Welcome to

Det moderne IT-sikkerhedslandskab

KEA

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

it-security-work-intro.tex in the repo security-courses

Kontaktinformation

- Henrik Kramselund, han/ham internet samurai, primært netværk og sikkerhed
- Netværk og it-sikkerhedskonsulent Zencurity, underviser på KEA og aktivist
- Cand.scient. fra Datalogisk Institut ved Københavns Universitet (DIKU)
- Email: hlk@zencurity.com Mobil: +45 2026 6000

I er velkomne til at sende email

Hvad laver Zencurity Aps – Security engineering a job role

On any given day, you may be challenged to:

- Create new ways to solve existing production security issues
- Configure and install firewalls and intrusion detection systems
- Perform vulnerability testing, risk analyses and security assessments
- Develop automation scripts to handle and track incidents
- Investigate intrusion incidents, conduct forensic investigations and incident responses
- Collaborate with colleagues on authentication, authorization and encryption solutions
- Evaluate new technologies and processes that enhance security capabilities
- Test security solutions using industry standard analysis criteria
- Deliver technical reports and formal papers on test findings
- Respond to information security issues during each stage of a project's lifecycle
- Supervise changes in software, hardware, facilities, telecommunications and user needs
- Define, implement and maintain corporate security policies
- Analyze and advise on new security technologies and program conformance
- Recommend modifications in legal, technical and regulatory areas that affect IT security

Source: https://www.cyberdegrees.org/jobs/security-engineer/
also https://en.wikipedia.org/wiki/Security_engineering

Core Concepts

Information Security is a huge domain:

> The (ISC)^2 CBK is a collection of topics relevant to cybersecurity professionals around the world. It establishes a common framework of information security terms and principles which enables cybersecurity and IT/ICT professionals worldwide to discuss, debate and resolve matters pertaining to the profession with a common understanding, taxonomy and lexicon.

Source: https://www.isc2.org/Certifications/CBK

List of 8 domains in CISSP CBK: Security and Risk Management, Asset Security, Security Architecture and Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, Software Development Security

- then add all the news about new tools, exploits, and networking

Hacker tools

Improving the Security of Your Site by Breaking Into it
by Dan Farmer and Wietse Venema in 1993

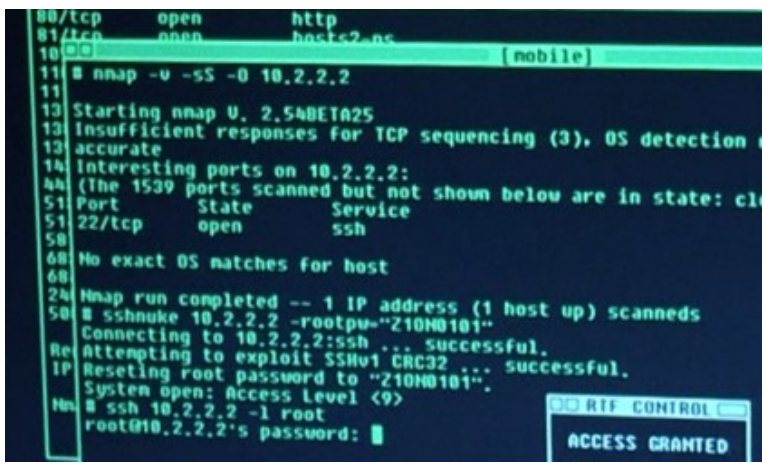
Later in 1995 released the software SATAN
Security Administrator Tool for Analyzing Networks

Caused some commotion, panic and discussions, every script kiddie can hack, the internet will melt down!

> We realize that SATAN is a two-edged sword – like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Source: http://www.fish2.com/security/admin-guide-to-cracking.html

Learning at different levels



To illustrate this, I will use the example of:
Nmap - a very famous port scanner.

Unfortunately there are about 100 options, and the man page is some 3100 lines ...

