



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: Marianne Sundby (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

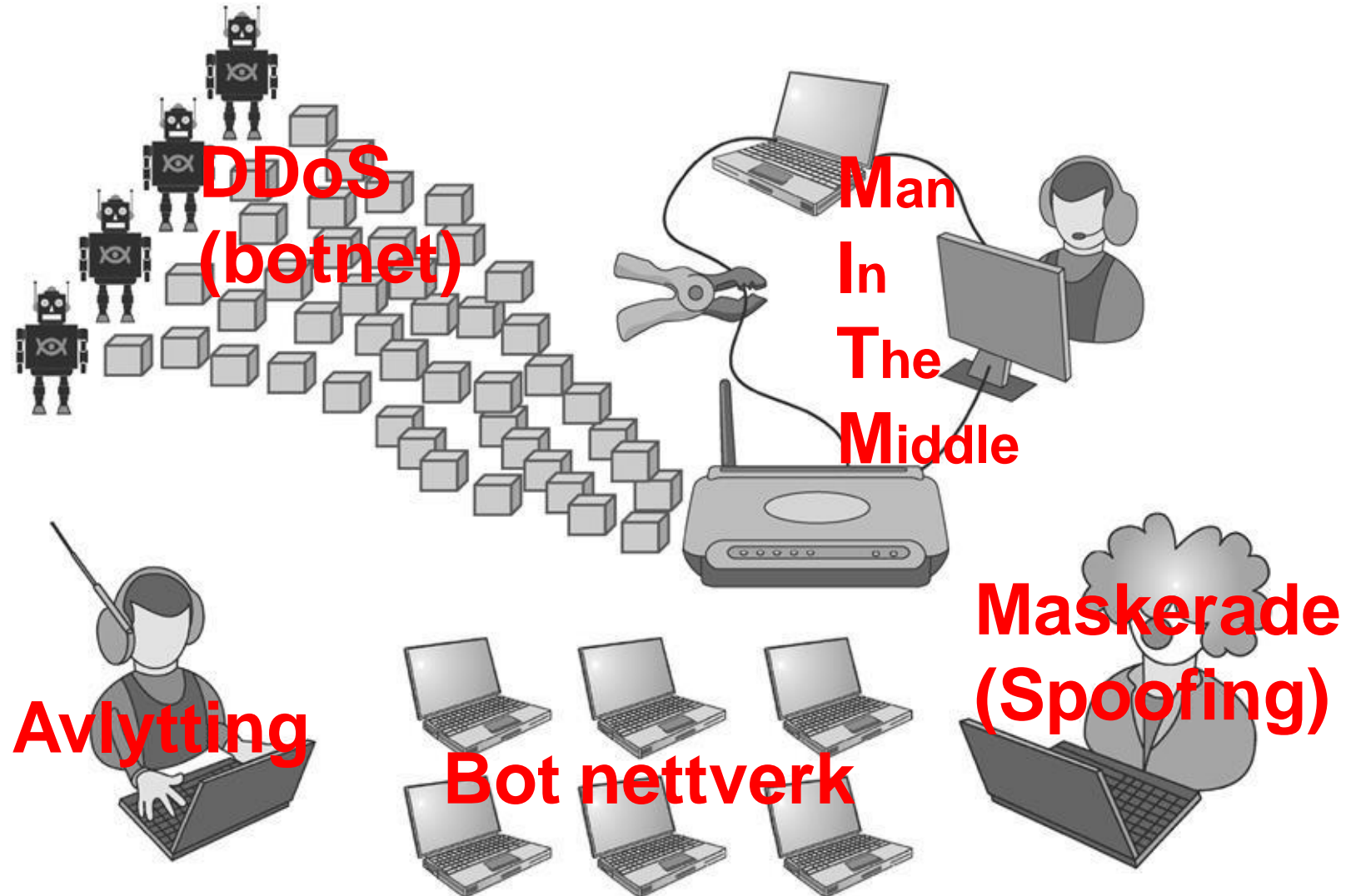
TK2100: Informasjonsikkerhet

Pensum:
Kap 5 (2011),
s.216-260

Kap. 5 (2014),
s. 221-263

6. forelesning: Nettverk og Internett

Noen nettverks-angrep



Hva vi skal kunne fra før (rep)

- TCP/IP-modellen
- HTTP, DNS, SMTP, MIME, FTP
- TCP, UDP
- IPv4, NAT, AS, BGP, ICMP, DHCP
- ARP, Ethernet 802.3 og 802.11

- Usikker? **Repeter** Leksjon 6-10 i TK1100!

- Noen slider her merket REPETISJON, men anbefales å repetere TK100 hvis usikker...

Sikkerhet (C.I.A.) og TCP/IP

- Konfidensialitet?
 - Ingen krav om det.
 - Kan støttes ved *kryptering* i applikasjon (f.eks. https) eller IPSec/VPN
- Integritet?
 - *Sjekksummer* sikrer en viss *pålitelighet*, men ikke på noen måte sikkerhet mot endring
- Tilgjenglighet
 - Har vært målet, men ofte vanskelig å *skalere* opp.

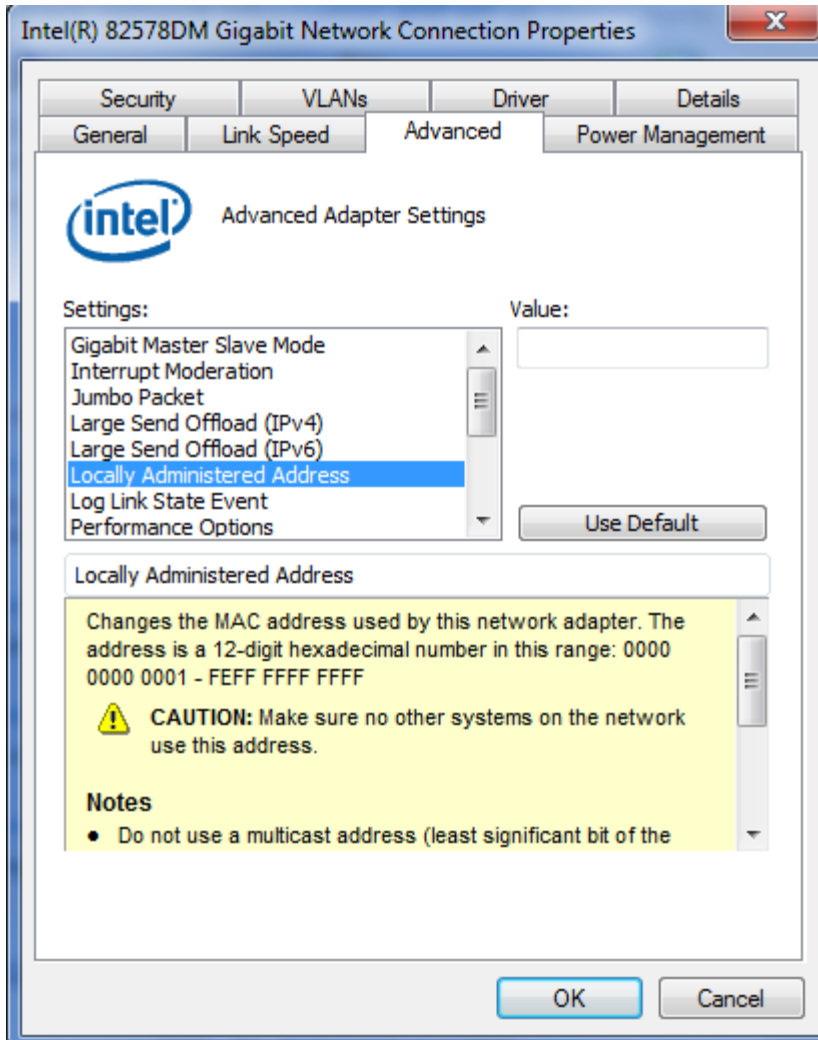
LINKLAGET

MAC-adresser

- 48 bit, noteres pr konvensjon i hex
`D8-D3-85-77-A0-3F`
- På adapter/interface/nettverkskort er det forhåndssatt.
 - Tre første byte tildelt en organisasjon av IEEE
- `FF:FF:FF:FF:FF:FF` er broadcast
- Dersom siste bit i første byte er 1 så er det multicast
 - Behandles vanligvis som broadcast

MAC-adresser kan endres lokalt

- Windows 7



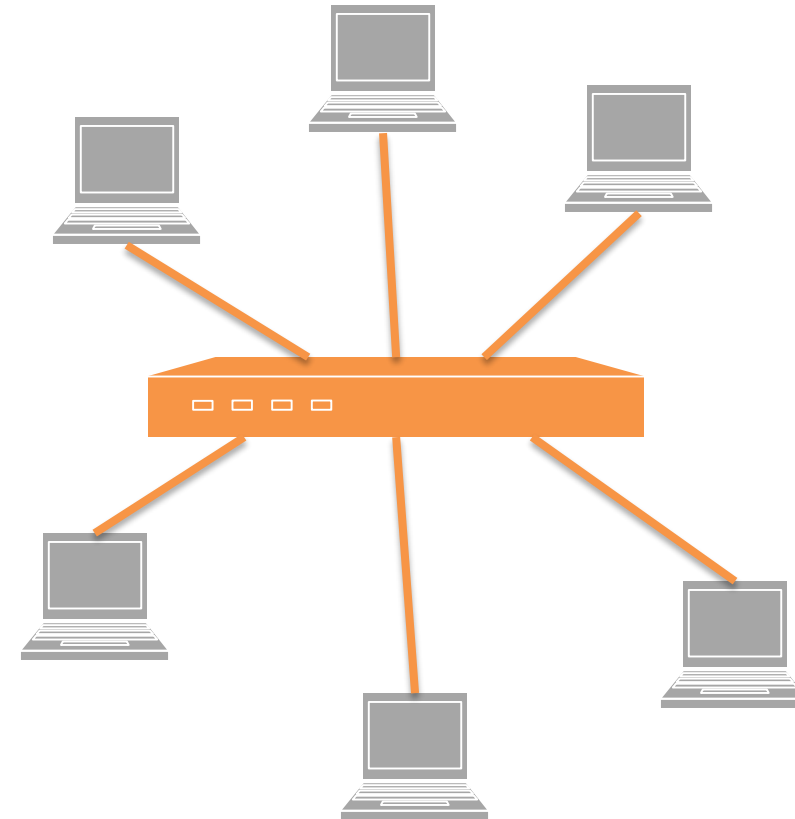
- OSX

```
McBOL:~ blistog$ ifconfig en0 |grep ether
ether b8:8d:12:18:33:06
McBOL:~ blistog$ sudo ifconfig en0 ether 02:33:33:33:33:33
Password:
McBOL:~ blistog$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=3<RXCSUM,TXCSUM>
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 02:33:33:33:33:33
inet6 fe80::ba8d:12ff:fe18:3306%en0 prefixlen 64 scopeid 0x4
inet 10.21.24.136 netmask 0xfffffc00 broadcast 10.21.27.255
media: autoselect
status: active
```

- I LAN private adresser «skal» syvende bit i første byte være 1

Switch

- Switcher skal gi en-til-en kontakt
- Har en switche-tabell basert på MAC-adresser
 - Lærer adresser etter hvert som de kommer inn på en inngang/port
 - Sender bare videre til riktig MAC
- De fleste hjemmeroutere inneholder en switch

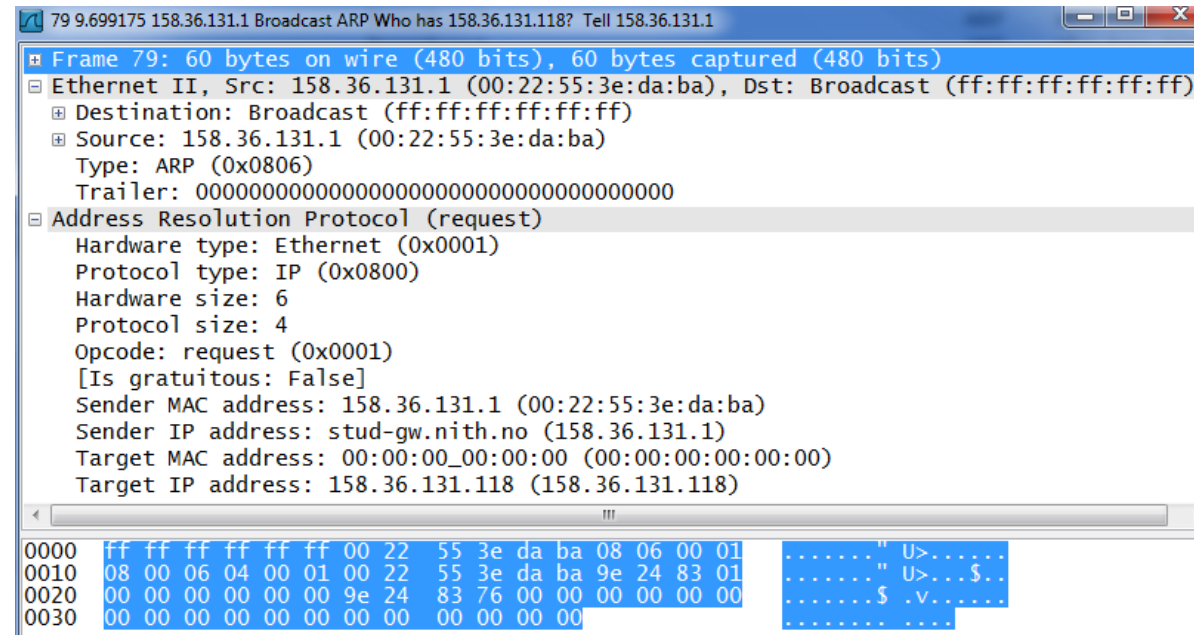


MAC adresse filtrering

- Kan sette opp switchen til å bare tillate bestemte MAC-adresser
- **MAC-spoofing** er å utgi seg for å ha en annen adresse
 - Finn ut («sniff») MAC-adressen du vil utgi deg for å ha
 - Sett den på din egen maskin
- Beskyttelse?
 - Ikke helt lett. Krever vanligvis blokkering-, autentisering- og autorisering-systemer utover det privatbrukere og de fleste firmaer er villig til å bruke.

ARP

- Address Resolution Protocol kopler nettverk- og link-lagsadressene
- Kringkaster forespørsler
- Cacher responser
- IPv6 bruker ikke ARP, men NDP



```
C:\>arp -a
```

```
Interface: 158.36.131.51 --- 0xc
Internet Address      Physical Address      Type
158.36.131.1          00-22-55-3e-da-ba    dynamic
158.36.131.5          00-0c-29-50-0b-99    dynamic
158.36.131.10         00-50-56-93-00-01    dynamic
158.36.131.13         00-50-56-93-00-12    dynamic
158.36.131.25         00-02-b3-bb-49-fc    dynamic
158.36.131.27         00-50-56-93-00-15    dynamic
158.36.131.29         00-50-56-93-00-12    dynamic
158.36.131.127        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
```

ARP spoofing

- ARP cache oppdateres på grunnlag av alle ARP-responsmeldinger
 - Ulike varianter og muligheter i ulike OS for å være mer «kresen».
- Mangelen på autentiseringsmekansime gjør deg sårbar for spoofing
 - Man-in-the-middle-attack (MITM)
 - Hvem er det egentlig som svarer?

ARP forgifning («poisoning»)

- ARP standarden tilsier en tilstandsløs protokoll
- ARP cache oppdateres ved hvert ARP-svar som ses, selv om man selv ikke har sendt forespørselen
- Gjør det mulig å forgifte ARP-cache ved å sende umotiverte («gratutious») svar
- Man kan beskytte seg ved å sette statiske oppslag
 - Vanskelig å holde orden på i lengden.

