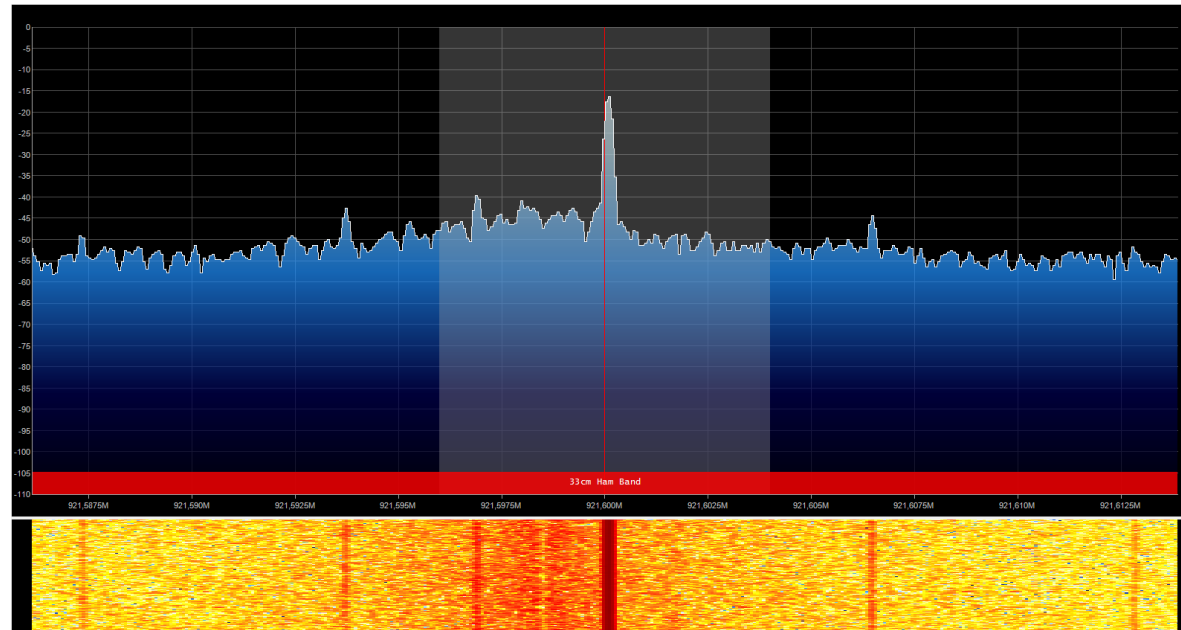
- Ikke bruk **Wireshark**, **nmap** eller andre sikkerhets-verktøy dersom du ikke har fått **eksplisitt tillatelse** til det!
- Privat kan du kun bruke dem i ditt eget nettverk, og kun for administrative formål

Jeg vil ikke anbefale noen av dere å gjøre det, men Norman (anti-virus selskapet) ble dømt for brudd på straffeloven § 145 for å ha forsøkt å skaffe seg tilgang til Universitetet i Oslo sine datasystemer – under et innslag på Dagsrevyen for å sette lys på sikkerhet.

- Norman ble frifunnet i Høyesterett...
  - <http://itavisen.no/1998/12/17/norman-vant-i-hoyesterett/>
  - Kjent som “portscan-dommen” (Rt. 1998 s 1971)
- Loven er endret, ikke sikkert man blir frikjent for det samme i dag

# Hva mer kan man lytte på?

- Radiosignaler
- Kan bruke en SDR – Software Defined Radio
- Her er en mobil telefon sitt downlink signal:



# Policy, rammeverk og modeller

- Flere norske lover krever at offentlige etater og bedrifter har sikkerhetspolicy og system for å følge den opp
- Personopplysnings-loven og –forskriften
  - Datatilsynet
- Kredittilsynets IKT-forskrift
  - Gjelder alle som driver med finansielle tjenester
- Sikkerhetsloven
  - Nasjonal Sikkerhetsmyndighet
  - Offentlige etater og leverandører til disse

- En sikkerhetspolicy er et sett med regler som definerer og beskriver
- **Subjekter**
  - Hvem som samhandler med systemet: individer, roller, grupper
  - Ex: Navn (og tittel), bruker/administrator/angriper/gjest...
- **Objekter**
  - Informasjons- og behandlings-ressursene som policyen er laget for å beskytte og administrere
  - Ex: dokumenter, filer, databaser, servere, arbeidstasjoner, programvare
- **Handlinger**
  - Hva en subjekt kan og ikke kan gjøre med objektene
  - Ex: Lese/skrive dokument, installere software, bruke database,...
- **Tillatelser**
  - Oversikt over sammenhengen mellom subjekter, handlinger og objekter, som klart sier hvilke handlinger som tillatt og ikke.

- En **sikkerhetsmodell** er en abstraksjon som bidrar med begrepsapparatet som administratorer trenger for å spesifisere sikkerhetspolicy'er.
- Typisk et **hierarki** av **adgangs**- og **modifiserings**-rettigheter som lett kan tildeles subjekter i en organisasjon basert på posisjon.
- F.eks. Sikkerhetslovens (militære): «Strengt hemmelig», «hemmelig», «konfidensielt», «begrenset»

# Discretionary Access Control (**DAC**)

- **DAC** («skjønnsmessig») er adgangskontroll der brukerne selv gis mulighet til å bestemme hvilke tillatelser/begrensinger som skal gjelde for egne filer
  - Typisk basert på kategoriene enkeltbrukere og grupper
  - Gir brukere typisk mulighet til å gi tilgang til ressurser til andre brukere innenfor samme system
- F.eks. Windows for Workgroups, de fleste privatmaskiner ellers.



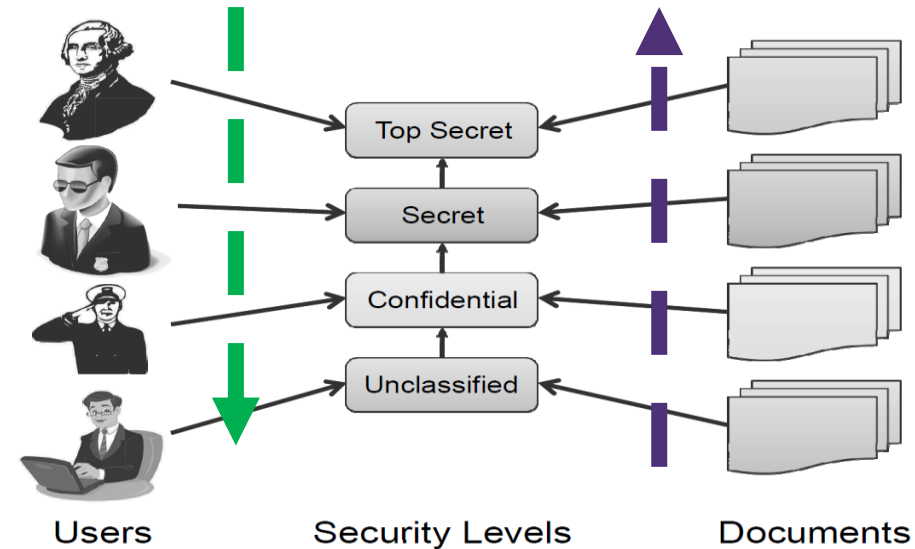
# Mandatory Access Control (**MAC**)

- **MAC** («tvungen») er mer restriktiv enn DAC og tillater ikke brukere å selv bestemme rettigheter på filer og ressurser. Alle sikkerhetsavgjørelser foretas av en sentral policy administrator
  - Hver sikkerhetsregel består av subjekt som vil ha adgang til et objekt og en liste som bestemmer hvem som har hvilke tilganger
- Ex
  - Security Enhanced Linux (SELinux)
  - OSX tilbyr og bruker default
  - Windows nettverk med Domene Controller (Active Directory)

- Ulike modeller utviklet for å **formalisere** mekanismene som beskytter konfidensialitet og integritet for (primært) dokumenter i datasystemer
  - **Bell-La Padula** (BLP)
  - **Biba**
  - Low-Watermark
  - Clark-Wilson model
  - Chinese Wall model (Brewer & Nash)
  - M.fl.
- Formalisere vil her si å gjøre det mulig å **bevise matematisk** at et system tilfredstiller en bestemt policy

# Bell-La Padula (BLP) modellen

- Klassisk tvungen adgangskontroll (MAC) modell for å beskytte **konfidensialitet**
- Basert på det **militære** flernivå sikkerhetsparadigmet for dokument-**klassifisering** og personell-**klarering**
- Strengt **lineær** orden av brukernivåer for dokumenter og adgang
- På norsk: Ugradert, begrenset, konfidensielt, hemmelig, strengt hemmelig  
(sivilt; fortrolig, strengt f.)



