“Kom og hent dem”

- Mange måter å bli infisert på...
- Hvem stenger port 80 ut?
- Browseren “er” OSet
  - Stadig flere applikasjoner
  - Stadig økende kompleksitet

- Dagens tema:

Drive-by-infeksjoner

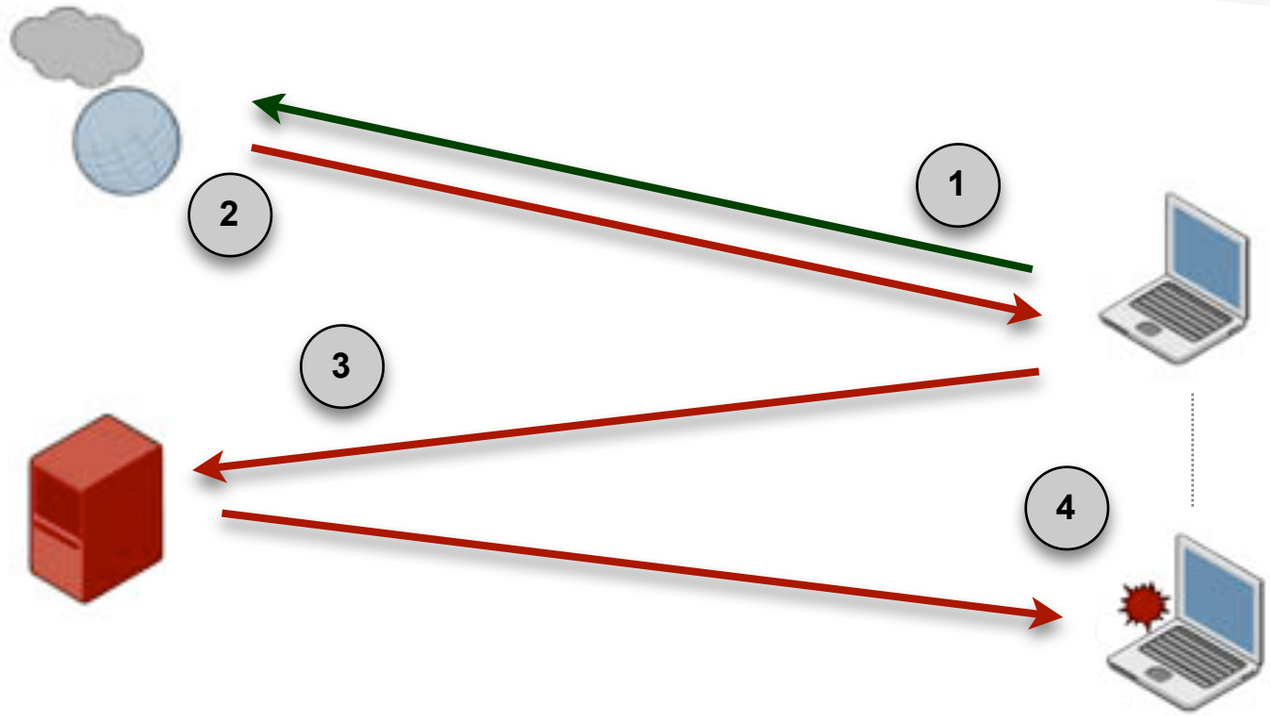
UNINETT

Agenda

- Drive-by-infeksjoner
  - Hva og hvordan
  - Svakheter på webserver-siden
- Live demo

UNINETT

Overblikk – typisk case



1. “Uskyldig” surfing på web
2. HTML m/ekstra grums
3. (Skjult) request til ny webserver
4. Ondsinnet kode kjøres i browseren

Tre hovedelementer

- "Trafikkgenerator"
  - Få brukeren til å surfe til "riktig" sted
- Exploit-engine
  - Skaff adgang til brukerens maskin
- Payload
  - Benytt maskinen til ønsket formål

UNINETT

Noen trafikkgeneratorer

- Spam
  - E-post med lenker, f.eks. type Storm
  - Kommentarspam i blogger o.l.
- Instant Messaging
  - Social engieneering med gode odds
  - Nå også i norsk språkdrakt

- XSS
  - Javascript/Vbscript (obfuskert)
  - ActiveX
  - IFRAME-injection
  - Holy grail: Facebook, MySpace o.l.
- Typo-squatting domener
  - www.goggle.com (2006)

