Welcome to

Vulnerability Management

Tools and Processes

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

Slides are available as PDF, kramse@Codeberg

vuln-mgmt-tools-processes.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

What are vulnerabilities and exploits

Patch management – asset discovery and management

Long term mitigation and protection – how can we achieve that

Photo by Pawel Janiak on Unsplash

Malware and Worms

Definition 23-1 *Malicious logic*, more commonly called *malware*, is a set of instructions that cause a site's security policy to be violated

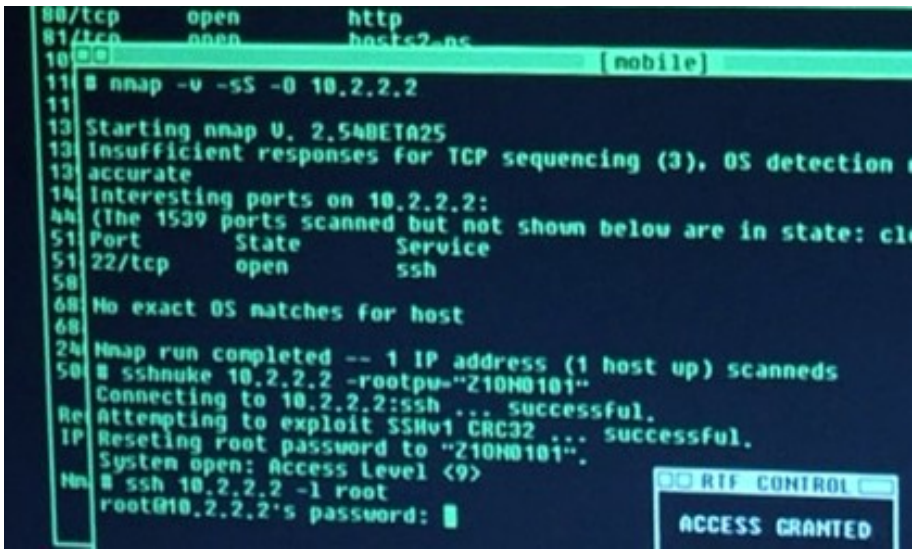
Definition 23-4 A *computer virus* is a program that inserts (a possibly transformed version of) itself into one or more files and then performs some (possibly null) action.

Definition 23-2 A *Trojan horse* is a program with an overt (documented or known) purpose and a covert (undocumented or unexpected) purpose

Definition 23-14 A *computer worm* is a program that copies itself from one computer to another. Computer worms has existed since research began mid-1970s

Source: *Computer Security: Art and Science*, 2nd edition 2019! Matt Bishop ISBN: 9780321712332
Virus, trojan or worm? Unless you work specifically in the computer virus industry, call it all malware

Vulnerability Analysis – Trinity breaking in



Very realistic: https://nmap.org/movies/ and https://youtu.be/51lGCTgqE_w

- *Vulnerability* or security *flaw* – exploiting the vulnerability happens by an attacker
- A program or script used for this is called an *exploit*

The Wikipedia definition

Vulnerabilities are **flaws** in a computer system that weaken the overall security of the system.

Despite intentions to achieve complete correctness, virtually all hardware and software contains bugs where the system does not behave as expected. If the bug could enable an attacker to compromise the confidentiality, integrity, or availability of system resources, it is called a vulnerability. Insecure software development practices as well as design factors such as complexity can increase the burden of vulnerabilities. There are different types most common in different components such as hardware, operating systems, and applications.

Vulnerability management is a process that includes identifying systems and prioritizing which are most important, scanning for vulnerabilities, and taking action to secure the system. Vulnerability management typically is a combination of remediation (fixing the vulnerability), mitigation (increasing the difficulty or reducing the danger of exploits), and accepting risks that are not economical or practical to eliminate.

Source: https://en.wikipedia.org/wiki/Vulnerability_(computer_security)

Included this specifically because I agree *virtually all hardware and software contains bugs*

What is an exploit?

```
sploit = {
  nil                    => /220.*Sendmail/,
  'DEBUG'                => /200 Debug set/,
  "MAIL FROM:<#{from}>" => /250.*Sender ok/,
  "RCPT TO:<#{to}>"      => /250.*Recipient ok/,
  'DATA'                 => /354 Enter mail.*itself/,
  # Indent PATH= so it's not interpreted as a mail header
  " PATH=#{path}"        => nil,
  'export PATH'          => nil,
  payload.encoded        => nil,
  '.'                    => /250 Ok/,
  'QUIT'                 => /221.*closing connection/
}
```

Source: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/smtp/morris_sendmail_debug.rb

- Command injection through debugging *feature*

The Internet Worm 2. nov 1988

Exploited the following vulnerabilities

- buffer overflow in fingerd - VAX code
- Sendmail - DEBUG functionality
- Trust between systems: rsh, rexec, ...
- Bad passwords

Contained camouflage!

- Program name set to 'sh'
- Used fork() to switch PID regularly
- Password cracking using intern list of 432 words and /usr/dict/words
- Found systems to infect in /etc/hosts.equiv, .rhosts, .forward, netstat ...

Made byRobert T. Morris, Jr.

Many Years ago around 1988

```
/usr/src/etc/fingerd.c from 4.3BSD:
main(argc, argv)
        char *argv[];
{
        register char *sp;
        char line[512];  // This is a fixed size buffer
        struct sockaddr_in sin;
...
        line[0] = '\0';
        gets(line);      // This line can overflow the buffer, buffer overflow vulnerability
```

Source code link https://www.tuhs.org/cgi-bin/utree.pl?file=4.3BSD/usr/src/etc/fingerd.c

More description in the articles:

https://spaf.cerias.purdue.edu/tech-reps/823.pdf *The Internet Worm Program: An Analysis* Purdue Technical Report CSD-TR-823 Eugene H. Spafford

https://blog.rapid7.com/2019/01/02/the-ghost-of-exploits-past-a-deep-dive-into-the-morris-worm/ The Ghost of Exploits Past: A Deep Dive into the Morris Worm

Stuxnet

Worm in 2010 intended to infect Iran nuclear program

Target was the uranium enrichment process

Infected other industrial sites

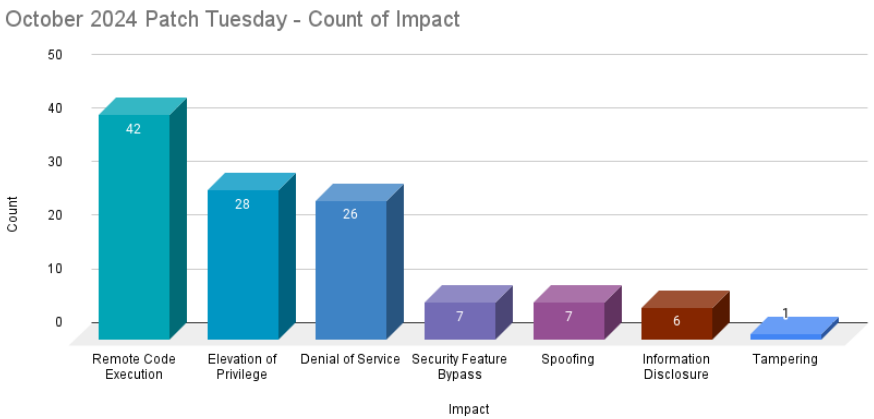
SCADA, and Industrial Control Systems (ICS) are becoming very important for whole countries

A small *community* of consultants work in these *isolated* networks, but can be used as infection vector - they visit multiple sites

More can be found in https://en.wikipedia.org/wiki/Stuxnet

Exploits are worth millions! Bug bounty is a concept, developing and selling exploits