- En bruker kan **lese** alle dokumenter på eget klareringsnivå og under
- En bruker kan **ikke skrive** til lavere nivå («forhindre lekkasje»), men en bruker på lavere nivå kan skrive oppover...
- «Informasjonsendringer flyter bare oppover»

# BLP Problem: «covert channel»

- BLP har en stor svakhet...
- Forutsetter at vi (alltid) vet hvordan informasjonen er kodet...
- Hva om man lekker via andre (uforutsette/skjulte) kanaler?
  - Jf Øving om Steganografi
  - Andre muligheter?
    - Kode informasjonen i når filer er tilgjengelige og ikke?
    - Kode informasjonen i hvor mange ark du printer?
    - Osv

- Ligner på BLP, men skal beskytte **integritet** snarere enn konfidensialitet
- Integritetsnivåer defineres for brukere og objekter og beskriver pålitelighet.
  - Et dokument lagret på sentraladministrert server vil typisk ha høyere nivå enn en fil på en laptop
  - En mangårig ansatt høyere enn en nyansatt
- Reglene er de stikk motsatte av i BLP
  - Tillater ikke lesing fra lavere nivå eller skriving til høyere
  - «Informasjonsendringer skal bare flyte nedover»!

- «Dødvannssmerke» («low-watermark»)
  - Utvidelse av BiBa som tillater lesing på lavere nivå
  - Etter lesing *nedgraderes* klarering for *brukeren* til integritetsnivået til lest objekt.
- Clark-Wilson
  - Skal sikre **transaksjoner** snarere enn konfidensialitet/integritet på dokumenter
  - Spesifiserer regler for **invarianter** ( $\text{saldo2} = \text{saldo1} - \text{uttak}$ ), **sertifiseringsmetoder** for invarianter på transaksjoner, rolle-skiller, mm
- «Kinesiske mur»
  - Skal forhindre **interessekonflikter**, f.eks. for børsmeglere («inside-trading»).
  - Definerer **konflikt-klasser**, der bruker kun har tilgang til **en enkelt** ressurs innenfor klassen

# «Litt om» norske Lover og Forskrifter

For en fullstendig informasjon om lover og forskrifter i Norge vises det til  
<http://www.lovdata.no>

*Virksomheten leder har ansvar for å påse at regelverket overholdes og skal sørge for at krav til sikkerhet innarbeides i avtaler med partnere, leverandører og andre det utveksles informasjon med*



- Definerer ulike former for datakriminalitet og andre relaterte former for forbrytelser
- Straffeloven gir også strafferammene for lovbruddene
- Paragrafer i Straffeloven som kan relateres til datakriminalitet; 145, 151, 261, 262, 291, 292 (som beskrevet på tidligere slider), samt 192, 201, 204, 205, 361, 344, 371-374, 351 og 352
- [https://www.politi.no/rad\\_fra\\_politiet/datakriminalitet/](https://www.politi.no/rad_fra_politiet/datakriminalitet/)

- Etterforskes av Kripos, eller ved lokale datakriminalitetavdelinger på politikammer
  - datainnbrudd
  - databedrageri
  - informasjonsheleri
  - skadeverk
  - ulovlig bruk av datakraft
  - dokumentfalsk
  - piratkopiering
  - beskyttelsesbrudd - TV- og radiosignaler

- Lovens formål:
  - Legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets sikkerhet og andre vitale sikkerhetsinteresser
  - Ivareta den enkeltes sikkerhet
  - Trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste
- Opprettet Nasjonal Sikkerhetsmyndighet (NSM) i 2003
  - Inntil da Forsvarets Overkommando/Sikkerhetstaben
  - <http://www.nsm.stat.no>
- Tidligere NorCERT, nå NCSC – Nasjonalt Cybersikkerhetssenter, er ansvarlig for kontinuerlig overvåkning og sikring av datanettverk av nasjonal betydning
  - <https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/>

# Arkivloven av 1992 (1999)

- Alle offentlige organ har plikt til å ha arkiv
- Sikre arkivene for samtid og ettertid
  - ingen konkrete sikringskrav
- I forskrift for offentlige arkiv av 1998 er det dog spesifisert fysiske sikringskrav.
  - Lagringsmedium, kort/langtidslagring, kassasjon osv

- Gir generelle saksbehandlingsregler for hele forvaltningen
  - Rett til innsyn
  - Taushetsplikt
    - Verne gradert informasjon mot innsyn av uautoriserte personer
    - Vi må stole på at opplysningene håndteres på en betryggende måte

# Offentlighetsloven 1970

- Formålet er å regulere allmennhetens rett til innsyn i dokumenter som håndteres av det offentlige
- Et dokument, eller opplysninger i et dokument, skal derfor utleveres på forespørsel med mindre dokumentet sitt innhold er unntatt offentligheten

# Lov om elektronisk signatur 2001

- Legge til rette for en sikker og effektiv bruk av elektroniske signaturer ved å fastsette krav til kvalifiserte sertifikater, til utstedere av sertifikatene og signaturfremstillingssystemer
- Forskrift gir Nasjonal Sikkerhetsmyndighet oppgaven med å godkjenne hvilke teknikker som tilfredsstiller kravene til signatur
  - Bank ID
- Å signere en avtale med Bank ID er like juridisk bindende som om man personlig møter opp i en bank, viser frem pass, og signerer foran vitner!
  - Svindel hvor noen har fått tak i offerets Bank ID og tatt opp lån i offerets navn resulter i at OFFERET blir avkrevet lånt beløp – selv om svindleren er dømt for svindelen!
  - Moral: ALDRI la andre kjenne ditt Bank ID passord, selv ikke ektefelle!