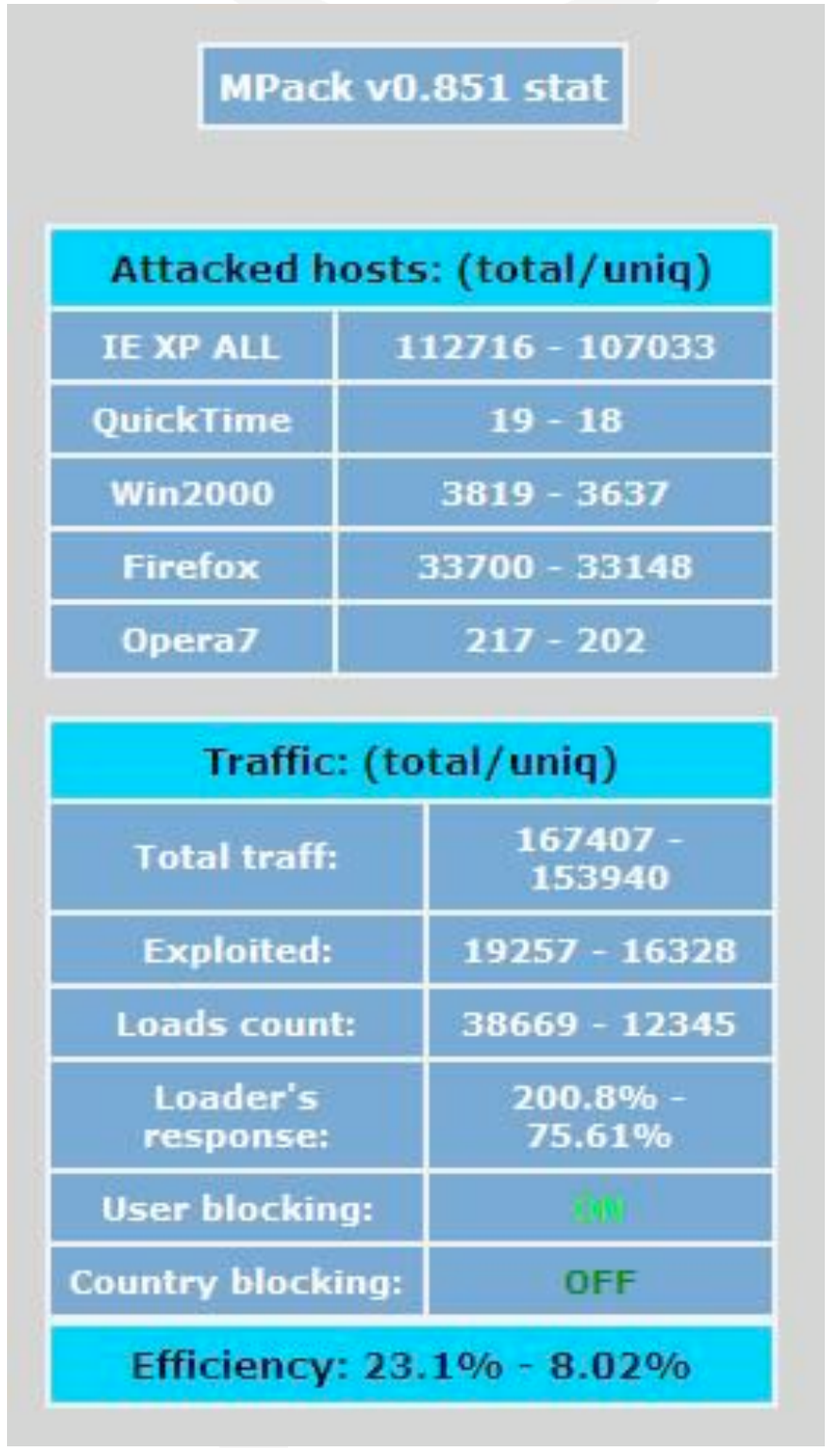
Exploit-engine, oppbygning

- Først: valgfritt antall redirects
- Om mulig: browser exploit
  - Prøv de mest sannsynlige først
  - Basert på info sendt i request
- Fallback: trojaner
  - Forsøk å få brukeren til å kjøre fila
  - "You need this video-codec to...."
- Hyllevare tilgjengelig
  - Neosploit
  - MPack

UNINETT

Eksempel: MPack

- Ferdig pakke
- Skrevet i PHP
- Kan kjøpes for $40
- Har mange exploits
- Oppdateringer



Payload

- Fantasien setter grenser
- Populære varianter:
  - Spyware/Adware
  - Spam proxy
  - Bot'er av ymse slag
- Mer subtile triks
  - Endring av lokale DNS-innstillinger
  - Endring av din hjemmeruters DNS-innstillinger (!) (vha. XSRF)

UNINETT

XSS

- Cross-Site Scripting
- Svakhet, oftest i web-applikasjoner
- Muliggjør tillegg av kode i websider
  - HTML/JS/VB-kode, iframe/ActiveX-komponenter/Flash
  - Tolkes og kjøres lokalt i besøkende nettleser
- Veldig ofte grunnet manglende eller feil håndtering av “rikt innhold”.

