Welcome to

Privacy, surveillance and hacking, protect yourself

DANSK IT IT-sikkerhed 2019

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

dansk-it-2019.tex in the repo security-courses

Happy New Year 2019

.

- Same problems
- Repeat last year?
- ... or try something new!
- 2019 will become a nightmare of break-ins and data leaks
- GDPR is here and the snow ball is rolling

Try not to panic, but there are lots of threats

Try something new

Do you think like an attacker?

Why not.

- This talk will try to convince you to start attacking yourself, your company, your life.
- Start using Nmap, Wireshark, Kali Linux
- Learn some hacking skills, so you can recognize bad and insecure design
- This will allow you to improve security

Hackers don’t give a shit

Your system is only for testing, development, ...

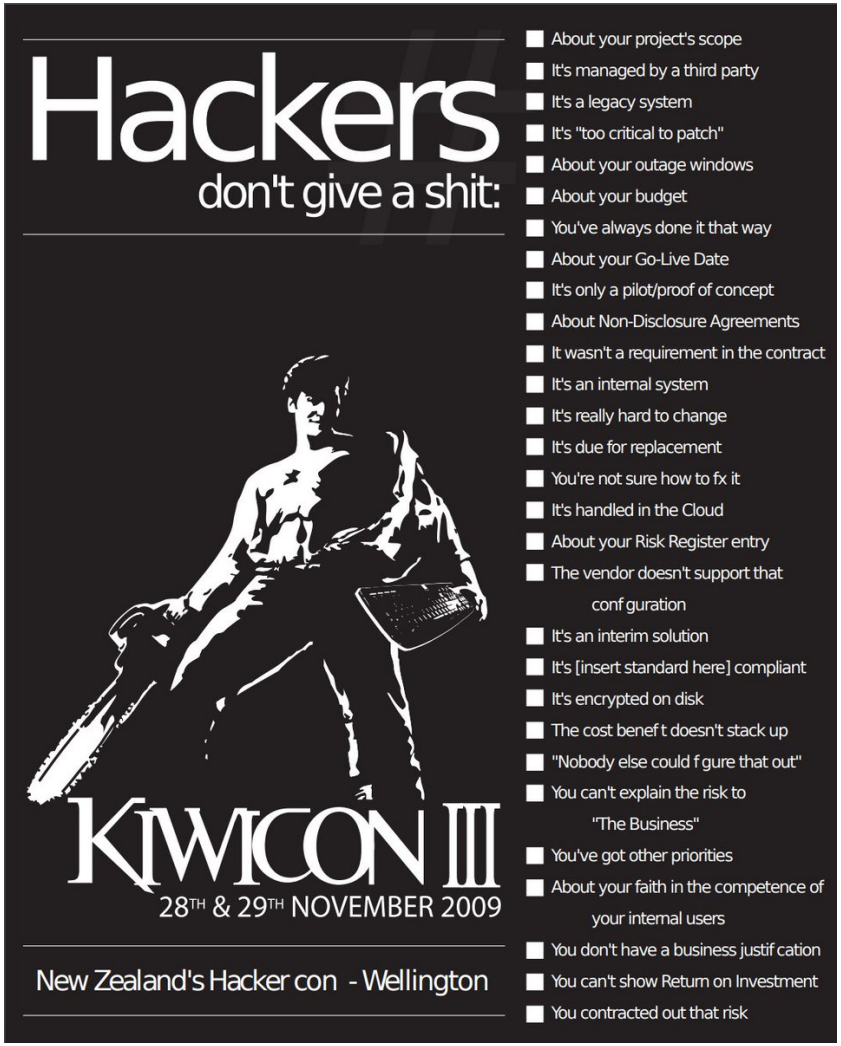
Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Ask for permission to go full monty on your security

Think like attackers - don’t hold back



Secure Laptops

Start with your laptops (and mobile devices if you wish)