## § 2-7 b. Bruk av informasjonskapsler/cookies

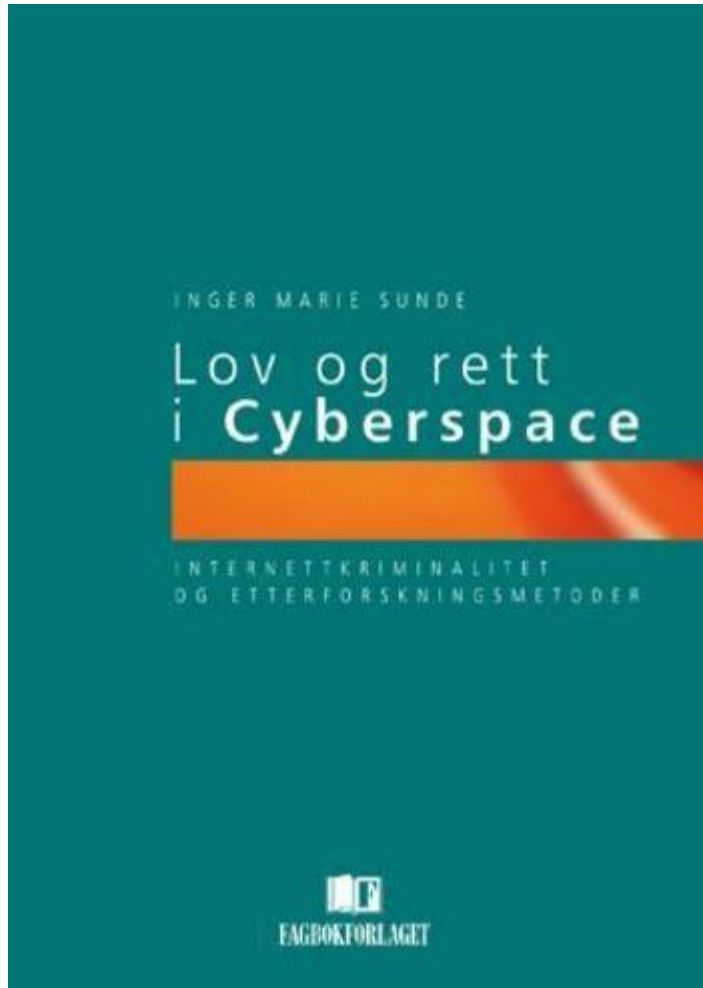
Lagring av opplysninger i brukers kommunikasjonsutstyr, eller å skaffe seg adgang til slike, er **ikke tillatt uten at brukeren er informert** om hvilke opplysninger som behandles, formålet med behandlingen, hvem som behandler opplysningene, og har samtykket til dette. Første punktum er ikke til hinder for teknisk lagring av eller adgang til opplysninger:

1. utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett
2. som er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel.

- Gjelder hele EU



# Norges Lover er komplekst – men spennende...

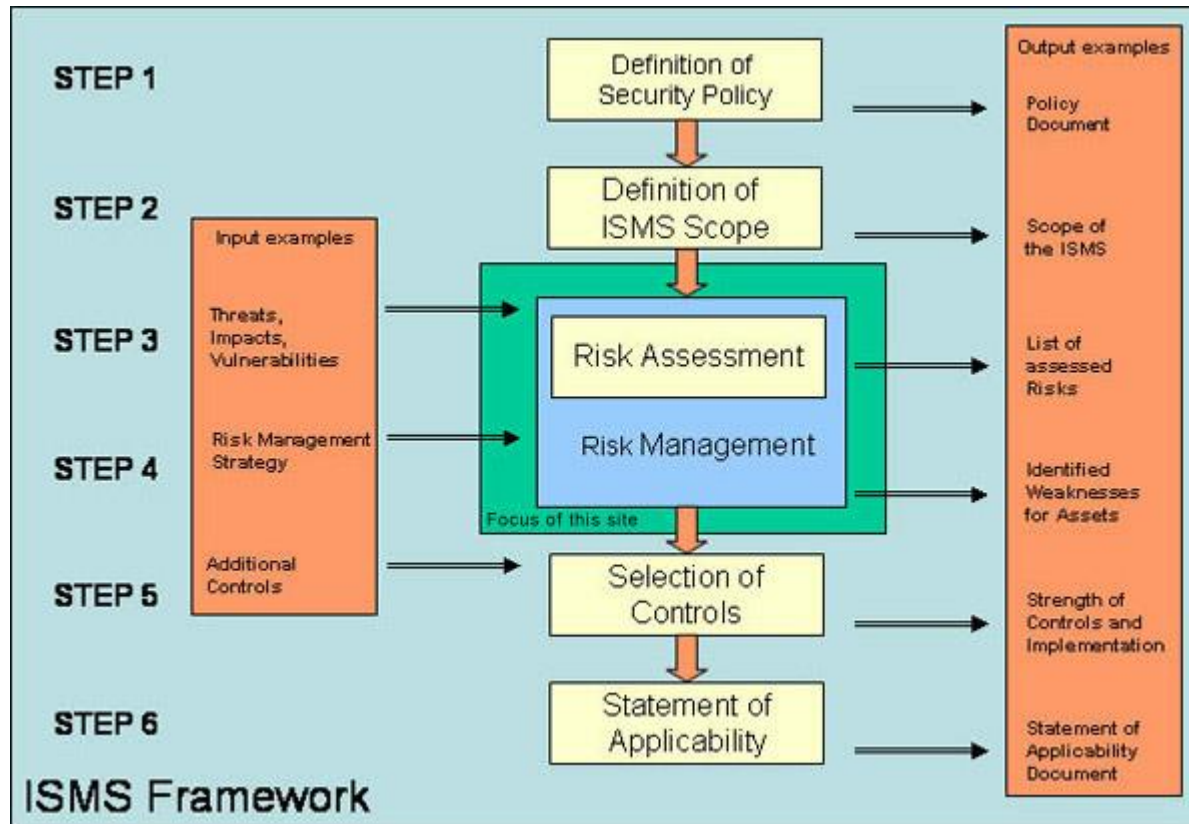


Tidligere pensumbok for politihøgskolen

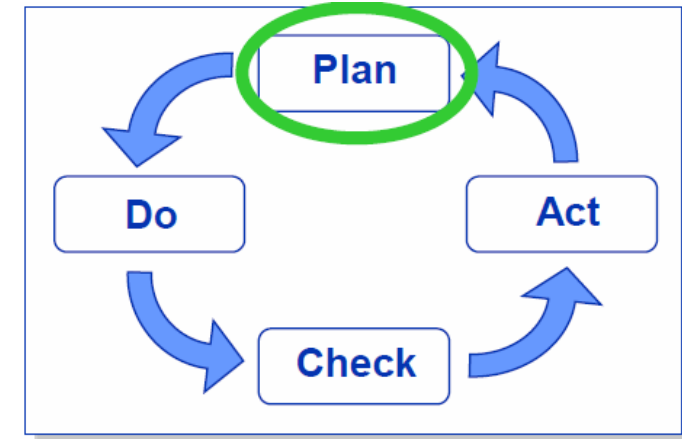


Nåværende pensumbok for politihøgskolen  
(i mine øyne ikke like god som den første)

# Sikkerhetstandarder og revisjon



- Følger Plan, Do, Check, Act syklus for QA
- Risikodrevet



- Uten en grundig forståelse om hva som er et foretaks **FAKTISKE** sikkerhetsbehov, vil en kunne sette kreftene inn på feil steder.
- Hele bedriftens informasjonssystem må kartlegges og vies opp mot risiko.
- De fleste store selskaper har en Risk avdeling, i henhold til International Institute of Auditors sine modeller (Three-layers-of-defence model) er Risk (og Compliance) «høyere» i selskapet, dvs nærmere ledelsen
- Det betyr at organisatorisk er det risiko som bestemmer tiltak for sikkerhet, med andre ord hvilken risiko selskapet kan operere med!

# Risiko=trussel+sårbarhet

- **Sårbarhet** -> et potensielt angrepspunkt, en svakhet som kan utnyttes av en angriper.

(Tekniske, administrative prosedyrer, sosialisering, fysiske løsninger etc.)

- **Trussel** -> hendelse som kompromitterer eller bryter sikkerheten.