Prerequisite knowledge

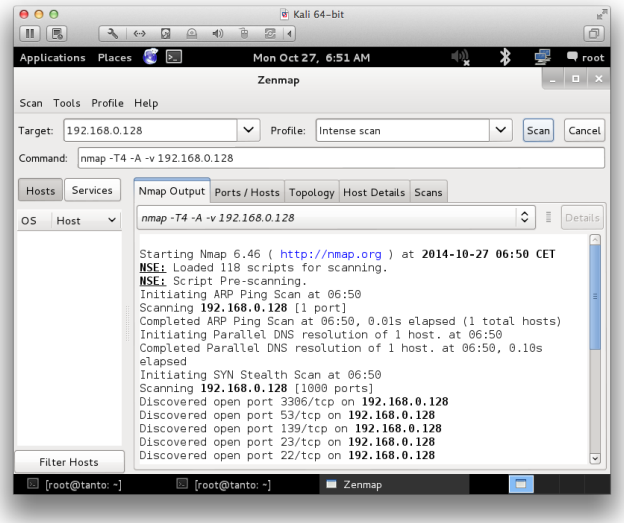
Plan: You want to learn Nmap!

Often we combine our knowledge with skills into competence,
which enable us to perform some job, task or function.

- Knowledge level: What is a port scanner
  Need to know TCP/IP, IP address, ports and services – example HTTP 80/tcp, TCP session setup

So get this sorted out first, otherwise you cannot understand what Nmap does, and output returned

Skills are needed



- Skills level: Running a port scanner
  Need to have operating system – luckily Nmap supports Mac, Windows, Linux, ...
- My recommendation: create a virtual machine with Kali Linux

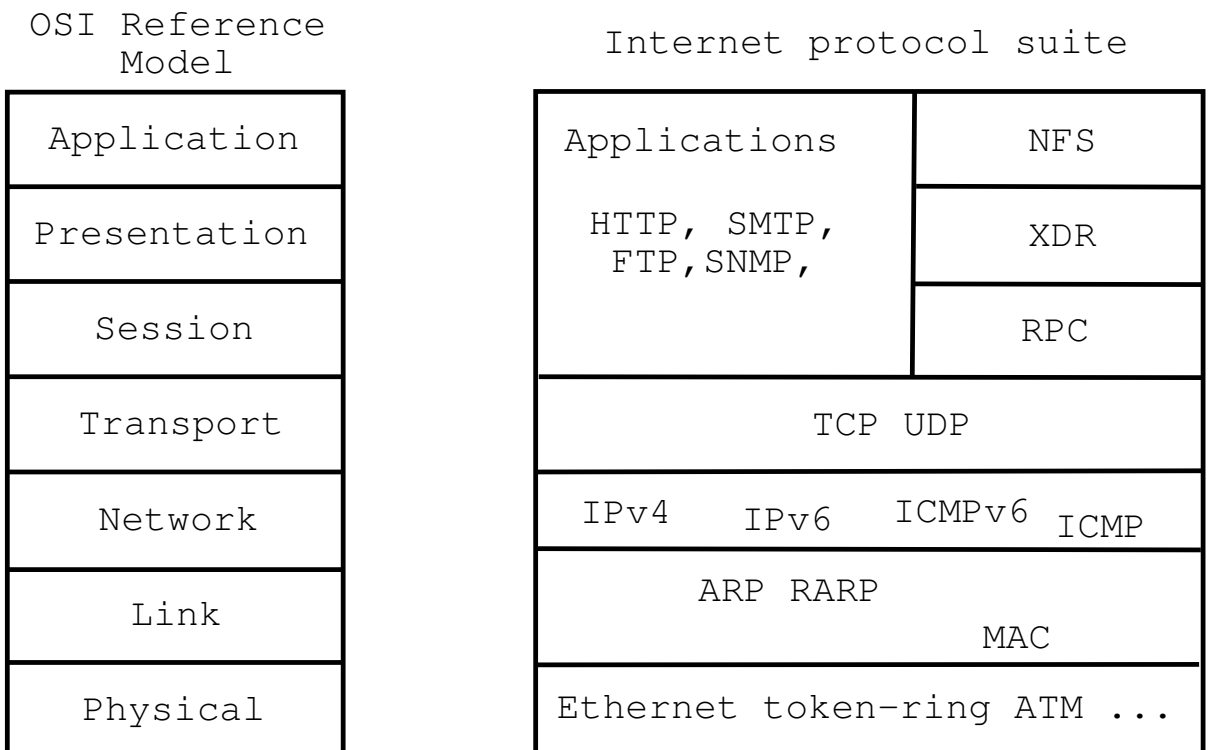
Combined it becomes a Competence

```
full-tcp-scan: nmap -p 1-65535 -A -oA full-tcp-scan -iL targets
dns-scan: nmap -sU -p 53 --script=dns-recursion -iL targets -oA dns-recursive
bgpscan: nmap -A -p 179 -oA bgpscan -iL $LINKNET
dns-recursive: nmap -sU -p 53 --script=dns-recursion -iL targets -oA dns-recursive
php-scan: nmap -sV --script=http-php-version -p80,443 -oA php-scan -iL targets
scan-vtep-tcp: nmap -A -p 1-65535 -oA scan-vtep-tcp 192.0.2.77 192.0.2.78
snmp-10.x.y.0.gnmap: nmap -sV -A -p 161 -sU --script=snmp-info -oA snmp-10xy 10.x.y.0/19
snmpscan: nmap -sU -p 161 -oA snmpscan --script=snmp-interfaces -iL targets
sshscan: nmap -A -p 22 -oA sshscan -iL targets
vncscan: nmap -A -p 5900-5905 -oA vncscan -iL targets
```