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

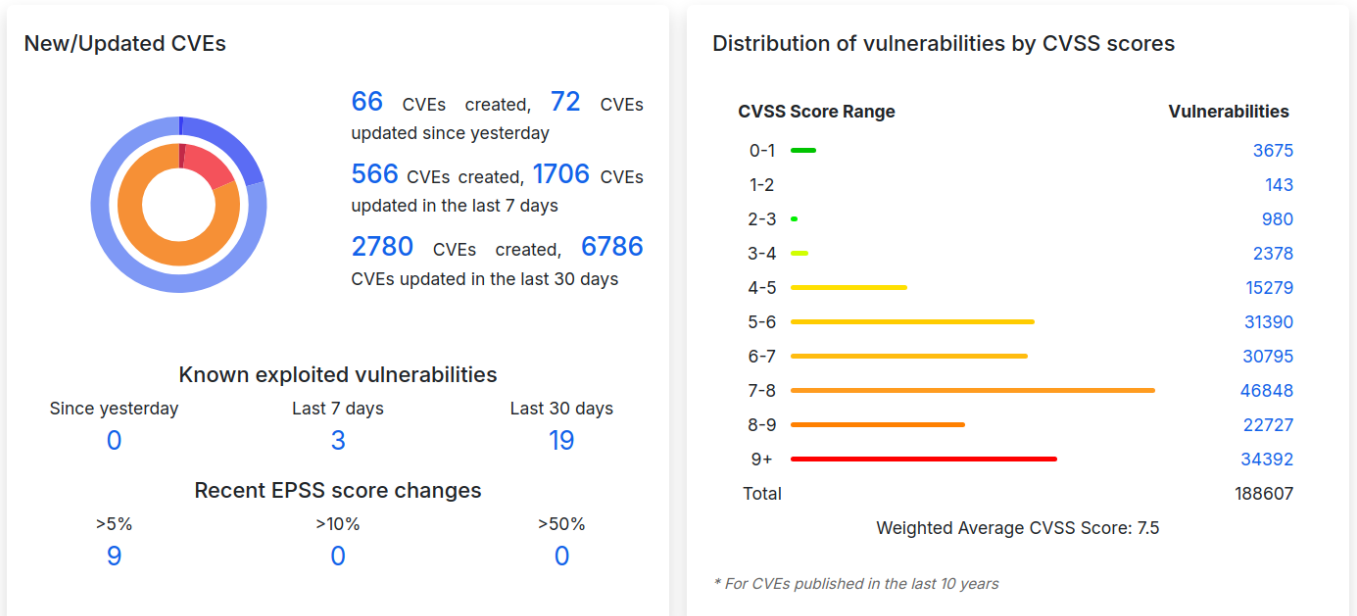
CVE maintained by MITRE - not-for-profit org for research and development in the USA.

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/

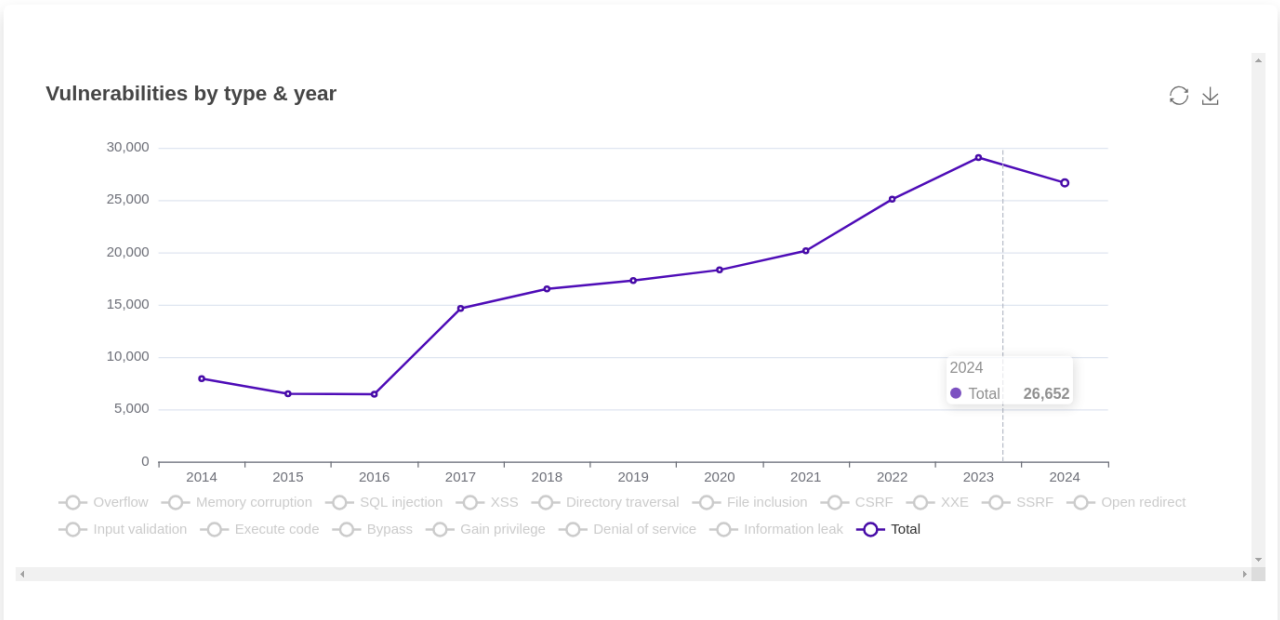
Vulnerabilities are everywhere!



Source: CVEdetails.com on 2024-09-02

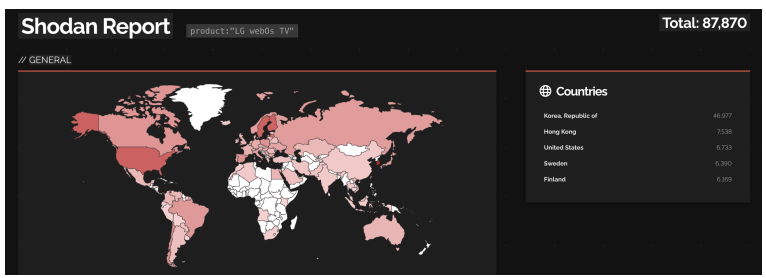
- This is crazy! https://www.cvedetails.com/

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/

Sample vulnerabilities

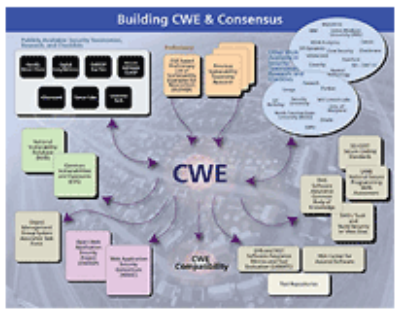
CVE-2000-0884
IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.

CVE-2002-1182
IIS 5.0 and 5.1 allows remote attackers to cause a denial of service (crash) via malformed WebDAV requests that cause a large amount of memory to be assigned.

Source:
http://cve.mitre.org/-CVE

And updates from vendors reference these too! A closed loop

CWE Common Weakness Enumeration



Enlarge

CWE™ International in scope and free for public use, CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

CWE in the Enterprise

- Software Assurance
- Application Security
- Supply Chain Risk Management
- System Assessment
- Training
- Code Analysis
- Remediation & Mitigation
- NVD (National Vulnerability Database)
- *Recommendation ITU-T X.1524 CWE,* ITU-T CYBEX Series

http://cwe.mitre.org/

CWE/SANS Monster mitigations

Monster Mitigations

These mitigations will be effective in eliminating or reducing the severity of the Top 25. These mitigations will also address many weaknesses that are not even on the Top 25. If you adopt these mitigations, you are well on your way to making more secure software.

A Monster Mitigation Matrix is also available to show how these mitigations apply to weaknesses in the Top 25.

ID	Description
M1	Establish and maintain control over all of your inputs.
M2	Establish and maintain control over all of your outputs.
M3	Lock down your environment.
M4	Assume that external components can be subverted, and your code can be read by anyone.
M5	Use industry-accepted security features instead of inventing your own.
GP1	(general) Use libraries and frameworks that make it easier to avoid introducing weaknesses.
GP2	(general) Integrate security into the entire software development lifecycle.
GP3	(general) Use a broad mix of methods to comprehensively find and prevent weaknesses.
GP4	(general) Allow locked-down clients to interact with your software.

See the Monster Mitigation Matrix that maps these mitigations to Top 25 weaknesses.