Are they *secure*, and to what extent

Recommendations - Comply Everywhere, Act Anywhere

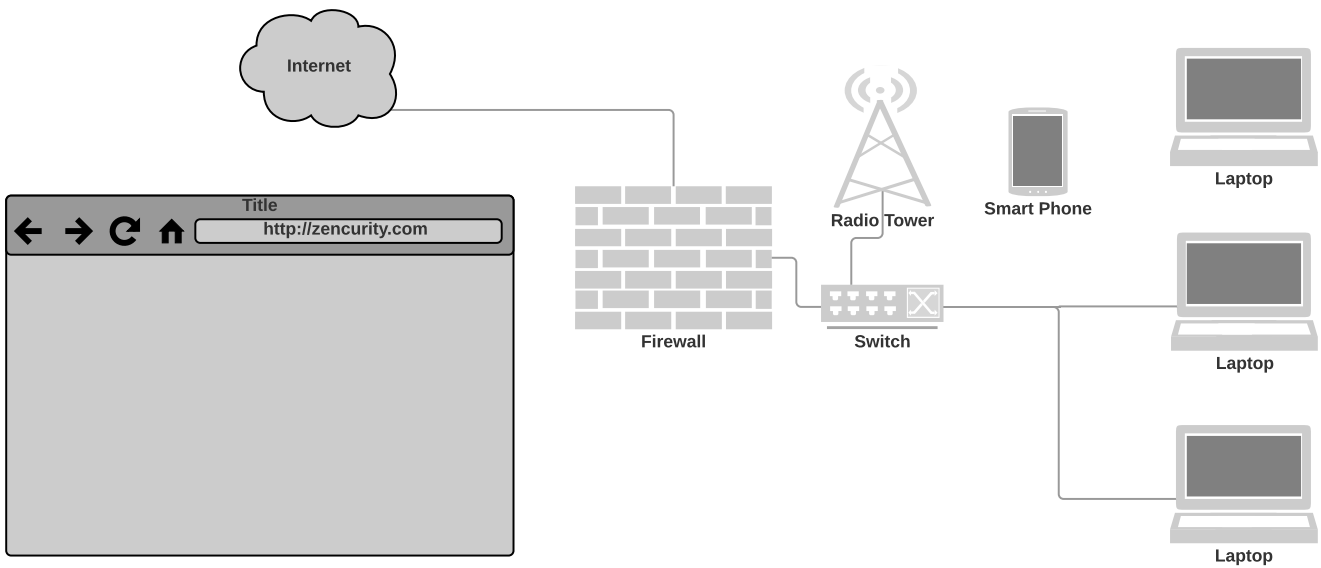
Laptop storage must be encrypted

Firewall must be enabled

Suggestions

- Try sniffing data from a laptop, setup Access Point/Monitor port
- Portscan your laptop networks - use Nmap
- Write an email to everyone in your organisation:
  "Hi All, we need to identify laptops without full disk encryption
  - come see us, we have christmas cookies left, Best regards IT"

Your Privacy



- Your data travels far
- Often crossing borders, virtually and literally

Data found in Network data

Lets take an example, DNS

Domain Name System DNS breadcrumbs

- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit

Advice show your users,ask them to participate in a experiment

Join this Wireless network SSID and we will show you who you are on the internet

Maybe use VPN more - or always!

Start Attacking from the Inside

- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
  Having a large open network may cost you 1.9 billion DKK - ref Maersk
- Try scanning everything, start in a small corner, expand
- Scan all you danish segments, one by one, then the nordic, then the world
- Yes, things may break - FINE, BREAKING is GOOD

