Welcome to

Attack and Defense

2022

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

Slides are available as PDF, kramse@Github

attack-and-defense.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: hkj@zencurity.dk Mobile: +45 2026 6000

You are welcome to drop me an email

Time schedule

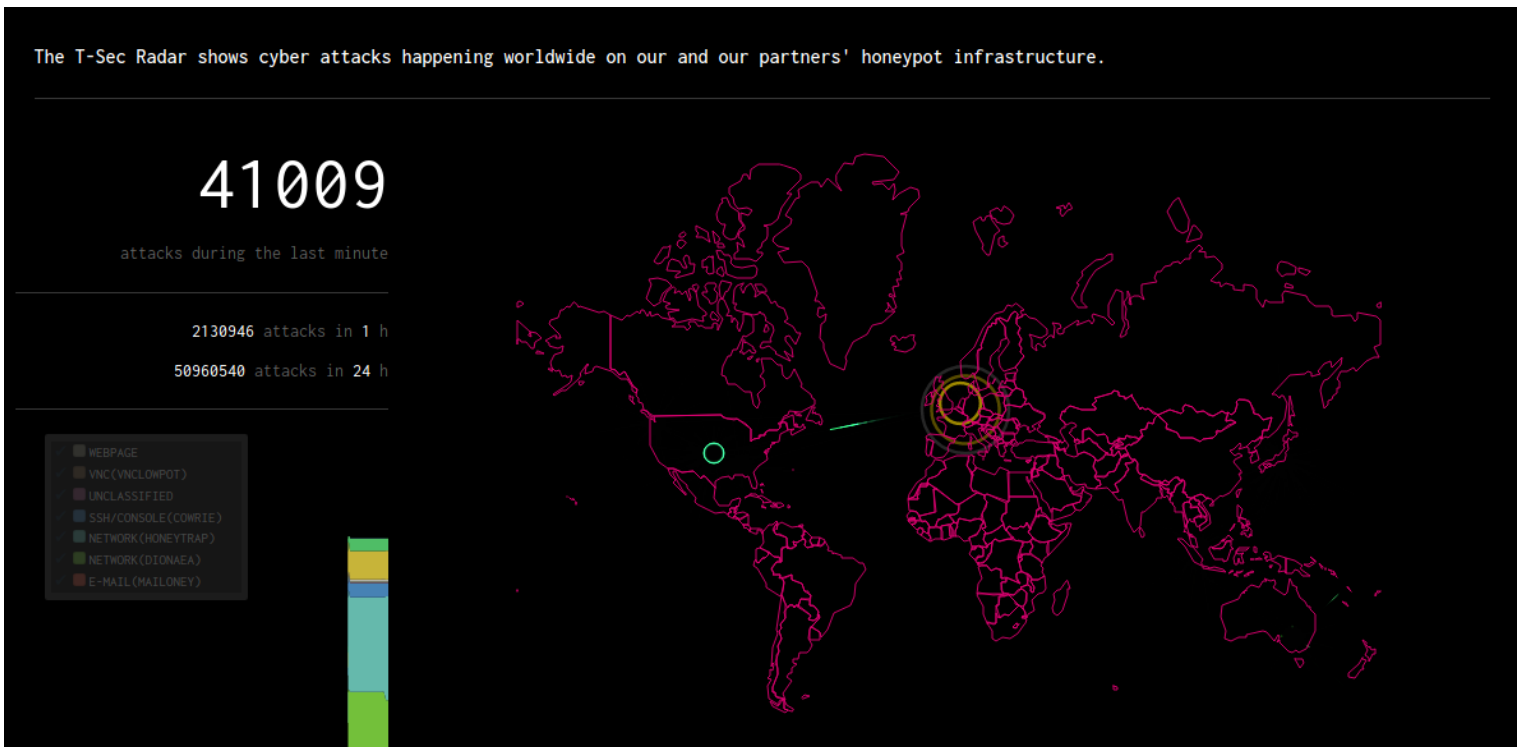
17:00 - 21:00 including breaks

- 17:00 - 18:15
  Introduction to Security problems and basics
- 30min break
  Go eat with your family, hang around, get coffee
- 18:45 - 19:30 45min
  Strategies for long-lasting protection in IT-security
- 15min break

- 19:45 -20:30 45min
  More strategies for long-lasting protection in IT-security and Summary
- 20:30 - 21:00 Roundtable – open discussion, share your experience