Source: http://cwe.mitre.org/top25/index.html

Reflecting on the Internet Worm at 35

> Thirty-five years ago today (November 2nd), the Internet Worm program was set loose to propagate on the Internet. ... All of that eventually led to a boom in add-on security measures, resulting in what is now a **multi-billion dollar cybersecurity industry.** ... The Worm provided us with an object lesson about many issues that, unfortunately, were not heeded in full to this day. **That multi-billion dollar cybersecurity industry is still failing to protect far too many of our systems.**

Source: *Reflecting on the Internet Worm at 35*, November 02, 2023 by spaf, Eugene Spafford
https://www.cerias.purdue.edu/site/blog/post/reflecting_on_the_internet_worm_at_35/

- Many of the same problems that plagued us earlier are still the same!
- My thoughts are we should try something else than *patch insanity*

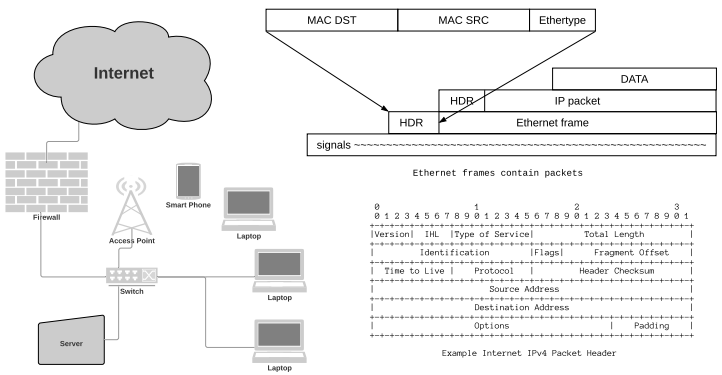
Case in point: SQL injection affecting airport security

> Bypassing airport security via SQL injection
> 08/29/2024
> Like many, Sam Curry and I spend a lot of time waiting in airport security lines. If you do this enough, you might sometimes see a special lane at airport security called Known Crewmember (KCM). KCM is a TSA program that allows pilots and flight attendants to bypass security screening, even when flying on domestic personal trips.
> The KCM process is fairly simple: the employee uses the dedicated lane and presents their KCM barcode or provides the TSA agent their employee number and airline. Various forms of ID need to be presented while the TSA agent's laptop verifies the employment status with the airline. If successful, the employee can access the sterile area without any screening at all.

Source: https://ian.sh/tsa

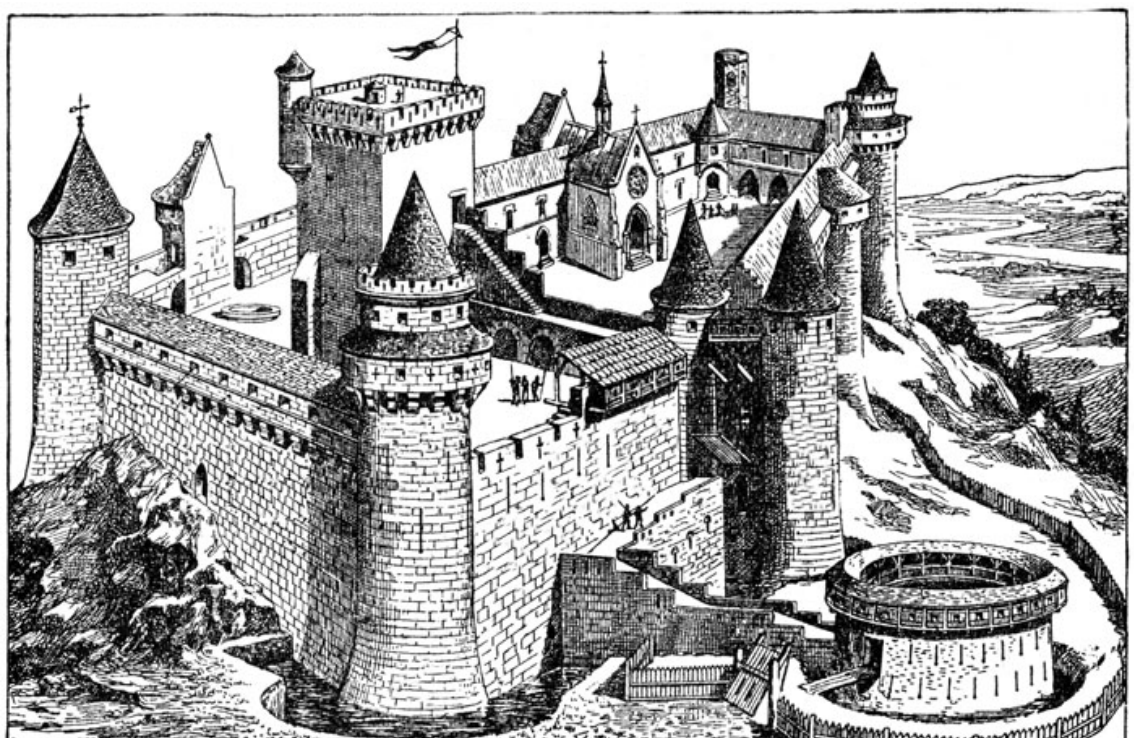
- And SQL injection is one of the *easiest* software security problems to guard against!

Protection, building secure and robust networks



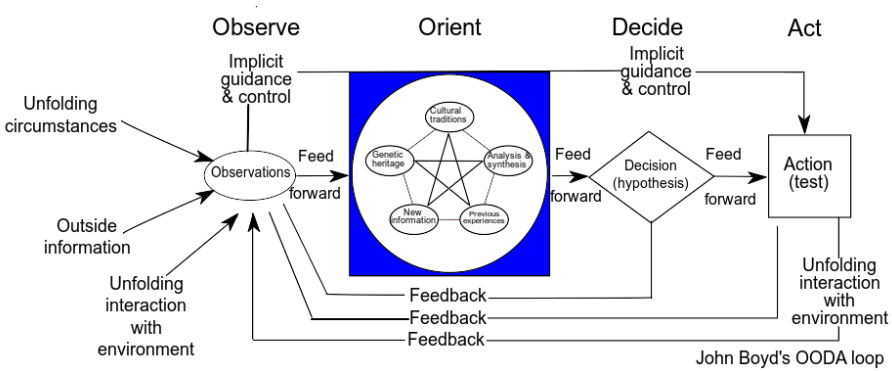
- We should prefer security mechanisms that does NOT require us to keep patching every month
- Can we change our infrastructure and networks to avoid this? **Yes!**
- Reduce complexity – note adding VLANs may seem to increase, but also reduce number of systems that can interact, and each *network* is afterwards easier to understand
- Limit the attack surface – fewer systems exposed ➔fewer vulns exposed, fewer services ➔less code!

Defense in depth



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

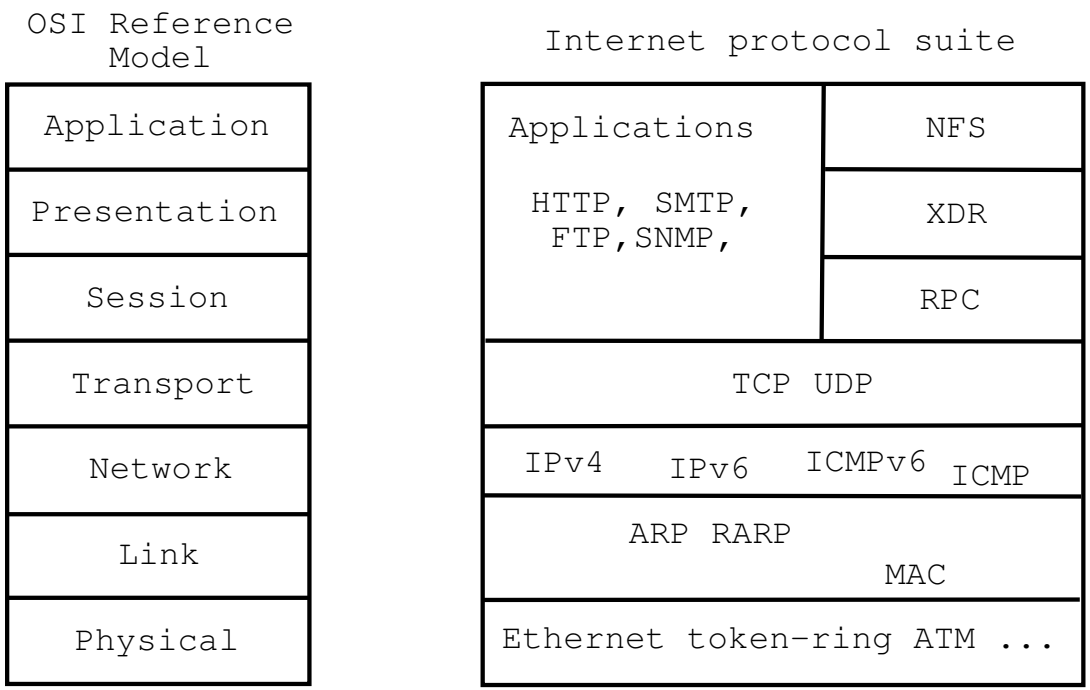
Goals of Security – short version



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

OSI Model and Internet Protocols



I recommend securing things from the bottom and from the outside

Books and courses

How:

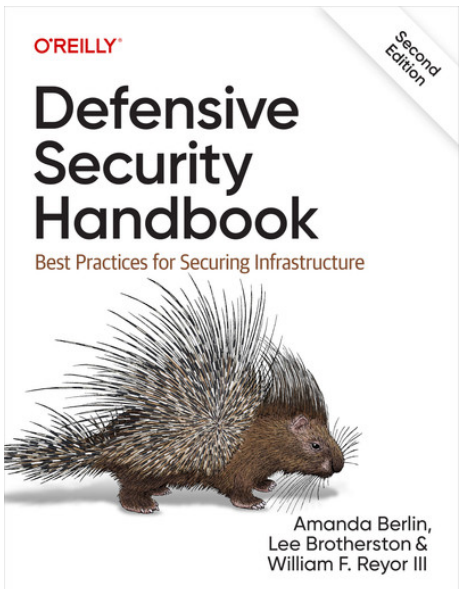
I like to learn new concepts from books

- 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/

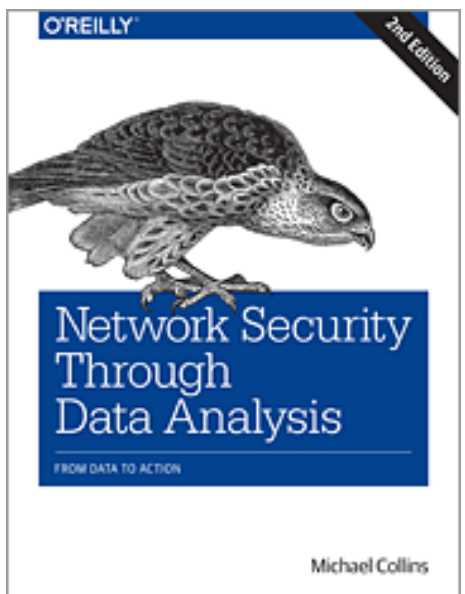
Book: Defensive Security Handbook (DSH)



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 – DevSecOps

- 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 – installing and configuring software for production, gathering information
- 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.

Learning DevSecOps: A Practical Guide to Processes and Tools

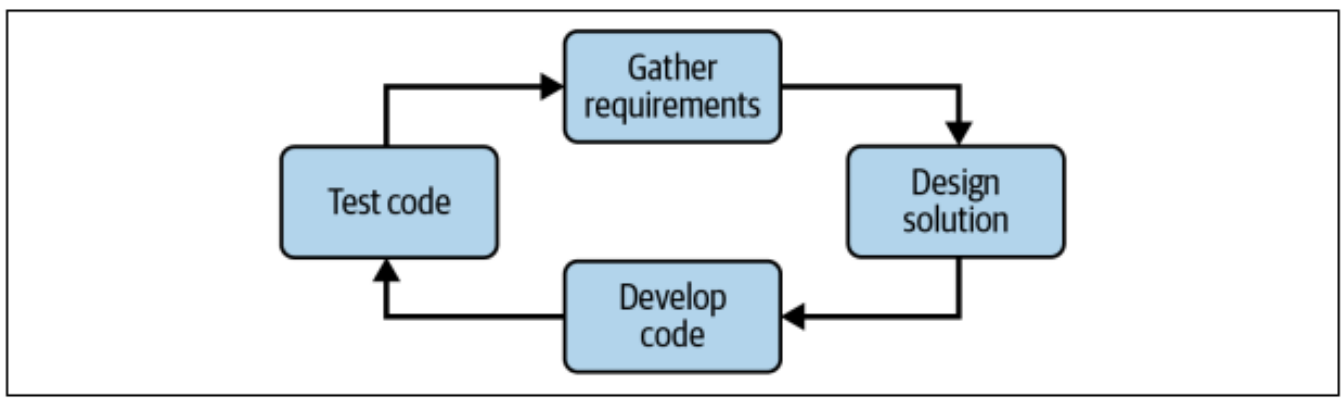
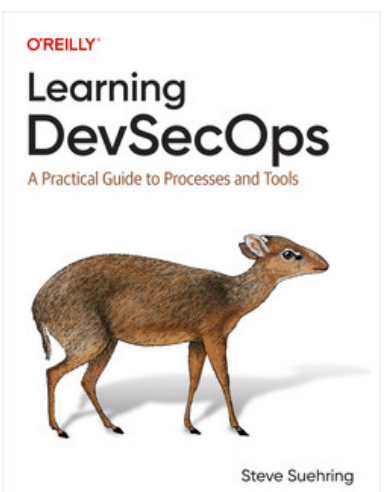
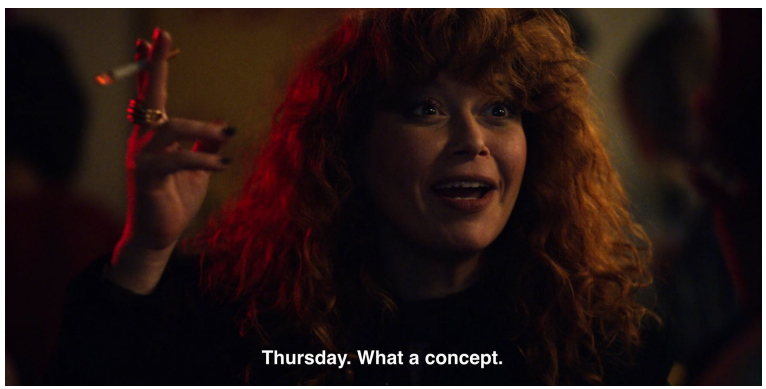


Figure 1-3. Iterating through each phase and then starting over with an Agile-like process



Learning DevSecOps, Steve Suehring Released May 2024, O'Reilly, ISBN: 9781098144869

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

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 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,

Ansible Configuration management and more!

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 infrastructure
- Depends on Python and SSH, or module for the network devices

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

Gathering information from Systems automatically

```
yamabushi$ ansible -m setup sunny | egrep "ansible_distribution|kernel"
        "ansible_distribution": "OpenBSD",
        "ansible_distribution_release": "release",
        "ansible_distribution_version": "7.5",
        "ansible_kernel": "7.5",
        "ansible_kernel_version": "GENERIC.MP#82",
```

- Quick and dirty, output it JSON – so could use jq instead https://jqlang.github.io/jq/

Creating automation playbooks with YAML

```
yamabushi$ cat os-release.yaml
---
- hosts: all
  gather_facts: yes
  become: false
  tasks:
  - name: Distribution
    debug: msg="{{ ansible_distribution }}"
  - name: Distribution version
    debug: msg="{{ ansible_distribution_version}}"
```

