Welcome to

Security on a Budget

Survive without drowning in information

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

Slides are available as PDF, kramse@Codeberg

security-on-a-budget.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.com Mobile: +45 2026 6000
- Run a small network for fun AS57860

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

List example programs, tools, frameworks, maybe you are not using them – allow your organizations to benefit from them!

Photo by Pawel Janiak on Unsplash

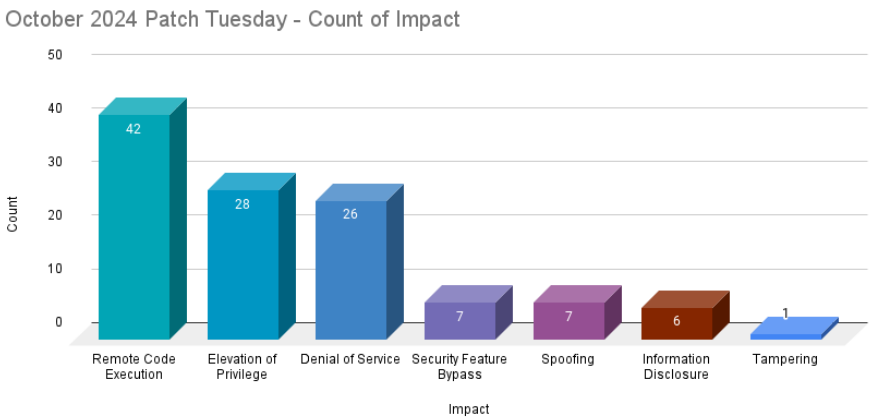
My daily job – Security engineering a job role

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

Reality Hits – every month



Microsoft addresses **117 CVEs** with three rated as critical and four zero-day vulnerabilities, two of which were **exploited in the wild**.

Source: https://www.tenable.com/blog/microsoft-october-2024-patch-tuesday-addresses-117-cves-cve-2024-43572-cve-2 originally from Microsoft October 2024 Security Updates https://msrc.microsoft.com/update-guide/releaseNote/2024-Oct

Vulnerabilities - CVE

Common Vulnerabilities and Exposures (CVE):

- classification
- identification

When discovered each vuln gets a CVE ID

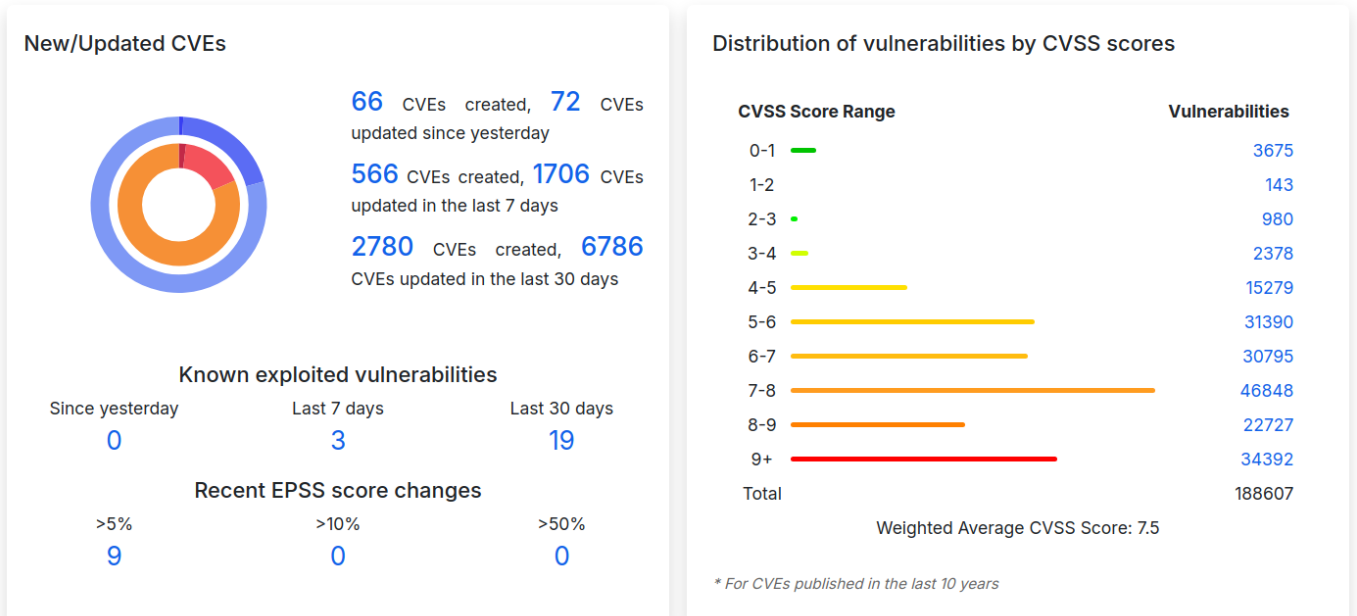
CVE maintained by MITRE - not-for-profit org for research and development in the USA.

National Vulnerability Database search for CVE.