3 komponenter:

- Mål (hva angriperen vil oppnå)
- Agenter (hvem angriperen er)
- Hendelsen (hva angriperen gjør)

**Sårbarhet \* trussel = risiko**

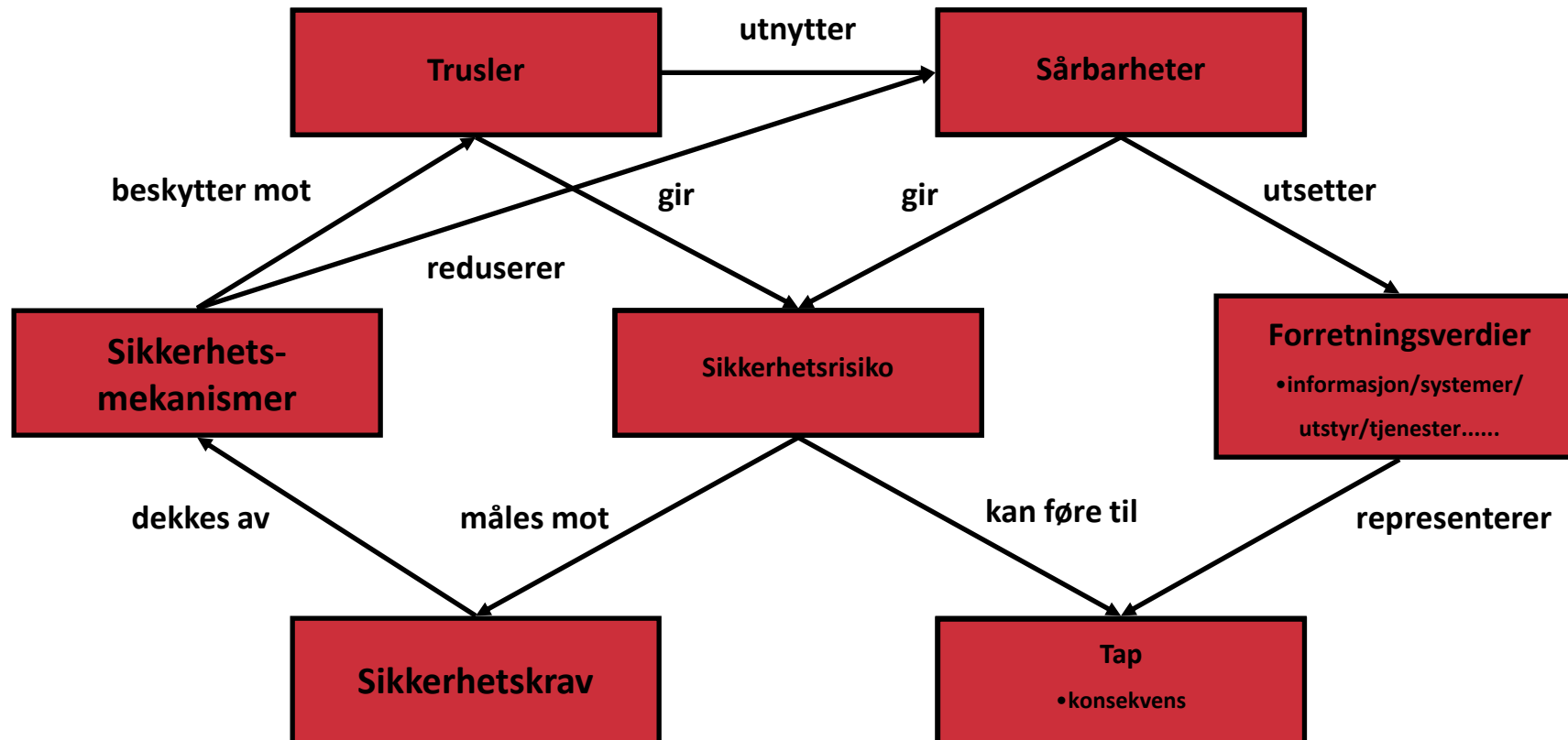
- Å identifisere sårbarheter:
  - **Administrative:**
    - Bevissthetsnivå
    - Kunnskapsnivå
    - Tilgang – "need to know"
  - **Fysiske:**
    - Tilgang (dører, vinduer, nøkler etc)
    - Brannslukking
    - Annen varsling
  - **Tekniske**
    - Kommunikasjon/avlytting
    - SW-leverandører
    - Brannvegg/virus

Finn minst et eksempel på hver av disse punktene.

Er det etter ditt syn åpenbare punkter som mangler?

- **Penger!!!**
- Kostnad for:
  - Å forhindre
  - Å reparere
- Kostnader kan ha mange komponenter:
  - Rene utgifter
  - Tapt tid
  - Ressurser
  - Rykte/omdømme
  - Tapt omsetning

# Risiko-vurdering og -håndtering





1. **Vurdere risiko:** Verdier, trusler, tap
2. **Utforme policy:** Informasjon, systemer, bruk, backup, tilgang, hendelser, avbruddsplan
3. **Innføre:** Rapportering, autentisering, innbrudds-deteksjon, kryptering, fysisk sikkerhet.
4. **Opplæring:** Ansatte, ledere, utviklere, sikkerhets-ansatte
5. **Revisjon:** Etterlevelse, periodisk vurdering, innbrudds-testing

# CIS 20

- Center for Internet Security (CIS) har laget et planverk basert på 20 kontroller som mange selskaper baserer sin sikkerhetsstrategi på
- Omtales fortsatt som «CIS 20», men har etter revision 8 kun 18 punkter 😊

<https://www.cisecurity.org/controls/cis-controls-list/>

<https://www.rapid7.com/solutions/compliance/critical-controls/>

# ISO 27001

- Fokuserer på sikring av tilgjengelighet, integritet og konfidensialitet av informasjon
- Sikringen foretas gjennom et sett kontroller, som angir konkrete krav. Kontrollene beskrives og vedlikeholdes i organisasjonen.
- Standarden kan opprettholdes og dokumenteres gjennom en sertifiseringsordning, og kontrolleres via intern og ekstern revisjon.

- Beskriver oppbygging og vedlikehold av et Information Security Management System (**ISMS**) for et foretak

ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1] [↗](#)