ARP Spoofing

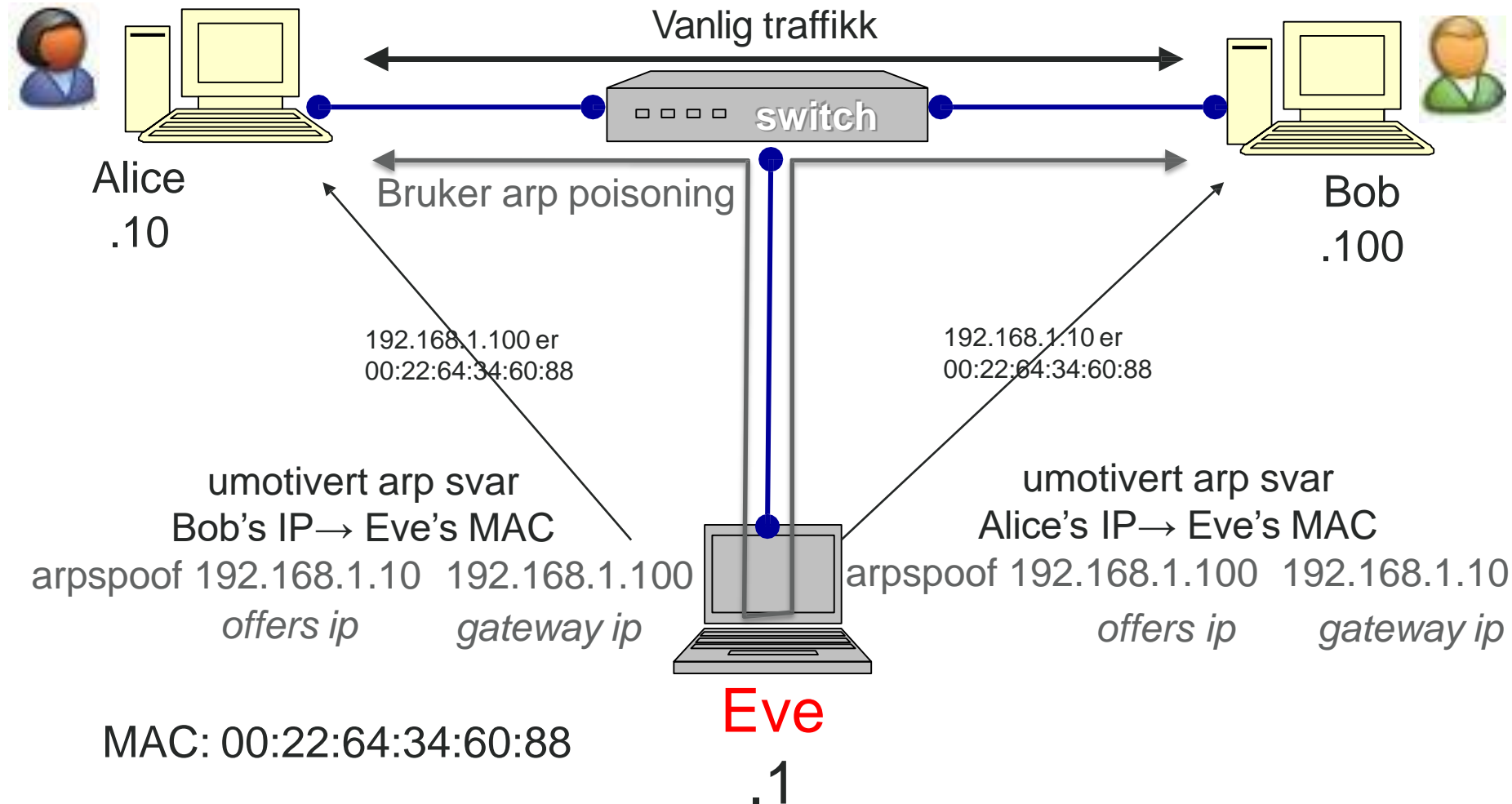
MAC: 00:0A:E4:2E:9B:11

LAN: 192.168.1.0/24

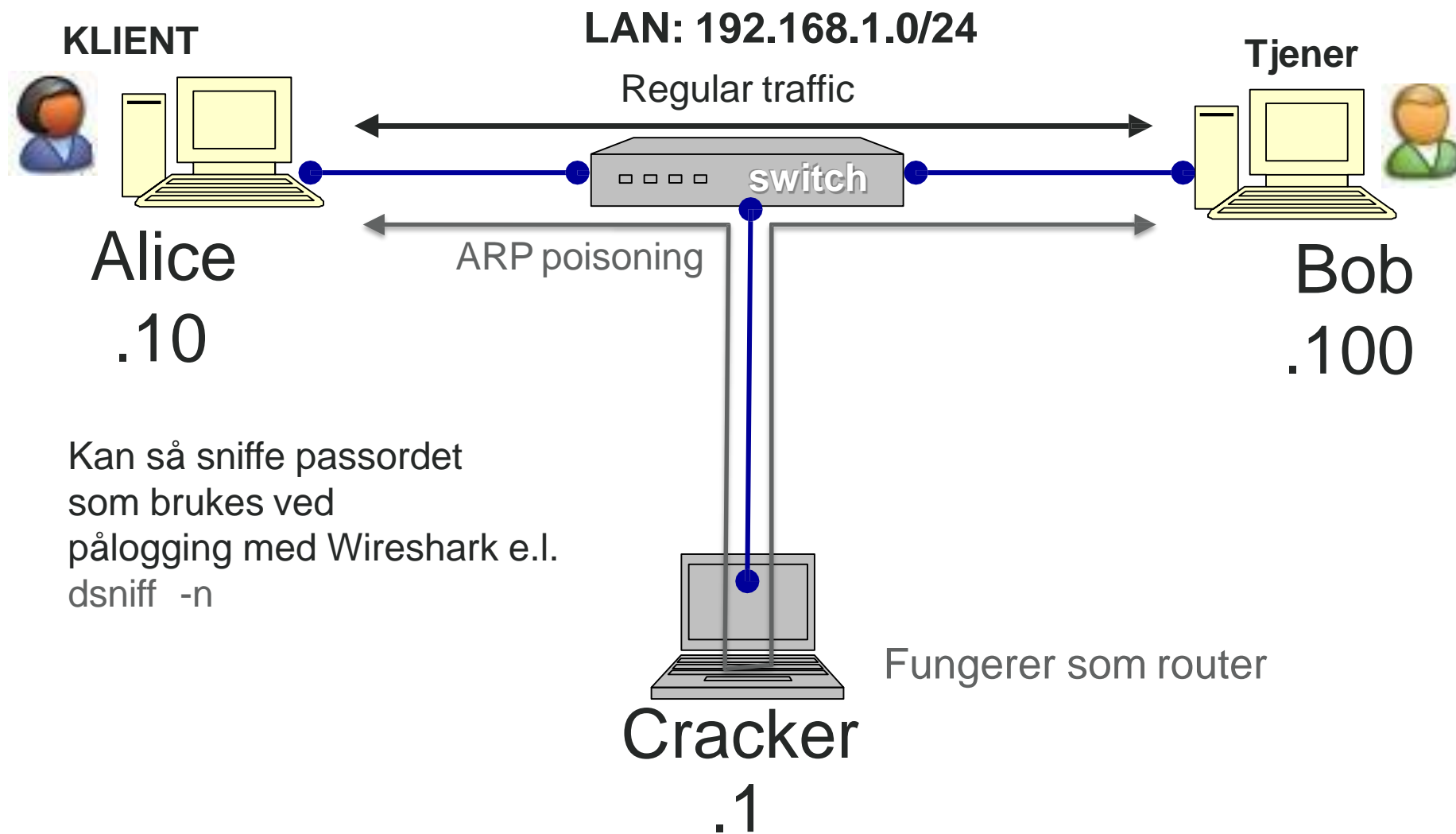
MAC: 00:0A:E4:3B:47:7E

KLIENT

TJENER



Stjele passord



NETTVERKSLAGET

Internet Protocol

- Forbindelsesløs
 - Prefix-routing
 - Hver pakke routes uavhengig av de andre
- Upålitelig
 - Levering på «best effort» basis
 - Ingen kvitteringer
- Datagram kan gå tapt, bli ødelagt eller duplisert
- IP datagram
 - Innkapsler TCP og UDP segment
 - Ligger inni link-rammer



IP-adresser

- IP-adresser
 - v4: 32 bit
 - v6: 128 bit
- Adresser delt i nettverk, subnet og host
 - Bruk av nettmaske
- Broadcast
 - F.eks. 10.21.27.255
- Private adresser
 - Ikke routbare
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16

```
C:\>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter e0:
```

```

Connection-specific DNS Suffix  . : 
IPv6 Address. . . . .           : 2001:700:2e00::51
Link-local IPv6 Address . . . . . : fe80::b46c:b98f:85ec:dba0%12
IPv4 Address. . . . .           : 158.36.131.51
Subnet Mask . . . . .           : 255.255.255.128
Default Gateway . . . . .       : 2001:700:2e00::1
                                  : 158.36.131.1

```

IP routing

- EN router står mellom to eller flere nettverk
 - Utfører routing ut fra IP-adresser og routing tabell
 - Oppdaterer routingtabeller ut fra hvilke routing-protokoller den kjører
 - Prefix-routing foregår kun ut fra IP nettverksadresse
- Routing-tabellen
 - Sender videre til andre routere
 - Gateway-router sitter på randen av et LAN/WAN

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	158.36.131.1	158.36.131.51	266
	127.0.0.0	255.0.0.0	0n-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	0n-link	127.0.0.1	306
127.255.255.255	255.255.255.255	255.255.255.255	0n-link	127.0.0.1	306
158.36.131.0	255.255.255.128	255.255.255.128	0n-link	158.36.131.51	266
158.36.131.51	255.255.255.255	255.255.255.255	0n-link	158.36.131.51	266
158.36.131.127	255.255.255.255	255.255.255.255	0n-link	158.36.131.51	266
224.0.0.0	240.0.0.0	240.0.0.0	0n-link	127.0.0.1	306
224.0.0.0	240.0.0.0	240.0.0.0	0n-link	158.36.131.51	266
255.255.255.255	255.255.255.255	255.255.255.255	0n-link	127.0.0.1	306
255.255.255.255	255.255.255.255	255.255.255.255	0n-link	158.36.131.51	266

Persistent Routes:

Network	Address	Netmask	Gateway Address	Metric
	0.0.0.0	0.0.0.0	158.36.131.1	Default

IP spoofing

- Legg inn en «falsk» avsender-adresse
 - Er bare en endring i headeren
 - Typisk brukt i DoS angrep
 - Angriper er ikke interessert i å få noe svar, bare i å overbelaste mottaker
- Kan «stoppes»
 - Router/Firewall kan stoppe pakker på vei ut som ikke har Avsender-adresser som i LAN/subnet

ICMP

- Internet **C**ontrol **M**essage **P**rotocol
 - Brukes mest til testing/debugging
 - Enkle meldinger inne i IP-datagram
- Verktøy basert på ICMP
 - Ping
 - Sender echo-forespørsler og viser statistikk basert på RTT og pakke-tap
 - Traceroute/tracert
 - Sender ICMP-pakker med stigende TTL-verdi for å avdekke hvilke routere det er langsmed ruten.

ICMP-angrep («klassisk»)

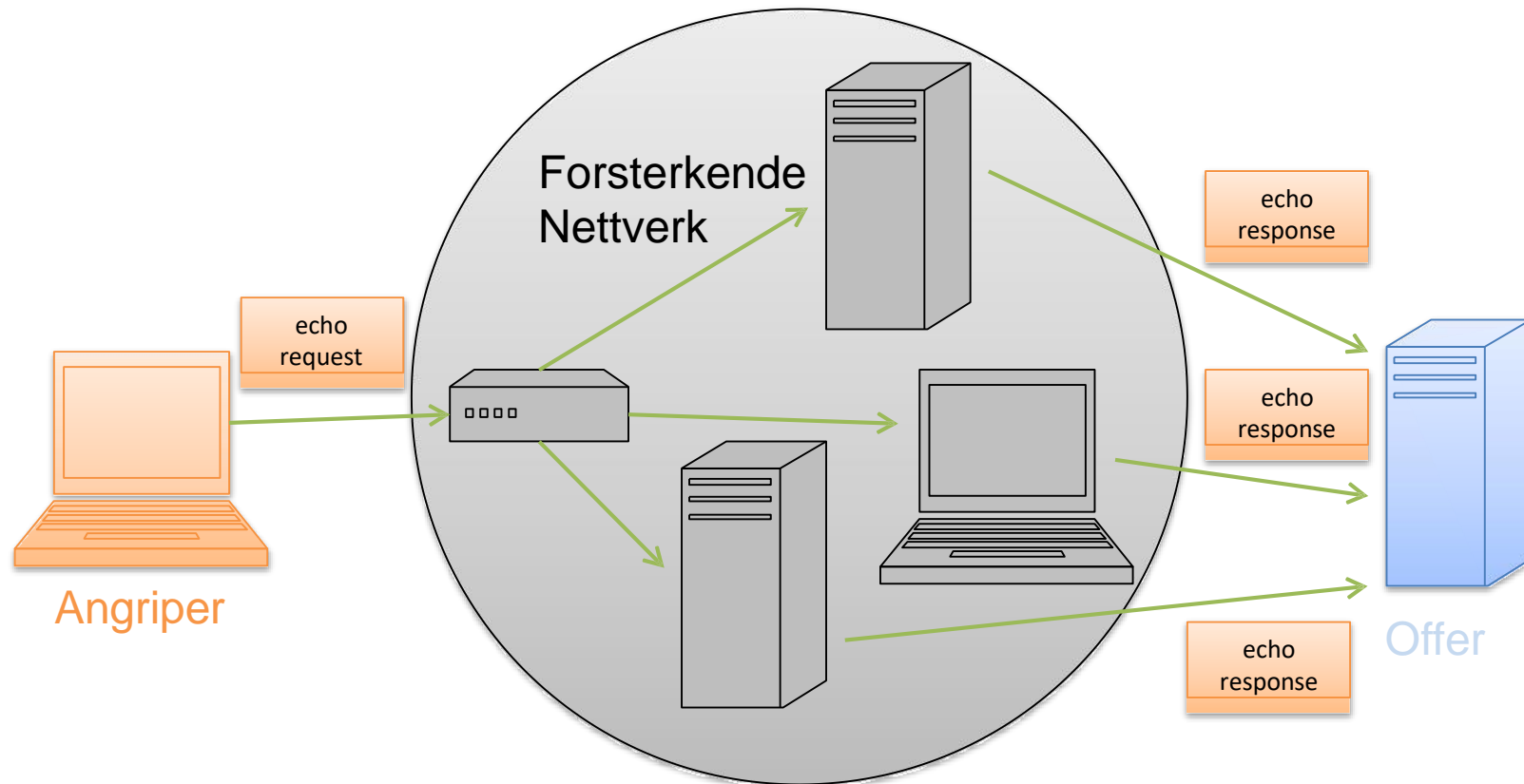
- **Ping of Death**
 - ICMP-standarden sier at en ICMP-melding er på max 64kB
 - Lag ping-pakker som benytter muligheten for å fragmenterte IP-pakker
 - Dele ICMP-«data» ut over flere IP-pakker
 - Resulterer i IP pakker større enn max limit
 - Mange OS kræsjet når de satte sammen igjen ICMP-pakken pga buffer-overflow!
- Tiltak
 - Patche OS
 - Legge grenser i ping og filtrer på routere

Smurfe -angrep



- Broadcast ICMP-echo pakker i nettverket med offerets spoofede IP-adresse som avsender

```
ping -S 10.21.24.1 10.21.27.255
```



Forsvar mot smurfer?