Most slides are in english, some in Danish! Sorry

Introduction: Attack overview



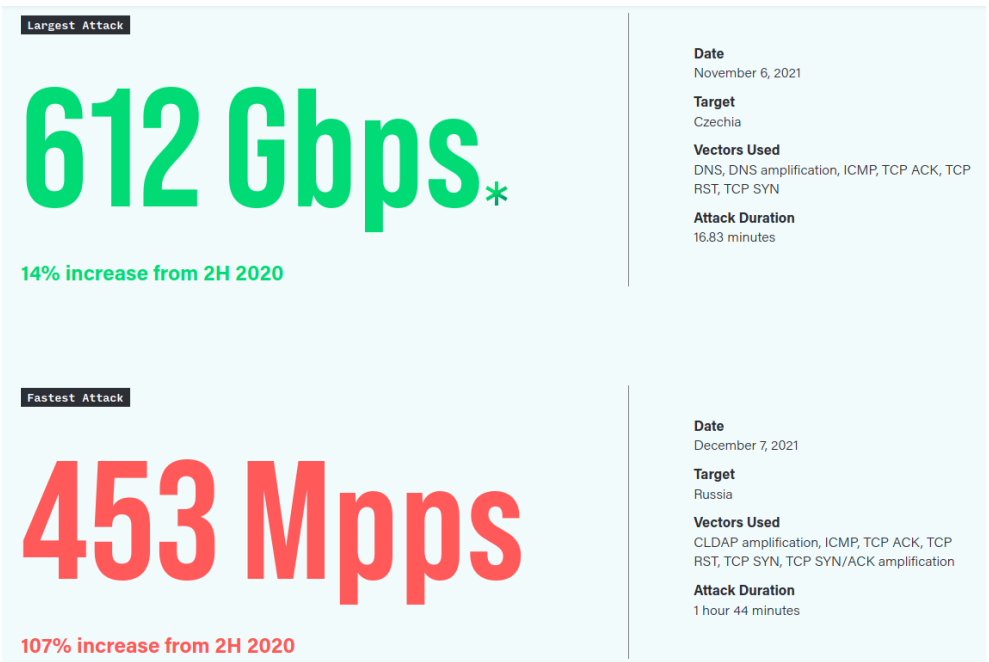
Source: http://www.sicherheitstacho.eu/

DDoS Attacks Still a Problem

Security attacks and DDoS is very much in the media

Source: linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/

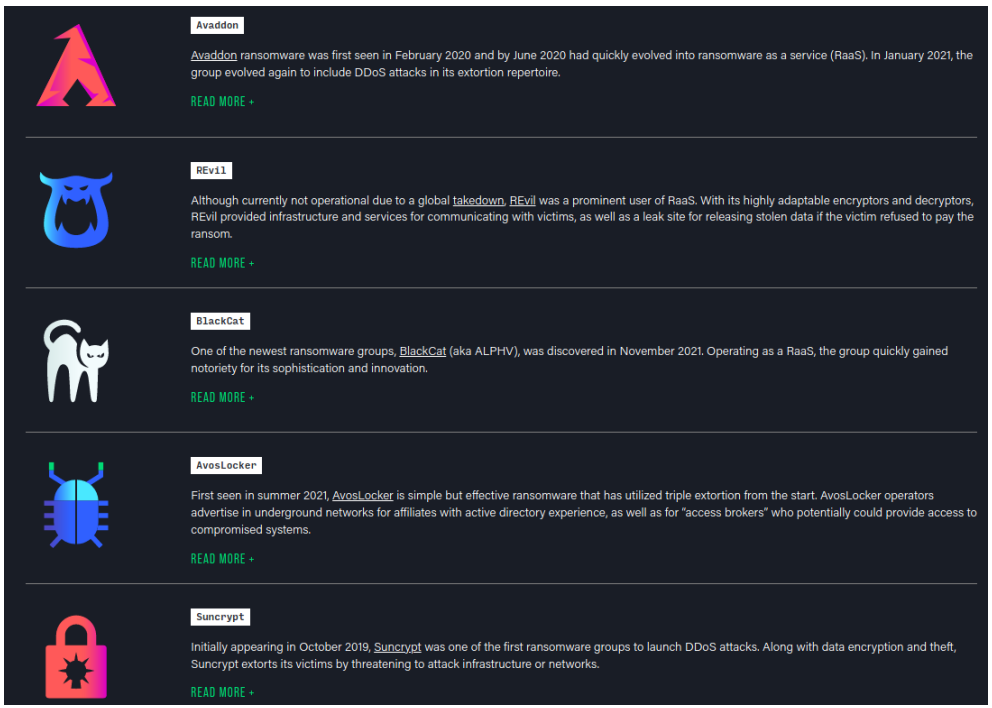
DDoS Attacks are HUGE



Extremely hard to protect against from a small network

Source: linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/

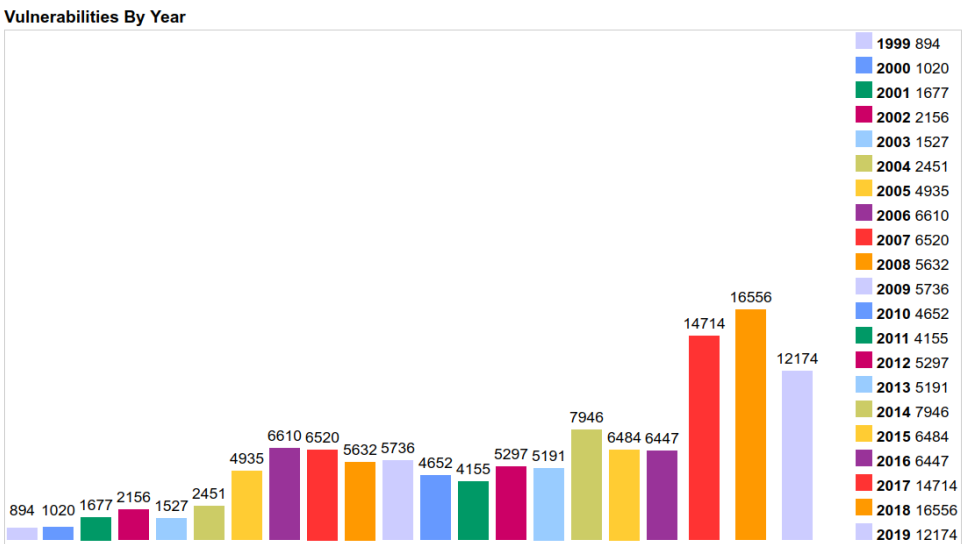
Ransomware Attacks are Common



Make sure to backup your data! Test your backups!

Source: linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/

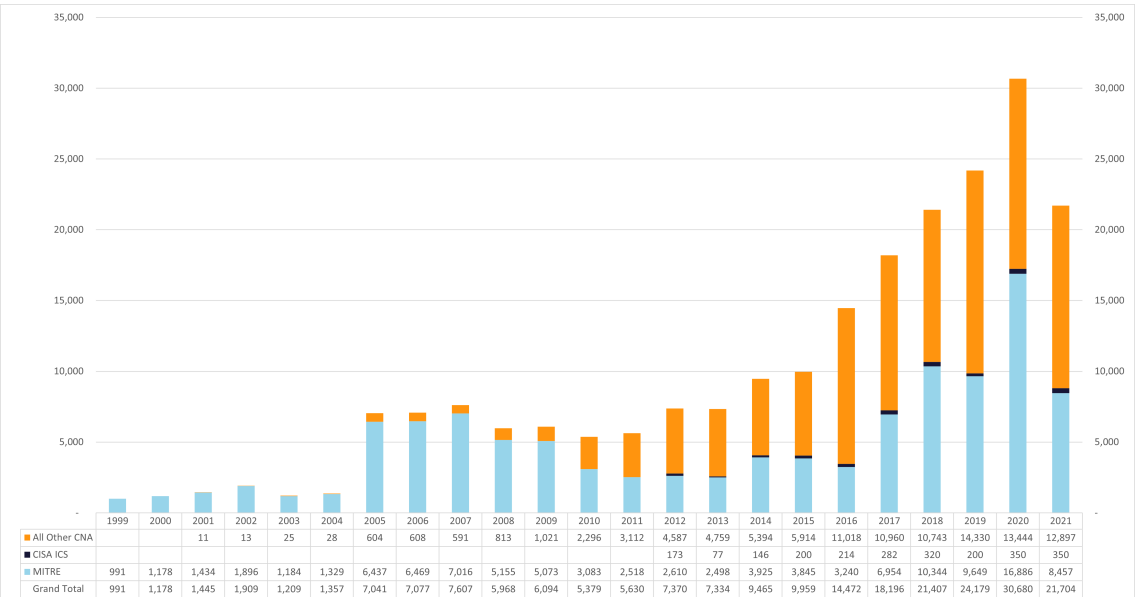
MITRE – Common Vulnerabilities and Exposure (CVE)



The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

20 years and one of the most critical projects for internet and information security, in my opinion

OMG CVE



	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
All Other CNA			11	13	25	28	604	608	591	813	1,021	2,296	3,112	4,587	4,759	5,394	5,914	11,018	10,960	10,743	14,330	13,444	12,897
CISA ICS														173	77	146	200	214	282	320	200	350	350
MITRE	991	1,178	1,434	1,896	1,184	1,329	6,437	6,469	7,016	5,155	5,073	3,083	2,518	2,610	2,498	3,925	3,845	3,240	6,954	10,344	9,649	16,886	8,457
Grand Total	991	1,178	1,445	1,909	1,209	1,357	7,041	7,077	7,607	5,968	6,094	5,379	5,630	7,370	7,334	9,465	9,959	14,472	18,196	21,407	24,179	30,680	21,704