- Competence level: Running a quality port scan of an enterprise
  Need to have plan for scanning, know which scan functions to use

  My recommendation: work through a 4 hour course with Nmap as the subject

OSI Model and Internet Protocols



Recommended technologies to learn

So to accomplish the goal of using Nmap efficiently you need some basics

Networking: Basic Protocols from the Internet Protocols suite IP/TCP, or TCP/IP

- Network Layer: Ethernet, Address Resolution Protocol (ARP), IPv4 and ICMP
  Later add Wi-Fi and IPv6
- Transport Layer: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- Common upper layer: Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP)
  Later add the encrypted/secure versions like Hypertext Transfer Protocol Secure (HTTPS) which uses Transport Layer Security (TLS)

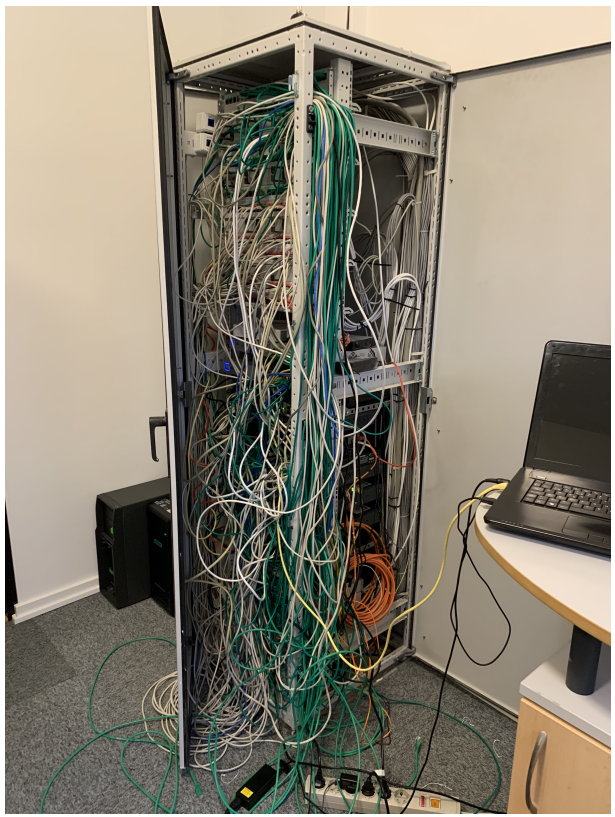
Pro tip: always say Ethernet frames and IP packets. No one uses datagram anymore.