UNINETT

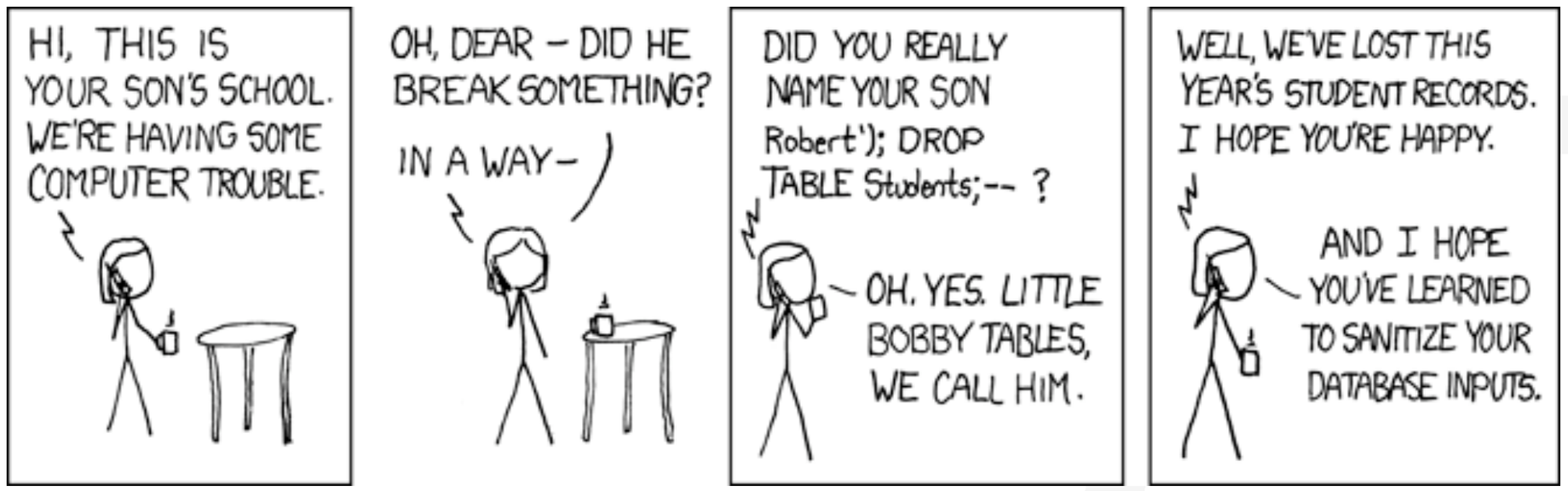
XSRF

- Cross-Site Request Forgery
- Send forespørsel på vegne av andre
  - Utnytter ett eller flere eksisterende autentiseringsforhold
- Muliggjør endringer på f.eks. hjemmerutere med standard-passord
  - <iframe src="http://admin:@192.168.0.1/cgi-bin/prim?attack-params-here"></iframe>