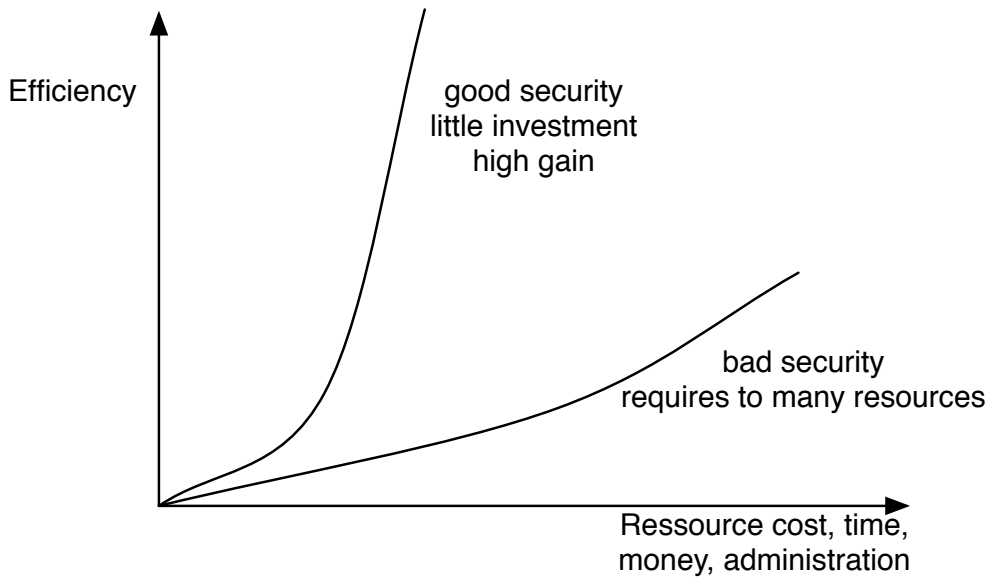
Source: https://www.cve.org/Media/News/item/blog/2021/11/16/CVE-Program-Report-for-Q3

- How many can you handle per day? How many are relevant for your organisation?

Konklusion: IT-sikkerhed og IT-drift er præget af kaos og panik

- Vi starter godt, struktureret arbejde!
- Vi bliver afbrudt ... og det sker tit
- Vi bliver ikke færdige! Det bliver man sjældent i virkeligheden
- Microsoft alene frigiver opdateringer for mere end 100 sårbarheder om måneden
- Al software har sikkerhedsproblemer, og skal opdateres!