Pro tip: If you *really know DNS* you can make a huge impact in the malware area!

Recommended tools to learn

- Open Source I really love open source. There is just too much great open source software, to ignore, and security budgets are tight in DK!
- Linux/Unix knowledge is necessary – because a lot of the newest tools are written for Linux/Unix/BSD
- Git and Github – where you can find lots of tools, libraries, applications
- Programming experience is an advantage for automating stuff – Python is a nice generic tool for this
- Ansible provisioning – installing and configuring software for production
- Elasticsearch – how to run a *service*, full fledged applications exist for Elasticsearch

Nice Rack you got there!



Physical Inspection is Needed

Yes, go through the server room!

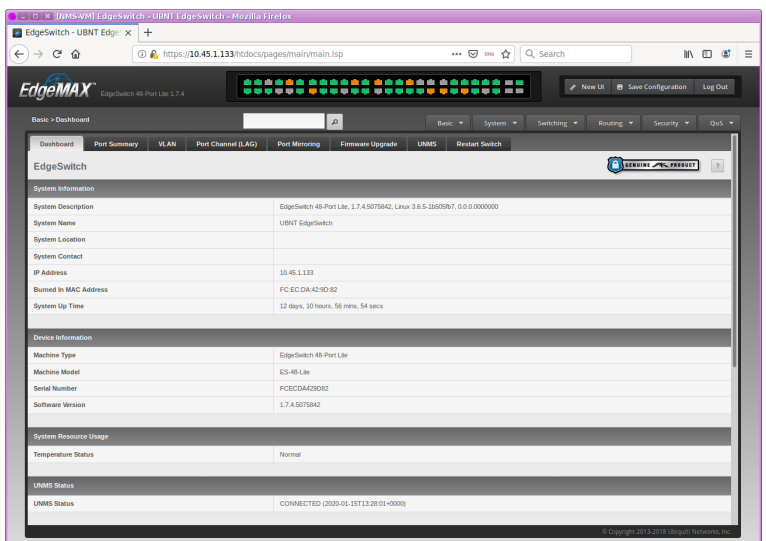
Things we find:

- Single firewall, running with a single power supply – single point of failure
- No Uninterruptable Power Supply – having NO UPS is bad if availability is important
- Bad cabling, disaster can strike, and no one can help you
- Bad cooling can take down your whole company

Advice: Start documenting your setup – buy a label maker today

Core Switch Administration

Then I also found switch administration with admin/admin *sigh*



- Is this the main switch for the whole office?! Yes - unfortunately
- I was also called up one time about a large core switch that had lost configuration, nothing worked

Cisco ACI (2019)

Vulnerability Analysis

- Remote Code Execution on Leaf Switches over IPv6 via Local SSH Server (CVE-2019-1836, CVE2019-1803, and CVE-2019-1804) – SSH access with specific source port, private key left on firmware image, and on all switches
- Cisco Nexus 9000 Series Fabric Switches ACI Mode Fabric Infrastructure VLAN Unauthorized Access Vulnerability (CVE-2019-1890)
- Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Link Layer Discovery Protocol Buffer Overflow Vulnerability (CVE-2019-1901)
- Cisco Application Policy Infrastructure Controller REST API Privilege Escalation Vulnerability (CVE2019-1889)

Source: https://static.ernw.de/whitepaper/ERNW_Whitepaper68_Vulnerability_Assessment_Cisco_ACI_signed.pdf

