Welcome to

Getting Started in Network and Security

Learning without drowning

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

Slides are available as PDF, kramse@Github

getting-started-in-infosec.tex in the repo security-courses

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen, DIKU
- Email: hlk@zencurity.dk Mobile: +45 2026 6000

You are welcome to drop me an email

Goals for today

"A goal without a plan is just a wish."
Antoine de Saint-Exupéry

Point you towards resources, so you can get started

List a few core concepts I think you should know and learn

Photo by Pawel Janiak on Unsplash

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

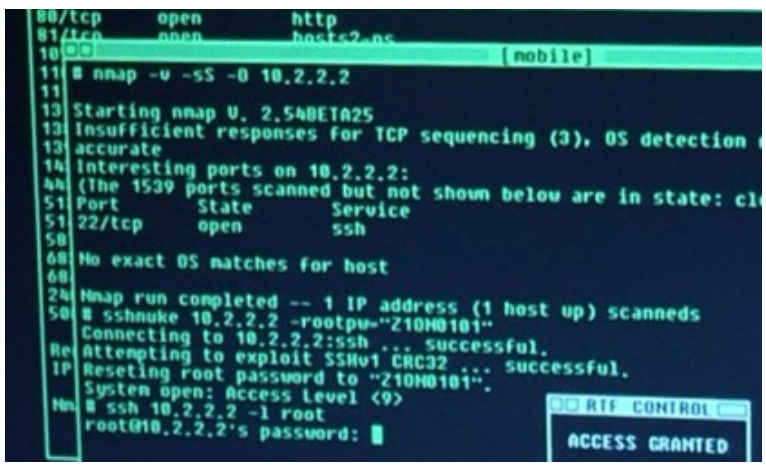
- then add all the news about new tools, exploits, and networking

Example: Juniper Networks Certifications

Certification Tracks	Associate Level	Specialist Level	Professional Level	Expert Level
Automation and DevOps	JNCIA-DevOps	JNCIS-DevOps	n/a	n/a
Cloud	JNCIA-Cloud	JNCIS-Cloud	JNCIP-Cloud	JNCIE-Cloud
Data Center	JNCIA-Junos	JNCIS-ENT	JNCIP-DC	JNCIE-DC
Design	JNCDA	• JNCDS-DC • JNCDS-SEC • JNCDS-SP	n/a	n/a
Enterprise Routing and Switching	JNCIA-Junos	JNCIS-ENT	JNCIP-ENT	JNCIE-ENT
Mist AI	JNCIA-MistAI	JNCIS-MistAI	n/a	n/a
Security	JNCIA-SEC	JNCIS-SEC	JNCIP-SEC	JNCIE-SEC
Service Provider Routing and Switching	JNCIA-Junos	JNCIS-SP	JNCIP-SP	JNCIE-SP

Source: https://www.juniper.net/us/en/training/certification.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

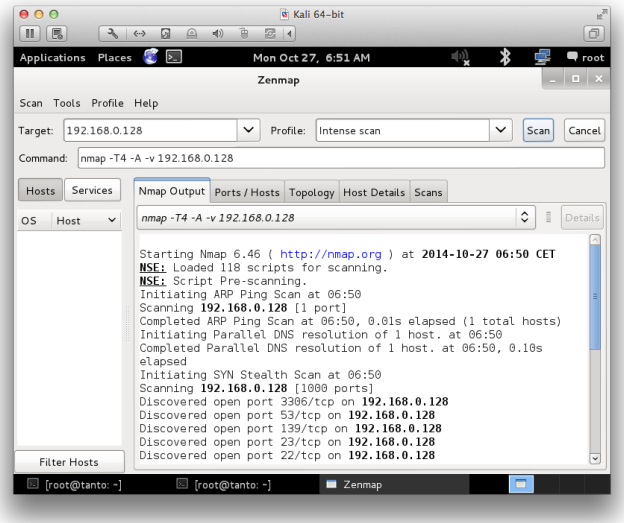
Plan: You want to learn Nmap!