- Enkelmaskiner kan settes opp til å ignorere broadcast-adresserte ping-meldinger
- Firewall/router kan filtrere ut av LANet
 - Se BCP-38
- De fleste korrekt oppsatte nettverk er nå «immune»
 - Er det andre måter man kan oppnå tilsvarende effekter på?
 - Se DNS-forsterkning jf The DDoS that almost broke the Internet (Cyberbunker vs Spamhouse)



Sårbarheter i IP (v4)

- **Ukryptert** overføring
 - Kan avlyttes hele veien fra avsender til mottager
 - Løses stort sett på applikasjonsnivå
- Ingen **avsender-autentisering**
 - Avsender-adresse kan spoofes
 - Gjør det vanskelig å spore opp gjerningsmannen
- Ingen **integritets-testing**
 - Pakken som helhet kan modifieres og innholdet endres; omdirigeres; mao MITM-angrep
- Ingen **bitrate-restriksjoner**
 - Kan injisere vilkårlige mengder pakker inn i nettet og starte DoS-angrep
 - Broadcast gjør DoS enda enklere

TRANSPORTLAGET

Transmission Control Protocol

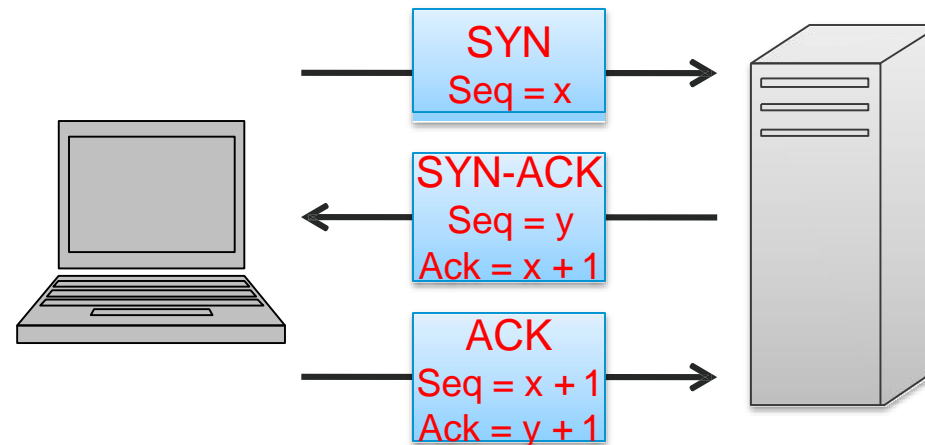
- Multiplexing ved 16-bit portnummer
- Pålitelig overføring av data i riktig rekkefølge
 - Sjekksum, sekvensnummer, kvitteringsnummer
- HTTP, FTP, HTTPS, SMTP m.fl. benytter alle TCP

Portnummer

- Sørger for at du kan ha flere samtidige applikasjoner på samme klient/tjener
- TCP- og UDP-headerne frakter avsender- og mottager-portnummer
- Velkjente porter: 0-1023
 - Kjører kjente tjenester
- User/registrerte porter: 1024-49151
 - Vanlige applikasjoner, kan registreres hos IANA
- Private porter: 49152-65535
 - Skal kun brukes lokalt og dynamisk. Kan ikke registreres til noe bestemt formål.

Three way handshake

- Klient/tjener
- Bruker SYN- og ACK-flagg i header
 - «avtaler» nummere, vindustørrelse m.m.



SYN flod («flood»)

- Typisk **DoS**-angrep
- Basert på å sende forespørsler om TCP-forbindelse raskere enn tjeneren kan prosessere dem
- Angriper lager en stor mengde pakker med «falske» avsender-adresser og setter SYN-flagget i disse
- Tjener svarer med SYN/ACK og åpner en socket, men får aldri noen respons
- Til slutt er all kapasitet på tjeneren brukt opp
 - Avhengig av oppsett kan åpnet socket bli stående i opp til tre minutter...

= **D**enial **o**f **S**ervice

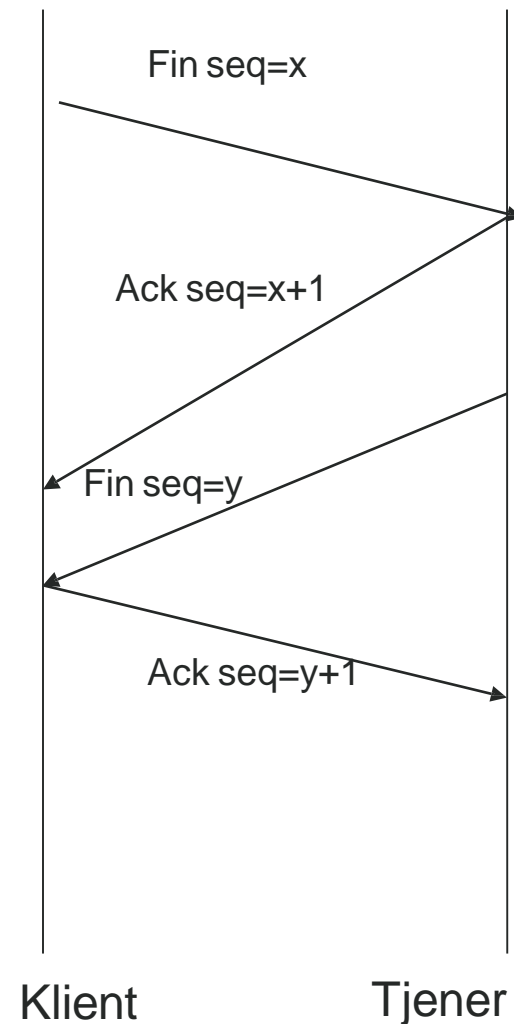
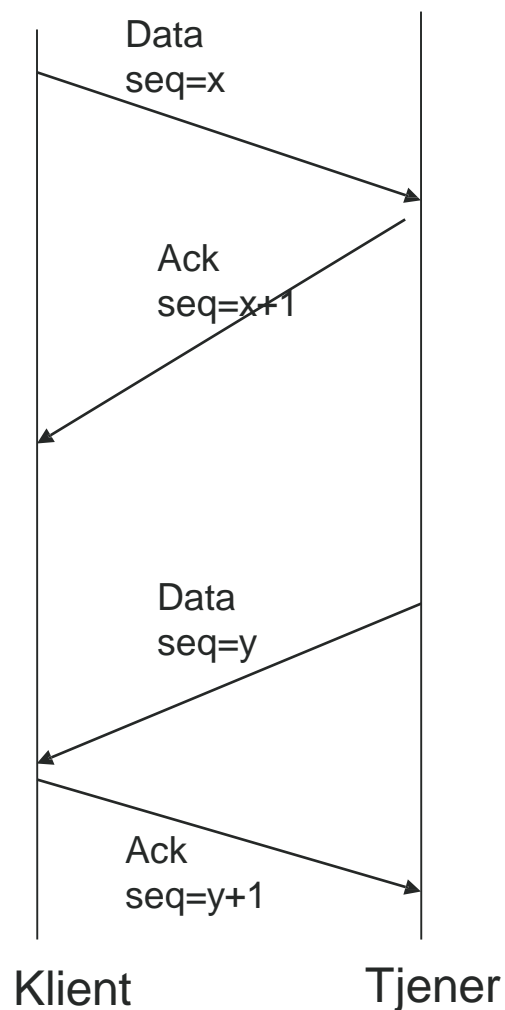
SYN flod -- forsvar

- **SYN cookie**
- Tjener åpner ikke en socket etter mottatt SYN-pakke
- Beregner en cookie-verdi til SYN/ACK-pakken basert på tidspunkt, mottatt pakkes parametre og en kryptografisk hash av avsender og mottager IP, portnr og server-tid.
 - Cookieverdien legges som sekvensnummer i SYN+ACK-pakken fra server.
- Åpner først en forbindelse/socket når ACK fra klient kommer og kvitteringsnummeret stemmer med SYN-cookie

TCP Data overføring

- ACK-nummer brukes av TCP for å sikre pålitelighet,
 - regulere mottager-vindu
 - og til metningskontroll
- Dette leder til **sårbarheten** (DoS) ACK-angrep i TCP...

TCP dataoverføring og slutt



Optimistisk ACK Angrep

- Utnytter TCPs metningskontroll
- Starter med at klient sender ACK for segment den ikke har mottatt ennå
- «Floden» av optimistiske ACK får tjeneren til å tro at det «alle routerne er ledige» og mye tilgjengelig båndbredde
 - Hever antall pakker den kan sende ut uten å ha måtte mottatt kvittering
 - Sender flere pakker
- Klienten sender enda flere overoptimistiske ACK...
- Teknikken kan benyttes mot flere tjenere og ta ned routere...
- Det finnes pr d.d. ikke noe kjent forsvar...

Sesjons-kidnapping

- «**Session hijacking**»
- Forsøk på å overta en forbindelse som offeret har etablert
- En sesjon er det tjeneren holder rede på om klienten (tilstand)
- Typisk vil dette:
 1. Handle om å overta TCP-sesjonen (alle variable)
 2. Sniffe og overta http-cookie
(Som vi nevnte forrige uke)

TCP session hijacking

- MITM angrep der man overtar en annens TCP-sesjon

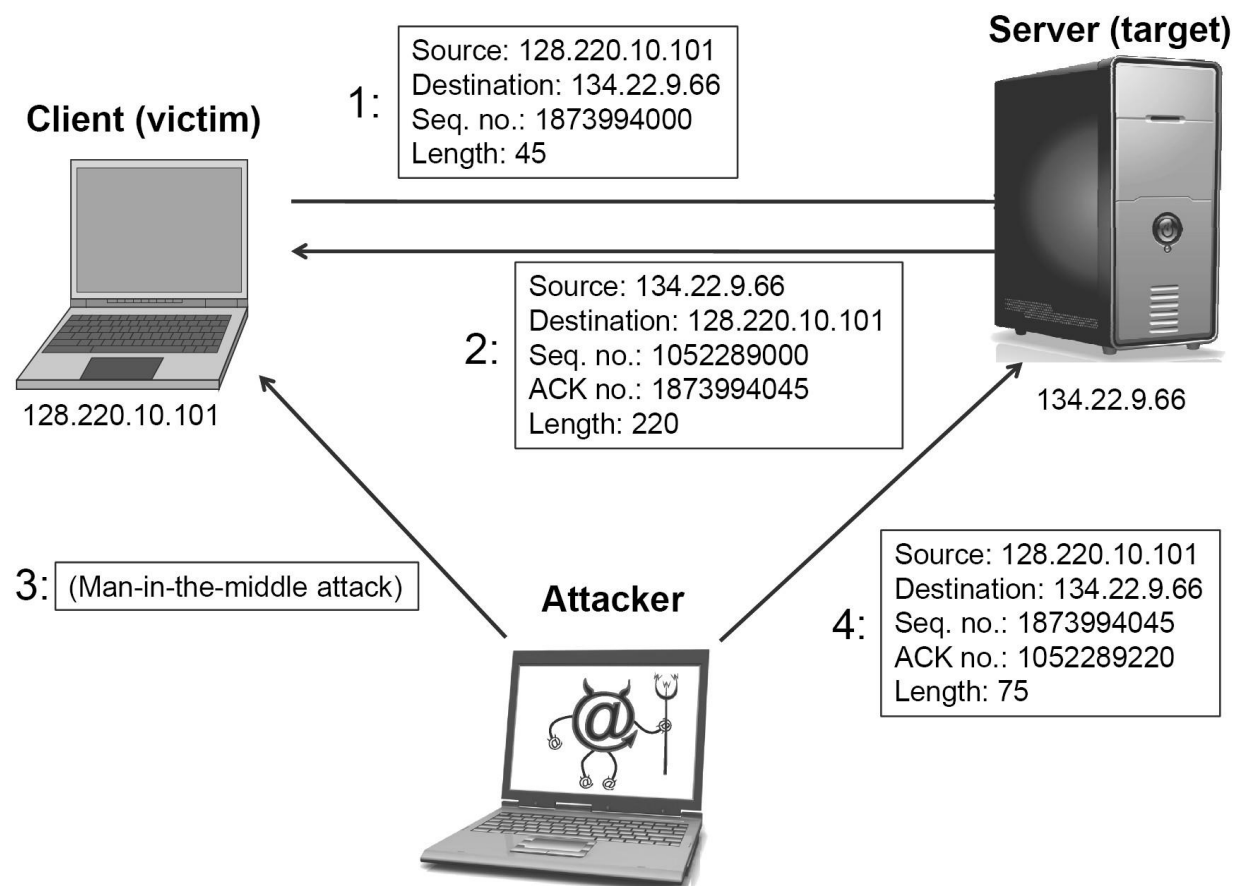


Figure 5.18: A TCP session hijacking attack.

Port-scanning (nmap)

- Hvilke porter som er åpne og måten de svarer på forteller mye om hvilket OS og hvilke tjenester som er tilgjengelige på en host-maskin

```
McBOL:~ blistog$ sudo nmap -O 10.21.25.56
```

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-02-21 19:54 CET
Nmap scan report for tablet.ad.nith.no (10.21.25.56)
Host is up (0.0059s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
5357/tcp  open  wsdaip
Warning: OSscan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7
OS details: Microsoft Windows 7

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.92 seconds
```

Port-scanning - forsvar

- En god Personal Firewall forsvarer mot alle former for port scan
- Løses ved å ha «stateful inspection», hvor en klient kun aksepterer innkommende data som matcher foregående utgående data
- Alle innkommende data som ikke er initiert fra maskinen blir droppet stille – som om maskinen ikke finnes, og da kan ikke et port scan finne noe på IP adressen som sjekkes

Port-scanning - online

- Det finnes et par verktøy for å teste din egen maskin fra en port-skanner
- GRC Shields Up test:
 - <https://www.grc.com/>
 - Både 'Common Ports' og 'All Service Ports' tester
 - Målet er å ha STEALTH rating på alle porter, dvs grønn
 - Hvis en port er CLOSED så er maskinen synlig, men porten er lukket – det betyr som oftest at du ikke har en Personal Firewall som skjuler maskinen din
 - Hvis de fleste porter er CLOSED, og noen få "STEALTH" så betyr det at ISP'en din stopper all trafikk på noen få porter – du er fortsatt synlig

22

SSH

Closed

Your computer has responded that this port exists but is currently closed to connections.



DENIAL OF SERVICE ANGREP

(D)DoS

- **D**enial **o**f **S**ervice handler om å forhindre andre (legitime) brukere fra å få tilgang til en tjeneste
 - enten ved å **kræsje** tjenesten
 - eller ved å **overbelaste** tjenesten
- De mest kjente **Distribuerte** DoS de seneste årene har enten vært
 - mot Web-servere: regjering + bank
 - politisk motivert: Anonymous (vg.no); Nord vs Sør Korea, Russland og Ukraina
 - Benytter ofte BotNet (ZombieNet)

Domain Name System

Se også Forelesning 7 i TK1100

DNS: Domain Name System

- Applikasjonslag protokoll som oversetter domene-navn til IP-adresser

```
Domain Name System (query)
[Response In: 273]
Transaction ID: 0xffd7
Flags: 0x0100 (Standard query)
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... ..0... .. = Truncated: Message is not truncated
... ..1... .. = Recursion desired: Do query recursively
... ..0... .. = Z: reserved (0)
... ..0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  home.nith.no: type A, class IN
    Name: home.nith.no
    Type: A (Host address)
    Class: IN (0x0001)
```

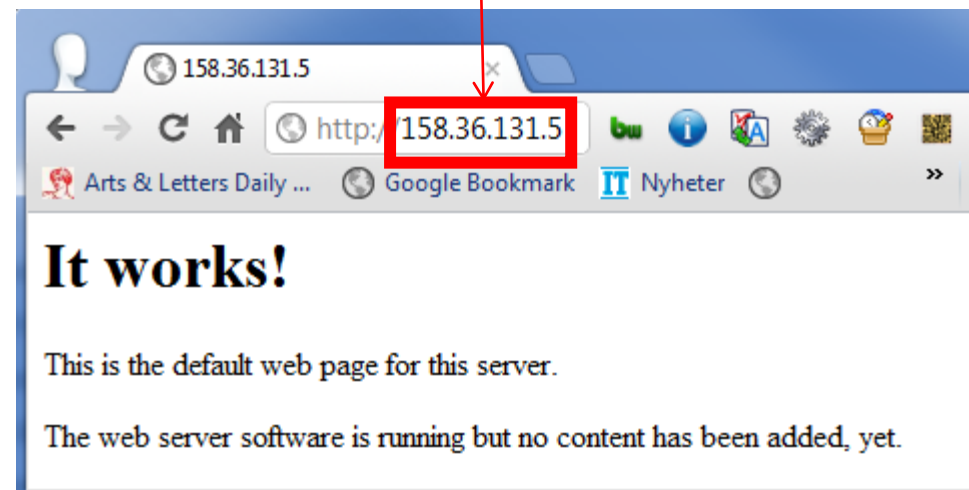
DNS query