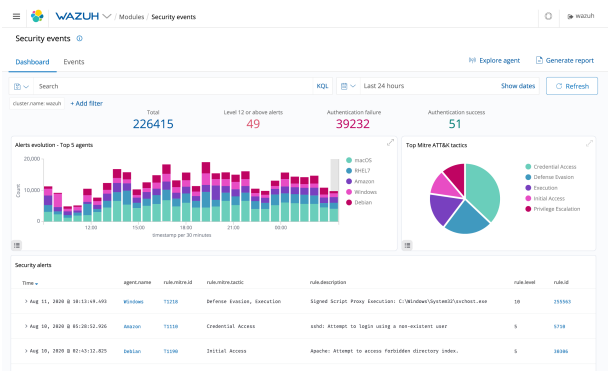
- Creating playbooks is not dificult

Output from Automation

```
TASK [Distribution version] ********************
...
ok: [sunny] => {
    "msg": "7.5"
}
ok: [shito] => {
    "msg": "7.4"
}
ok: [conserver01] => {
    "msg": "7.5"
}
ok: [pumba] => {
    "msg": "7.6"
}
```

- So it seems I have upgraded some systems to OpenBSD 7.5, and 7.6
- One is only OpenBSD 7.4 – plan ugrade soon

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

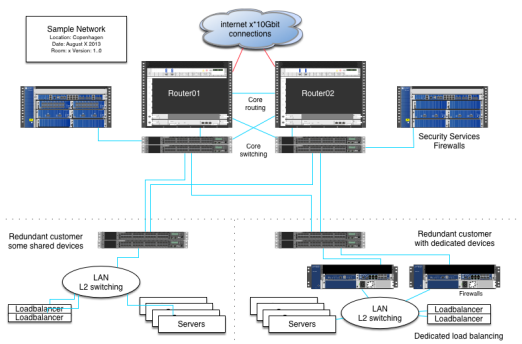
The Wazuh lightweight agent is designed to perform a number of tasks with the objective of detecting threats and, when necessary, trigger automatic responses. The agent core capabilities are:

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

Asset inventory



- Routers on the way to critical systems and networks – especially availability
- Firewall – is the environment protected sufficiently, discarding probes
- Mail servers – relay testing and also critical data
- Web servers – holds data, typically has a lot of functionality
- Cloud systems, storage systems, anywhere data is saved
- I recommend Nmap for both offensive and defensive purposes! https://nmap.org

Reporting – results

What is in a pentest report:

- Title, Table of contents, formal report thanks
- Confidentiality agreement – Write "Confidential" on each page
- Executive summary – big companies always want this
- Information about the scan done, what was it
- Scope and targets
- Review of all targets – detailed information and recommendations
- Conclusion – may be more technical
- Appendices – various information, Whois info about subnets and prefixes

BTW When delivering a report, it is up to the organisation to decide which recommendations to implement

Sample report available at: https://github.com/kramse/pentest-report

Basic Portscan

What is port scanning

- Testing all ports from 0/1 up to 65535
- Goal is to identify open ports – vulnerable services
- Typically TCP and UDP scans
- TCP scanning is more reliable than UDP scanning
- TCP handshake is easy to see, due to session setup – services must respond to SYN with SYN-ACK. Otherwise client programs like browsers will not work
- UDP applications respond differently – if at all
  They might respond to queries and probes in the correct format,
  If no firewall the operating systems will respond with ICMP on closed ports
- Use Zenmap while learning Nmap

Nmap port sweep for web services

```
root@cornerstone:~#  nmap -p80,443 172.29.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT    STATE    SERVICE
80/tcp  open     http
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

Nmap Advanced OS detection

```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).
PORT    STATE    SERVICE VERSION
80/tcp  open     http    Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
or iOS 4.1 - 7.1 (Darwin 10.0.0 - 14.0.0), Apple Mac OS X 10.8 - 10.8.3 (Mountain Lion)
or iOS 5.1.1 - 6.1.5 (Darwin 12.0.0 - 13.0.0)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```

- Low level operating system identification, often I use `nmap -A`
- Send packets, observe responses, match with tables of known operating system fingerprints
- An early reference for this was: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin, 2001

Scan for Specific Vulns – Heartbleed and TLS

Nmap includes Nmap scripting engine (NSE)

