SOLIDO
NETWORKS

Welcome to

Sikkerhed - sniffning på netværket

Henrik Lund Kramshøj
hlk@solidonetworks.com

`http://www.solidonetworks.com`

Slides are available as PDF

Hvorfor? Sidste år :-)

Sniffe - demoer hvordan man henter post med POP3 og en FTP server, update af webhotel scenarier

BackTrack 5 bruger vi til at sniffe, vi bruger Wireshark til primære demo, nævner Ettercap osv.
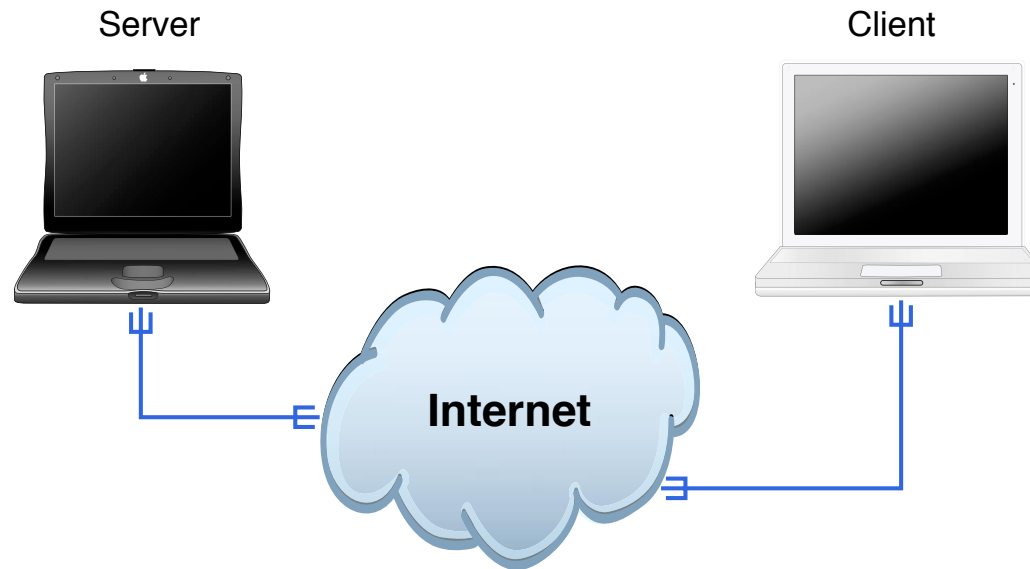
Demo: løsninger, POP3S, SSL/TLS, SMTP over TLS osv.

Mere avanceret: OpenSSH tunnel, SSL VPN - generelt, eksempel med OpenVPN, FileZilla - understøtter vist SFTP/SCP

sniffe igen

Advanced sniffing:

Tcpdump wizardry Tyklol

HLK: netflow opsamling

Server   Client
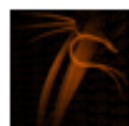
Internet

Clients and servers

Rooted in academic networks

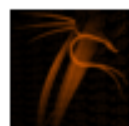Protocols which are more than 20 years old, moved to TCP/IP in 1981

Henrik Lund Kramshøj

hlk@solidonetworks.com
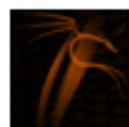
```
http://www.solidonetworks.com
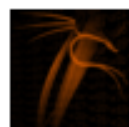```

You are always welcome to send me questions later via email

Twitter has become an important new ressource for lots of stuff

Twitter has replaced RSS for me

*Guidelines for the Secure Deployment of IPv6*, SP800-119, NIST
`http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf`

*The Second Internet: Reinventing Computer Networks with IPv6*, Lawrence E. Hughes, October 2010,
`http://www.secondinternet.org/`

*IPv6 Network Administration* af David Malone og Niall Richard Murphy - god til real-life admins, typisk O'Reilly bog

*IPv6 Essentials* af Silvia Hagen, O'Reilly 2nd edition (May 17, 2006) god reference om emnet

*IPv6 Core Protocols Implementation* af Qing Li, Tatuya Jinmei og Keiichi Shima

*IPv6 Advanced Protocols Implementation* af Qing Li, Jinmei Tatuya og Keiichi Shima

- flere andre