ISO/IEC 27001 — Information security management systems — Requirements

ISO/IEC 27002 — Code of practice for information security management

ISO/IEC 27003 — Information security management system implementation guidance

ISO/IEC 27004 — Information security management — Measurement

ISO/IEC 27005 — Information security risk management

ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

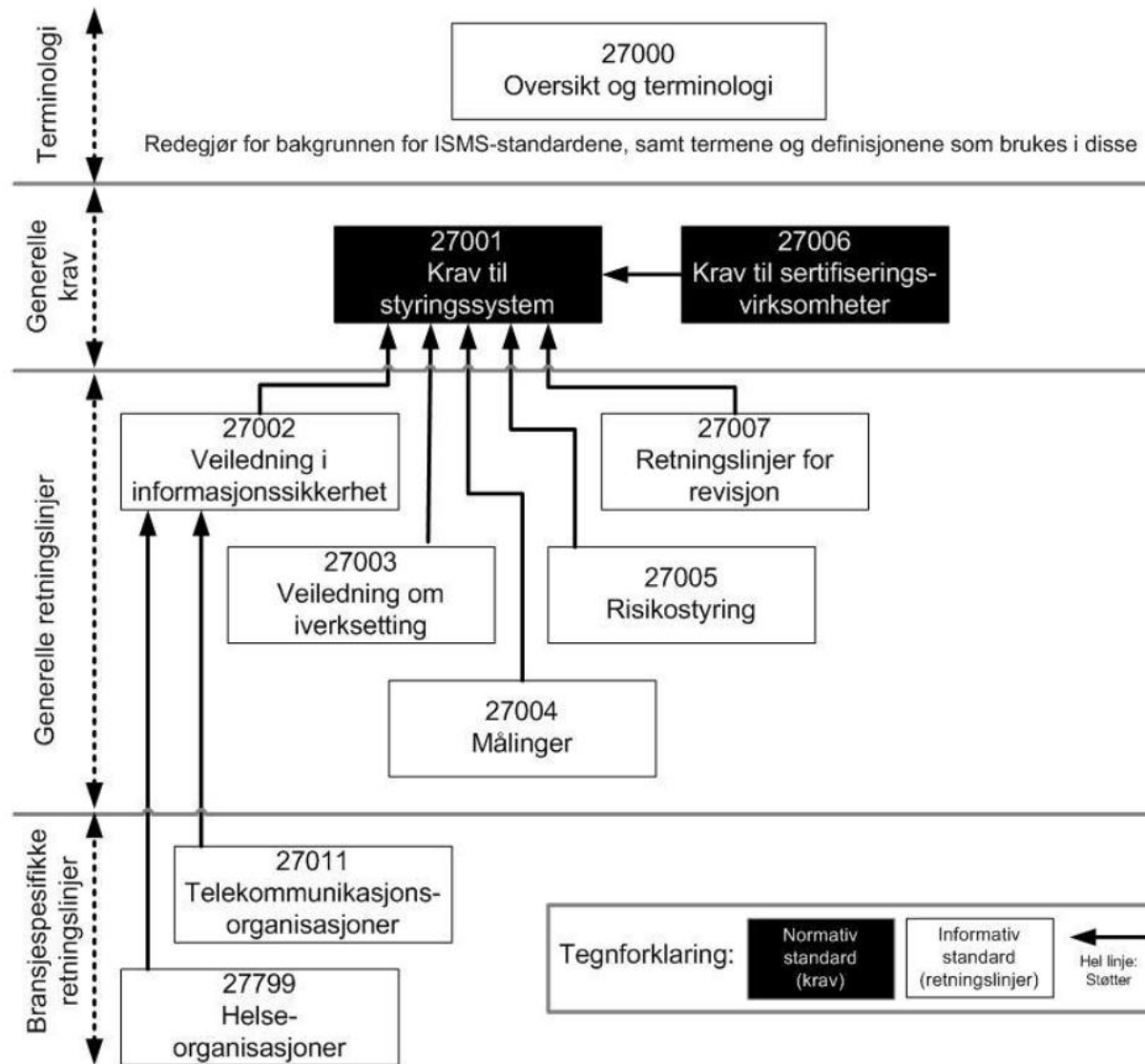
ISO/IEC 27031 — Guidelines for information and communications technology readiness for business continuity

ISO/IEC 27033-1 — Network security overview and concepts

ISO/IEC 27035 — Security incident management

ISO 27799 — Information security management in health using ISO/IEC 27002

# ISO 270xx



- ISO 17799: 2005 (= 27001) fokuserer på sikring av *tilgjengelighet, integritet og konfidensialitet* av informasjon
- Sikringen foretas gjennom et sett kontroller, som angir konkrete krav. Kontrollene beskrives og vedlikeholdes i organisasjonen.
- Standarden kan opprettholdes og dokumenteres gjennom en sertifiseringsordning, og kontrolleres via intern og ekstern revisjon.

# ISO 27000: **Ti områder for IT-sikkerhet**

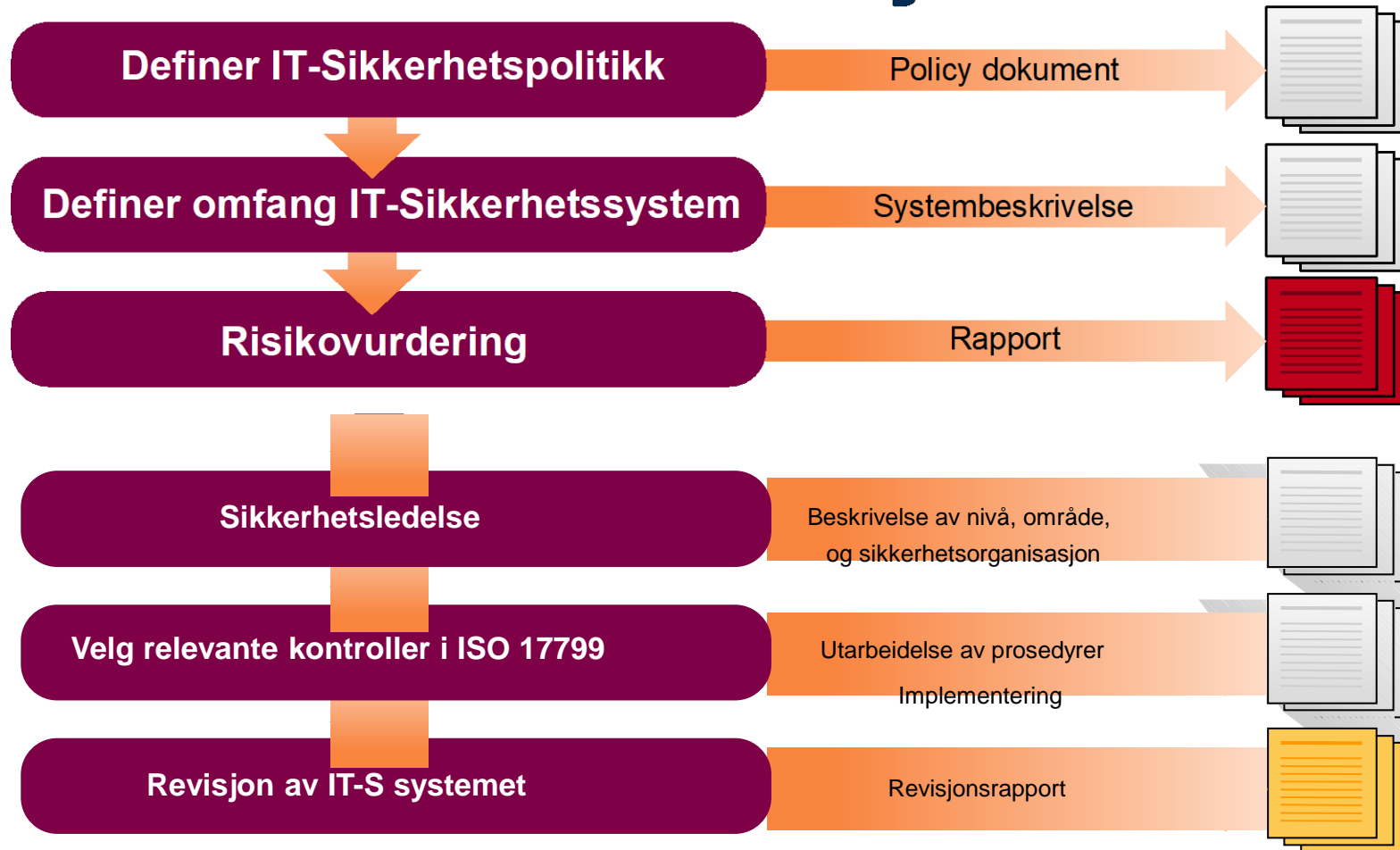
1. **Sikkerhetspolitikk og - mål**
2. **Organisasjon for sikkerhet**
3. **HW/SW klassifikasjon og kontroll**
4. **Personellsikkerhet**
5. **Fysisk sikkerhet**
6. **PC, servere og nettverk**
7. **Tilgang til systemer**
8. **Systemutvikling og vedlikehold**
9. **Beredskapsplan**
10. **Sikkerhetsrevisjon**

# ISO 27001: **Ti nøkkelkontroller**

1. Dokumentert sikkerhetspolitikk
2. Krav til sikkerhetsansvarlig
3. Sikkerhetsutdanning og trening
4. Rapportering av sikkerhetshendelser
5. Viruskontroll
6. Beredskapsplaner
7. Styring av softwarelisenser
8. Beskyttelse av elektroniske registeringer
9. Vern av persondata
10. Sikkerhetsrevisjon



## IT-sikkerhetssystem



- Justervesenet ved Norsk Akkreditering godkjenner hvem som kan foreta sertifisering
  - Det norske Veritas
  - NEMKO Certification Services
  - Teknologisk Institutt Sertifisering AS
  - M.fl.