Sources: http://cve.mitre.org/ og http://nvd.nist.gov

also checkout OWASP Top-10 http://www.owasp.org/

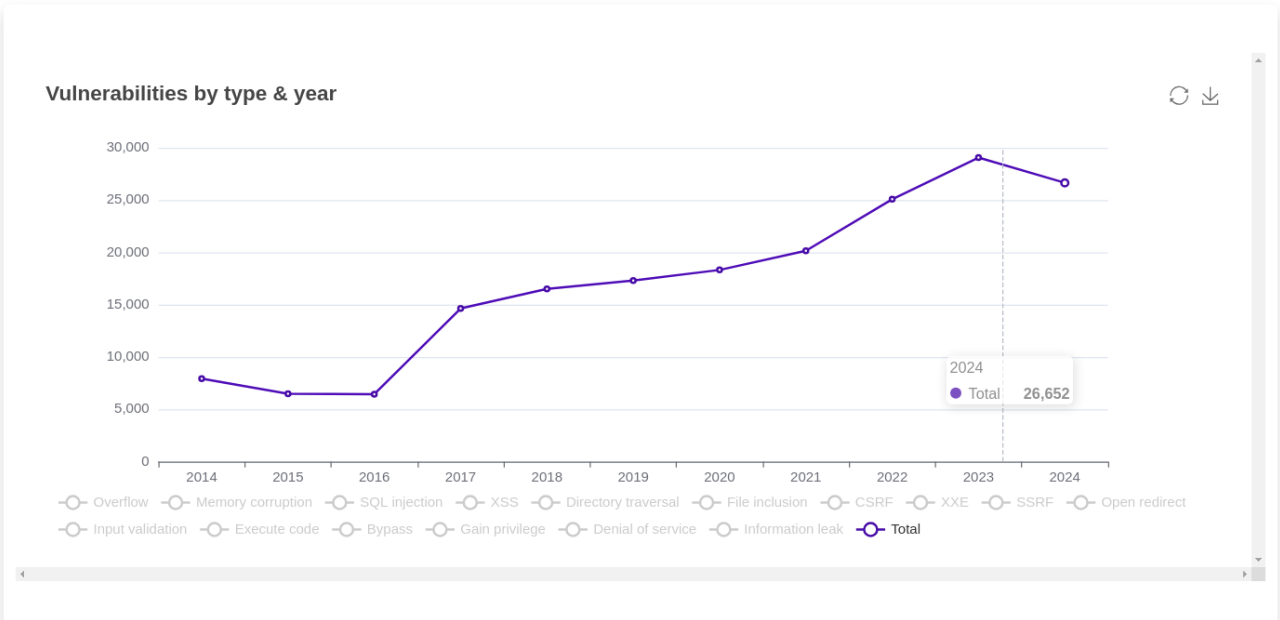
Vulnerabilities are everywhere!



Source: CVEdetails.com on 2024-09-02

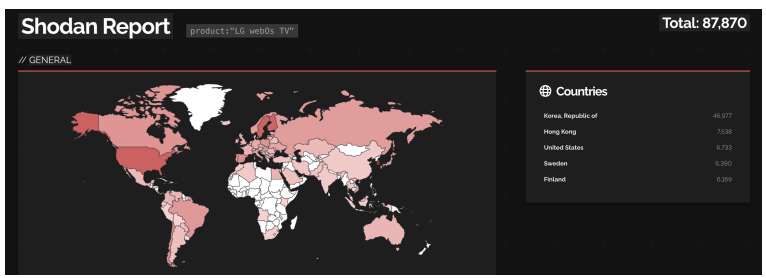
- This is crazy! https://www.cvedetails.com/

Vulnerabilities by type & year



Source: CVEdetails.com on 2024-09-02 Graph on the web site is interactive https://www.cvedetails.com/

LG TVs 2024 – CVE-2023-6317 up to CVE-2023-6320



90,000+ LG TVs Vulnerable to Authorization Attacks Due to WebOS Vulnerabilities

Bitdefender Labs has revealed a critical security flaw in over 90,000 LG smart TVs running the company's proprietary WebOS platform.

If exploited, the vulnerability could allow attackers to gain unauthorized access to the TV's functions and potentially the user's home network.

Source: https://cybersecuritynews.com/lg-tvs-vuauthorization-attacks/

Overlapping Security Incidents – Demant 2019

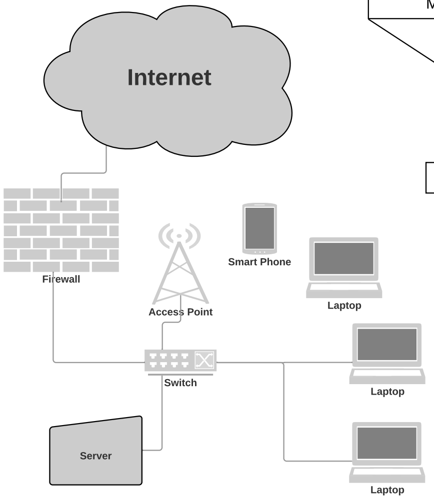
- For året 2019 rapporterede vi et tab i omsætning på **575 millioner kroner**. Det i sig selv er alvorligt. Hvad angår vores opmærksomhed på it-sikkerhedsområdet, har it-hændelsen været med til at understrege nødvendigheden af, at tage dette felt seriøst. Angreb mod it-infrastruktur er uden tvivl en af de største trusler mod en virksomhed, og det kan gå galt, hvis man ikke er i stand til at lukke ned for skaden og bruge sin back-up.