Example Usage

```
nmap -sV -sC <target>
```

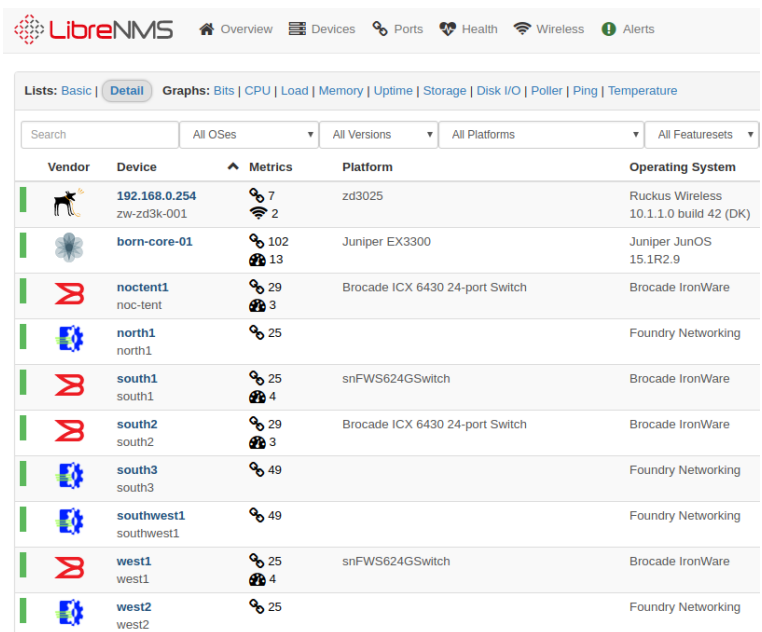
Script Output

```
443/tcp open   https   syn-ack
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

`nmap -p 443 --script ssl-heartbleed <target>`
https://nmap.org/nsedoc/scripts/ssl-heartbleed.html

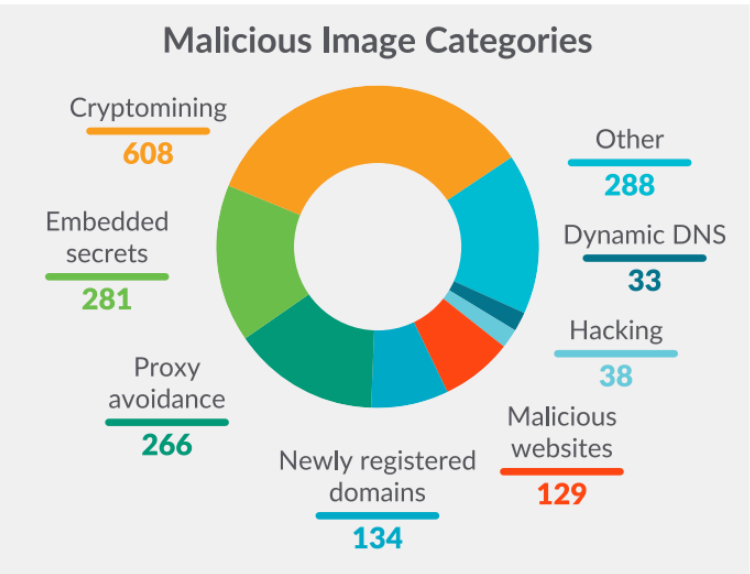
Almost every new popular vulnerability will have Nmap recipe

LibreNMS Automatic discovery – inventory management



Automatically discover your entire network using CDP, FDP, LLDP, OSPF, BGP, SNMP and ARP
See all the versions, what do you have, what needs to be secure https://www.librenms.org/

Analysis on Docker Hub malicious 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/

Introducing firewalls

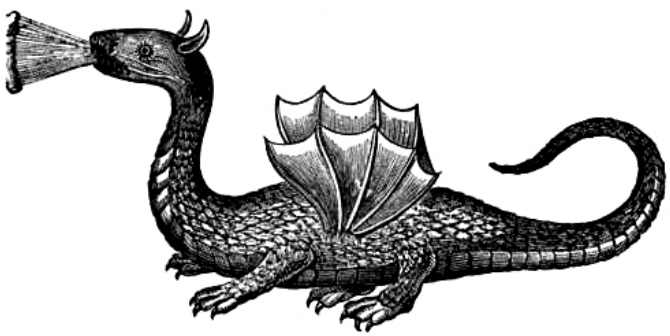
Some of these slides are part of the course:
Communication and Network Security at KEA, next course April 2. 2024
https://kompetence.kea.dk/kurser-fag/netv%C3%A6rk-og-kommunikationssikkerhed

specifically the slideshow
3. Traffic Inspection and Firewalls

I also have multiple presentations and materials about related subjects in my Github:

- Attack and Defense
- DDoS Testing
- Security in a Mixed IPv4 and IPv6 World
- SIEM and Log analysis
- Kubernetes Security

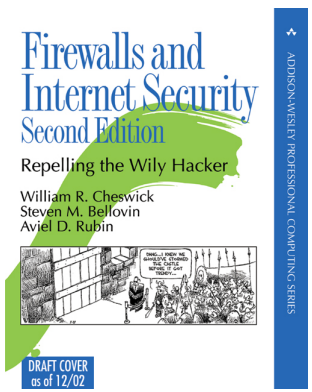
Networks are trouble



Internet here be dragons

- Networks are constantly evolving
- Increased threat landscape, World wide networks, attacks from everywhere
- Vulnerabilities are found daily, Software quality - even security and firewall software has flaws
- Even more vulnerabilities are *developed* and *installed*
  Sorry developers, but some of you don't care, and it shows!

Back in the day: Firewalls and Internet Security, 1994



- *Firewalls and Internet Security: Repelling the Wily Hacker* , Second Edition 2003, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin, **2003** http://www.wilyhacker.com/
- The full PDF—and the full LaTeX source of the book. Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
- How to configure firewalls often boil down to, should we allow protocol X
- If we allow certain protocols through a firewall, we are asking for trouble

Network Segmentation – Firewalls

$ firewall

1. (I) **An internetwork gateway that restricts data communication traffic to and from one of the connected networks** (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). (See: guard, security gateway.)
2. (O) **A device or system that controls the flow of traffic between networks using differing security postures.** Wack, J. et al (NIST), "Guidelines on Firewalls and Firewall Policy", Special Publication 800-41, January 2002.

Tutorial: A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies policy rules to control traffic that flows in and out of the protected network.

Source: RFC4949 *Internet Security Glossary, Version 2*
https://datatracker.ietf.org/doc/html/rfc4949 2007

Continued

A firewall is not always a single computer. For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN (see: buffer zone) between the two routers. The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher-layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers. The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep unauthorized traffic (i.e., intruders) out, but usually also needs to let authorized traffic pass both in and out.

Source: RFC4949 *Internet Security Glossary, Version 2*

https://datatracker.ietf.org/doc/html/rfc4949 2007

What is a packet filter

We may want to distinguis between different types of firewalls/devices:

- Network layer, we often call them packet filters, stateless
- Application level, we often call them, stateful filtering and gateways
- Firewalls are by design a choke point, natural place
  to do network security monitoring!

They are all firewalls – or firewall devices!

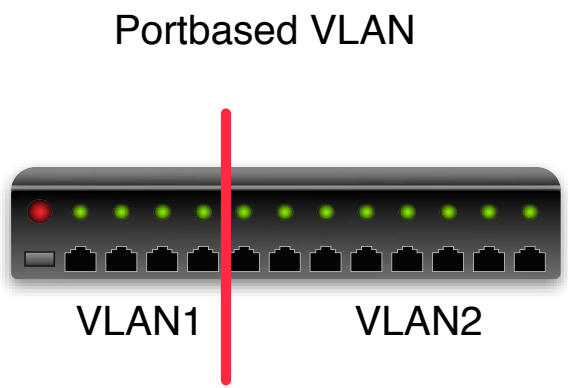
Best Current Practice

Lets get this out of the way immediately, you should already be doing

- Network segmentation and filtering – we could write a book about this! 🚩
- Monitor your network – both bandwidth, error, netflow etc. 🚩
- Take control of your network, no more admin/admin logins on core devices 🚩
- Turn on authentication for protocols – routing protocols but also any http service within your org 🚩
- Configure host-based firewalls 🚩
- Control DNS – internally and externally, recursive, authoritative etc. 🚩

This goes for IPv4-only, IPv6-only, and mixed networks!

Isolation and Network Segmentation – Virtual LAN (VLAN)



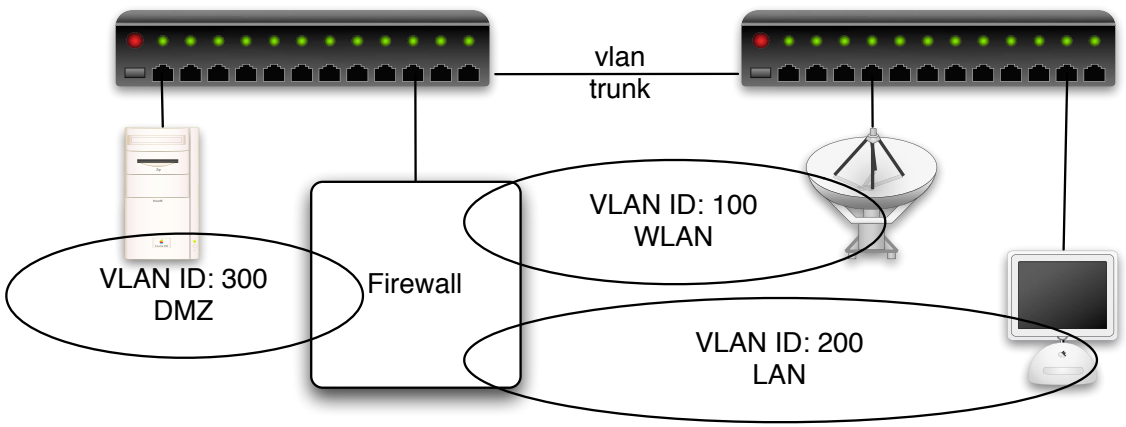
Managed switches often allow splitting into zones called virtual LANs

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

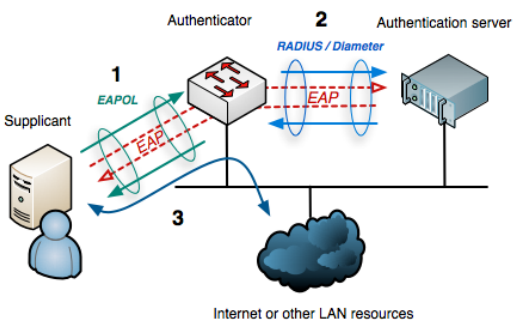
Virtual LAN, to pass from one to another, must use a router/firewall

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

Network Access Control – Connecting clients more securely

Talking about standard, another useful one:
IEEE 802.1x – Port Based Network Access Control



Authentication protocol ensures user validation before port access

Can authenticate using username and then password or certificate

Typically RADIUS and 802.1x which can use LDAP or Active Directory

Already used in Wi-Fi networks, so can be turned on for wired Ethernet ports

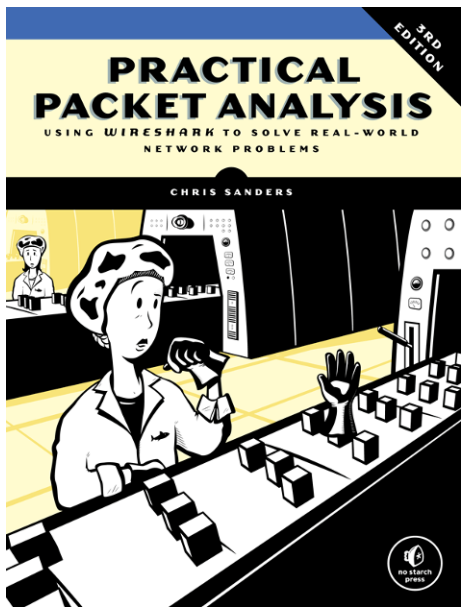
Network Protocol Knowledge Needed for Network Security

To work with network security the following protocols are the bare minimum to know about.

- ARP Address Resolution Protocol for IPv4
- NDP Neighbor Discovery Protocol for IPv6
- IPv4 & IPv6 – the basic packet fields source, destination,
- ICMPv4 & ICMPv6 Internet Control Message Protocol
- UDP User Datagram Protocol
- TCP Transmission Control Protocol
- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System

These protocols are part of the Internet Protocol suite, or TCP/IP for short. The canonical document describing this is from 1981 RFC-0791 **RFC0791**. The protocols were deployed on the internet around 1983.

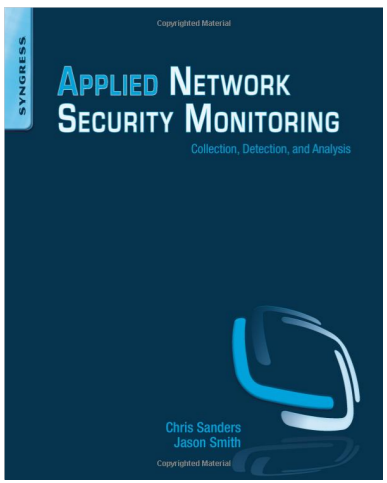
Book: Practical Packet Analysis (PPA)



Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition April 2017, 368 pp. ISBN-13: 978-1-59327-802-1

https://nostarch.com/packetanalysis3

Book: Applied Network Security Monitoring (ANSM)



Applied Network Security Monitoring: Collection, Detection, and Analysis 1st Edition

Chris Sanders, Jason Smith eBook ISBN: 9780124172166 Paperback ISBN: 9780124172081 496 pp. Imprint: Syngress, December 2013

Firewall configuration

Best firewall starts with the design

- Drawings – lots of drawings and topology
- An addressing plan! This is very important
- Then use a GUI for your first experience
- Plan for long term care
- Plan for updates
- Systems and services behind the firewall must still be hardened and configured securely

Block outgoing traffic too

Some services should *not* cross firewalls, at least not to the internet

Some services are too *fragile*

- Windows SMB file sharing is *only* for small internal networks
- Unix NFS is like-wise *only* for internal use
- Outgoing email should only go via dedicated relays
- LDAP outgoing, why?! See the log4j CVE-2021-44228
- Create a list, document them and consider them dead!