- Payment Card Industry  
Data Security Standard
- Standarden som f.eks. Visa, Mastercard og andre (kort-)leverandører av betalingstjenester bruker
  - Stiller krav til sikring av kunde, leverandør og transaksjon.
  - Må sertifiseres og revideres etter denne standarden dersom du f.eks. skal drive en server-farm for en bank, nettbutikk e.l.

# PCI DSS: (12)Krav til å ...

Sikkert nettverk	1. Installere og vedlikeholde en brannmur som beskytter kortdata
	2. Påse at det ikke benyttes standardinnstillinger til systempassord og andre sikkerhetsparametre
Beskytt kortdata	3. Beskytt kortdata
	4. Krypter kortdata som sendes over åpne offentlige nettverk
Håndter sårbarheter med faste prosedyrer	5. Benytt antivirus-programvare og oppdater den jevnlig
	6. Påse fortløpende utvikling og vedlikehold av sikkerhet i systemer og applikasjoner
Implementer sterk adgangskontroll	7. Begrens adgangen til kortdata i forhold til forretningsbehovet slik at færrest mulig kan få adgang til dem
	8. hver bruker av nettverket skal ha en unik ID
	9. færrest mulig skal ha fysisk adgang til kortdata
Overvåk og test nettverket fortløpende	10. Overvåk all adgang til nettverk og kortdata
	11. Test av sikkerhetssystemer og prosesser skal foretas jevnlig
Stram sikkerhetspolicy	12. Opprettholde en stram sikkerhetspolitikk

# Security Operation Center

- Et Security Operations Center (SOC) er en avdeling i et selskap som overvåker nettverk og maskiner for å oppdage og stoppe datainnbrudd
- Alle store selskaper har egne SOC teams
- Mindre selskaper kan ha en SOC «funksjon» (ofte bare 1 person, teknisk sett en sikkerhetsmedarbeider i en IT avdeling)
- Selskaper kan kjøpe SOC tjenester fra større aktører, feks Telenor, Sopra Steria, Mnemonic
- Finnes også nasjonale funksjoner, ofte kalt CERT (NCSC/NorCERT, KraftCERT, FinansCERT)

# Telenor SOC



# Sårbarhetsanalyse og testing



- Standardene er en form for internkontroll, men garanterer primært **systematikken** i sikkerhetsarbeidet – ikke nødvendigvis hvor effektivt det faktisk er.
- Sikkerheten bør derfor også testes fra angriperes perspektiv.
- Slik «simulert hacking» omtales som penetrasjonstesting
- Forutsetter juridisk bindende avtale med offeret for ikke å være straffbart.
- Kan benytte metodikken fra OSSTMM, OWASP, PTES, LPT, mfl
- Arbeidet «pentesting» utføres av en Etisk Hacker

# Nivåer av “etisk hacker” oppdrag

## Sikkerhetsrådgivning

- Gå gjennom arkitektur og gi råd til oppdragsgiver
- Eventuelt som en «table top øvelse»

## Sikkerhetsrevisjon (aka “pentest”) – for de fleste er dette 95-99% av oppdrag

- Teste systemet i praksis – mål å finne ALLE sårbarheter
- Sårbarhetsskannere mot kode og infrastruktur
- Manuelle tester mot åpne server porter, inkl testing av standard brukere/passord

## Avansert angrepssimulering

- Mål å finne EN sårbarhet, og demonstrere at man kan komme inn
- Typisk et eller flere definerte mål
- Simulering av en faktisk angriper, inkl social engineering

## Etterretningsbasert realistisk angrepssimulering

- Innledende fase med etterretning for å finne hvilke aktører som er en trussel
- Simulering av den type angrep disse aktørene er kjent for å bruke, med den tid og de ressurser de aktørene faktisk bruker

# Kategorier av pentester

- Blackbox test
  - Tester har ingen informasjon
  - Tester må finne alt selv = tar lenger tid
  - Mange mener dette er den mest realistiske testen
- Graybox test
  - Tester har tilgang til selskapet og kan be om informasjon underveis
- Whitebox (crystal) test
  - Tester har tilgang til alt av informasjon
  - Tilgang til kildekode og all intern dokumentasjon
  - Jeg mener dette er den mest realistiske testen – en ekte angriper har «uendelig tid», en pentester har 100 timer; dette jevner ut forskjellen litt

# OWASP Top 10

- OWASP Top 10 er en liste over de 10 mest utbredte sårbarhetene i web applikasjoner
- Bør ikke brukes som en pentest «standard» (men jeg ser at noen gjør det)

Globally recognized by developers as the first step towards  
more secure coding.

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

<https://owasp.org/Top10/>

# OWASP Testing Guide

- Komplett rammeverk for testing av web applikasjoner
- OWASP Mobile Testing Guide er en variant for mobilapplikasjoner
- Både hovedkapitler og underkapitler er god basis for en grundig test og rapport
- <https://owasp.org/www-project-web-security-testing-guide/>

# OWASP ASVS

- Verifikasjonsstandard
- Liste med krav basert på 3 sikkerhetsnivåer
  - L1: Low assurance level
  - L2: Applications that contain sensitive data, recommended level for most apps
  - L3: Critical applications, high value transactions, sensitive medical data, highest level of trust

#	Description	L1	L2	L3	CWE	<u>NIST</u> <u>§</u>
3.4.1	Verify that cookie-based session tokens have the 'Secure' attribute set. <a href="#">(C6)</a>	✓	✓	✓	614	7.1.1
3.4.2	Verify that cookie-based session tokens have the 'HttpOnly' attribute set. <a href="#">(C6)</a>	✓	✓	✓	1004	7.1.1
3.4.3	Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks. <a href="#">(C6)</a>	✓	✓	✓	16	7.1.1
3.4.4	Verify that cookie-based session tokens use "__Host-" prefix (see references) to provide session cookie confidentiality.	✓	✓	✓	16	7.1.1
3.4.5	Verify that if the application is published under a domain name with other applications that set or use session cookies that might override or disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible. <a href="#">(C6)</a>	✓	✓	✓	16	7.1.1

- OBS: Veldig tidkrevende, og stort sett unødvendig sammenlignet med «Complete Testing Guide»

<https://owasp.org/www-project-application-security-verification-standard/>

# PCI Penetration Testing Guide

- Selskaper som behandler kortbetaling må følge PCI DSS standarden
- PCI 3.2 (fra 2016) setter som krav at penetration testing må være en del av sårbarhetshåndteringen
- Følges typisk av banker og betalingsløsninger (de aller fleste nettbutikker i dag bruker tredjeparts betalingsløsninger som paypal, Klarna, el)

## PTES – Penetration Testing Execution Standard

- Generell angrepsmetodikk som viser fasene en pentest kan bygges opp av
- Disse stegene er ofte referert, men ikke alltid de blir kreditert til PTES rammeverket
- Pre-engagement interactions
- Intelligence-gathering
- Threat-modeling
- Vulnerability analysis
- Exploitation
- Post-exploitation
- Reporting



# Open Source Security Testing Methodology Manual

- Avansert standard for «infrastruktur testing»
- Kontinuerlig oppdatert, vedlikeholdes av Institute for Security and Open Methodologies
- Deler inn en penetrasjonstest i 5 «kanaler»:
  - Human Security
  - Physical Security
  - Wireless Communication
  - Telecommunication
  - Data Networks
- Har også sertifisering av testere

# LPT methodology

- Metodologi for «infrastruktur testing» av selskaper
- Utviklet av EC-Council og en del av CEH, ECSA og LPT sertifiseringene
  - Footprinting og OSINT
  - Social Engineering
  - Eksponerte servere
  - Scanning av nettverk
  - Enumerering av tjenester
  - Sårbarhetsanalyser
  - Passord og adgangskontroll
  - Malware trusler
  - Sniffing av trafikk i nettverk
  - Denial of Service angrep
  - IDS og brannmurer
  - Interne webservere
  - Trådløse nettverk
  - Fysisk sikkerhet
  - Mobile enheter og Internet of Things
  - Skytjenester og infrastruktur

# Faser i en pentest

- Rekognosering
- Scanning og enumerering
- Skaffe tilgang
- Eskalering av privilegier
- Beholde tilgang
- Slette spor
- Rapportering

# Nessus (Professional)

- Markedets fremste sårbarhets-scanner
- Nessus Professional er den klassiske scanneren som kjøres fra en laptop mot nettverket, men det finnes også nå flere versjoner for automatisk scanning i nettverk (Tenable.io)
- Genererer automatiske rapporter (vær obs på «billige» pentestere som bare leverer en Nessus rapport direkte til kunder - og fakturerer for en full pentest...)