```
Server: eks-dns02.ad.nith.no
Address: 2001:783:2:33::1
Name: home.nith.no
Address: 158.36.131.5
```

```
Domain Name System (response)
[Request In: 272]
[Time: 0.000304000 seconds]
Transaction ID: 0xffd7
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  home.nith.no: type A, class IN
Answers
  home.nith.no: type A, class IN, addr 158.36.131.5
    Name: home.nith.no
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 10 minutes
    Data length: 4
    Addr: home.nith.no (158.36.131.5)
```

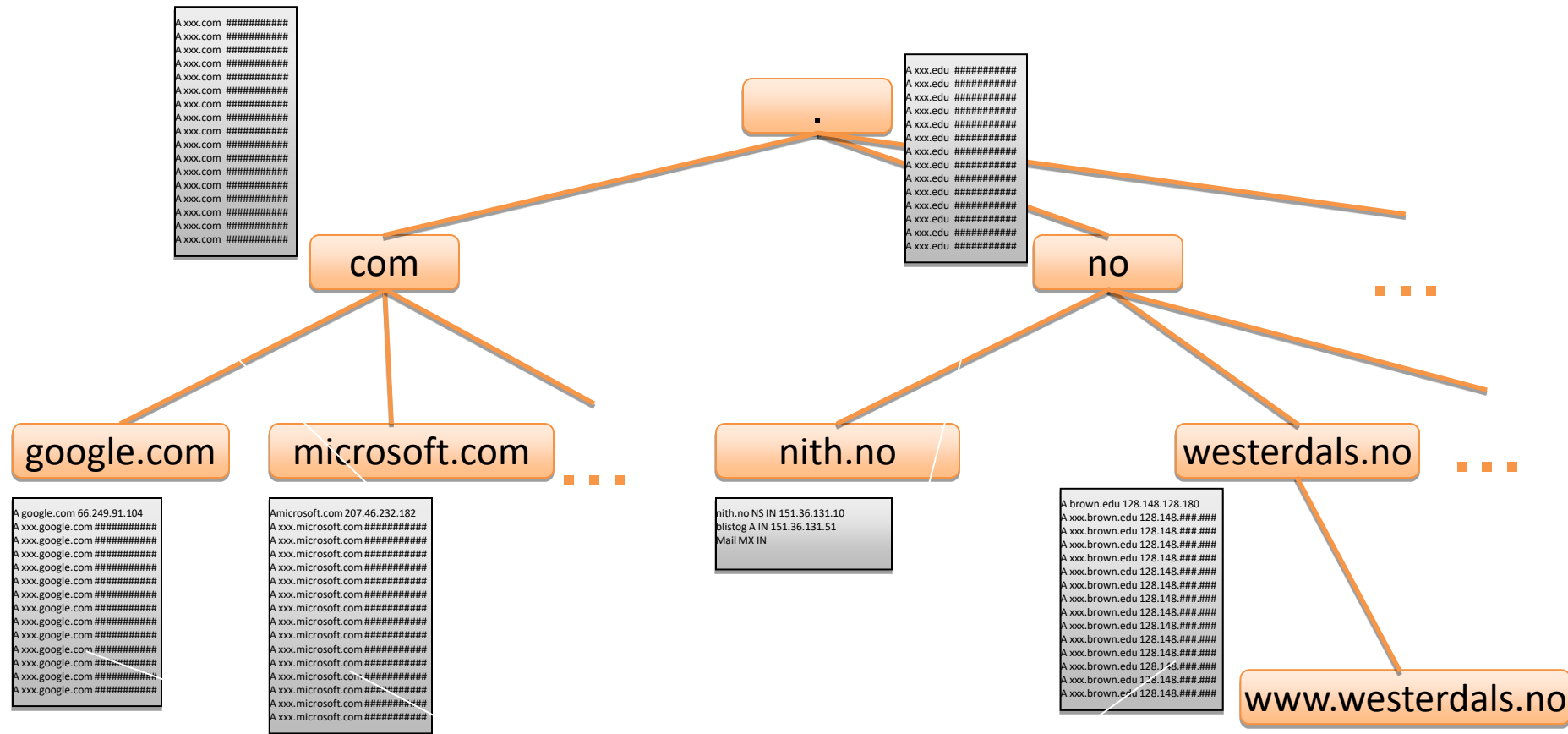
DNS response



Navnetjenere

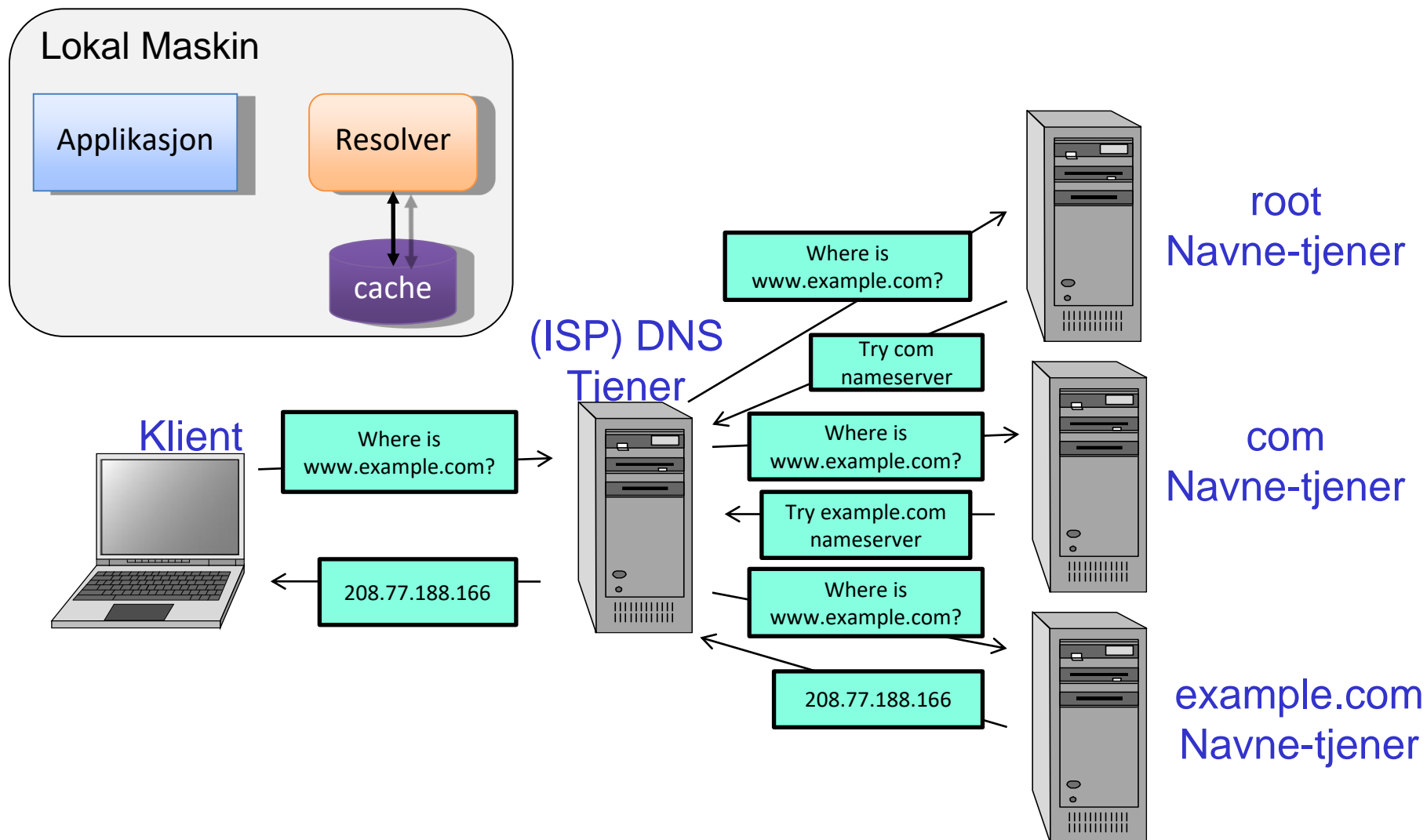
- Øverst har vi 13 rot-navnetjenere
 - **A-M**: 4 av dem i USA, resten spredd verden rundt (routes med **Anycast**)
- Domenenavnet består av
 - To eller flere merkelapper skilt fra hverandre med punktum
 - Merkelappen lengst til høyre er TLD («Top Level Domain»)
- Autoritativ Navnetjener
 - Oppbevarer sone-filene («zone files») for et gitt domene
 - Sonefilene inneholder RR'er, inkl referanser til andre navnetjenere og domener
- Rot- og TLD-tjenere endres sjelden
- DNS-tjenere refererer til andre DNS-tjenere ved DNS-navn, ikke IP; må derfor legge inn spesielle «**glue records**»

DNS Treet



Navneoppslag i DNS

- Når svaret ikke er cachet



Pharming og phishing

- **Phishing**

- Å lage en webside e.l. som ser ekte ut, og får offeret til å oppgi informasjon (passord, kredittkortnummer, ...)
- Ulempe: Må lure offeret til å trykke på en (feil) link

- **Pharming**

- Å legge inn falske IP-adresser forbundet med ekte DNS-navn
- Mål: å lede offeret til å laste ned malware eller legge inn brukernavn/passord e.l.
- Fordel: Offeret går SELV til nettsiden (feks banken) og blir derfor lettere lurt!

DnB Bank dnb@dnb.com
to undisclosed recipients ▾



Sikkerhet Notice

DNB ATM card: Suspendert
Internett-kontoen tilgang: Suspendert

Denne sikkerhetsoppdateringen merke til er å gi deg råd om at du har mistet ditt
Password Reset ble nylig forsøkt på Internet Banking konto.

Hvis du er uvitende om disse endringene, kan du gjenopprette kontoen
braker:

<http://www.dnb.no/appo/logson/no/Start/>

Takk for at du bruker DNB Bank

Postadresse: N-0021 Oslo
Org.nr. DNB ASA: 981 276 957

Du mottar denne e-posten som registrert abonnent av DNB Bank varsler.
Ved å abonnere på og / eller bruke DNB Bank,
du erkjenner avtale til våre Vilkår for bruk.

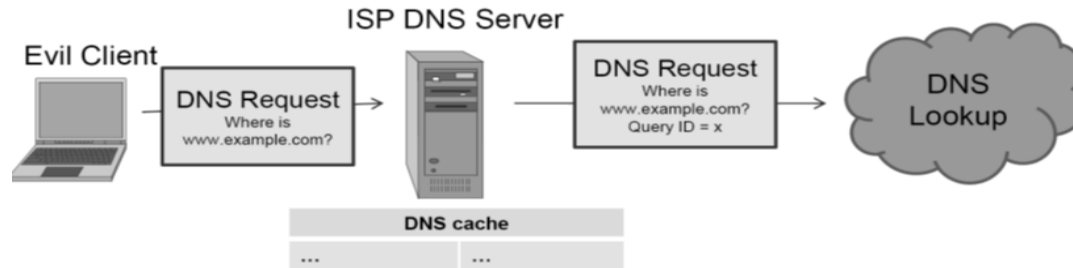
PHISHING

DNS cache-forgiftning

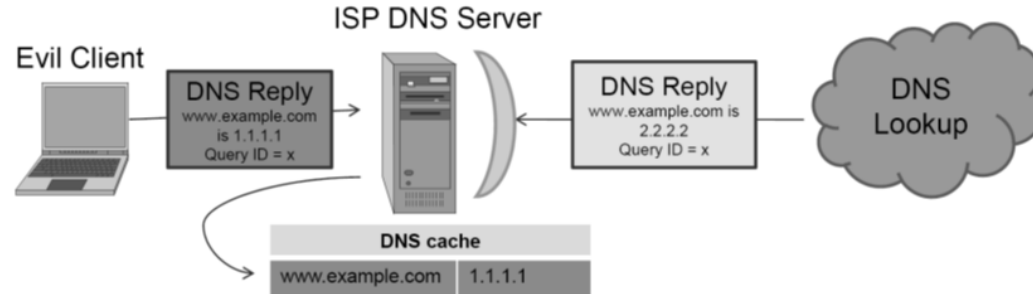
- Gi DNS tjenere (eller resolvere) falske svar og få dem cachet
- DNS benytter en 16 bits Request ID
 - Samordner spørsmål mot svar ut fra ID
- Cache kan dermed f.eks. forgiftes dersom en NS:
 - Ser bort fra ID
 - Har forutsigbare ID
 - Aksepterer DNS RR som den ikke har spurt om (jf Bonjour multicast)
 - MITM: Noen fanger opp request og sender reply som ankommer før det «ekte»

Forgiftnings-taktikk

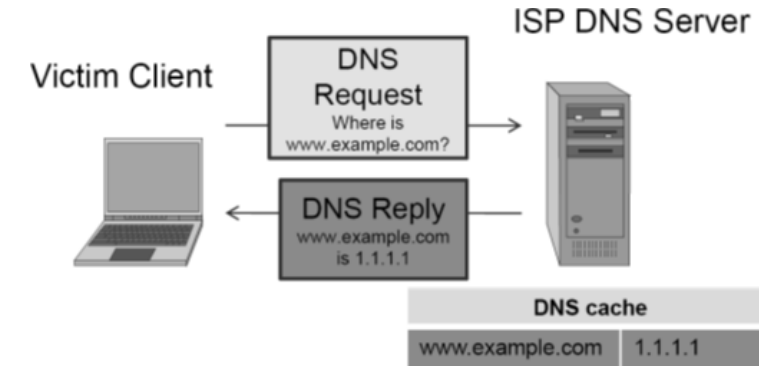
Vi vil forgifte en ISP sin DNS-tjener



1. Vi sender en vanlig forespørsel om domenet til navnetjener



2. Vi sender selv et falskt svar til ISPs navnetjener
 - Hva med ID?
 - **Det tipper vi!**



3. Klienter som benytter ISPs navnetjener vil så bli foret med vår IP-adresse for domenet
 - Legg inn bankkort

Hvor vanskelig er det å treffe ID? ★

- Bursdags-«paradoxet»
 - I et rom med 23 personer er sannsynligheten for at to har samme fødselsdag 50,7%
 - 23 personer er $\binom{365}{23} = 253$ forskjellig par av personer!
 - Sannsynlighet: $1 - \frac{n! \cdot \binom{365}{n}}{365^n} = 1 - \frac{365 \cdot 364 \cdot \dots \cdot 343}{8,5651 \cdot 10^{58}} = 0,507$
- Å gjette riktig DNS-ID er et beslektet problem
 - Sender du n responser på n ulike forespørsler vil du **bomme** i $(1 - \frac{n}{2^{16}})^n$ av tilfellene
 - Etter 213 forsøk har du 50% sannsynlighet for å ha truffet riktig
 - Etter 400 forsøk har 92,4% ...

Svakheter ved taktikken

- TTL-feltet er ofte satt til kort tid
- Kan bare få sendt så mange forespørsler og svar som det tar før ISPs navnetjener får et ekte fra Autoritativ navnetjener.
- En annen teknikk utnytter subdomener og «glue records»:

1) Subdomene-cache-forgifting



- Oppdaget i 2008
- I stedet for å spørre og forfalske svar for et bestemt domene kan man heller spørre/svare om ikke-eksisterende underdomener
 - F.eks. 0000.westerdals.no til ffffff.westerdals.no
- Autoritativ navnetjener vil ignorere spørsmål om ikke-registrerte domener
- Vi får god tid til å tippe oss frem til riktige ID-nummer
- Og så?

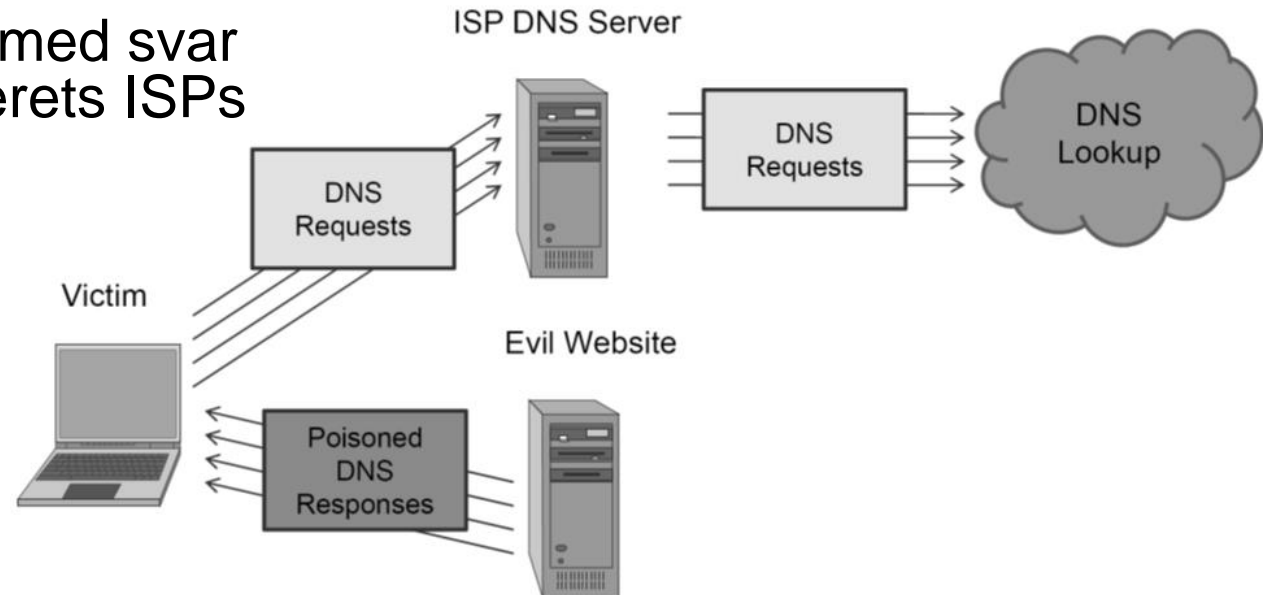
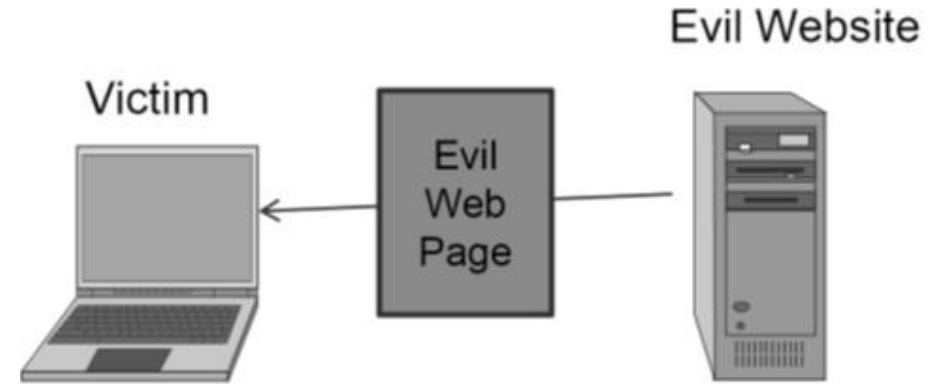
2) «glue records»



- I våre «forfalskede» svar legger vi også inn **vår falske navnetjener** for domenet i **Additional** feltet i DNS-pakken!
 - Dette er der man vanligvis finner info om hva som er **autoritativ navnetjener** som brukes for domenet.
- => **Pharm** established

Forgiftning av klient-cache

- Mange ulike teknikker, en enkel er å lage en webside full av bilder med height= «0», width=«0»; som så har en src=«<http://falsktunderdomene.domenet-vi-vil-forgifte.com/bildefinnesikke/>»
- Så pøser angriper på med svar på DNS-spørsmål offerets ISPs navnetjener aldri får til å besvare..