Making a positive list of allowed protocols would be best, but may require too many resources to implement and update

Proxy servers and Web Application Firewalls (WAF)

- Filtrering at higher layers is also possible
- Web proxies for clients can help security a lot – a centralized filter for everyone
- Reverse proxies for web applications are called Web Application Firewalls (WAF) – and filter incoming web requests, and outgoing answers. Can help with attacks like SQL injection and exfiltration of data
- Depending on your network it can replace or be combined with filtering on DNS servers, and I would prefer to filter domains with DNS
- I would also prefer blocking large prefixes of IP destinations using routers/stateless packet filters – maybe use BGP for distributing *lists*

Netflow and Session Logging

- Netflow is getting more important, more data share the same links
- Accounting is important
- Detecting DoS/DDoS and problems is essential
- Netflow sampling is vital information - 123Mbit, but what kind of traffic
- NFSen is an old but free application http://nfsen.sourceforge.net/
- Currently also investigating sFlow - hopefully more fine grained
- sFlow, short for "sampled flow", is an industry standard for packet export at Layer 2 of the OSI model, https://en.wikipedia.org/wiki/SFlow

Netflow is often from routers, we dont have any here

Collect Network Evidence from the network

Network Flows

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share the following 7 values:

- Ingress interface (SNMP ifIndex)
- IP protocol, Source IP address and Destination IP address
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

today Netflow version 9 or IPFIX

Source:

https://en.wikipedia.org/wiki/NetFlow

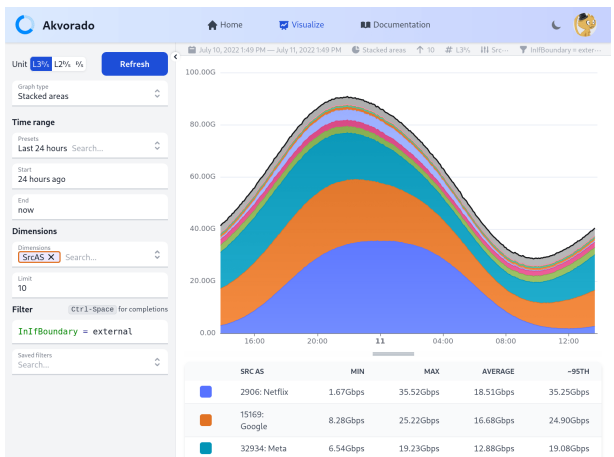
https://en.wikipedia.org/wiki/IP_Flow_Information_Export

ElastiFlow – Elasticsearch based

ElastiFlow™ provides network flow data collection and visualization using the Elastic Stack (Elasticsearch, Logstash and Kibana). It supports Netflow v5/v9, sFlow and IPFIX flow types (1.x versions support only Netflow v5/v9).

Source: Picture and text from https://github.com/robcowart/elastiflow

Akvorado: flow collector, enricher and visualizer



This program receives flows (currently Netflow/IPFIX and sFlow), enriches them with interface names (using SNMP), geo information (using IPinfo.io), and exports them to Kafka, then ClickHouse. It also exposes a web interface to browse the collected data.

Source: Picture and text from https://github.com/akvorado/akvorado

Who are you gonna call?

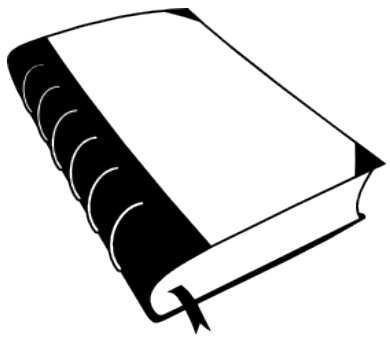
> Cyberangreb kan blive en dyr omgang for SMV'erne Et ransomware angreb koster 376.350 kr. alene i tabt omsætning fra e-handel for en virksomhed med 10-49 ansatte. I lyset af at truslen for cyberkriminalitet er på sit højeste, skal flere SMV'er have hjælp til at øge deres IT-sikkerhed. Særligt efter en hård tid under COVID-19, som har tvunget virksomhedernes 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 incident
- Expect an incident to cost at least 100.000DKK plus time, lost hours, lost orders, etc.

Primary Incident Response Literature

Primary literature:



Free graphics by Lumen Design Studio

- *Intelligence-Driven Incident Response*
  Scott Roberts. Rebekah Brown, ISBN: 9781098120689 **2nd edition**- short IDIR
- *Computer Security Incident Handling Guide*, NIST SP 800-61 Rev. 2, August 2012,
  https://doi.org/10.6028/NIST.SP.800-61r2 – also uploaded to Fronter
- *Forensics Discovery* (FD), Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages.
  ISBN: 9780201634976
  This book is currently available for "free":
  http://fish2.com/security/ – also uploaded to Fronter

These resources are used by me for the introduction to incident response courses, it all boils down to having data available to perform investigations!

Risk management defined

Information Risk Management

Life is full of risk.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. ***Information risk management (IRM)*** is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

Security Controls and Frameworks

Multiple exist

- CIS controls Center for Internet Security (CIS) https://www.cisecurity.org
- PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019
- NIST Cybersecurity Framework (CSF)
  Framework for Improving Critical Infrastructure Cybersecurity
  https://www.nist.gov/cyberframework
  https://csrc.nist.gov/publications/sp800 - SP800 series
- National Security Agency (NSA)
  https://www.nsa.gov/Research/
- NSA security configuration guides
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/
- Information Systems Audit and Control Association (ISACA)
  http://www.isaca.org/Knowledge-Center/

Center for Internet Security CIS Controls

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

The CIS ControlsTM are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

Source: https://www.cisecurity.org/ CIS-Controls-Version-7-1.pdf

SIEM

Security information and event management (SIEM) is a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes.[1]

The term and the initialism SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.[2]

Source: https://en.wikipedia.org/wiki/Security_information_and_event_management

- Note: there are alerting examples towards the bottom of the page, with sources
- Closely related to log management, incident response

SOC

An information security operations center (ISOC or SOC) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

...

A **security operations center (SOC)** can also be called a security defense center (SDC), security analytics center (SAC), network security operations center (NSOC),[3] security intelligence center, cyber security center, threat defense center, security intelligence and operations center (SIOC). In the Canadian Federal Government the term, infrastructure protection center (IPC), is used to describe a SOC.

Source: https://en.wikipedia.org/wiki/Information_security_operations_center

Incident Handling, phases

The procedures developed for incident response must cover the complete life-cycle

- Preparation for an attack, establish procedures and mechanisms for detecting and responding to attacks
- Identification of an attack, notice the attack is ongoing
- Containment (confinement) of the attack, limit effects of the attack as much as possible
- Eradication of the attack, stop attacker, block further similar attacks
- Recovery from the attack, restore system to a secure state
- Follow-up to the attack, include lessons learned improve environment

MITRE ATT&CK framework

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

Source: https://attack.mitre.org/ Great resource for attack categorization

Incident Response Checklists

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

This checklist is from the NIST document *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-61 Revision 2, August 2012.

CIS Controls also recommend Incident Response

CIS Control 19:

Incident Response and Management Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf from https://www.cisecurity.org/controls/

Anatomy of an Auditing System

Sample logs from login with Secure Shell (SSH) and performing the command `sudo su -`