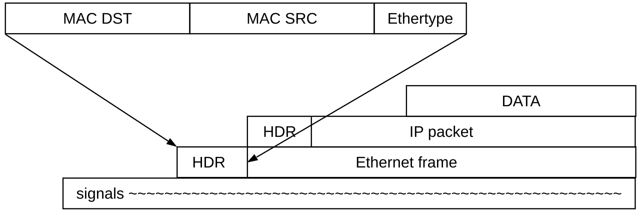
...

- På det konkrete plan har vi fået et mantra der lyder **'Active Directory is king, and backup is Queen'**. Men mere overordnet har vi også lært at Fokus skal helt op på øverste niveau i virksomheden, at man skal skaffe høj faglig indsigt i sikkerhed og trusler, og at det er et arbejde, der skal være under konstant observation og udvikling.

Kilde: https://dit.dk/Nyheder/2021/Demant

Protection, building secure and robust networks





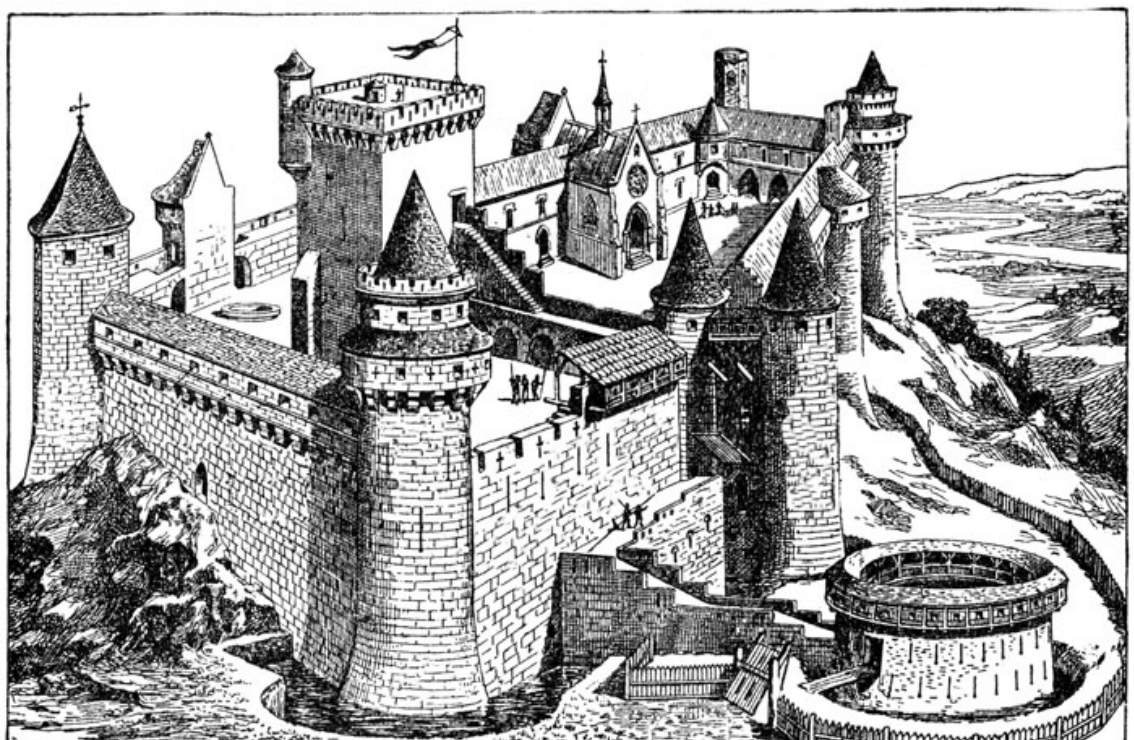
Ethernet frames contain packets

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet IPv4 Packet Header

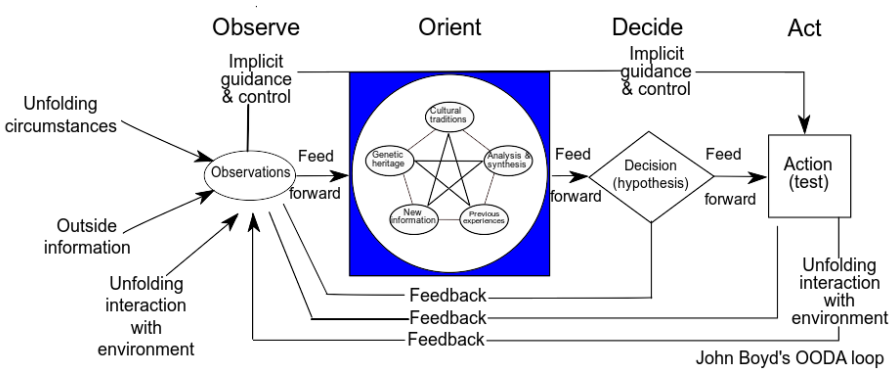
- We should prefer security mechanisms that does NOT require us to keep patching every month
- Can we change our networks to avoid this? Yes!

Defense in depth



Picture originally from: http://karenswhimsy.com/public-domain-images

Goals of Security – short version



Source: Patrick Edwin Moran - Wikipedia https://en.wikipedia.org/wiki/OODA_loop

- Prevention - means that an attack will fail
- Detection - determine if attack is underway, or has occured - report it
- Recovery - stop attack, assess damage, repair damage

Tight budgets everywhere!

