



Welcome to

Privacy, surveillance and hacking, protect yourself

DANSK IT IT-sikkerhed 2019

Henrik Lund Kramshøj hlk@zecurity.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

Hackers don't give a shit:



KIWICON III
28TH & 29TH NOVEMBER 2009

New Zealand's Hacker con - Wellington

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

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

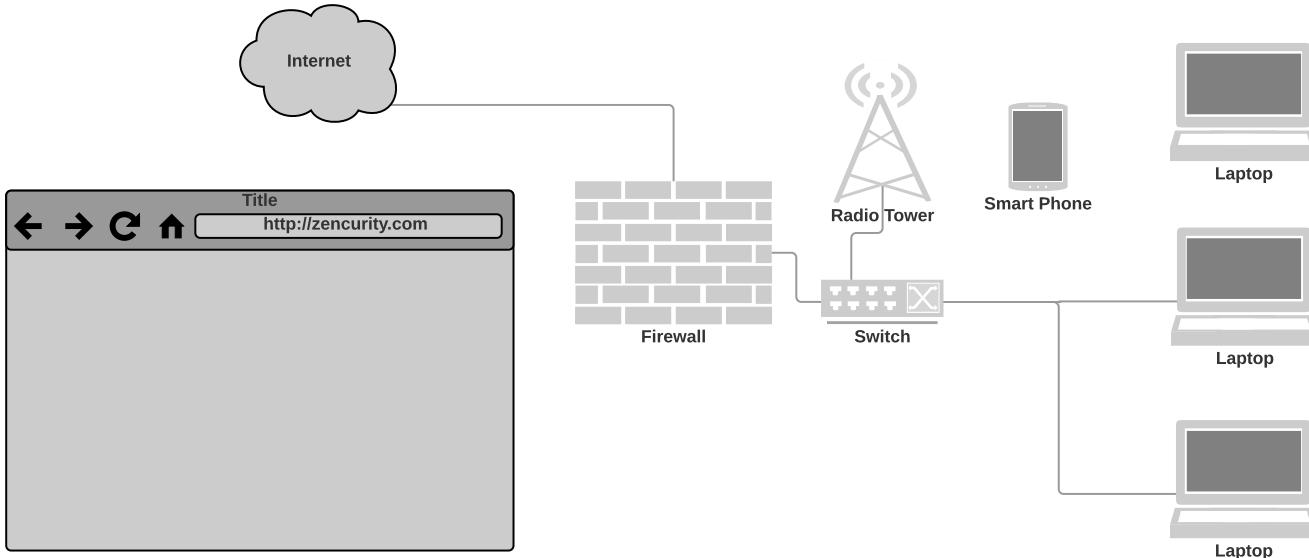
Firewall must be enabled

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

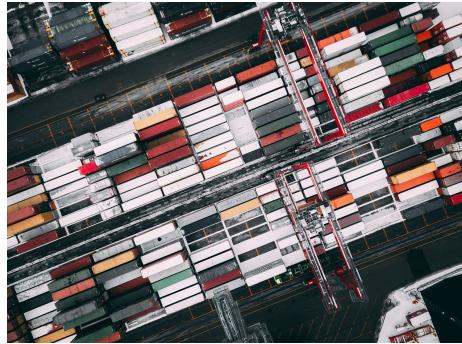
- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit

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 your 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

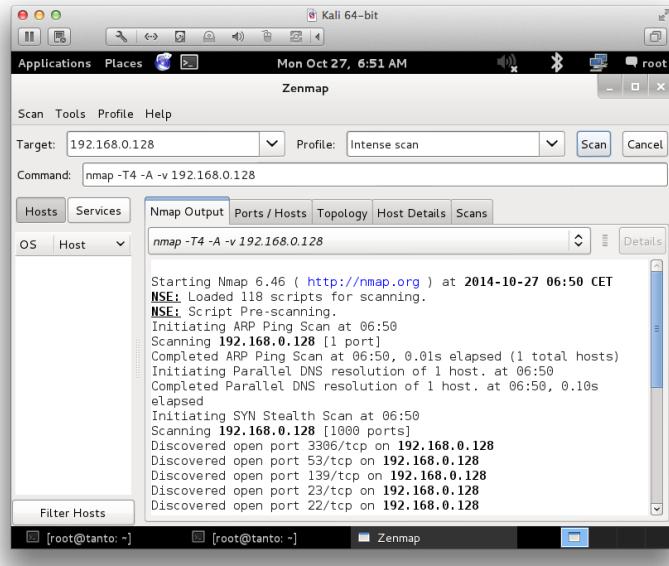
Nmap the world



```
80/tcp      open     http  
81/tcp      open     hosts2-nc  
10 [REDACTED] [REDACTED] (mobile)  
11 $ nmap -v -S5 -O 10.2.2.2  
11  
13 Starting nmap 0.2.5NBEta25  
13 Insufficient responses for TCP sequencing (0). OS detection is  
13 inaccurate.  
14 Interesting ports on 10.2.2.2:  
44 (The 1539 ports scanned but not shown below are in state: cl  
51 Port      State       Service  
51 22/tcp    open        ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned.  
50 $ sshnuke 10.2.2.2 -rootpw="Z10HD101"  
Connecting to 10.2.2.2:ssh ... successful.  
Reattempting to exploit SSHv1 CRC32 ... successful.  
IP Resetting root password to "Z10HD101".  
System open: Access Level <9>  
Hn $ ssh 10.2.2.2 -l root  
root@10.2.2.2's password: [REDACTED]
```

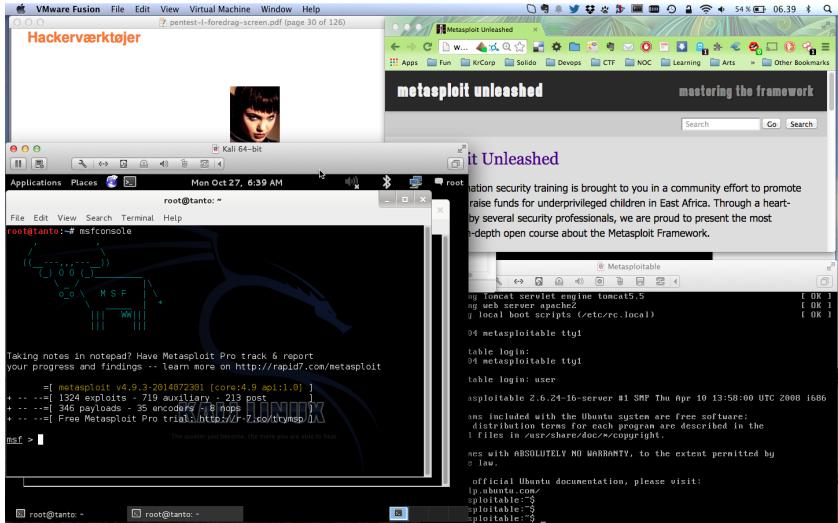


Really do Nmap your world



- 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