Motgift?

- Alltid bruke tilfeldige ID
 - Fint, men utilstrekkelig
- Alltid sjekke at det er riktig ID
 - Fint, men utilstrekkelig
- Tilfeldige avsender-porter på DNS-req
 - Fint, men utilstrekkelig (NAT FW endrer og systematiserer gjerne disse igjen)
- Rull ut og ta i bruk **DNSSEC**
 - Ikke så lett som man skulle ønske/tro
 - Mye av den overordnede infrastrukturen er ikke der ennå.

Lokal forgiftning av klient-cache

- Pcer har en lokal DNS oppslagsfil som kan overstyre DNS, kalt «hosts» fil
- På Windows ligger den på
c:\windows\system32\drivers\etc\hosts
- Hvis malware legger inn oppføringer i denne filen vil man redirecte oppslag til feil sted

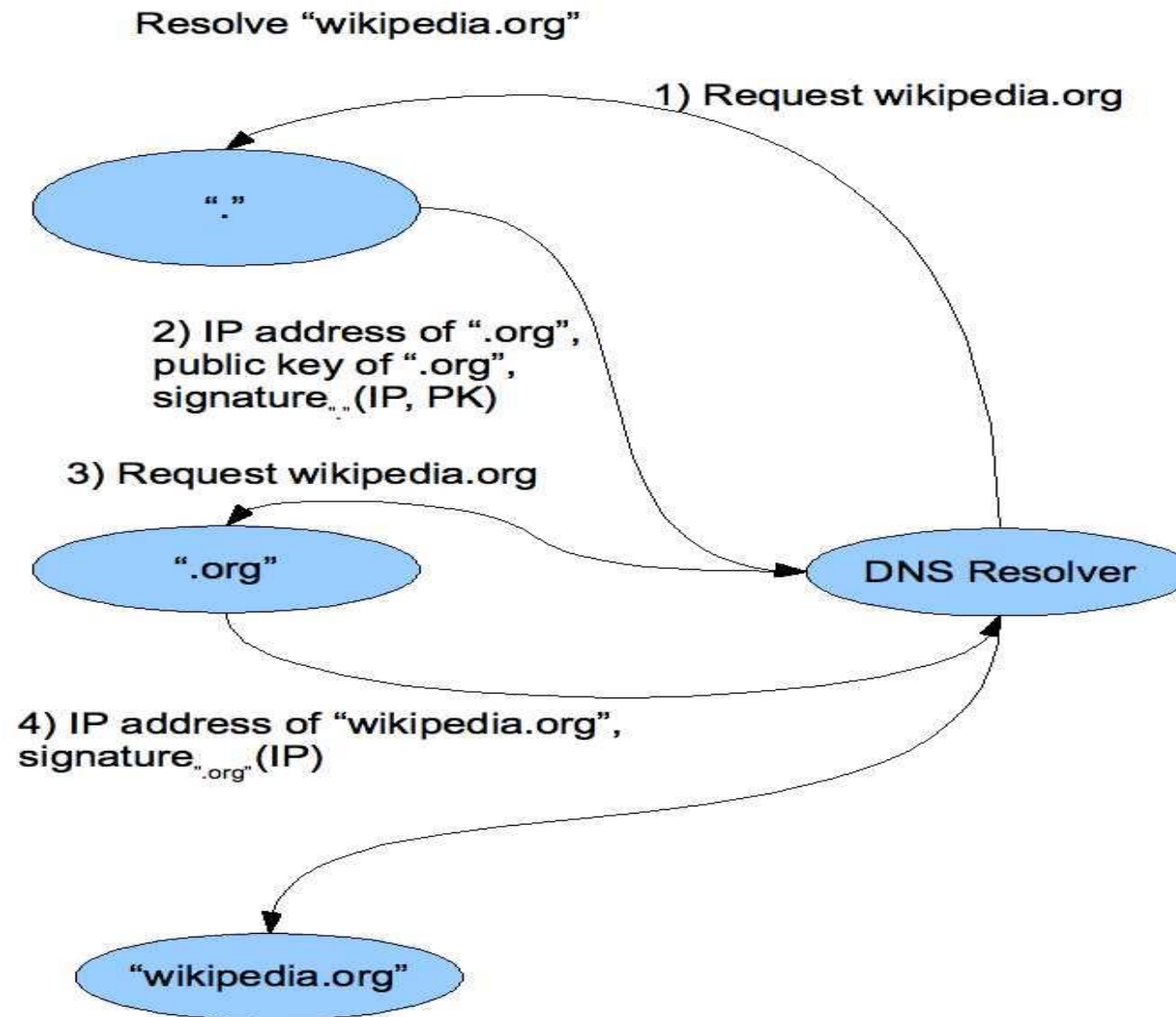
195.88.54.16 www.dagbladet.no

- Tar deg til VG når du prøver å gå til Dagbladet

DNSSEC

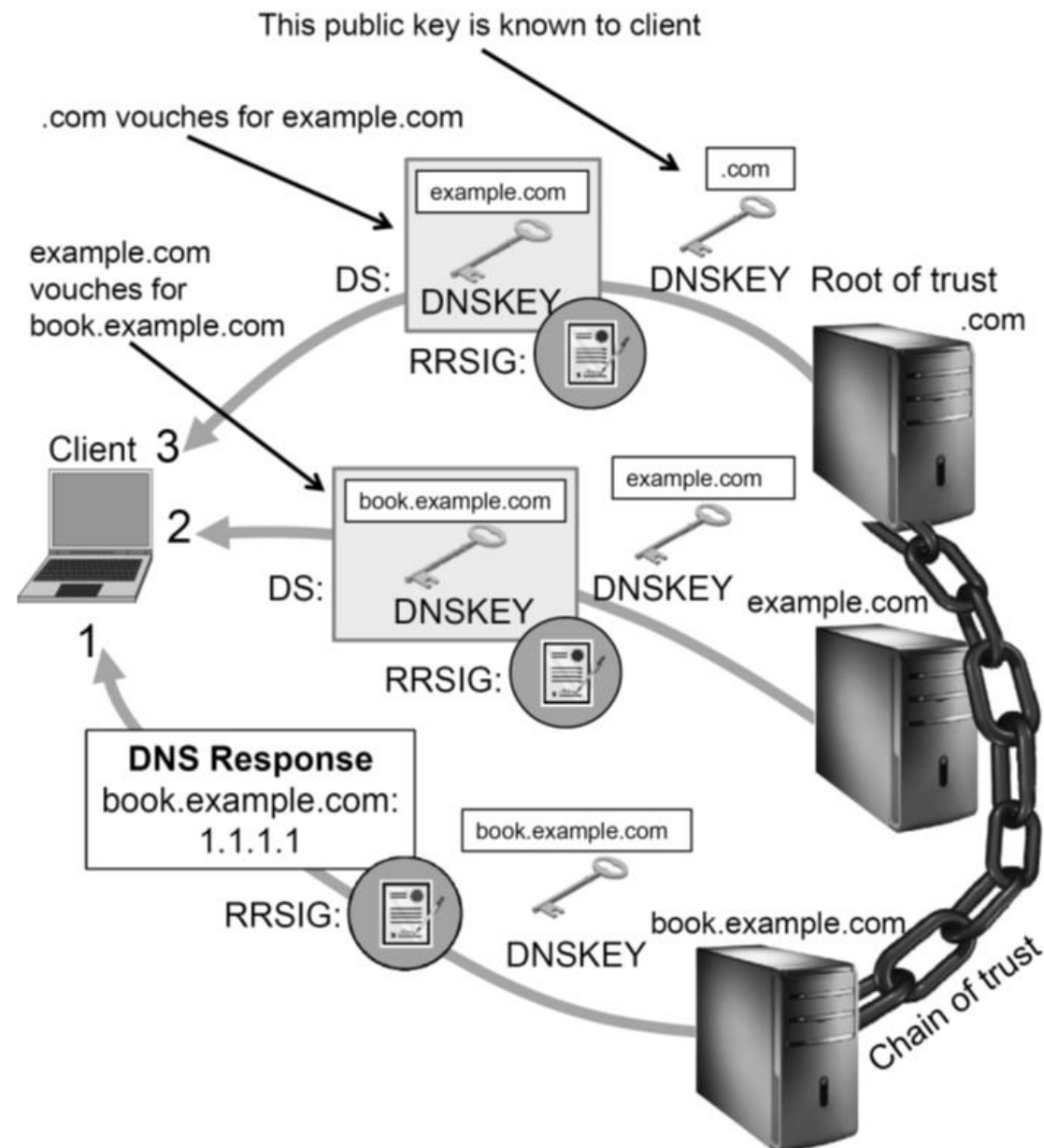
- **DNSSEC** skal rette opp fundamentale svakheter med DNS
 - 16 bit ID
 - Responsen på spørsmål om ikke-eksisterende underdomene er taushet
- Skal garantere
 - Autentisere svar-leverandør
 - Integritet på svar
 - Sporbarhet og sikre eksistens-fornektelse
- Signerer DNS-svar på hvert trinn
- Bruker public-key kryptering for å signere responser
 - Basert på **chain-of-trust** opp til TLD'er

Eksempel: DNSSEC



DNSSEC

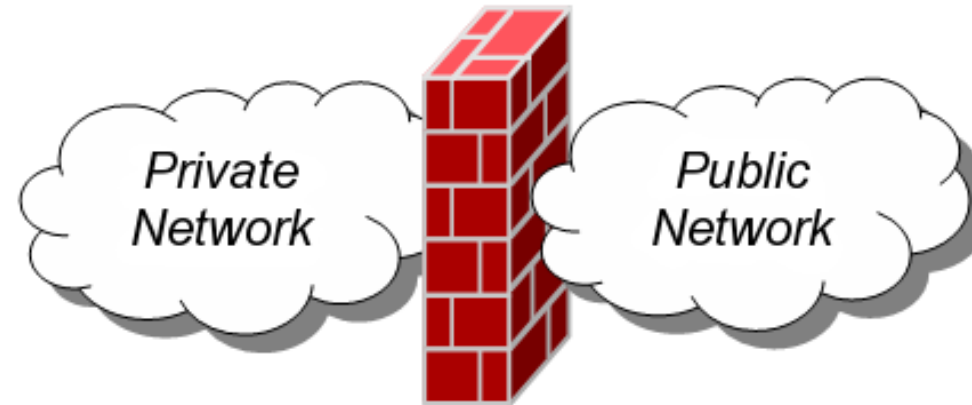
- Juli 2010 var sertifikater for rot-sonen på plass
- Politisk kontroversielt
 - USA får røttene?
 - Ikke alle regimer ønsker kryptert DNS...
- Krever kraftigere DNS-tjenere
- Nye RR'er
- Win7 og 8 støtter DNSSEC, men ikke default
- .no har valgt å utsette DNSSEC
- Begynner nå i 2020 å bli tatt mer og mer i bruk



Brannmurer («Firewall»)

Brannmur

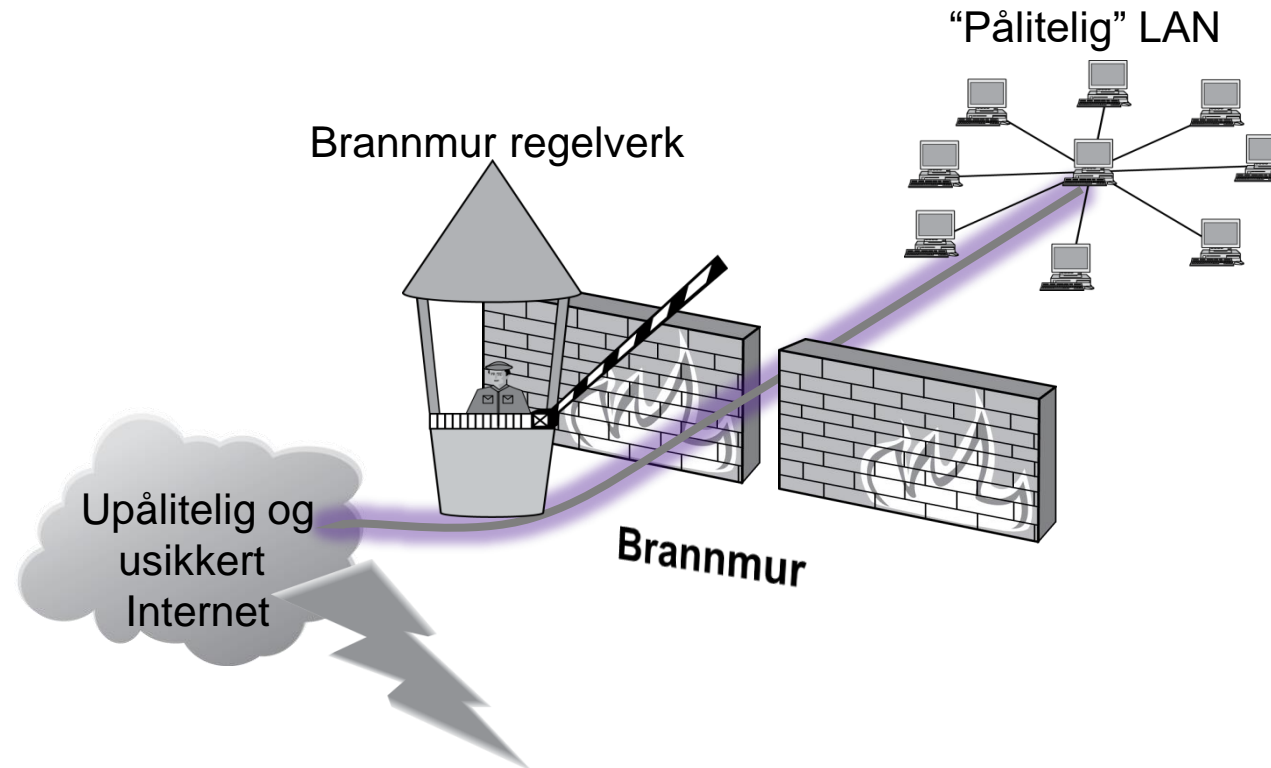
- En **brannmur** («firewall») er en samling av sikkerhetstiltak som skal forhindre uautorisert tilgang til et nettverk (av computere)



- Begrepet er myntet over samme lest som i byggebransjen.
 - Brannmuren skal isolere LAN'et og hindre at «brann» sprer seg inn/ut fra/til andre steder (Internett).

Brannmur regelverk

- For å beskytte nettverk og individuelle maskiner er gjerne brannmuren satt opp til å **filtrere** inngående og utgående trafikk basert på forhåndsdefinerte **regler** («firewall policies»)



Handlinger

- Pakkene som flyter gjennom brannmuren kan lide tre ulike skjebner:
 - **Accepted**: slipper gjennom
 - **Dropped**: slipper **ikke** gjennom, men utløser ingen særlige meldinger/handlinger
 - **Rejected**: slipper **ikke** gjennom, kilden informeres om at pakken ble stoppet.
- Reglene er basert på **egenskaper** ved selve pakkene slik som:
 - TCP, UDP (eller annet)
 - Kilde- og mål- IP-adresser
 - Kilde- og mål-porter
 - Applikasjonslag nyttelasten («deep packet inspection»)

Black- vs White-List

- To forskjellige strategier
 - Minimere sårbarhet (mot eksterne trusler)
 - Beholde funksjonalitet (for interne tjenester)
- **Blacklist** tilnærming
 - **Alle** pakker slipper **gjennom** bortsett fra de som er definert i reglene
 - Mest **flexibel**, men **naiv** da den forutsetter at man kan forutse alle trusler som kan oppstå
- Whitelist tilnærming
 - **Ingen** pakker slipper **gjennom**, bortsett fra de som er definert i reglene

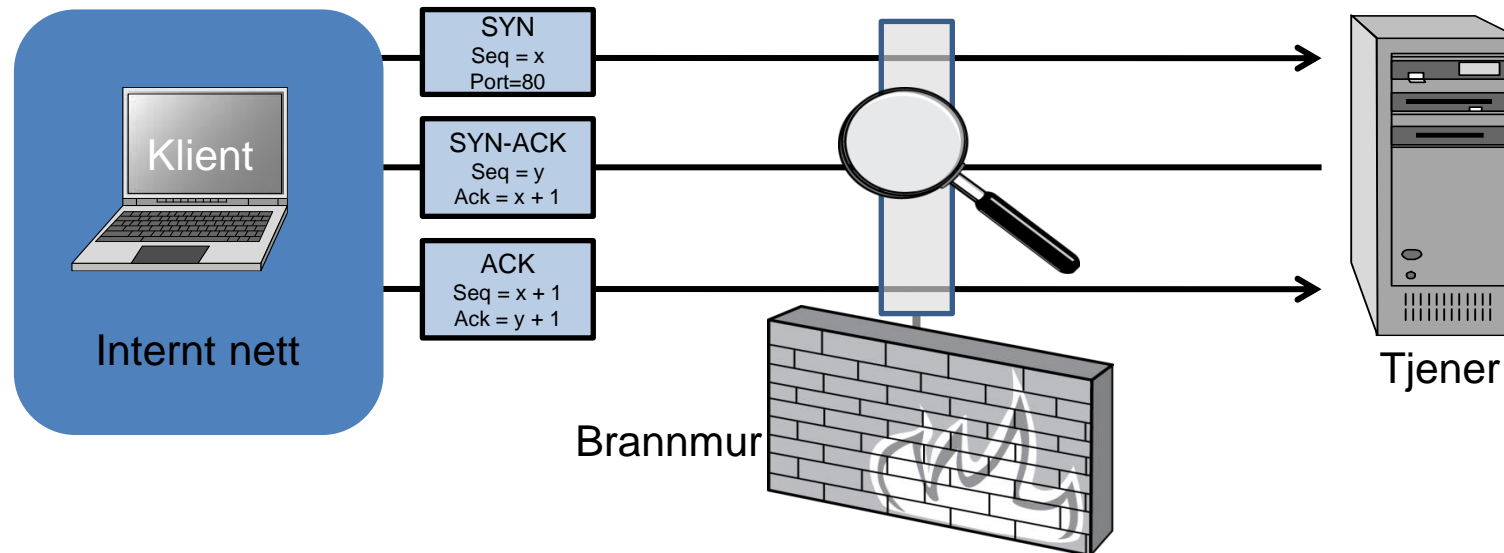
Whitelist

Brannmur TYPER

- **Pakke filter** («tilstandsløse»)
 - Dropper eller aksepterer hver enkelt ankommen pakke kun ut fra regelen
- **«Tilstandsorienterte» filtre**
 - Holder oversikt over alle forbindelser
 - Kan avgjøre om en pakke er starten på en ny forbindelse, del av en etablert, eller ikke akseptabel
- **Applikasjonslag**
 - Fungerer som en «proxy» og kjenner reglene for protokoller og bestemte applikasjoner
 - Inspiserer innholdet og blokkerer det som er definert som uakseptabelt (websteder, virus, sårbarheter, ...)

Tilstandsløs FW

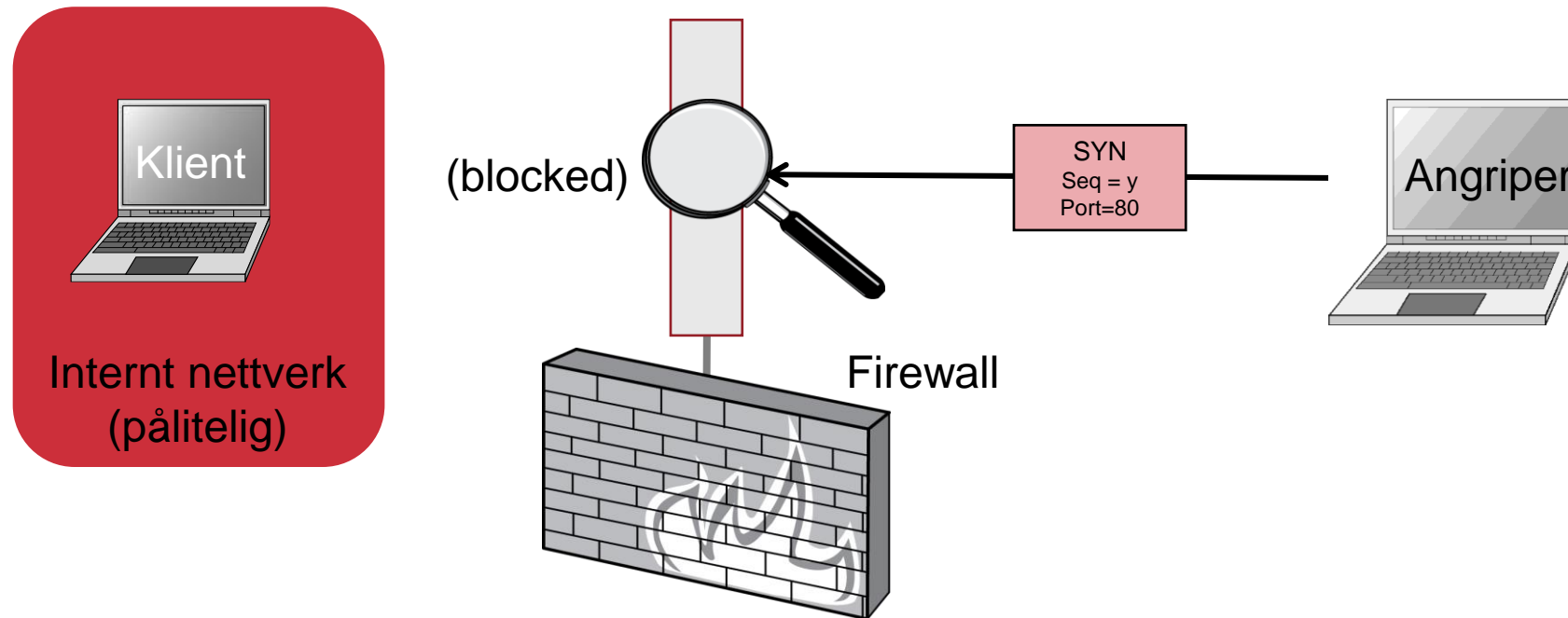
- En tilstandsløs brannmur opprettholder ikke info om sammenhengen («tilstand») for pakkene den prosesserer. Den behandler hver pakke isolert, og tar ingen hensyn til hva den har prosessert tidligere.



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

Tilstandsløs: restriksjoner

- Tilstandsløse brannmurer kan måtte være svært restriktive for å kunne hindre de fleste typer angrep



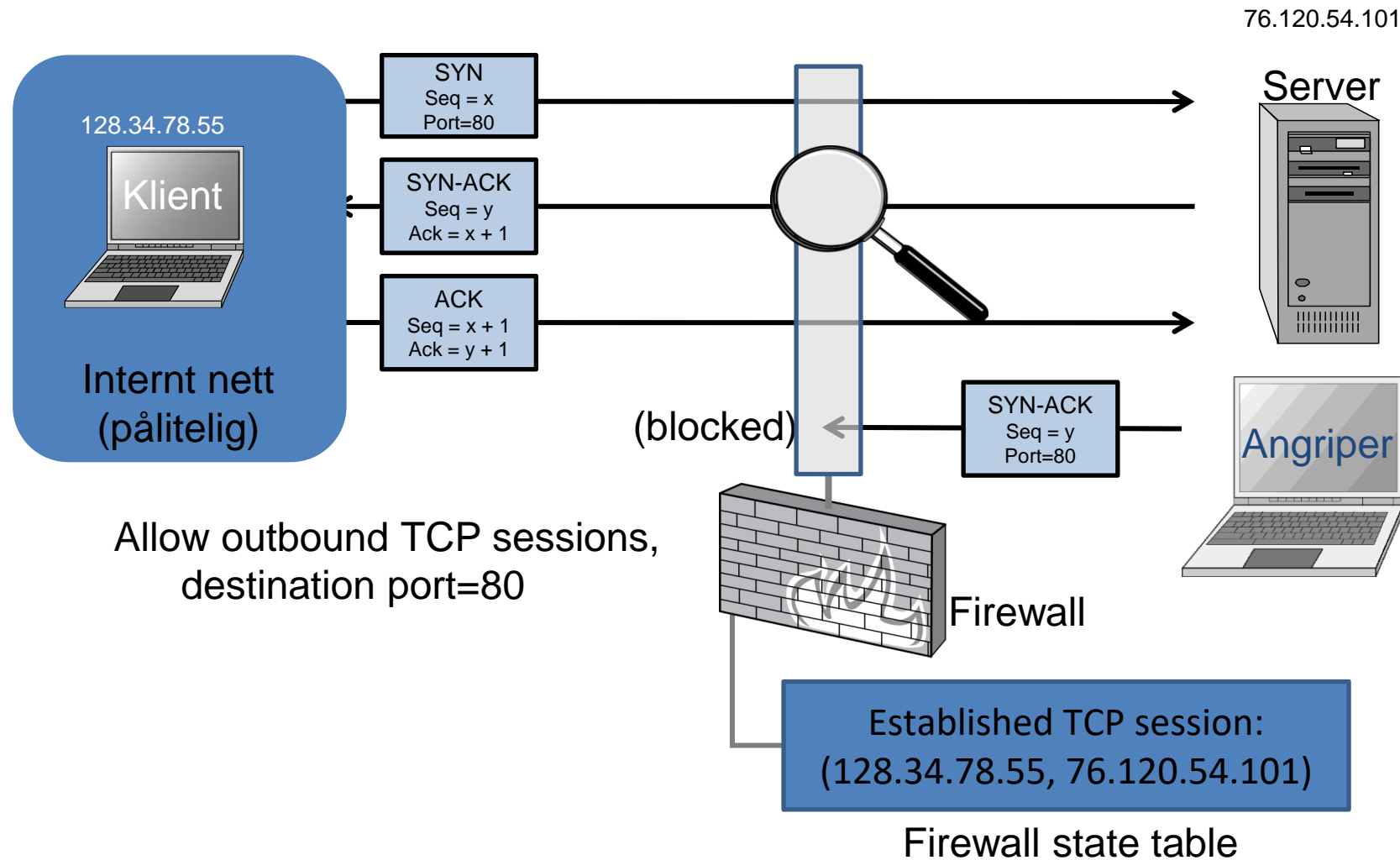
Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Tilstandsorientert FW

- Tilstandsorienterte brannvegger kan se når pakker er del av en legitim sesjon med opphav i et pålitelig nettverk
- Tilstandsorienterte brannmurer opprettholder tabeller med info om hver aktiv forbindelse, inkl IP-adresser, porter, sekvensnummer, osv
- Ved hjelp av tabellene så kan brannmuren f.eks. tillate bare inngående TCP-pakker som inngår i en forbindelse som er initiert fra det pålitelige nettverket

Ex: Tilstandsorientert FW

- Tillat bare TCP forbindelser opprettet innenfra



(Lokal) Personal Firewall

- Software installert på hver maskin som fungerer som en «soft» firewall, i stede for en fysisk boks i nettverket
- Har bedre mulighet til å inspisere på applikasjonslaget da den kjører på samme maskin
- Kan kun se trafikk på EN maskin, mens en hardware firewall kan se på hele nettverket

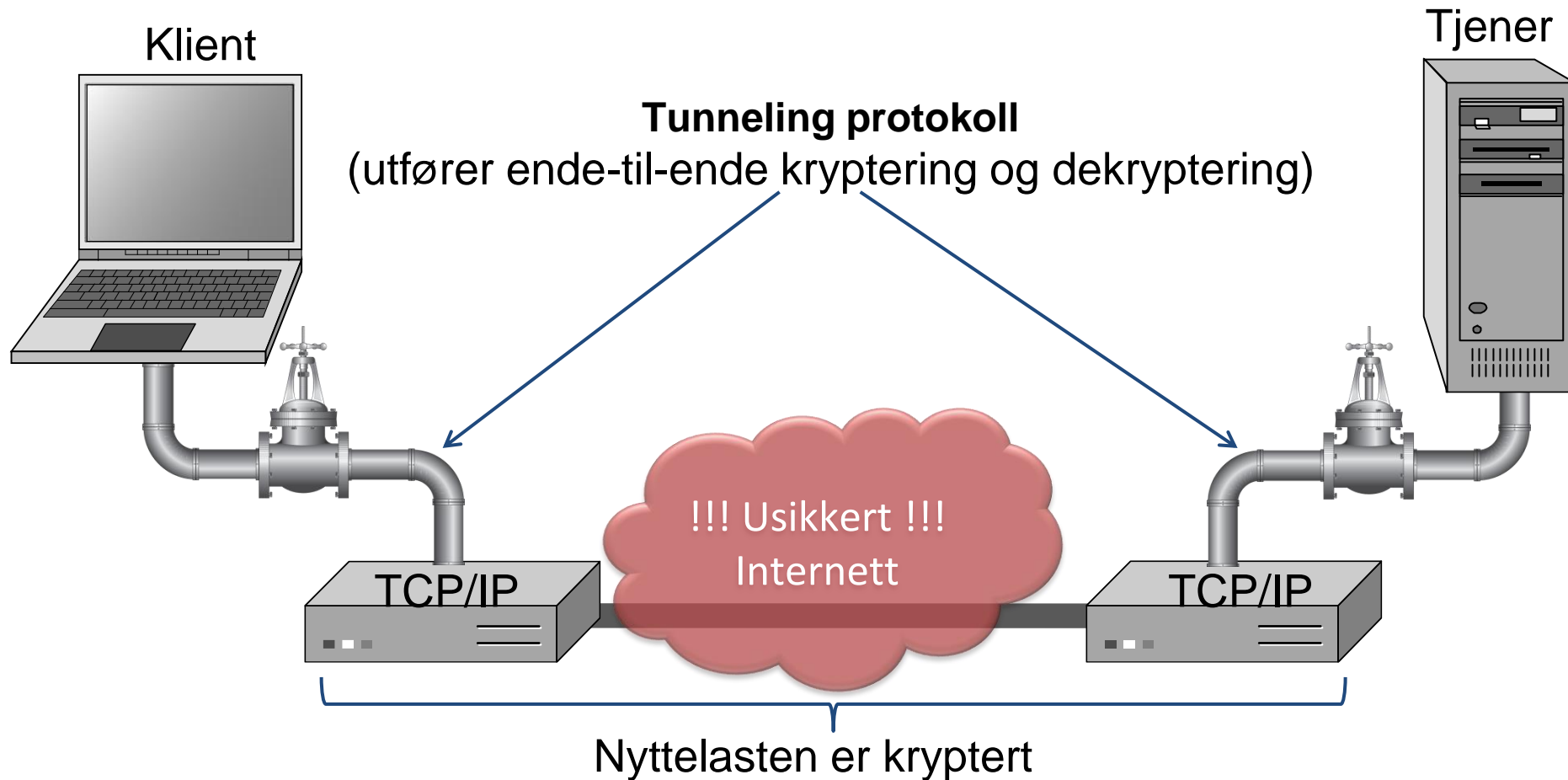