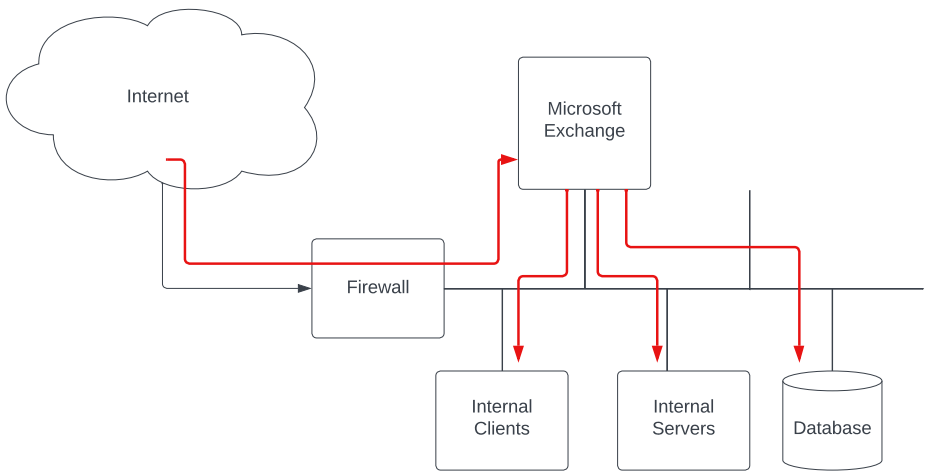
Further all processes run as root user – good job Cisco

HP Switches are very user friendly

```
$ telnet 172.16.1.21
Connected to 172.16.1.21.
HP J9772A 2530-48G-PoEP Switch
Software revision YA.16.08.0015
(C) Copyright 2020 Hewlett Packard Enterprise Development LP
RESTRICTED RIGHTS LEGEND
...
Press any key to continue
Your previous successful login (as manager) was on 1990-02-19 21:27:21
from 172.16.1.250
SW04Stuen# show configuration
Running configuration:
; J9772A Configuration Editor; Created on release #YA.16.08.0015
; Ver #14:01.44.00.04.19.02.13.98.82.34.61.18.28.f3.84.9c.63.ff.37.27:45
```

- Nothing to see here – just log me in without a password, thank you HP
  No NTP servers, no log servers, default credentials, using bad default SNMP public, configured with VLANs

In 2022 Don't keep your Exchange server on the LAN!



Another service which is being attacked in recent years is Microsoft Exchange
This customer had their Exchange server directly on the LAN?!

- There is a high risk that a single vulnerability in Microsoft Exchange would open this network to complete compromise

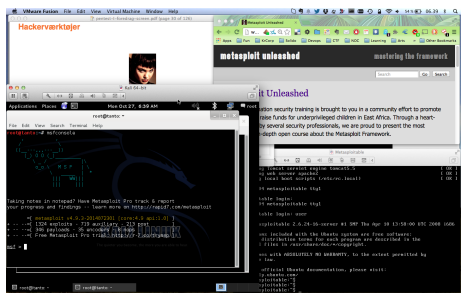
Microsoft Exchange vulnerabilities with CVSS 7 or higher

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-34523	287			2021-07-14	2022-07-12	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34470.														
2	CVE-2021-34473	918		Exec Code	2021-07-14	2022-07-12	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-31206.														
3	CVE-2021-31206			Exec Code	2021-07-14	2021-09-20	7.9	None	Local Network	Medium	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-34473.														
4	CVE-2021-28483			Exec Code	2021-04-13	2021-04-14	7.7	None	Local Network	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28482.														
5	CVE-2021-28482			Exec Code	2021-04-13	2021-04-14	9.0	None	Remote	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28483.														
6	CVE-2021-28481			Exec Code	2021-04-13	2021-04-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28482, CVE-2021-28483.														
7	CVE-2021-28480			Exec Code	2021-04-13	2021-04-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28481, CVE-2021-28482, CVE-2021-28483.														
8	CVE-2021-26855	918		Exec Code	2021-03-03	2022-07-12	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078.														

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-21978				2022-05-10	2022-05-18	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Elevation of Privilege Vulnerability.														
2	CVE-2022-21969			Exec Code	2022-01-11	2022-01-21	7.7	None	Local Network	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21846, CVE-2022-21855.														
3	CVE-2022-21855			Exec Code	2022-01-11	2022-01-14	7.7	None	Local Network	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21846, CVE-2022-21969.														
4	CVE-2022-21846	94		Exec Code	2022-01-11	2022-01-14	8.3	None	Local Network	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21855, CVE-2022-21969.														

- Lesson: Don't put Exchange on your LAN!