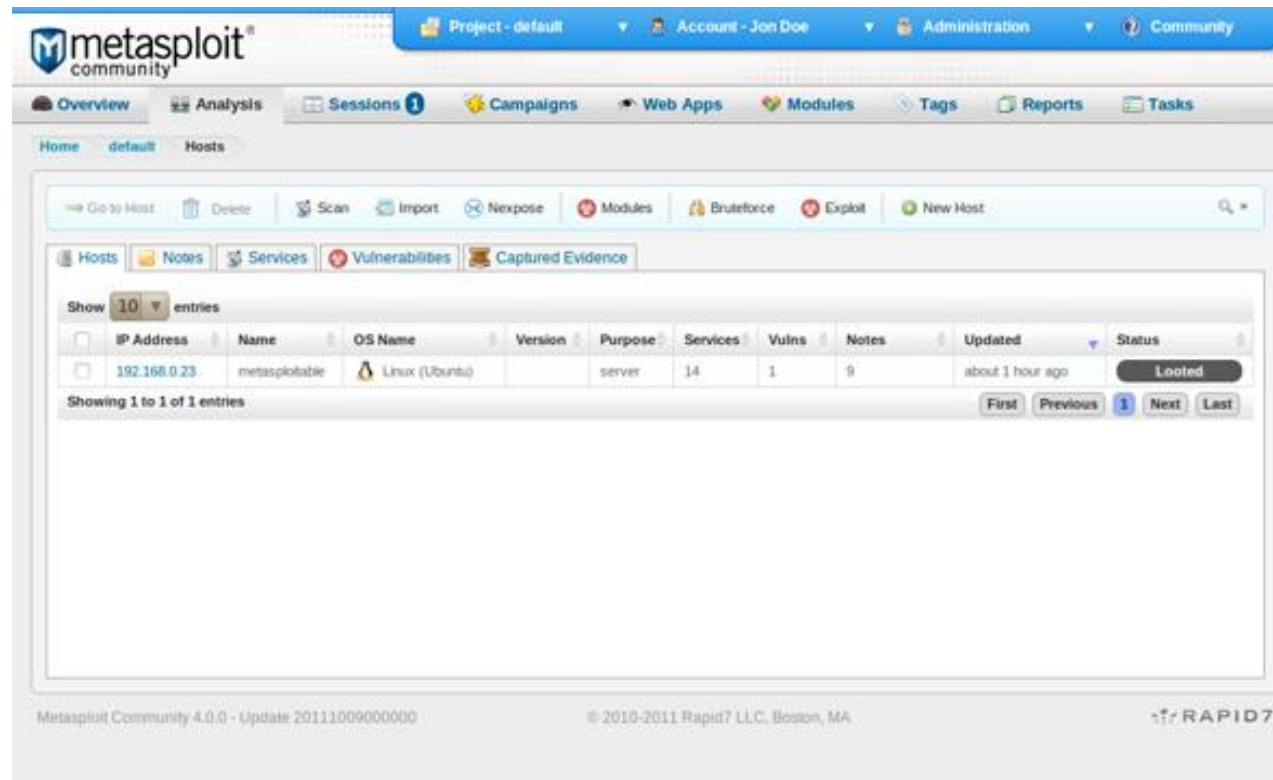
The screenshot displays the Nessus Professional web interface. At the top, there's a navigation bar with 'Scans' and 'Policies' tabs. The main header shows 'First Scan' with buttons for 'Configure', 'Audit Trail', and 'Launch'. A red box highlights the 'Export' dropdown menu, which includes options for 'Nessus', 'PDF', 'HTML', 'CSV', and 'Nessus DB'. Below this, a table lists various vulnerabilities. The table has columns for 'Severity', 'Plugin Name', 'Plugin Family', and a count. The vulnerabilities listed include 'CodeMeter - 5.20 Local Privilege Escalation V...', 'Linksys Router Default Password (admin)', 'SMB Signing Disabled', 'SSL Certificate Cannot Be Trusted', 'DNS Server Cache Snooping Remote Informat...', 'IP Forwarding Enabled', 'SSL Certificate Expiry', 'SSL Certificate Signed Using Weak Hashing Al...', 'SSL Certificate with Wrong Hostname', 'SSL Self-Signed Certificate', 'SSL Version 2 and 3 Protocol Detection', and 'SSLv3 Padding Grade On Downgraded Legac...'. To the right of the table, a 'Scan Details' sidebar provides information about the 'First Scan', including its status (Completed), policy (Basic Network Scan), scanner (Local Scanner), folder (My Scans), start and end times, elapsed time (17 minutes), and targets (192.168.1.0/24). At the bottom right, a 'Vulnerabilities' donut chart shows the distribution of severity levels: High (yellow), Medium (orange), Low (green), and Info (blue). The 'ALLXPSOFT.COM' logo is also visible in the bottom right corner.

Severity	Plugin Name	Plugin Family	Count
High	CodeMeter - 5.20 Local Privilege Escalation V...	CGI abuses	1
High	Linksys Router Default Password (admin)	CISCO	1
Medium	SMB Signing Disabled	Misc.	2
Medium	SSL Certificate Cannot Be Trusted	General	2
Medium	DNS Server Cache Snooping Remote Informat...	DNS	1
Medium	IP Forwarding Enabled	Firewalls	1
Medium	SSL Certificate Expiry	General	1
Medium	SSL Certificate Signed Using Weak Hashing Al...	General	1
Medium	SSL Certificate with Wrong Hostname	General	1
Medium	SSL Self-Signed Certificate	General	1
Medium	SSL Version 2 and 3 Protocol Detection	Service detection	1
Medium	SSLv3 Padding Grade On Downgraded Legac...	General	1

# Metasploit: Utnytte svakheter



- Kan gjøres med Metasploit («rammeverket»)
  - Plugins for å levere nyttelast til oppdagede feil...