Photo by Kelly Sikkema on Unsplash

Whats the goal, where are the strawberries!

- And you have a limited budget, always!
- Use the resources available in the best way is your mission!

Core Concepts – use existing knowledge!

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

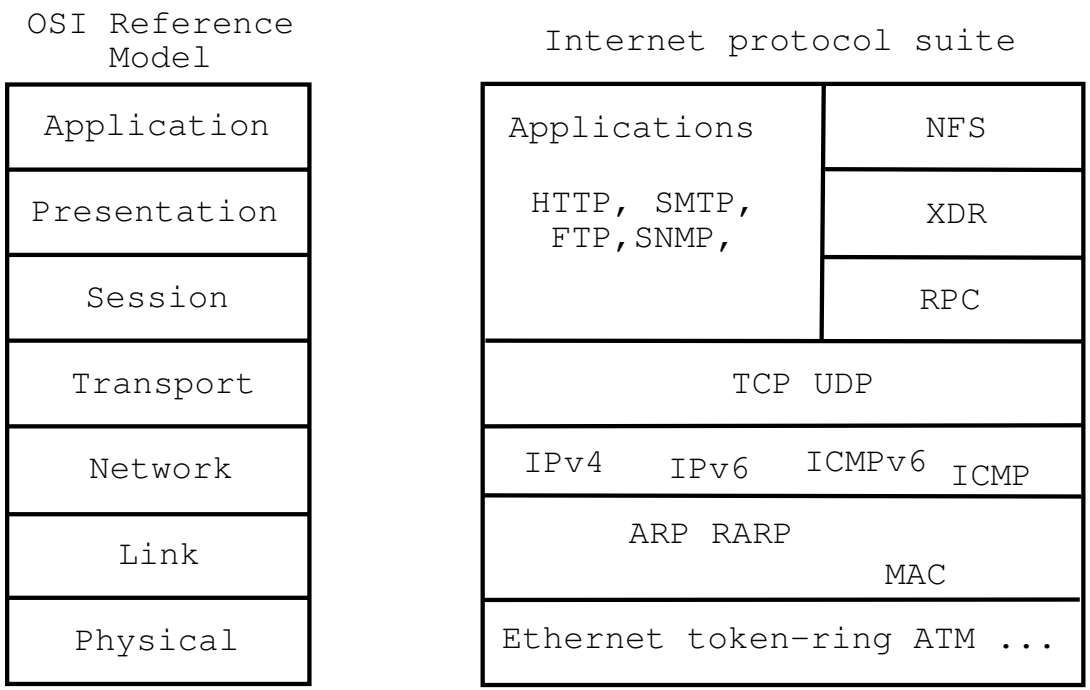
Work together

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

OSI Model and Internet Protocols



I recommend securing things from the bottom and from the outside

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
- Can function as inspiration and a checklist

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

Humble Bundle! https://www.humblebundle.com/

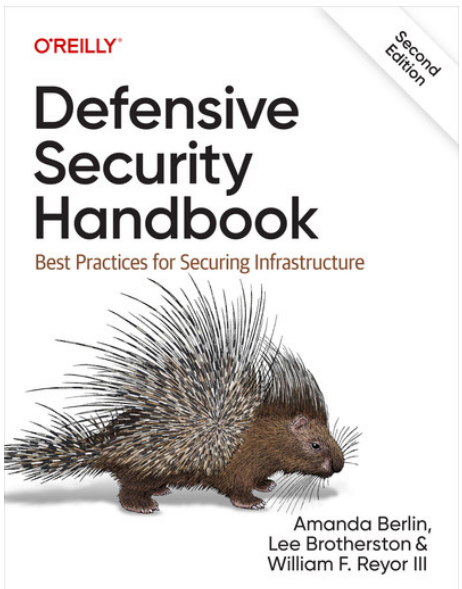
Other Materials

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

- 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

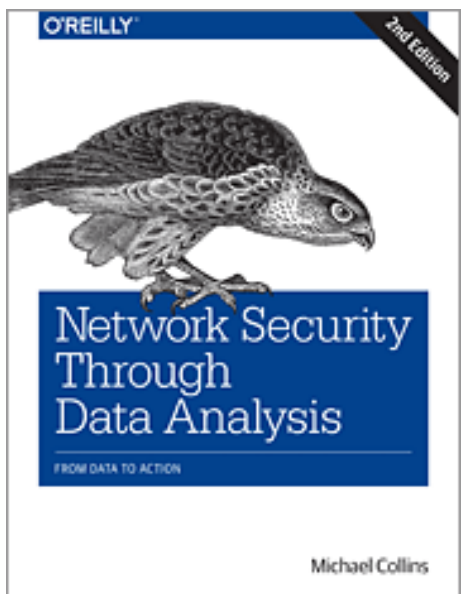
Book: Defensive Security Handbook (DSH)



Defensive Security Handbook: Best Practices for Securing Infrastructure, Lee Brotherston, Amanda Berlin, William F. Reyor ISBN: 9781098127237, 362 pages – Note: 2nd edition updated 2024

https://learning.oreilly.com/library/view/defensive-security-handbook/9781098127237/