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

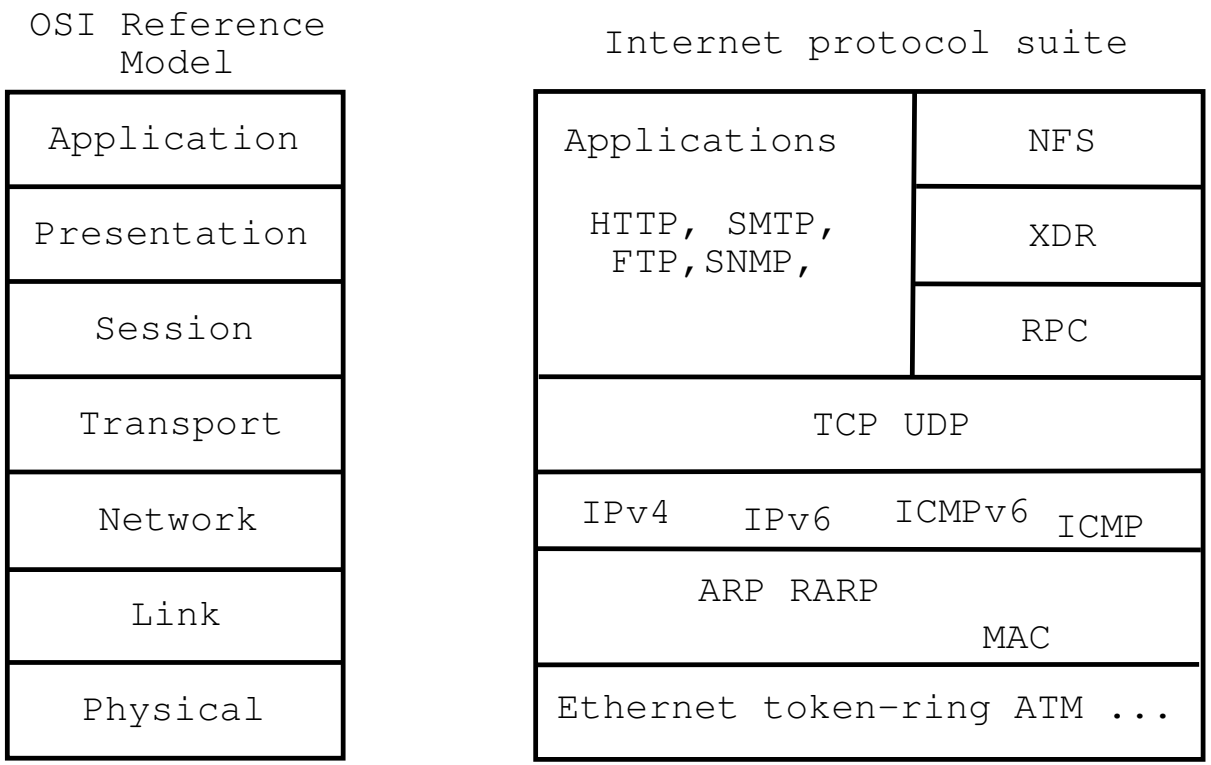
Combined it becomes a Competence

```
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!

Books and courses

How:

I like to learn new concepts from books

- Have a clear structure, less confusion
- They go from a basic level towards a complete goal
- Often have exercises available with nice progression
- Lots of nice books available from http://www.nostarch.com/ and others
- Often you can get Humble bundles with many books for $25
- Some books are "free" if you give your email address, example
  Web Application Security, Andrew Hoffman, 2020, ISBN: 9781492053118 - download for free through Nginx:
  https://www.nginx.com/resources/library/web-application-security/

Pro Tip: all my courses and exercise booklets are available on Github!

Networking and Security: Basic investigation

When you know the basic protocols, you can decide to dig deeper, or go in different directions.

- Packets, packet analysis dive deeper into what they are,
- Capturing packets, working with packet captures
- Port mirroring – essential for debugging network problems, and pre-requisite for intrusion detection systems etc.

Wireshark can help a lot, multiple courses and books about this.

Pro tip: also mentioned later, the Practical Packet Analysis 3rd ed book is awesome for this!

Pro tip: ENISA, the european agency publishes nice materials, including course materials: https://www.enisa.europa.eu/publications

Other Materials

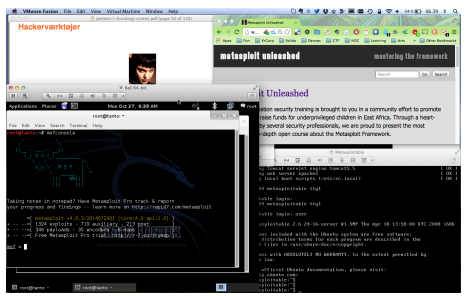
- Information comes in many formats, resources, programs, people, authors, documents, sites that further your exploration into network and security
- I force my students to read older hacker texts files, computer science papers, web articles, books chapters, standard documents, internet request for comments (RFCs)
- Goal is to kickstart their journey into the subjects
- Also serves to mention organizations, groups, persons, authors that I recommend you follow and read from

Example list from a course, supporting literature:
https://zencurity.gitbook.io/kea-it-sikkerhed/net-og-komm-sikkerhed/lektionsplan

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