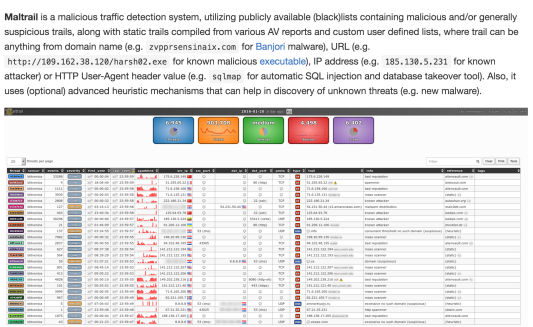
Open Source – Linux hackerlab



- Create your own playground, a hackerlab
- kramse-labs – Guide to preparing your laptop for training with Kramse
  https://github.com/kramse/kramse-labs
- Recommend two VMs, Debian and Kali Linux
- Don't forget to find the Debian Handbook and Kali Linux Revealed, free PDFs

I consider Linux/Unix knowledge a must for working in Networking and Security

Tools: Open Source and Python



- Open Source is already written *doh*
- Can provide solutions or parts of a solution
- Often feature-rich, mature, tested, maintained, and even when *not* can be brought back to life
- Picture from Maltrail https://github.com/stamparm/maltrail
  Maltrail is a malicious traffic detection system, utilizing publicly available lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists,

Why Ansible

Platform options Ansible:

```
CloudEngine OS, CNOS, Dell OS6, Dell OS9 Dell OS10, ENOS, EOS, ERIC_ECCLI, EXOS,
FRR, ICX, IOS, IOS-XR, IronWare, Junos OS, Meraki, Pluribus NETVISOR, NOS, NXOS,
RouterOS, SLX-OS, VOSS, VyOS, WeOS 4

plus routers based on Linux, OpenBSD, FreeBSD etc.
```

One management system with many uses, free to download and use

- Generic configuration management – and you end up running support systems, network near systems
- Ansible for Network Automation
  https://docs.ansible.com/ansible/latest/network/index.html
- Allows you to install, configure and run your network management systems – like LibreNMS, Nipap

Python and YAML

- We need to store configurations of devices and systems
- Run Ansible playbooks
- Problem: Remember what we did, when, how
- Solution: use git for the playbooks
- Not the only version control system, but my preferred one
- Git can also be used by Oxidized which I also love https://github.com/ytti/oxidized

Why Elasticsearch

> The Elastic Common Schema (ECS) is an open source specification, developed with support from the Elastic user community. ECS defines a common set of fields to be used when storing event data in Elasticsearch, such as logs and metrics.

One storage system with many uses, free to download and use

- Logstash - can take logs and SNMP traps easily
- Packetbeat https://www.elastic.co/beats/packetbeat
- Elastiflow https://github.com/robcowart/elastiflow
- Has defined an Elastic Common Scheme (ECS) https://www.elastic.co/guide/en/ecs/current/ecs-reference.html

The Future in IT-Security, software development – IT in general

It-anvendelse i virksomheder (tema) 2022 It-sikkerhed i mikrovirksomheder

Dokumentation og dermed delbar viden om it-sikkerhedstiltag og -regler er et væsentlig element i virksomhedernes arbejde med digital sikkerhed. **Over halvdelen af Danmarks godt 14.000 mikrovirksomheder (5-9 ansatte) havde i 2022 ingen dokumentation** om forholdsregler, aktiviteter og procedurer vedr. it-sikkerhed. Der var således 53 pct. af virksomhederne med 5-9 ansatte, der ikke havde dokumenteret deres it-sikkerhedstiltag, mv. Til sammenligning var den tilsvarende andel 45 pct. blandt virksomheder med minimum 10 ansatte og blot 8 pct. blandt de største virksomheder med minimum 250 ansatte.

Source: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=50382

- We need more resources, a lot more!