Network Security Through Data Analysis



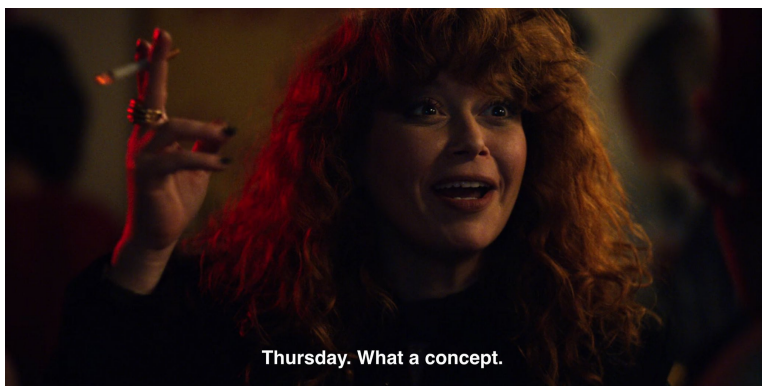
Network Security through Data Analysis , Michael S Collins, 2nd Edition, 2017

https://learning.oreilly.com/library/view/network-security-through/9781491962831/

Recommended tools to learn

- Open Source I really love open source. There is just too much great open source software, to ignore
- 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, PowerShell is another alternative
- Ansible provisioning – installing and configuring software for production
- Elasticsearch – how to run a *service*, full fledged applications exist for Elasticsearch
- OpenSSH – included in Linux and Windows, allows for Rsync, Git, port forward etc.

Thursday What a concept



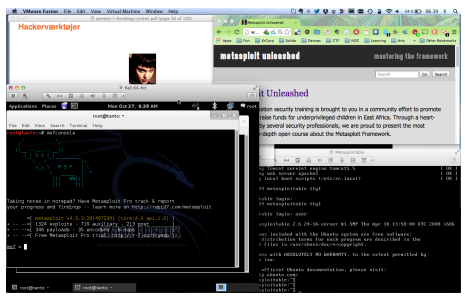
Alt text: Nadia from the Russian Doll fearing that she would never see a Thursday again says, "Thursday. What a concept" while smoking a cigarette

- Mastodon bot https://botsin.space/@thursday post the same picture each thursday
- Github Actions Workflows, se https://github.com/devashishp/thursday and https://docs.github.com/en/actions/writing-workflows

Github Actions Workflows

```yaml
jobs:
  deploy:
    runs-on: ubuntu-latest
    steps:
    - uses: actions/checkout@v3
    - name: Set up Python 3.10
      uses: actions/setup-python@v3
      with:
        python-version: "3.10"
    - name: Install dependencies
      run: |
        python -m pip install --upgrade pip
        pip install Mastodon.py
        if [ -f requirements.txt ]; then pip install -r requirements.txt; fi
    - name: Run Script
      run:
        python bot.py
```

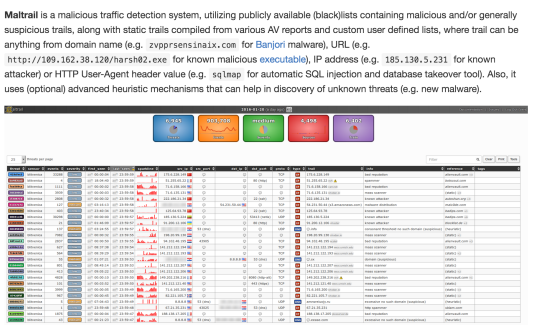
Open Source – Linux hackerlab



- 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

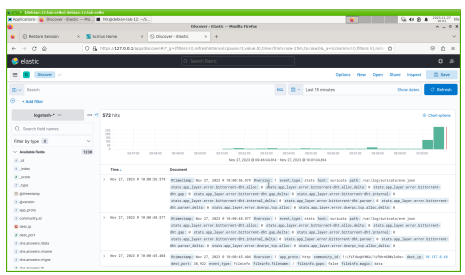
Why Elasticsearch

> 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

SELKS



SELKS™ is a free, open-source, and turn-key Suricata network intrusion detection/protection system (IDS/IPS), network security monitoring (NSM) and threat hunting implementation created and maintained by Stamus Networks.

Released under GPL 3.0-or-later license, the live distribution is available as either a live and installable Debian-based ISO or via Docker compose on any Linux operating system.

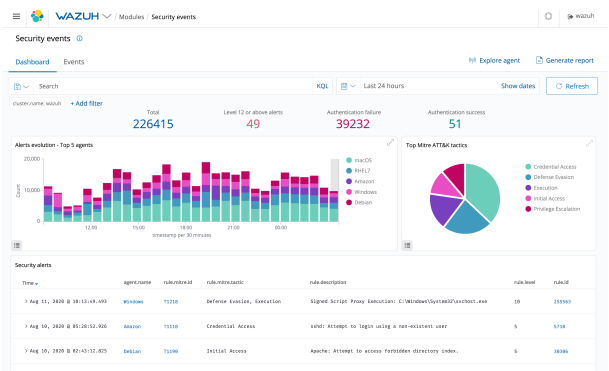
Source: https://www.stamus-networks.com/selks