Tunneling

Tunnel?

- Innholdet i TCP segmenter er vanligvis ikke kryptert
 - Dersom noen avlytter («sniffer») kan han se den komplette nyttelasten for sesjonen
- En måte å forhindre avlytting uten å endre annen software er å bruke en tunneling protokoll
- I slike protokoller krypteres kommunikasjonen automatisk og gjør avlytting vanskelig/umulig

Tunneling forhindrer avlytting

- Pakker sendt over Internett kan automatisk krypteres med *tunneling*



Virtual Private Networking (VPN)

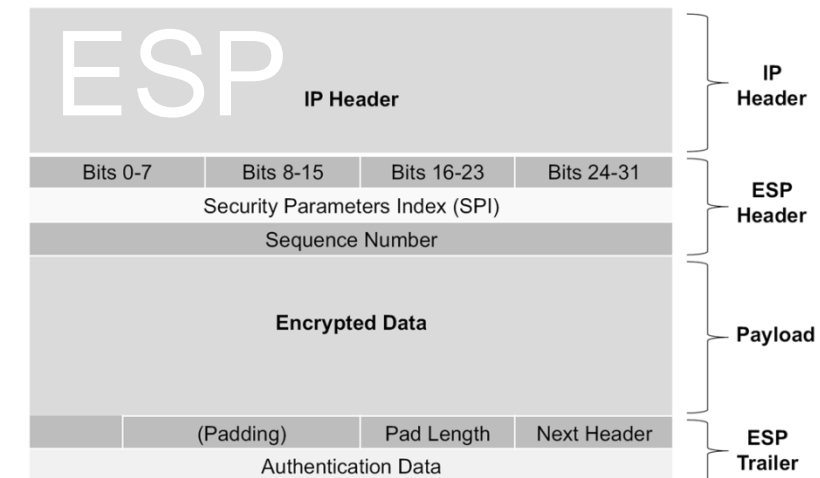
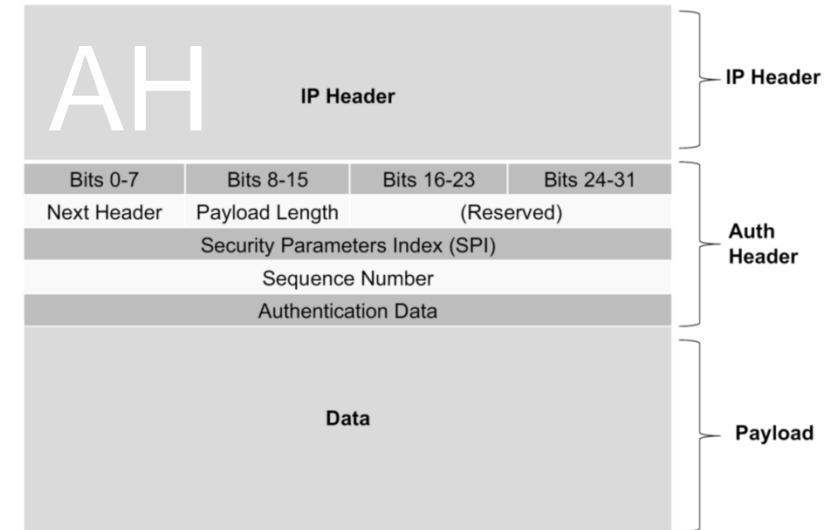
- **VPN** er en fellesbetegnelse på ulike teknologier som tillater sikker tilgang til private nettverk over Internett
- **VPN** skal garantere data konfidensialitet, integritet og autentisering, til tross for usikkert transport-nettverk
- To hovedtyper
 - Remote Access VPN
 - Site-to-site VPN
- Typisk sikret med enten IPSec eller SSL/TLS

Typen VPN

- **Remote Access:** VPN som gir autoriserte klienter tilgang til et privat nettverk («intranett»)
 - Brukeren har installert VPN-klient på egen maskin og kopler seg opp til en NAS («Network Access Server»)/ VPN konsentrator
 - Gir tilgang til LAN-interne ressurser, som ser ut som om du sitter i LANet
- **Site-to-site:** VPN løsninger som knytter sammen et WAN og fungerer som en sikker bro mellom to/flere fysisk adskilte nettverk (rundt i verden) over Internett
 - Typisk VPN-konsentrator på Gateway på begge sider.
 - Før VPN brukte man **leide linjer**, og det var dyrt
- **«Personlig» VPN / Anonymisering:** VPN man kjøper som privatperson har en annen hensikt, ved å gå gjennom VPN som privatperson kan man oppnå anonymitet fordi trafikken går gjennom en VPN tjeneste
 - Blir som en site-to-site VPN, mellom en klient og VPN tjenesten?

IPSec

- IPSec definerer flere protokoller som tilbyr
 - **Autentisering** (AH-protokoll)
 - og **integritet** og **konfidensialitet** (ESP-protokoll)
 av IP-datagram
- Hver protokoll kan operere i to ulike modus:
 - **Transport**: Det legges inn en IPsec-header før nyttelasten i den opprinnelige pakken.
 - Det er bare nyttelasten som krypteres og autentiseres.
 - **Tunnel**: hver IP-pakke **krypteres i sin helhet** og så legges det på en IPSec-header
- Se <http://www.unixwiz.net/techtips/iguide-ipsec.html>



Innbruddsalarmer («Intrusion detection»)

Intrusion Detection System

- Intrusion («innbrudd»)
 - Handlinger som utføres for å **kompromittere** sikkerheten til offeret (konfidensialitet, integritet, tilgang til maskin-/nettverks-ressurser)
- Intrusion Detection
 - **Identifisering** og rapportering ved hjelp av innbrudds-**profiler** («signatures») av innbrudds**aktiviteter**.
- Intrusion Prevention
 - Å både **oppdage** innbruddsforsøk og **administrere** automatiske **responser** i nettverket

Typer IDS

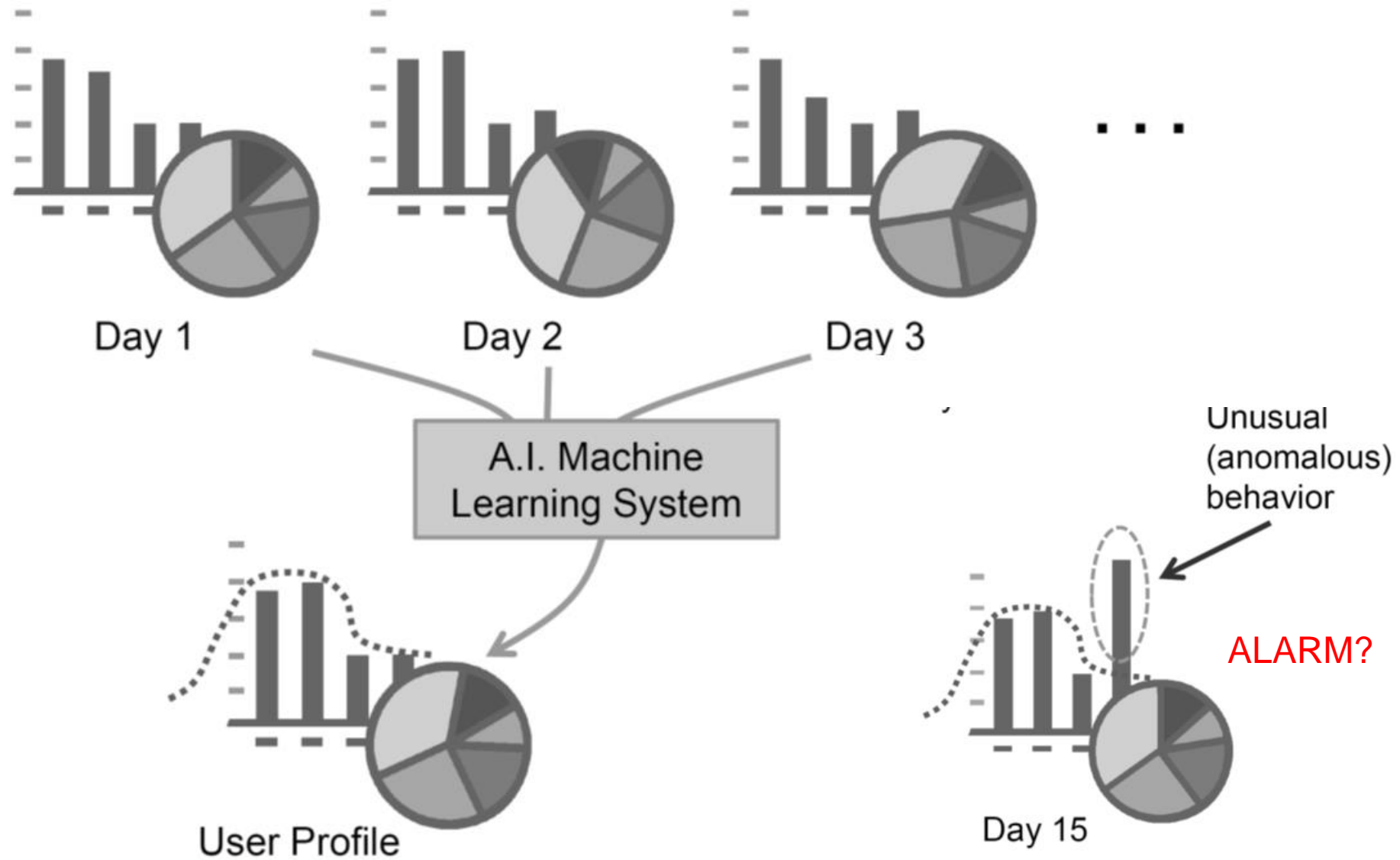
- Regel-basert

- Reglene identifiserer typene handlinger som matcher kjente profiler på innbrudd («signatur»)
 - F.ex. 300% økning i ICMP-trafikk
- IDS manager kjører alarm ved hendelsen
- Styrke: kraftig, lett å sette opp (mye ferdig laget)
- Svakheter: angriperne kjenner reglene...

- Statistisk

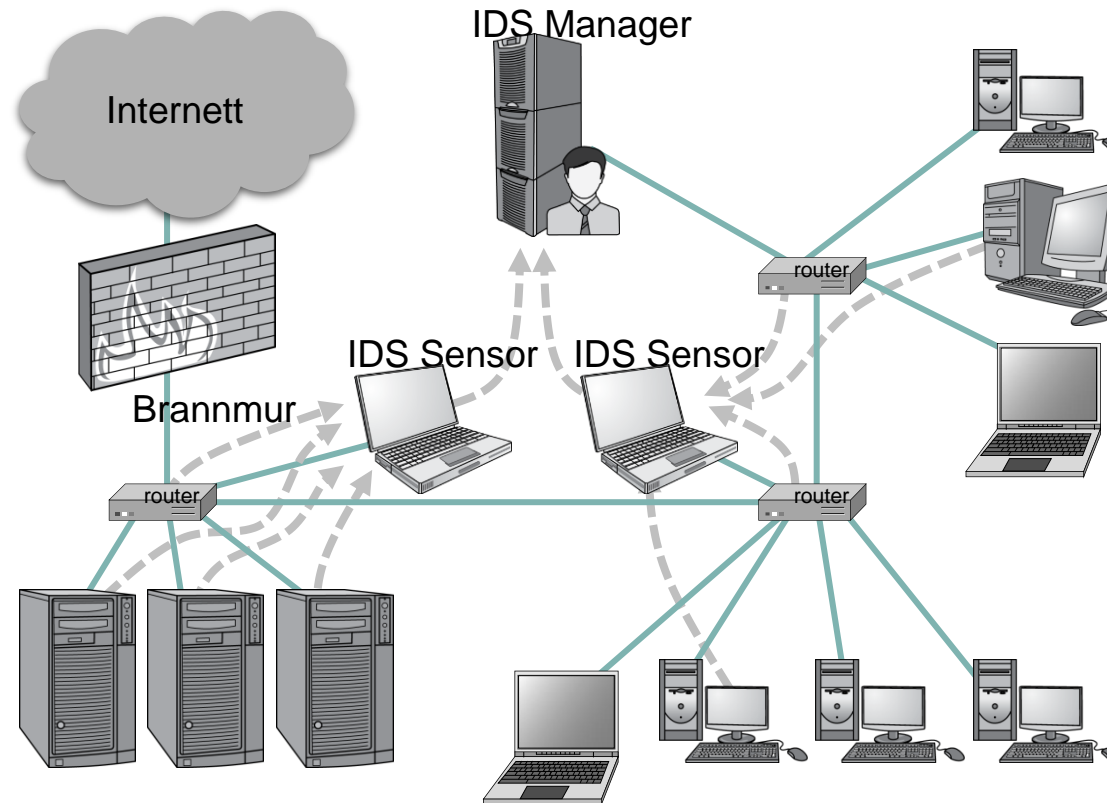
- Bygger opp en *statistisk* profil av typisk bruker- og host-adferd
- IDS manager («sys adm») bestemmer terskler for hva som er unormal adferd og skal utløse alarm når en bruker/host avviker betraktelig fra den lagrede profilen

Statistisk IDS



IDS komponenter

- IDS manager samler data fra **sensorer** for å avgjøre om et innbrudd har skjedd eller er i gang
 - Avgjørelsen baseres på et sett regler («site policies») som definerer ulike **indikatorer** på **sannsynlig** innbrudd
- Dersom IDS manager oppdager et innbrudd, går en **alarm**



Mulige Alarmer

- Vi kan gruppere ulike alarmer vs innbrudd ut fra hvor vidt det faktisk er innbrudd og om alarmen gikk eller ikke

		Intrusion Angrep	Ikke Intrusion Angrep
Alarm Gikk		Sann Positiv	Falsk Positiv
	Alarm Gikk IKKE	Falsk Negativ	Sann Negativ

- Det at alarmen går kan bety to vidt forskjellige ting
- Det at alarmen **ikke** går kan bety to vidt forskjellige ting

Grunnsannsynlighet-problemet

- Det er vanskelig å lage et IDS som har både høy sann-positiv og lav falsk-negativ
 - Dersom antall faktiske innbrudd er lavt i forhold til mengden data som IDSet analyserer, så kan effektiviteten bli meget dårlig.
- Det er lett å mistolke antall alarmer ut fra en statistisk feiltolkning som er kjent som «base-rate fallacy»
 - Oppstår når man tolker sannsynligheten til en **betinget** hendelse uten å ta hensyn til grunn-sannsynligheten for hendelsen

Eksempel

- Anta at IDS er 99% korrekt med 1% sannsynlighet for **falske positive** og **falske negative**
- IDSet logger 1.000.100 hendelser
 - Bare 100 av disse er faktiske innbrudd (0,001% av alle loggede hendelser er faktisk angrep)
- Av de 100 innbruddene vil 99 bli oppdaget, vi har da 1 falsk negativ
- Av 1.000.000 hendelser vil likevel 10.000 bli feildiagnostisert som ondsinnede. M.a.o. **10000 falske positive!**
- Vi hører 10099 alarmer. Ca 99% av dem er falsk alarm!

86

Portscanning?

- Portnummerne er veien til prosessene