```
Jun  5 11:53:15 pumba sshd[64505]: Accepted publickey for hlk from 79.142.233.18 port 43902
 ssh2: ED25519 SHA256:l8OJMcywyBcraJiCWJ06uZ2yzHfu0VuiArqVvlVyfEI

Jun  5 11:53:19 pumba sudo:      hlk : TTY=ttyp2 ; PWD=/home/hlk ; USER=root ; COMMAND=/usr/
```

Example systems: Unix syslog, IBM main frame RACF and Windows Event Logs service

Logs should be protected and considered confidential information

Anatomy of an Auditing System

When data has been gathered it should be analyzed.

Logger functions - collect

Analyzer - analyze it, creating dashboard can provide some insights

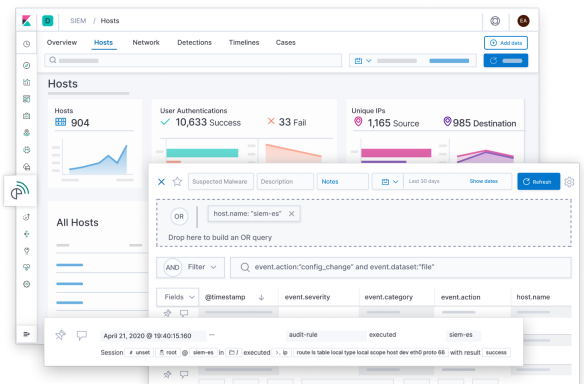
Notifier - report results by email or other means

Example systems Windows Event Logs service can inform of successful and failed logins, both should be collected

Logs should be protected and considered confidential information, by sending it to a centralized system with a high security level protects it

Modern systems exist to take all data from logging and provide high capacity storage, searching and sorting.

Why Elasticsearch



Screenshot from https://www.elastic.co/siem

Recommend building a proof-of-concept infrastructure using the Elastic stack and gather experience with logging. This can be done without a license fee and the organization can then see what works and doesn't. Then using the experiences as input an informed decision can be made, to continue with this as a home grown logging and auditing solution, or buy a premade one.

Sources: Strategy for implementing identification and detection

We recommend that the following strategy is used for implementing identification and detection – logging:

- ☐ Enable system logging from servers
- ☐ Enable system logging from network devices
- ☐ Enable logging from client devices
- ☐ Centralize logging
- ☐ Add search facilities and dashboards
- ☐ Perform system audits manually or automatically
- ☐ Setup alerting and notification with procedures

Intrusion Kill Chains

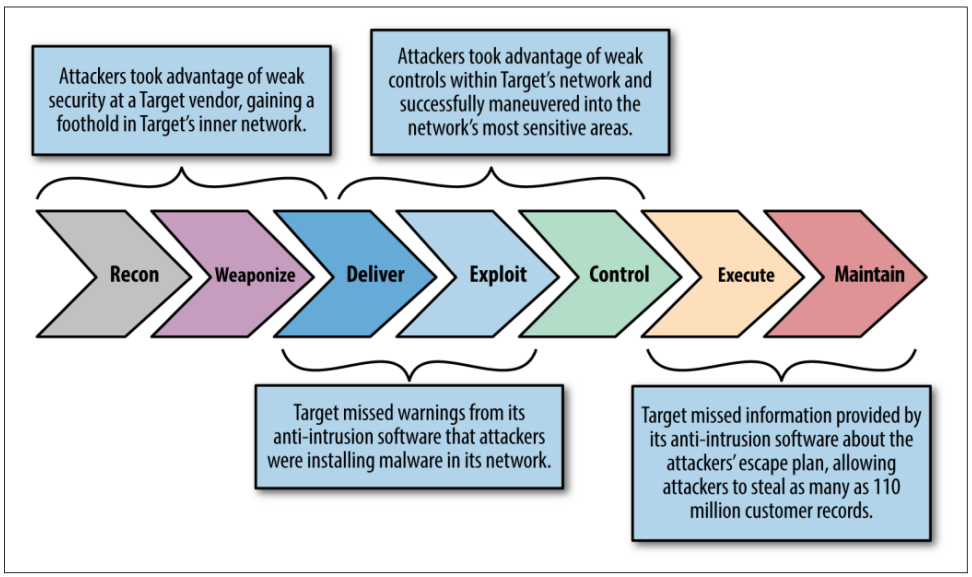


Figure 7-1. The kill chain

- See also *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corporation

  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Detection Capabilities

Security incidents happen, but what happens. One of the actions to reduce impact of incidents are done in preparing for incidents.

> *Preparation* for an attack, establish procedures and mechanisms for detecting and responding to attacks

Preparation will enable easy **identification** of affected systems, better **containment** which systems are likely to be infected, **eradication** what happened – how to do the **eradication** and **recovery**.

Data Analysis Skills

Although we could spend an entire book creating an exhaustive list of skills needed to be a good security data scientist, this chapter covers the following skills/domains that a data scientist will benefit from knowing within information security:

- Domain expertise—Setting and maintaining a purpose to the analysis
- Data management—Being able to prepare, store, and maintain data
- Programming—The glue that connects data to analysis
- Statistics—To learn from the data
- Visualization—Communicating the results effectively

It might be easy to label any one of these skills as the most important, but in reality, the whole is greater than the sum of its parts. Each of these contributes a significant and important piece to the workings of security data science.

Source: *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis
ISBN: 978-1-118-79372-5 February 2014 https://datadrivensecurity.info/ - short DDS

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

The Zeek Network Security Monitor

Together with firewalls – The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework

The Zeek Network Security Monitor

> While focusing on network security monitoring, Zeek provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Zeek has successfully bridged the traditional gap between academia and operations since its inception.

Zeek is the tool formerly known as Bro, changed name in 2018. https://www.zeek.org/

Suricata IDS/IPS/NSM

Together with firewalls – Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

http://suricata-ids.org/ http://openinfosecfoundation.org

Workshop materials available:

https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop

Mutually Agreed Norms for Routing Security (MANRS)

> Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

Source: https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf

- Problems related to incorrect routing information
- Problems related to traffic with spoofed source IP addresses
- Problems related to coordination and collaboration between network operators
- Also BCP38 RFC2827 *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

You should all ask your internet providers if they know about MANRS, and follow it. We should ask our government and institutions to support and follow MANRS and good practices for network on the Internet

Routing Security

- Use MD5 passwords or better authentication for routing protocols 🚩
- TTL Security – avoid routed packets
- Max prefix – of course, only allow expected networks
- Prefix filtering – only parts of IPv6 space is used
- TCP Authentication Option [RFC 5925] replaces TCP MD5 [RFC 2385]
- Turn ON RPKI for both IPv4 and IPv6 prefixes, 🚩
  https://nlnetlabs.nl/projects/rpki/about/
- Drop bogons on IPv4 and IPv6, article with multiple references YMMV
  https://theinternetprotocolblog.wordpress.com/2020/01/15/some-notes-on-ipv6-bogon-filtering/