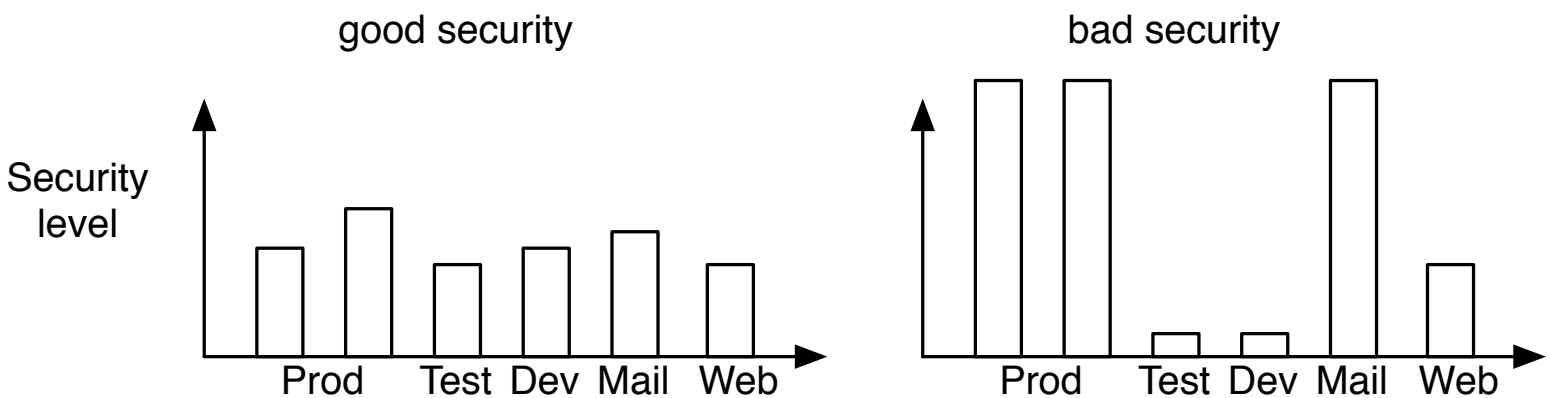
What can we do? – Good security



You always have limited resources for protection - use them as best as possible

Good security comes from structured work

Balanced security



Better to have the same level of security

If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security

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

Risk management defined

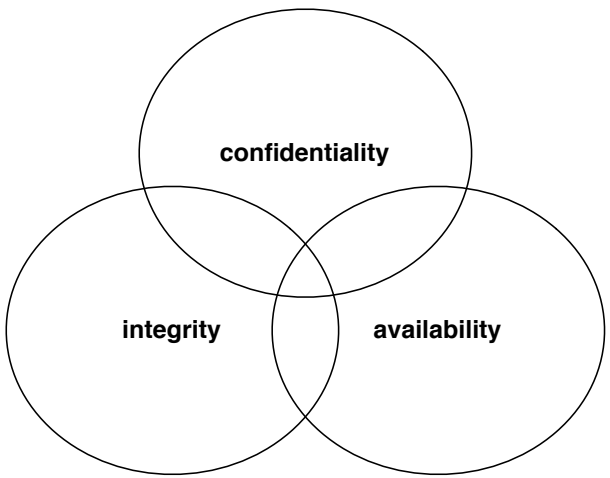
Information Risk Management

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*

Confidentiality, Integrity and Availability



We want to protect something

Confidentiality - data kept a secret

Integrity - data is not subjected to unauthorized changes

Availability - data and systems are available when needed

Security is a process

Remember:

- what is information and security?
- Data kept electronically
- Data kept in physical form
- Dont forget the human element of security

Incident Response and Computer Forensics reaction to incidents

Good security is the result of planning and long-term work

Security is a process, not a product, Bruce Schneier

Source for quote: https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

Security Controls and Frameworks

Multiple exist – only subset listed below

- 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

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

Note: The CIS Controls were developed starting in 2008

Kom igang med CIS

CIS-kontrollerne består af 20 praktiske, pragmatiske kontroller, som er målbare og med direkte henvisning til, hvordan de implementeres samt forslag til, hvilke KPI'er der bør opstilles for målinger.

Forskellen på CIS-kontrollerne og fx ISO27001 er, at du ikke kan blive certificeret efter CIS, men til gengæld opdateres CIS-kontrollerne løbende, og de indeholder prioriterede lister af, hvad du i praksis skal gøre for din cybersikkerhed. Det australske forsvar har fx vist, at hvis man implementerer de første fire kontroller fuldt ud, kan man mitigere op mod 90+% af alt malware.

Dansk artikel fra Deloitte, version 7 indeholder 20 kontroller men version 8 med 18 kontroller
https://www2.deloitte.com/dk/da/pages/risk/articles/vi-stiller-skarpt-pa-cis-kontroller.html

Basic Security Controls

CIS controls 1-6 are Basic, everyone must do them. Today I have replaced 6 with 10.

- **CIS Control 1: Inventory and Control of Hardware Assets**
- **CIS Control 2: Inventory and Control of Software Assets**
- **CIS Control 3: Continuous Vulnerability Management**
- **CIS Control 4: Controlled Use of Administrative Privileges**
- **CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**
- **CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs**
- **CIS Control 10: Data Recovery Capabilities**

Inventory and Control of Hardware Assets

CIS Control 1:
Inventory and Control of Hardware Assets
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

What is connected to our networks?

What firmware do we need to install on hardware?

Where IS the hardware we own?

What hardware is still supported by vendor?

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Inventory and Control of Software Assets

CIS Control 2:
Inventory and Control of Software Assets
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

What licenses do we have? Paying too much?

What versions of software do we depend on?

What software needs to be phased out, upgraded?

What software do our employees need to support?

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Continuous Vulnerability Management

CIS Control 3:
Continuous Vulnerability Management
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Scan for updates automatically

Update when vendors publish critical patches

Listen to news sources about software and vulnerabilities

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Controlled Use of Administrative Privileges

CIS Control 4:
Controlled Use of Administrative Privileges
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Remove local administrator from Windows workstations

Change default passwords

Use good passwords

Log if somebody tries to break in

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Secure Configuration for Hardware and Software

CIS Control 5:
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Create secure configuration – check security settings

Select security mechanisms

Automate security settings

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Maintenance, Monitoring and Analysis of Audit Logs

CIS Control 6:
Maintenance, Monitoring and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

... and present it, use it daily, report it to management!

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Data Recovery Capabilities

CIS Control 10:
Data Recovery Capabilities
The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it

Backup is critical

If we loose orders we loose money

Data loss, means production capacity loss

Separation of duty – can one person delete both production and backup

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

How do we get started?

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

- Get management support – without it, don't bother, get a new job, avoid the stress
- Create goals and plans
- Aquire the skills
- Follow the plan, let some servers burn, shut them down if you are doing something more important
- My suggestion is to start with the network, since it supports everything else

And, I mean it seriously, without management support, eject and go somewhere else!