Hackers don't give a shit

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

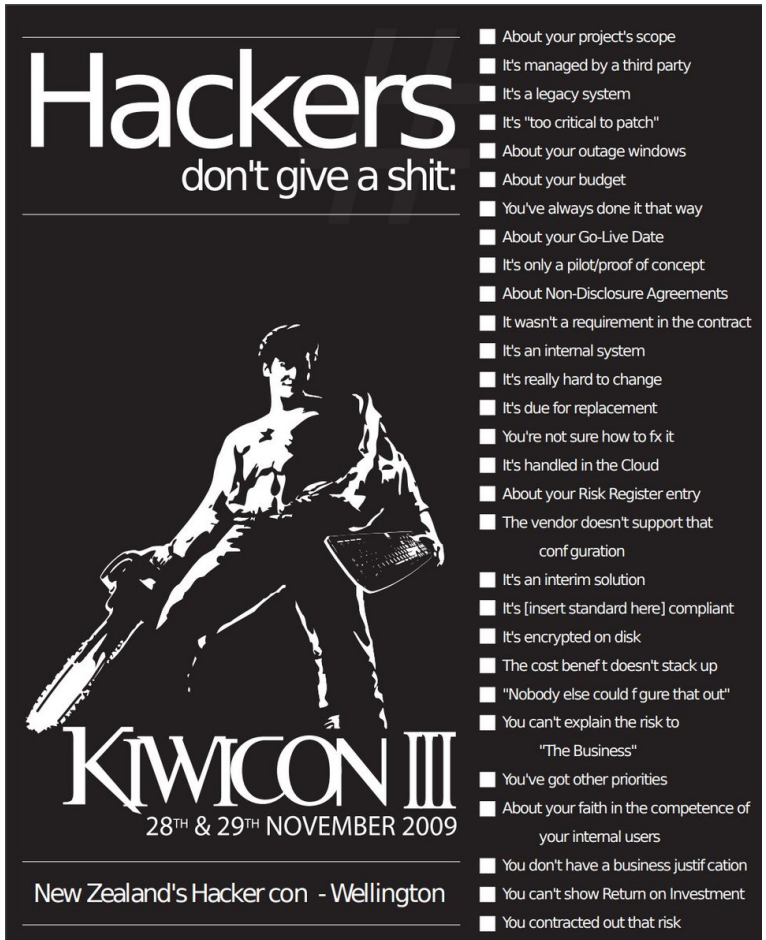
Your network is a research network, under construction, being phased out, ...

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:
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 fx it
It's handled in the Cloud
About your Risk Register entry
The vendor doesn't support that conf guration
It's an interim solution
It's [insert standard here] compliant
It's encrypted on disk
The cost benef t doesn't stack up
"Nobody else could f gure 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 justif cation
You can't show Return on Investment
You contracted out that risk
KIWICON III
28TH & 29TH NOVEMBER 2009
New Zealand's Hacker con - Wellington

Questions?

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

Email: hlk@zencurity.com

Books: Communications and Network Security course

Primary literature

- *Applied Network Security Monitoring Collection, Detection, and Analysis*, 2014 Chris Sanders ISBN: 9780124172081 - shortened ANSM
- *Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems*, 3rd edition 2017, Chris Sanders ISBN: 9781593278021 - shortened PPA
- *Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali*. OccupyTheWeb, December 2018, 248 pp. ISBN-13: 978-1-59327-855-7 - shortened LBfH
- The *Lecture Plan* https://zencurity.gitbook.io/kea-it-sikkerhed/net-og-komm-sikkerhed/lektionsplan
- Presentations – slides for each lecture, 14 evenings in total for this course

  https://github.com/kramse/security-courses/tree/master/courses/networking/communication-and-network-security

Price check – all three books can be bought in hardcopy for approx 1.000-1.100DKK

Other books I use in courses - some are free

- *The Debian Administrator's Handbook*, Raphaël Hertzog and Roland Mas
  https://debian-handbook.info/
- *Kali Linux Revealed Mastering the Penetration Testing Distribution*
  Raphaël Hertzog, Jim O'Gorman
  https://www.kali.org/download-kali-linux-revealed-book/
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, 5. ed. Allen Harper and others ISBN: 978-1-260-10841-5
- *Web Application Security*, Andrew Hoffman, 2020, ISBN: 9781492053118 - download for free through Nginx:
  https://www.nginx.com/resources/library/web-application-security/
- *Hacking, 2nd Edition: The Art of Exploitation*, Jon Erickson, February 2008, ISBN-13: 9781593271442
- All my training and educational materials are open source, including exercises booklets with small exercises that you can do with virtual machines like Debian and Kali Linux using lots of open source tools.
  https://github.com/kramse/security-courses