The "install" on Debian 12 – in less than 30minutes

- [ ] Clone the Github repo: https://github.com/kramse/kramse-labs
  `git clone https://github.com/kramse/kramse-labs`
- [ ] Go into this repository and install Docker, there is a small README.md too:
  `cd kramse-labs/docker-install` and then `ansible-playbook 1-dependencies.yml`
- [ ] Enable Docker: `systemctl enable docker` and reboot the VM,
- [ ] Clone the SELKS repository:
  `git clone https://github.com/StamusNetworks/SELKS.git`
- [ ] Go into this and run docker-compose as described in the instructions:
  https://github.com/StamusNetworks/SELKS/wiki/Docker
  make sure to select the right network interface, so Suricata can sniff packets

This will provide a basic Elasticsearch version 7, with Kibana and Suricata

Example system: Wazuh



Wazuh agents scan the monitored systems looking for malware, rootkits and suspicious anomalies. They can detect hidden files, cloaked processes or unregistered network listeners, as well as inco nsistencies in system call responses.
Source: text and picture from https://wazuh.com/

- Wazuh initially a fork of the OSSEC project, and has integration with Elastic Stack

Wazuh agent

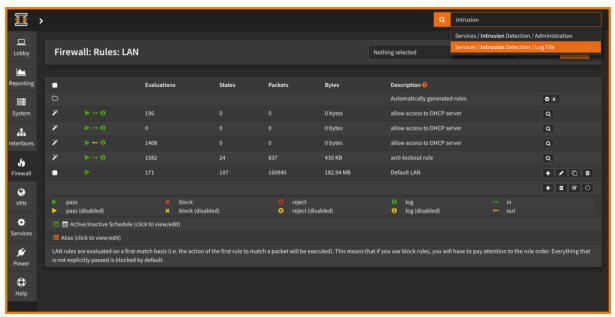
The Wazuh lightweight agent is designed to perform a number of tasks with the objective of detecting threats and, when necessary, trigger automatic responses. The agent core capabilities are:

The Wazuh agents run on many different platforms, including Windows, Linux, Mac OS X, AIX, Solaris and HP-UX. They can be configured and managed from the Wazuh server.

Source: https://wazuh.com/

- Log and events data collection
- File and registry keys integrity monitoring
- Inventory of running processes and installed applications
- Monitoring of open ports and network configuration
- Detection of rootkits or malware artifacts
- Configuration assessment and policy monitoring
- Execution of active responses

OPNsense GUI based and easy to install



OPNsense https://opnsense.org/

Firewall built on FreeBSD with web interface

Originally thoughts from m0n0wall and later https://www.pfsense.org/

Danish companies have been using these for many years now

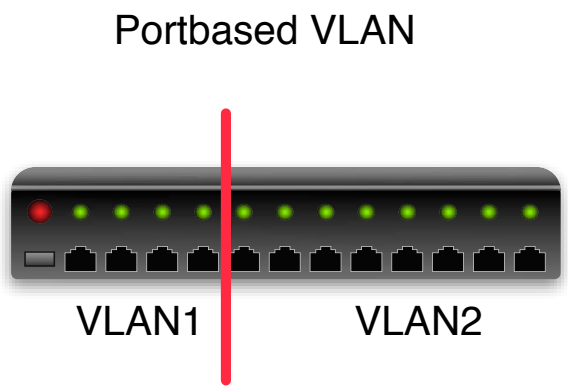
All servers should have firewall enabled!