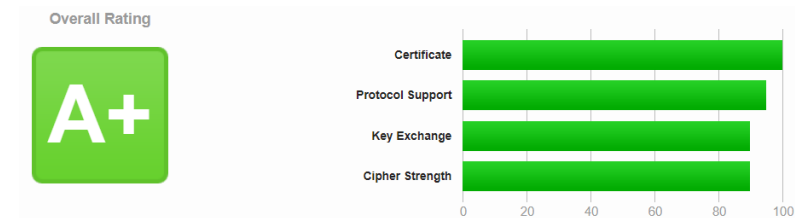
<http://www.metasploit.com/download/>

- Egen Linux distro som inneholder alle mulige slags sikkerhetsverktøy
  - Wireshark
  - nmap
  - Nessus
  - OWASP Zap/Burp Suite
  - Metasploit
  - Social engineering toolkit
  - Browser Exploitation Framework
  - Og mange, mange, mange flere

```
link/ether 00:0c:29:8a:73:02 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
    link/ether 00:0c:29:8a:73:0c brd ff:ff:ff:ff:ff:ff
    inet 192.168.253.130/24 brd 192.168.253.255 scope global dynamic nopref
ixroute eth1
        valid_lft 1771sec preferred_lft 1771sec
    inet6 fe80::20c:29ff:fe8a:730c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
kali@kali:~$ cd beef
kali@kali:~/beef$ ./beef
Would you like to check and download the latest BeEF update? y/n: n
[18:25:42][*] Browser Exploitation Framework (BeEF) 0.5.3.0
[18:25:42] |   Twit: @beefproject
[18:25:42] |   Site: https://beefproject.com
[18:25:42] |   Blog: http://blog.beefproject.com
[18:25:42] |   Wiki: https://github.com/beefproject/beef/wiki
[18:25:42][*] Project Creator: Wade Alcorn (@WadeAlcorn)
-- migration_context()
   -> 0.0157s
[18:25:43][*] BeEF is loading. Wait a few seconds ...
[18:25:44][!] [AdminUI] Error: Could not minify JavaScript file: web_ui_
[18:25:44] |   [AdminUI] Ensure nodejs is installed and `node` is in
ATH` !
[18:25:44][*] 8 extensions enabled:
[18:25:44] |   Demos
[18:25:44] |   XSSRays
[18:25:44] |   Events
[18:25:44] |   Social Engineering
[18:25:44] |   Requester
[18:25:44] |   Admin UI
[18:25:44] |   Proxy
[18:25:44] |   Network
[18:25:44][*] 305 modules enabled.
[18:25:44][*] 2 network interfaces were detected.
[18:25:44][*] running on network interface: 127.0.0.1
[18:25:44] |   Hook URL: http://127.0.0.1:3000/h.js
[18:25:44] |   UI URL:   http://127.0.0.1:3000/ui/panel
[18:25:44][*] running on network interface: 192.168.253.130
[18:25:44] |   Hook URL: http://192.168.253.130:3000/h.js
[18:25:44] |   UI URL:   http://192.168.253.130:3000/ui/panel
```

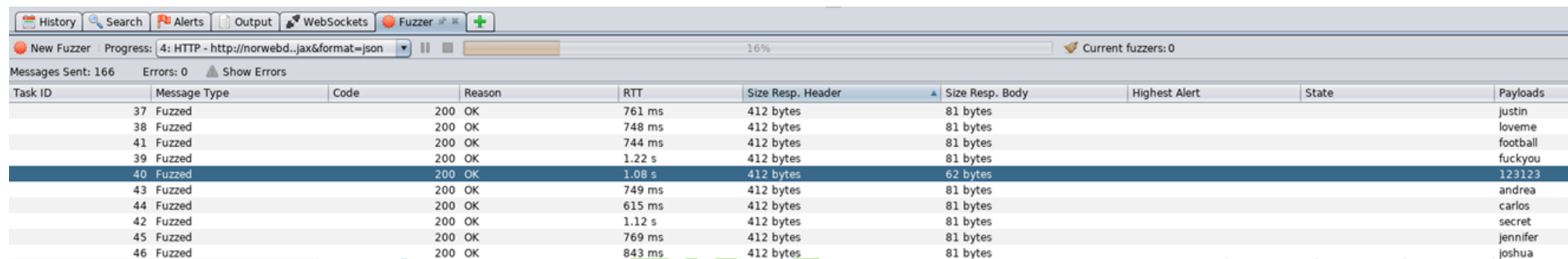
# Online web server scan

- To gratis online verktøy
- <https://www.ssllabs.com/>
  - Sjekker sikkerheten i TLS
- <https://securityheaders.com>
  - Sjekker Security Headers
  - Security Headers instruerer moderne browsere til å utføre forskjellige beskyttelser mot web angrep, slik som Cross Site Scripting



Security Report Summary	
	Site: <a href="https://www.westerdals.no/">https://www.westerdals.no/</a>
	IP Address: 5.79.36.157
	Report Time: 09 Apr 2019 07:09:08 UTC
	Headers: <span>✔ Strict-Transport-Security</span> <span>✔ X-Content-Type-Options</span> <span>✔ X-Frame-Options</span> <span>✘ Content-Security-Policy</span> <span>✘ X-XSS-Protection</span> <span>✘ Referrer-Policy</span> <span>✘ Feature-Policy</span>

OWASP ZAP er et avansert verktøy som setter opp en proxy server for en browser. Testereren bruker så systemet som skal testes som normalt, inklusive autentisering. I bakgrunnen vil OWASP ZAP generere en site map. Alle web ressurser som er funnet og som inngår i site map kan testereren så sette som Target i en grundig Vulnerability assessment, denne analysen vil da bruke sesjonen som testereren satt opp ved normal testing / bruk.



Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
37	Fuzzed	200	OK	761 ms	412 bytes	81 bytes			justin
38	Fuzzed	200	OK	748 ms	412 bytes	81 bytes			loveme
41	Fuzzed	200	OK	744 ms	412 bytes	81 bytes			football
39	Fuzzed	200	OK	1.22 s	412 bytes	81 bytes			fuckyou
40	Fuzzed	200	OK	1.08 s	412 bytes	62 bytes			123123
43	Fuzzed	200	OK	749 ms	412 bytes	81 bytes			andrea
44	Fuzzed	200	OK	615 ms	412 bytes	81 bytes			carlos
42	Fuzzed	200	OK	1.12 s	412 bytes	81 bytes			secret
45	Fuzzed	200	OK	769 ms	412 bytes	81 bytes			jennifer
46	Fuzzed	200	OK	843 ms	412 bytes	81 bytes			joshua



# Litt mer om tre forelesninger

- Vi kommer litt tilbake til dette når vi skal prate om Defensive Programming
- Da skal vi også se på noen eksempler på resultater fra penetrasjonstester

# Hva skal vi kunne?

- Hva en sikkerhets*policy* er.
- Tilgangskontroll: DAC vs MAC
- Modeller: Bell LaPaluda, BiBa, Chinese Wall, ...
- Lover og forskrifter
  - Straffeloven og Kriplos, Sikkerhetsloven og NSM, m.fl.
- Vit hva ISO 27000, Cis20 og PCI DSS er til og brukes
  - Sertifisering og revisjon
- Hva *penetrasjonstesting* går ut på

- Les om NorCERT og NSM, skriv to sider om ansvarsområde til de to og om hvilke arbeidsoppgaver ansatte der kan utføre
- Les om Kali Linux, skriv en halv side om hva Kali kan brukes til og hvordan penetrasjonstester kan gjennomføres (dette er en teoretisk oppgave)
- Oppgavesett

[https://norsis.no/wp-content/uploads/2021/03/NorSIS\\_Trusler\\_Trender\\_2021\\_Digital.pdf](https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf)

Denne rapporten er PENSUM, hvilket betyr at dere må laste den ned og lese hele.

- Løsepengevirus
- Konto kapring
- Phishing og annen svindel
- Verdikjedeangrep

[https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM\\_rapport\\_final\\_online\\_enkeltsider.pdf](https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enkeltsider.pdf)

Denne rapporten er PENSUM, hvilket betyr at dere må laste den ned og lese hele. Kravet er å kjenne denne «overordnet», trenger ikke pugge 40 sider 😊

«NSMs rapport «Risiko» er én av tre offentlige trussel- og risikovurderinger som utgis i første kvartal hvert år. De øvrige gis ut av Etterretningstjenesten og Politiets sikkerhetstjeneste.»