Better to break while we are ready to un-break

How to break stuff

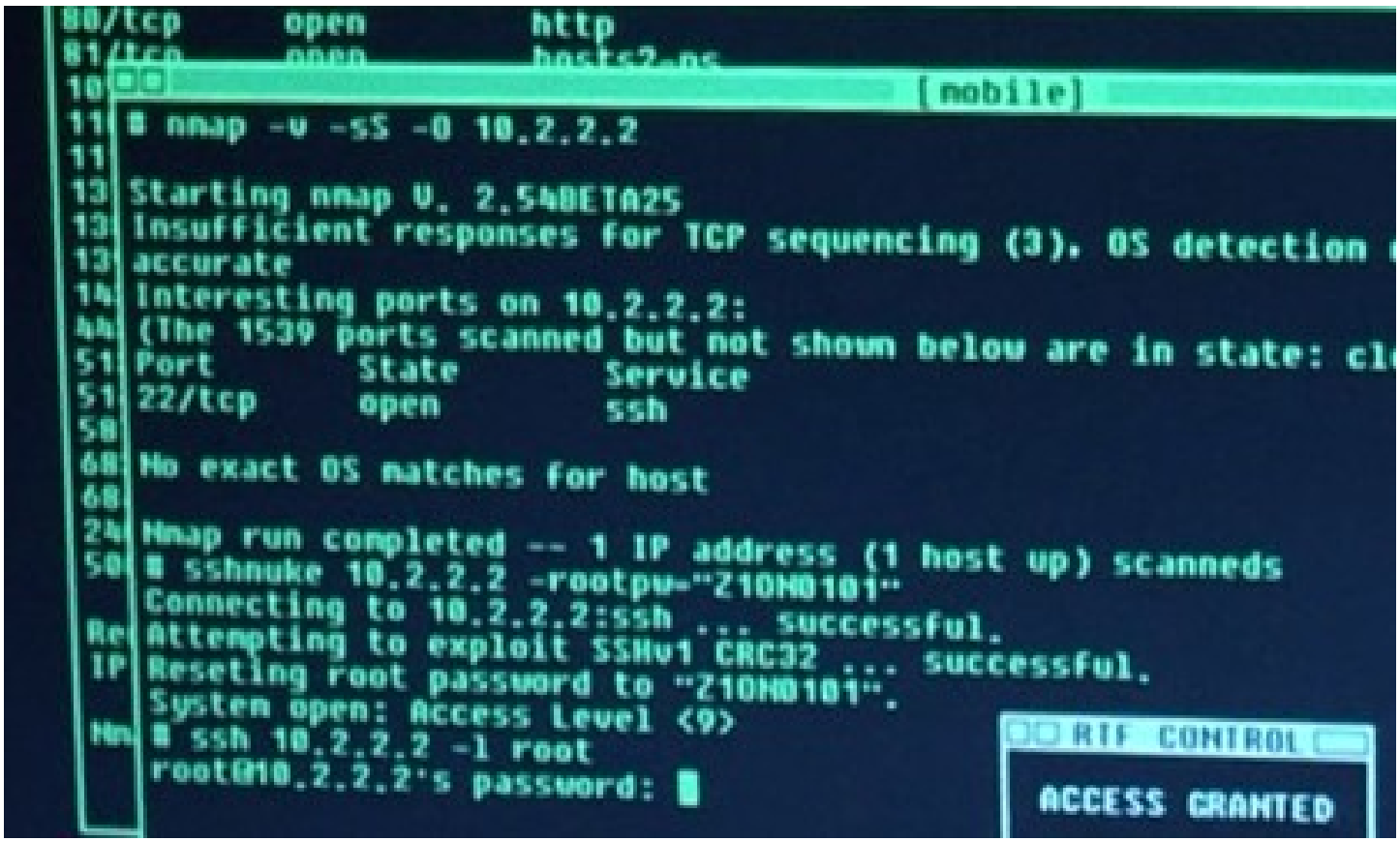
Think like an attacker

I sit here, but where am I connected:

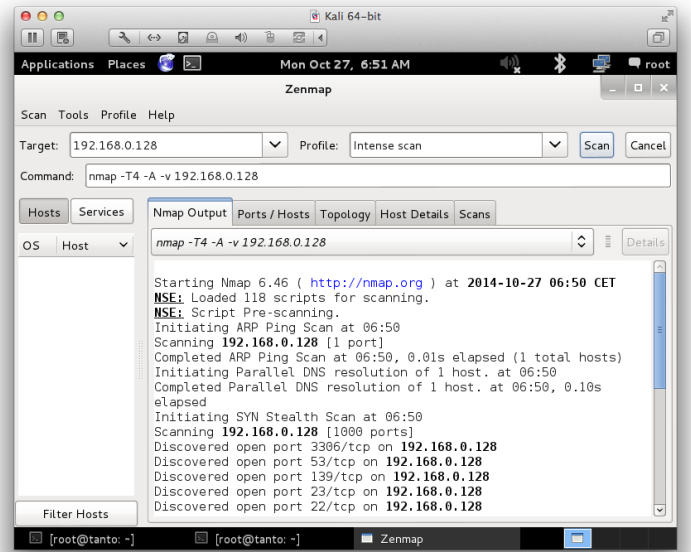
```
reading from file cisco-lldp-1.cap, link-type EN10MB (Ethernet)
16:39:43.468745 LLDP, length 328
Chassis ID TLV (1), length 7
  Subtype MAC address (4): 70:ff:1a:01:03:02 (oui Unknown)
  0x0000:  0470 ea1a a0b3 2f
Port ID TLV (2), length 8
  Subtype Local (7): Eth1/47
  0x0000:  0745 7468 312f 3437
Port Description TLV (4), length 12: Ethernet1/47
  0x0000:  4574 6865 726e 6574 312f 3437
System Description TLV (6), length 158
  Cisco Nexus Operating System (NX-OS) Software 14.0(2c) TAC support: http://www.cisco.com/tac Copyright (c) 2002-
2020, Cisco Systems, Inc. All rights reserved.
```

I love LLDP, but it does reveal software version, so flaws available

Nmap the world

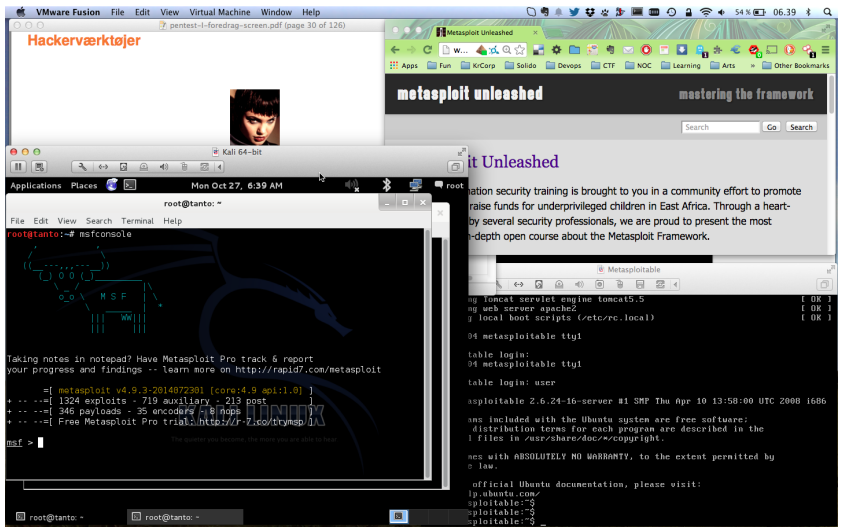


Really do Nmap your world



- Nmap is a port scanner, but does more
- Finding your own infrastructure available from the guest network?
- See your printers having all the protocols enabled AND a wireless?

Hackerlab setup



- Create hacker labs, encourage hacker labs!
- Hardware: almost any laptop can use virtualisation
- Software: keep your favourite: Windows, Mac, Linux
- Hackersoftware: Use Kali Linux as a VM `https://www.kali.org/`

Hacking is not magic

- Hacking only requires some ninja training
- We have been doing this since 1995 when SATAN was released
- Listen, Plan, Act, Do hacking

Questions?

Henrik Lund Kramshøj hlk@zencurity.com

Need help with infrastructure security or pentesting, ask me!

You are always welcome to send me questions later via email