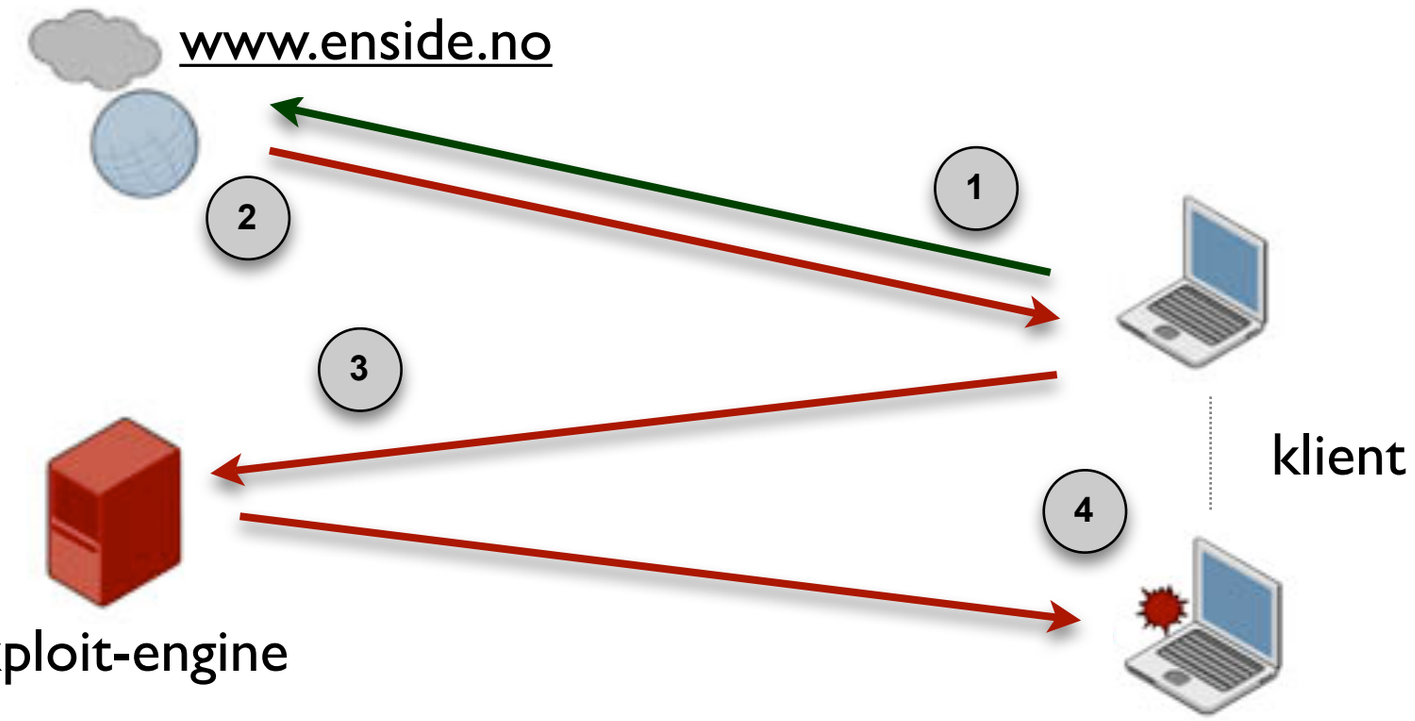
UNINETT

Hvordan utnyttes web-servere?

- Directory traversal
- Remote file-inclusion
- Kommando-eksekvering (system(), exec() mv.)
- SQL-injection



Satt ut i praksis – demo



- Klient: WinXP SP2, IE7
  - mangler et par patcher :)
- www.enside.no: Debian Linux
- Exploit-engine: metasploit

Mulige åtgjerder

- Husk: datasikkerhet består av
  - 20% teknologi
  - 80% kunnskap/organisering/holdninger

- Det finnes ingen sølvkule!
  - Ingen enkeltprodukt eller enkelttiltak kan løse alt, men litt av alt hjelper mye!
- Sikkerhetsarbeidet bør organiseres!
  - Revidere IT-reglementet
  - Innøv gode datavaner
  - Det er ikke tilstrekkelig å kaste teknologi på problemet!
  - Vær forberedt på at noe kan gå galt – ikke få panikk men arbeid systematisk og helst etter en gjennomtenkt plan

- Følgelig:
  - ”Voksenopplæring”
  - Påvirke programutviklere til å tenke sikkerhet
  - Dele ut, evt inndra privileger etter behov
  - Innføre systemer som oppmuntrer til at brukerne velger å kjøre i uprivilegert modus
  - Tekniske sperrer og løsninger av ulike slag

UNINETT

Spørsmål?

- Referanser/Mer info
  - cgisecurity.com > Articles > Xss-faq
    http://www.cgisecurity.com/articles/xss-faq.shtml
  - squarefree.com > Securitytips > Web-developers
    http://www.squarefree.com/securitytips/web-developers.html
  - drive-by-pharming
    http://www.symantec.com/enterprise/security_response/weblog/2007/02/driveby_pharming_how_clicking_I.html
    http://www.symantec.com/enterprise/security_response/weblog/2008/01/driveby_pharming_in_the_wild.html
  - http://en.wikipedia.org/wiki/Category:Web_security_exploits
  - http://ha.ckers.org/
  - The Ghost In The Browser: Analysis of Web-based Malware
    http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf
  - Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority
    http://www.citi.umich.edu/u/provos/papers/ndss08_dns.pdf

UNINETT