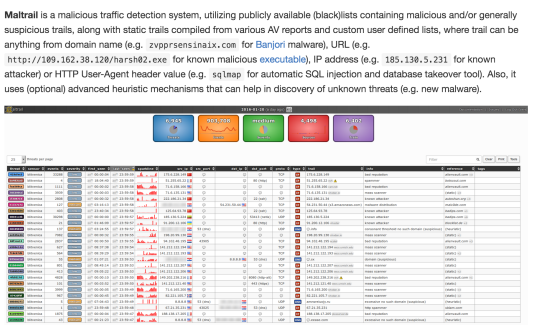
Open Source – Linux hackerlab



- 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 (black)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

Larger Example: Communications and Network Security

- Using one of my courses, I will go through the process

Course Description

From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018

Indhold:
Modulet går ud på at forstå og håndtere netværkssikkerhedstrusler samt implementere og konfigurere udstyr til samme.

Modulet omhandler forskellig sikkerhedsudstyr (IDS) til monitorering. Derudover vurdering af sikkerheden i et netværk, udarbejdelse af plan til at lukke eventuelle sårbarheder i netværket samt gennemgang af forskellige VPN teknologier.

My translation:
The module is centered around network threats and implementing and configuring equipment in this area.

Module includes different security equipment like IDS for monitoring. The evaluation of security in a network, developing plans for closing security vulnerabilities in the network and a review of various VPN technologies.

Final word is the Studieordning which can be downloaded from

https://kompetence.kea.dk/uddannelser/it-digitalt/diplom-i-it-sikkerhed

Studieordning_for_Diplomuddannelsen_i_IT-sikkerhed_Aug_2018.pdf

Overview Diploma in IT-security

Afgangsprojektet (15 ECTS)	
Der udvikles løbende nye valgfag til Diplom i it-sikkerhed. Disse vil løbende blive beskrevet i en allonge (bilag 2) til studieordningen.	
Sikkerhed i it-governance (it-sikkerhedsledelse) (5 ECTS)	Systemsikkerhed (10 ECTS)
Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)	
Softwaresikkerhed (10 ECTS)	
Netværks- og kommunikationssikkerhed (10 ECTS)	

I teach at Københavns Erhvervsakademi KEA, both KEA Kompetence and KEA

https://kompetence.kea.dk/

Example: 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

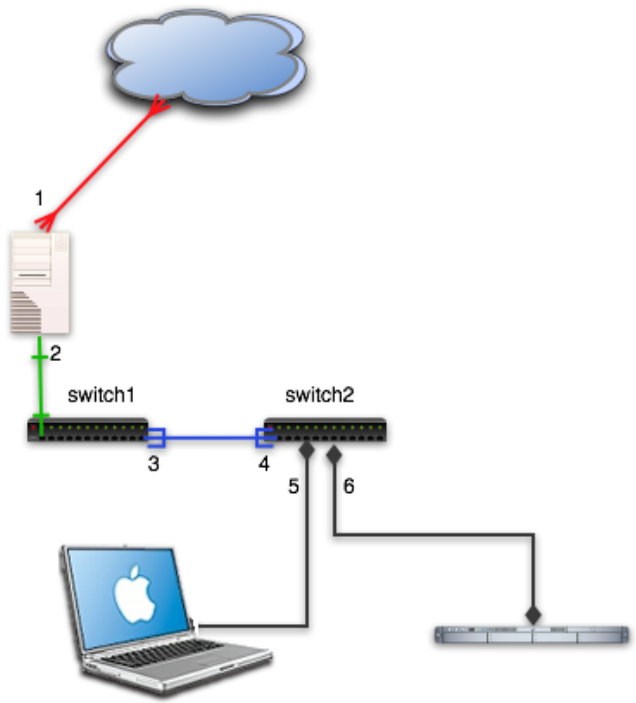
Equipment – wanna work with networks

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.

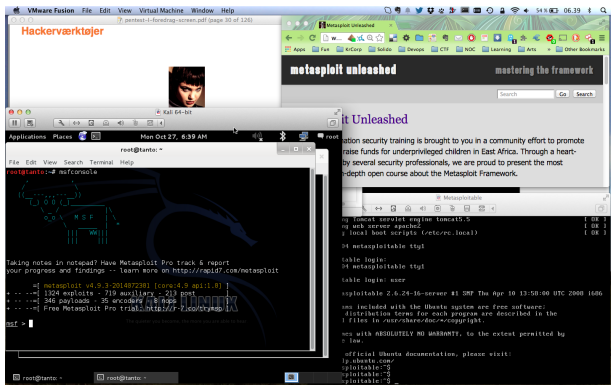
A wireless USB network card with external antenna can be used for many purposes.

- 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, ...

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