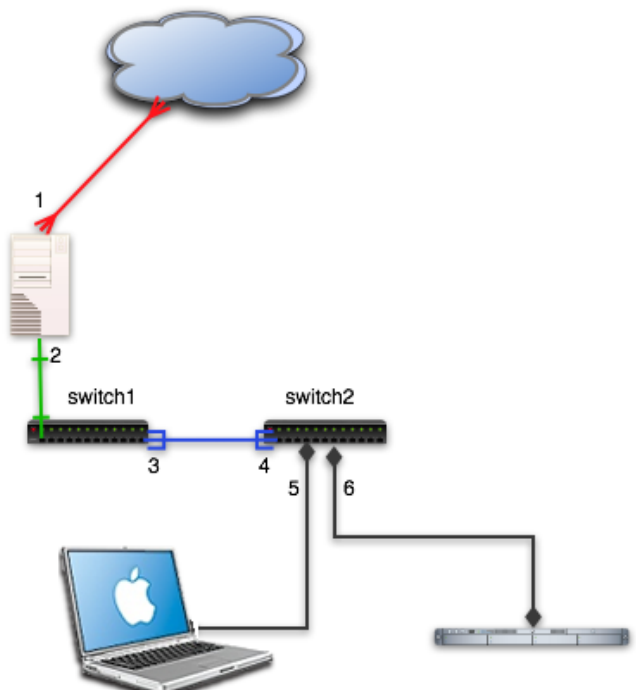
Equipment – wanna work with networks

Laptops, one is enough to get started

.

I have a network with me when needed,
which has the following systems:

- OpenBSD router
- Switches Juniper EX2200-C and small TP-Link
- UniFi AP wireless access-point



Above or similar can often be found lying around in offices, ask if you can take it.

Wifi Hardware

I recommend getting an extra wireless network card for your laptop.

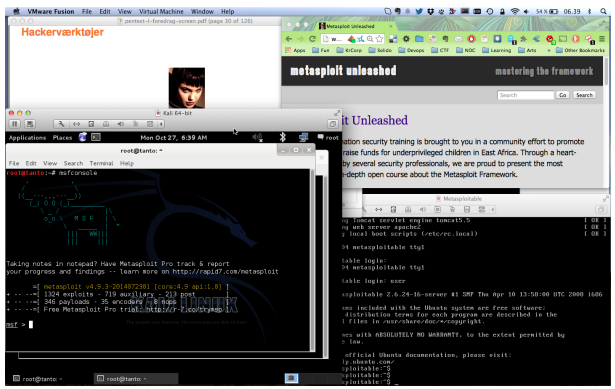
A wireless USB network card with external antenna can be used for many purposes.

- The following are two recommended models:
- TP-link TL-WN722N hardware version 2.0 cheap but only support 2.4GHz
- Alfa AWUS036ACH 2.4GHz + 5GHz Dual-Band and high performing
- Both usually work great in Kali Linux
- Newer, better, cheaper may exist – YMMV

I have some available for people to try if you dont want to buy them.

And if you have the money, USB Ethernet for playing with raw frames in your VM
I use 200DKK StarTech USB Ethernet – works for me

Hacker lab setup – tips



- Hardware: any modern laptop with CPU and virtualisation
  Don't forget to enable it in the BIOS
- Software: your favourite operating system Windows, Mac, Linux, ...
- Virtualisation software: VMware, Virtual box, pick your poison
- Hacker software: Kali as a Virtual Machine https://www.kali.org/
- Soft targets: Metasploitable, Linux, Microsoft Windows, Microsoft Exchange, Windows server, ...