```
C:\>netstat -b
```

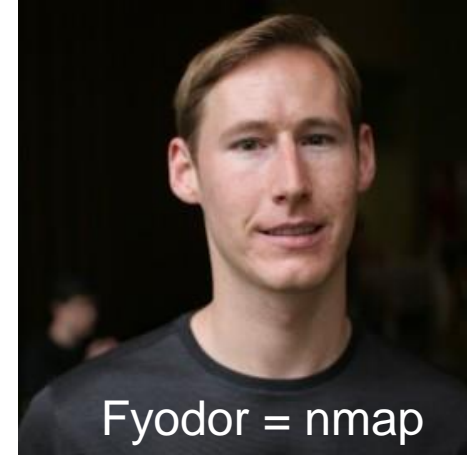
```
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	10.21.24.224:25306	bk-in-f125:5222	ESTABLISHED
[googledrivesync.exe]			
TCP	10.21.24.224:31836	r-199-59-148-147:http	ESTABLISHED
[chrome.exe]			
TCP	10.21.24.224:31837	r-199-59-148-147:http	TIME_WAIT
TCP	10.21.24.224:31868	158.36.187.204:https	ESTABLISHED
[chrome.exe]			
TCP	10.21.24.224:31890	r-199-59-150-7:https	ESTABLISHED
[chrome.exe]			
TCP	127.0.0.1:1218	localhost:27015	ESTABLISHED