Example: Uncomplicated Firewall (UFW)

```
root@debian01:~# apt install ufw
...
root@debian01:~# ufw status numbered
Status: active
     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

- Extremely easy to use – I recommend and use the (Uncomplicated Firewall) UFW
- Integrated with Ansible
- Windows and Mac also has firewall – enable it!

Together with Firewalls - Virtual LAN (VLAN)



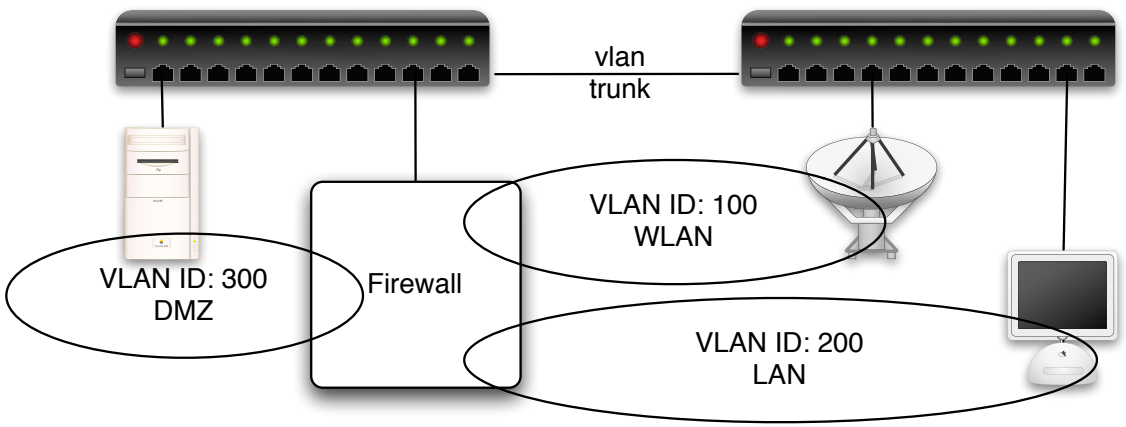
Managed switches often allow splitting into zones called virtual LANs

Most simple version is port based

Like putting ports 1-4 into one LAN and remaining in another LAN

Packets must traverse a router or firewall to cross between VLANs

Virtual LAN (VLAN) IEEE 802.1q



Using IEEE 802.1q VLAN tagging on Ethernet frames

Virtual LAN, to pass from one to another, must use a router/firewall

Allows separation/segmentation and protects traffic from many security issues

Used in most, if not all, Wi-Fi networks – each SSID has a VLAN behind it

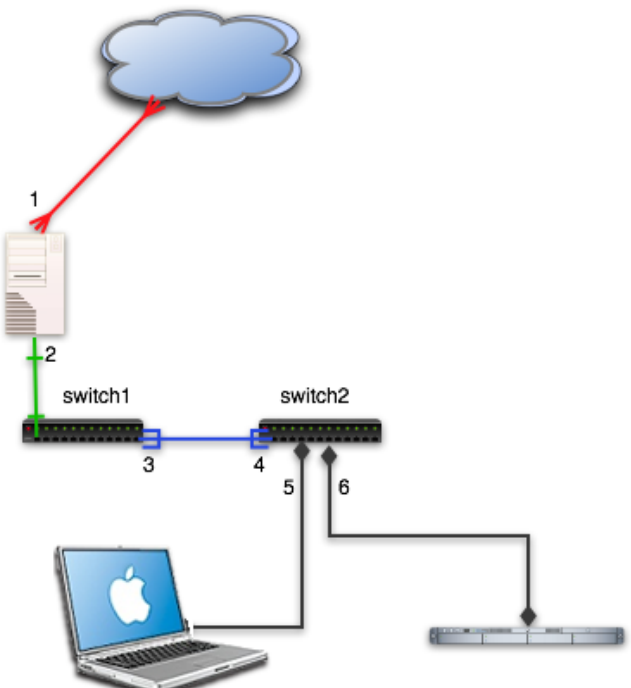
Equipment – wanna work with networks

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
- Getting an extra wireless network card for your laptop
- USB Ethernet for sniffing network – 200DKK StarTech USB 3.0



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

Who are you gonna call?

> Cyberangreb kan blive en dyr omgang for SMV'erne Et ransomware angreb koster 376.350 kr. alene i tabt omsætning fra e-handel for en virksomhed med 10-49 ansatte. I lyset af at truslen for cyberkriminalitet er på sit højeste, skal flere SMV'er have hjælp til at øge deres IT-sikkerhed. Særligt efter en hård tid under COVID-19, som h fokus væk fra IT-sikkerhed.

Source: SMVdanmark Marts 2022 https://smvdanmark.dk/analyser/temaanalyser/cyberangreb-kan-blive-en-dyr-omgang-

- You need friends!
- Incident Response is a specialized area
- They cost upwards of 1.500DKK / hour – more if outside of business hours
- Pre-arranged is recommended, agree on *who can call them*, decide up front when to call them – not for every little incid
- Expect an incident to cost at least 100.000DKK plus time, lost hours, lost orders, etc.

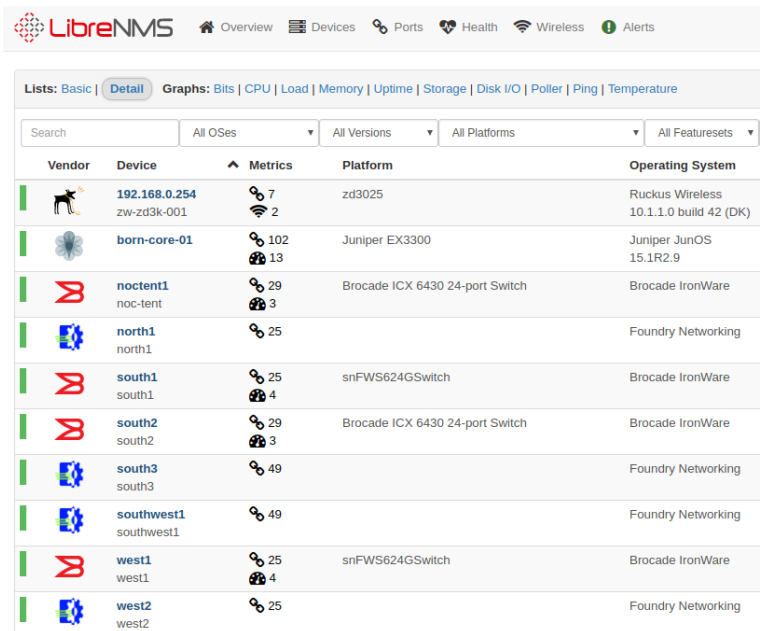
Automate it all!

Some things probably cannot be automated!

- Do not trust the automation will fix everything, and don't mention AI

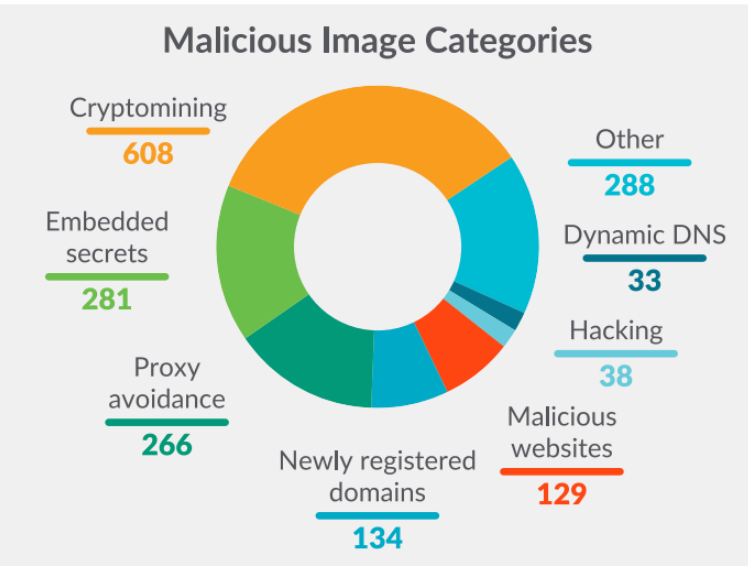
- Make *manual tasks* easier!
- I usually update server myself – but have a scripted process
- Put commands into small script – even a one-line for doing a task
- Example: Look up a MAC address, find a port in a switch

LibreNMS Automatic discovery



Automatically discover your entire network using CDP, FDP, LLDP, OSPF, BGP, SNMP and ARP
https://www.librenms.org/

Analysis on Docker Hub malicious images: Attacks through public container images



This article is relevant, talking about malicious docker images
https://sysdig.com/blog/analysis-of-supply-chain-attacks-through-public-docker-images/

Keeping Container Images secure

- 🔧 `anchore` open-source project that provides a centralized service for inspection, analysis, and certification of container images https://github.com/anchore/anchore-engine
  "As of 2023, Anchore Engine is no longer maintained. There will be no future versions released. Users are advised to use Syft and Grype."