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

Prerequisites for network security

Network security and most internet related security work has the following requirements:

- Network experience
- TCP/IP principles - often in more detail than a common user
- Programming is an advantage, for automating things
- Some Linux and Unix knowledge is in my opinion a **necessary skill** for infosec work
  – too many new tools to ignore, and lots found at sites like Github and Open Source written for Linux

IF you have some basic Linux skills you can immediately use 1.000s of existing projects like: Ansible, Git, Suricata, Zeek, Nmap, logging solutions, LibreNMS, maltrail, packetbeat, Elastic ECS, ...

They WILL make your work more efficient

Aquire Skills – books are one example

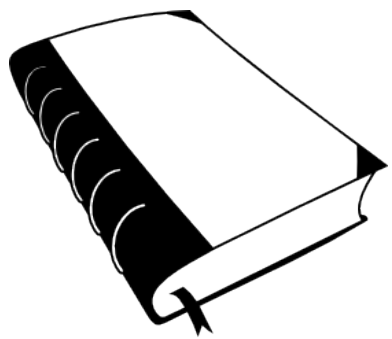
Recommended literature from my system security and communication and network security course::

- *Defensive Security Handbook: Best Practices for Securing Infrastructure*, Lee Brotherston, Amanda Berlin ISBN: 978-1-491-96038-7 284 pages
- *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
- *Forensics Discovery*, Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages. Can be found at http://www.porcupine.org/forensics/forensic-discovery/
- *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

All lecture plans for my courses are freely available at: https://github.com/kramse/kea-it-sikkerhed

Primary literature for SIEM and Logging course

Primary literature:

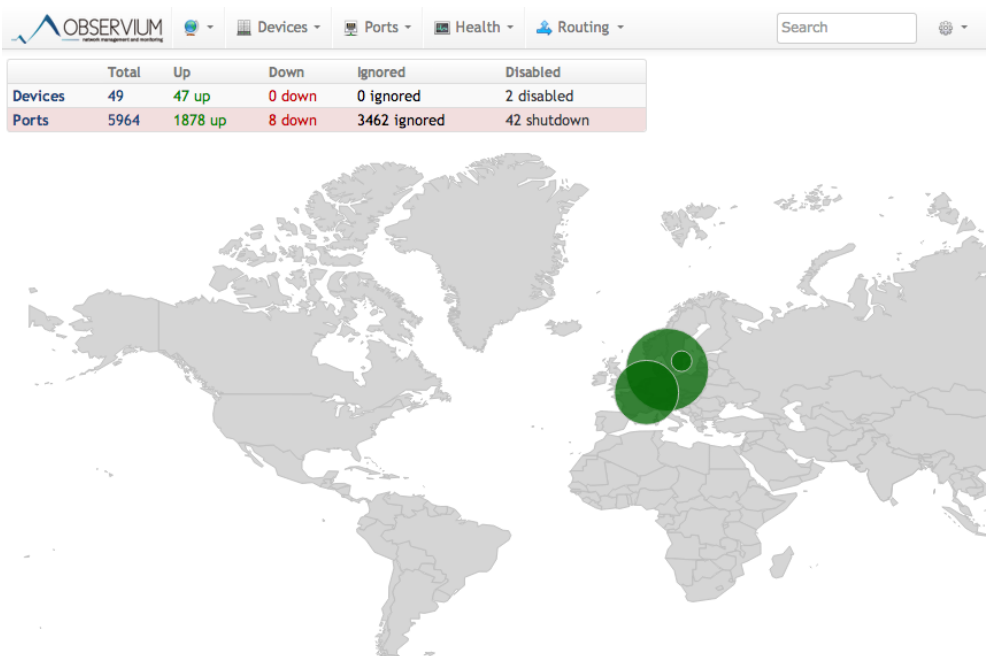


Free graphics by Lumen Design Studio

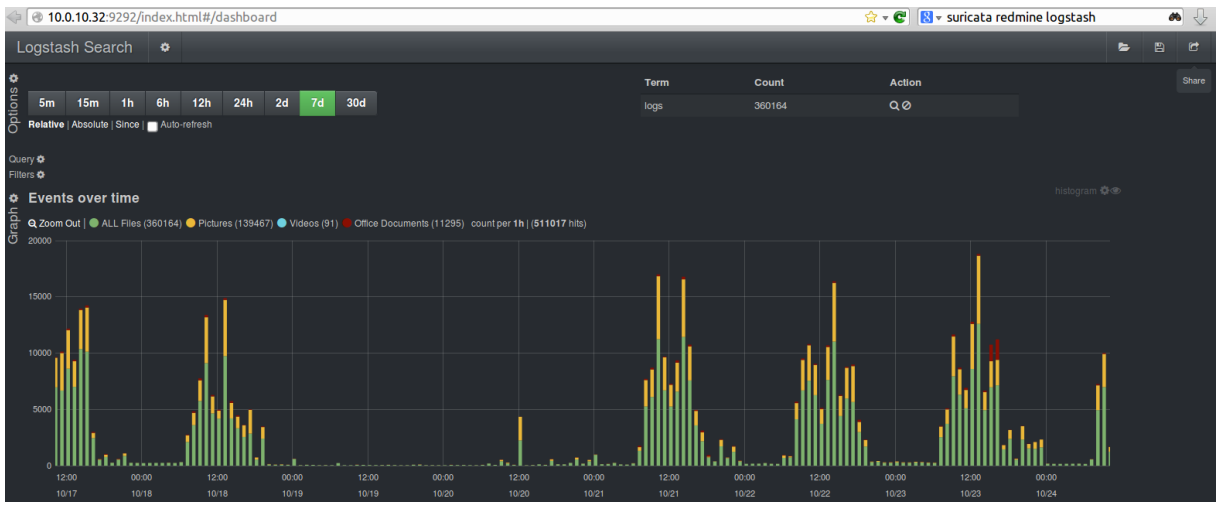
- *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis ISBN: 978-1-118-79372-5 February 2014 https://datadrivensecurity.info/ - short DDS
- *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan* by Jeff Bollinger, Brandon Enright, and Matthew Valites ISBN: 9781491949405 - short CIP
- *Intelligence-Driven Incident Response* Scott Roberts ISBN: 9781491934944 - short IDI
- *Security Operations Center: Building, Operating, and Maintaining your SOC* ISBN: 9780134052014 Joseph Muniz - short SOC

All lecture plans for my courses are freely available at: https://github.com/kramse/kea-it-sikkerhed

Goals: Gain insight using Graphs and Dashboards!

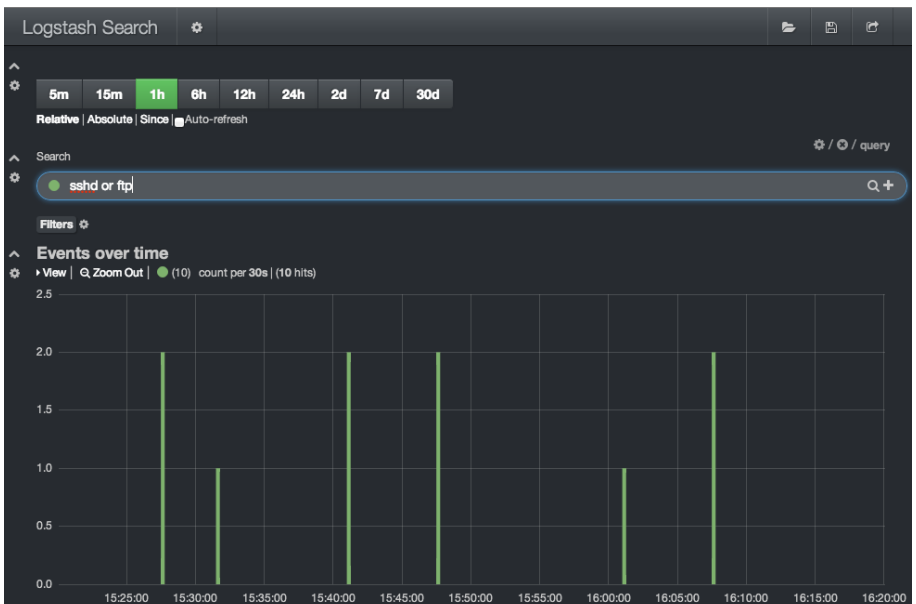


Graphs and Dashboards!



- Screenshot from Peter Manev, OISF
- Shown are Suricata IDS alerts processed by Logstash and Kibana