- Brukes av **oss** for å avdekke våre egne svakheter og fixe dem

nmap

- Stadig kåret til det beste av alle sikkerhetsverktøy
- Ekstremt kraftig
 - I datasammenheng betyr det ofte at det også er uoversiktlig, har dårlig dokumentasjon og det er **lett** å gjøre alvorlige feil
- Ekstremt innpåslitent og sleipt
- Ekstremt lett å oppdage for IDS (dersom man ikke er forsiktig)
- Ofte ulovlig dersom man ikke har tillatelse og bruker det korrekt.



Kartlegg LAN (ping-scan)



- **-sP** ping-skanner IP-range oppgitt og lister opp responsene

```
C:\>nmap -sP 10.21.4.0/22

Starting Nmap 5.51 ( http://nmap.org ) at 2012-02-28 20:44 W.
me
Nmap scan report for 10.21.4.1
Host is up (0.00s latency).
MAC Address: 00:22:55:3E:DA:BA (Cisco Systems)
Nmap scan report for dhcp.ad.nith.no (10.21.4.2)
Host is up (0.0020s latency).
MAC Address: 00:50:56:93:00:0A (VMware)
Nmap scan report for 10.21.4.4
Host is up (0.0010s latency).
MAC Address: 00:23:33:B2:BB:03 (Cisco Systems)
Nmap scan report for prometheus.ad.nith.no (10.21.4.101)
Host is up (0.0020s latency).
MAC Address: 00:0C:29:F2:0B:E2 (VMware)
Nmap scan report for 10.21.4.103
Host is up (0.0010s latency).
MAC Address: 00:0C:29:A0:DA:FC (VMware)
Nmap scan report for windows-hm857el.ad.nith.no (10.21.4.121)
Host is up (0.0010s latency).
MAC Address: D8:D3:85:77:CD:E6 (Hewlett Packard)
Nmap scan report for 10.21.4.122
Host is up (0.0010s latency).
MAC Address: D8:D3:85:77:A0:67 (Hewlett Packard)
Nmap scan report for windows-675bm5s.ad.nith.no (10.21.4.126)
Host is up (0.0010s latency).
MAC Address: D8:D3:85:77:A0:46 (Hewlett Packard)
Nmap scan report for windows-s96hjb4.ad.nith.no (10.21.4.127)
```

Hvordan oppgi mål?



- Enkeltadresse
 - DNS-navn: `www.westerdals.no`
 - IP-adresse: `158.36.131.51`
 - Nettverk:
 - `10.21.24.0/22` (hele student-WLAN på skolen)
 - Utvalgte områder i mange nett
 - `10.21.4-24.1-35`
 - Brede områder
 - `0-155.0-255.13.23` (alle adresser som slutter på `13.23..`)
 - Gambling
 - `iR <antall>` (scan <antall> tilfeldige adresser...)
-
- Husk at man ikke skal portscanne uten tillatelse, og dere har IKKE tillatelse til å teste skolens nettverk :-)

Port scanning

- Nmap skanner «default» i overkant av 1660 («interessante») porter
- Status angis som
 - Open
 - Aksepterer TCP eller UDP
 - Closed
 - Host har IP-adressen
 - Ser ikke ut til at noen appikasjon lytter
 - Prøv senere?
 - Filtered
 - Ingen respons på probe
 - Brannmuren stoppet sannsynligvis
 - Unfiltered
 - Porten er tilgjengelig, men tilstand uklar
 - Brukes til å kartlegge brannmurens regler
 - Prøv SYN, Win og FIN scan
 - Open|filtered
 - Usikkert om åpen eller filtrert (FW)
 - Closed|filtered
 - Usikkert om lukket eller filtrert (FW)

OS detektering



- Bruker ulike TCP og UDP scans
 - Utnytter forskjellene i TCP/IP-implementasjonene mellom ulike OS og versjoner
- Sammenligner med `nmap-os-fingerprints` databasen
 - O (prøv å finne hva slags OS)

```
C:\>nmap -O 10.21.4.163
```

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-02-28 21:17 W. Europe Standard Time
Nmap scan report for 10.21.4.163
Host is up (0.00027s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-term-serv
5357/tcp  open  wsddapi
MAC Address: D8:D3:85:7F:94:BC (Hewlett Packard)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|2008|7 (92%)
Aggressive OS guesses: Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (92%), Microsoft Windows Server 2008 (90%), Microsoft Windows Server 2008 Beta 3 (90%), Microsoft Windows 7 Professional (90%), Microsoft Windows Server 2008 R2 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Ex: Sjekk bestemte porter



- -p <portliste>
- -v (verbos – få vite hva som foregår under scanningen)

```
nmap -sV -p 80,443,3306 -v 127.0.0.1|_http-server-header: nginx/1.9.4
```

```
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up (0.0010s latency).
```

PORT	STATE	SERVICE	VERSION
80/tcp	closed	http	
443/tcp	closed	https	
3306/tcp	open	mysql?	

Ex: Spennende skript



-script parameter kjører ferdig skript for å finne blant annet sårbarheter

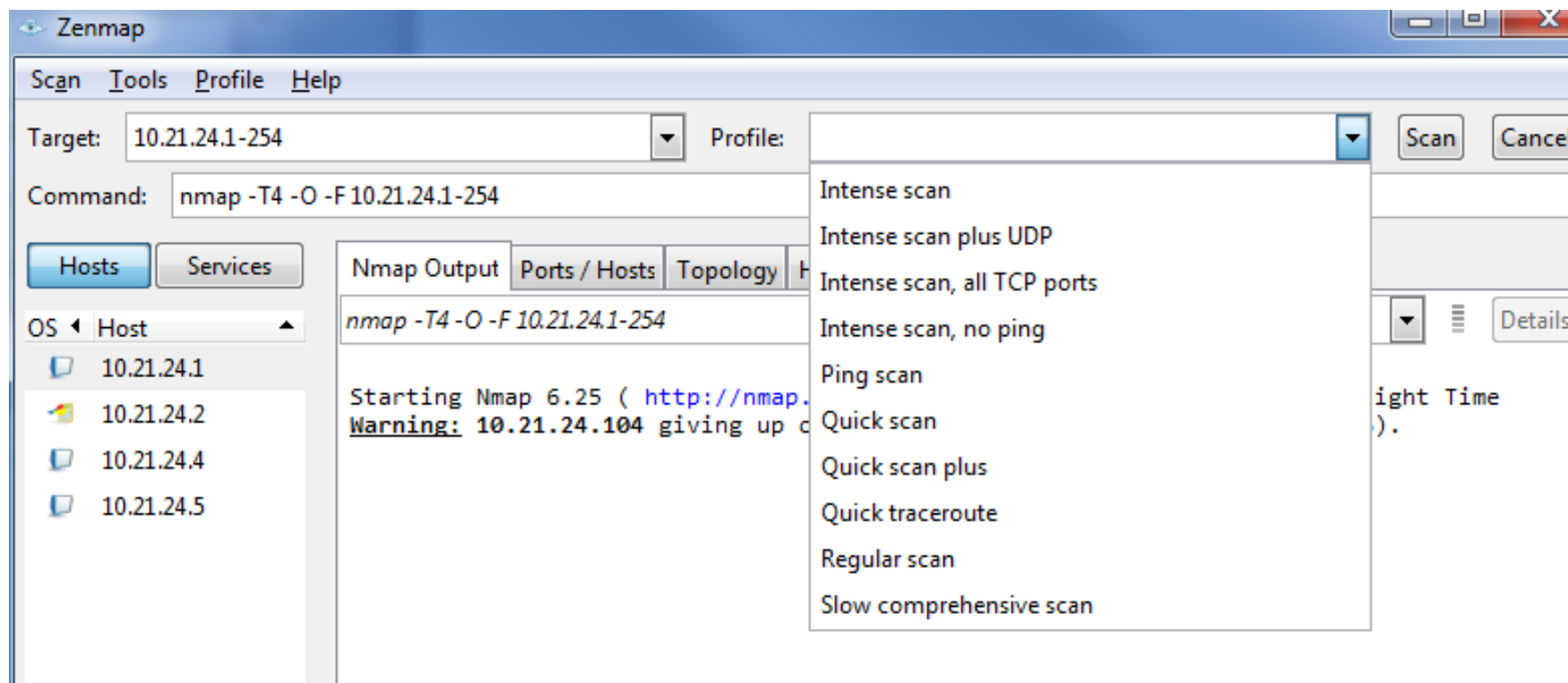
Nmap –script vuln 127.0.0.1

Veldig bra skript som finner interessante sårbarheter på åpne porter.

```
80/tcp  open  http          nginx 1.9.4
|_http-server-header: nginx/1.9.4
| http-vuln-cve2011-3192:
|   VULNERABLE:
|     Apache byterange filter DoS
|       State: VULNERABLE
|       IDs:  OSVDB:74721  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|       Disclosure date: 2011-08-19
|       References:
|         http://nessus.org/plugins/index.php?view=single&id=55976
|         http://osvdb.org/74721
|         http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|         http://seclists.org/fulldisclosure/2011/Aug/175
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_
```

ZenMap

- GUI med profiler (ferdige oppsett for forskjellige typer scan



Med på lasset..



- Når du installerer nmap får du også med nping og ncat
- **nping**
 - Lar deg «spikke til» de fleste typer pakker med det innholdet og de headerene du vil...
- **ncat**
 - Lar deg åpne porter lokalt og bestemme responser
 - Lar deg sende
 - Modernisering av nc..

Avslutning

Hva skal vi kunne?

- **Link-laget**
 - MAC-adresser kan «forfalskes»
 - ARP-spoofing og –poisoning
 - Beskyttelsesmuligheter
- **Nettverkslaget**
 - IP-spoofing (f.eks. i DoS)
 - Brukes i de fleste typer angrep på lag over
 - ICMP (og smurfing)
- **Transportlaget**
 - TCP: SYN- og ACK-angrep; sesjons-kidnapping
- De fleste typer angrep på de nederste lagene er enten destruktive DoS-angrep, eller ulike former for MITM/Maskerade-angrep.

Hva skal vi kunne?

- DNS funksjonsmåte og sårbarheter
 - Oppbyggingen av DNS
 - Spoofing og ulike typer forgiftning
 - Definere pharming og phishing
 - (fødselsdagsparadoxet)
 - DNSSEC
- Brannmur
 - Definere og forklare
 - Typer: Filter, Tilstandsorientert, Deep Packet Inspection
 - Kjenne igjen FW-regler
 - Definere black vs white-list
- Tunneling
 - Definere og eksemplifisere
 - Definere VPN
 - IPSec typer og anvendelse
- Hva IDS er og kan reagere på.
 - Hvordan forholde seg til falske positive/negativer
- Nmap
 - Hva portscanning kan og ikke kan fortelle om offeret

Dagens teori oppgaver

TK2100_F06_del1_øvingsoppgaver.pdf

TK2100_F06_del2_øvingsoppgaver.pdf

Det er ganske mange spørsmål i dag, og mye stoff og sette seg inn i, jeg forventer at dere må fortsette på disse oppgavene neste uke – til gjengjeld er det «færre» spørsmål til Forelesning 7 og 8 (i alle fall relativt til denne uken)

Dagens praktiske labøvelse

NMAP

Oppgave 1: Installer ZENMAP; <https://nmap.org/download.html>

Oppgave 2: Scan 127.0.0.1

Oppgave 3: Start Flowershop – scan 127.0.0.1

Oppgave 4: Hvis man ønsker å finne noen sårbarheter (parameter –script vuln) kan dere prøve å finne en gammel versjon av Apache eller OpenSSH