- 🔧 `Syft` https://github.com/anchore/syft and 🔧 `Grype` https://github.com/anchore/grype
- Allow direct download from the internet into your cluster, may become a problem
- Malicious people are typosquatting popular containers!
- Suply chain attacks in general are a problem

Harden Container Images and Update Your Procedures

- Change the goddamn passwords!
  Container postgresql with user postgres and password *postgres*, REALLY!!!!!!1111
- and NO MORE ROOT! Dont run as root, we realized this was bad in the 1990s!
- CIS Docker Benchmarking also Learn Kubernetes Security *Chapter 8: Securing Kubernetes Pods*
- Hacking Kubernetes *Chapter 8: Policy* - describe things like Resource Quotas, Runtime Policies

Recommendations from CIS Docker Benchmark

Container Images and Build File Configuration

Container base images and the build files used to create them dictate what is inside a container and how it operates. Ensure your base images and build files are safe and trusted. Here are CIS recommendations for images.

Configuration Element	Recommendations
Permissions	1. Create a user for the container 2. Remove setuid and setgid permissions
Container content	1. Avoid unnecessary packages in the container 2. Only install verified packages 3. Define HEALTHCHECK instructions for the container 4. Enable content trust for Docker
Images	1. Only use trusted base images 2. Perform security scans on images 3. Rebuild images to include security patches
Dockerfiles	1. Ensure update instructions are not use alone 2. Use COPY instead of ADD 3. Do not store secrets in Dockerfiles

Summary from: https://www.aquasec.com/cloud-native-academy/docker-container/docker-cis-benchmark/

- Latest version: CIS Docker Benchmark v1.5.0 - 12-28-2022

Benchmarking tools

🔧 `Kube-bench` is the industry-standard tool to automate checking Kubernetes compliance with the Center for Internet Security (CIS) Benchmark.

Kube-bench makes it easy for operators to check whether each node in their Kubernetes cluster is configured according to security best practices.

Source: https://info.aquasec.com/open-source

- CIS Kubernetes V1.24 Benchmark v1.0.0 - 09-21-2022 – other versions exist
- CIS Docker Benchmark v1.5.0 - 12-28-2022

Tool example kube-bench

```
hlk@timon:~/bin/kube-bench/kube-bench$ kubectl logs kube-bench-gdf62
[PASS] 1.1.7 Ensure that the etcd pod specification file permissions are set to 600 or more restrictive (Automated)
[PASS] 1.1.8 Ensure that the etcd pod specification file ownership is set to root:root (Automated)
[WARN] 1.1.9 Ensure that the Container Network Interface file permissions are set to 600 or more restrictive (Manual)
[WARN] 1.1.10 Ensure that the Container Network Interface file ownership is set to root:root (Manual)
[PASS] 1.1.11 Ensure that the etcd data directory permissions are set to 700 or more restrictive (Automated)
[FAIL] 1.1.12 Ensure that the etcd data directory ownership is set to etcd:etcd (Automated)
...
== Summary policies ==
0 checks PASS
0 checks FAIL
35 checks WARN
0 checks INFO

== Summary total ==
63 checks PASS
10 checks FAIL
58 checks WARN
0 checks INFO
```

- https://github.com/aquasecurity/kube-bench also check out Lynis https://cisofy.com/lynis/

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