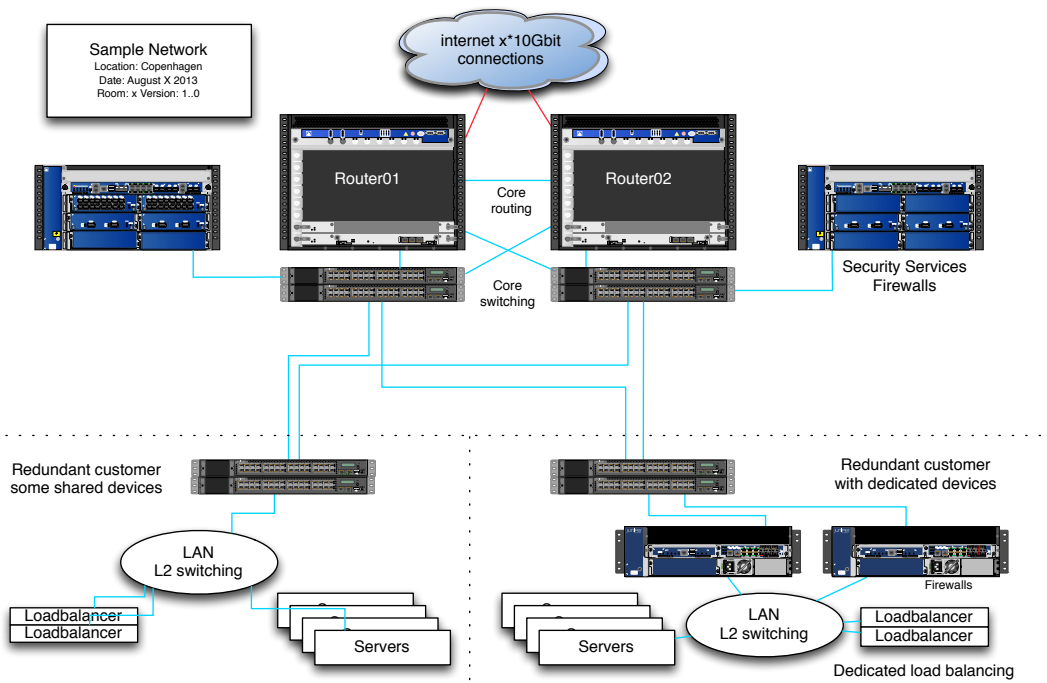
View data efficiently



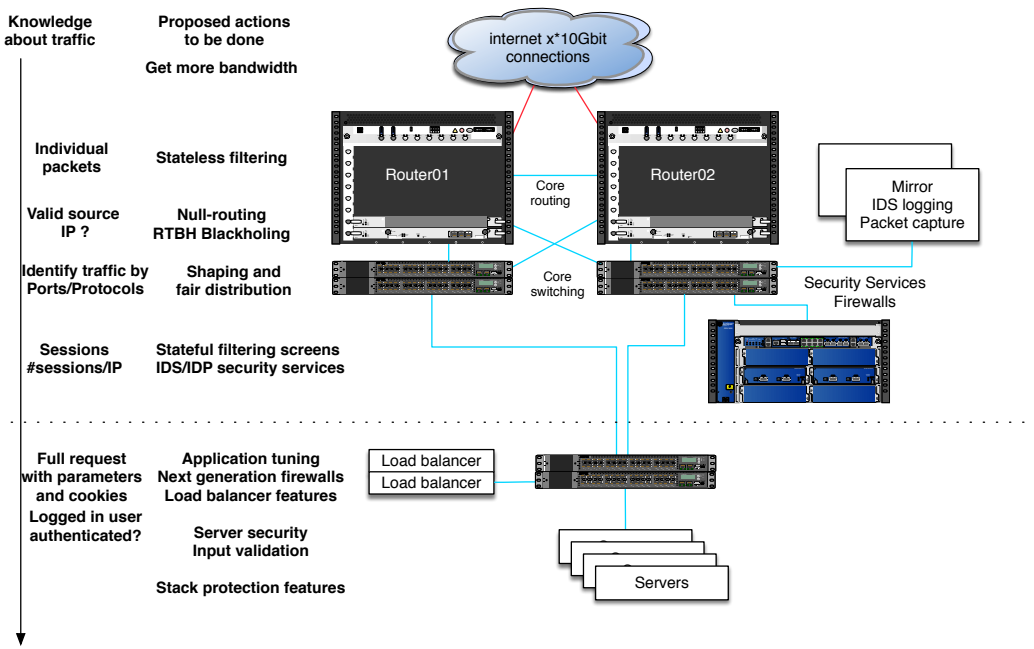
View data by digging into it easily - must be fast

Logstash and Kibana are just examples, but use indexing to make it fast!

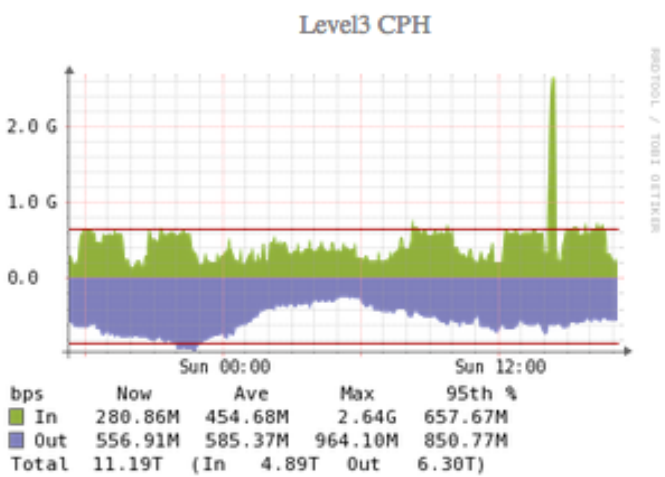
Networks today

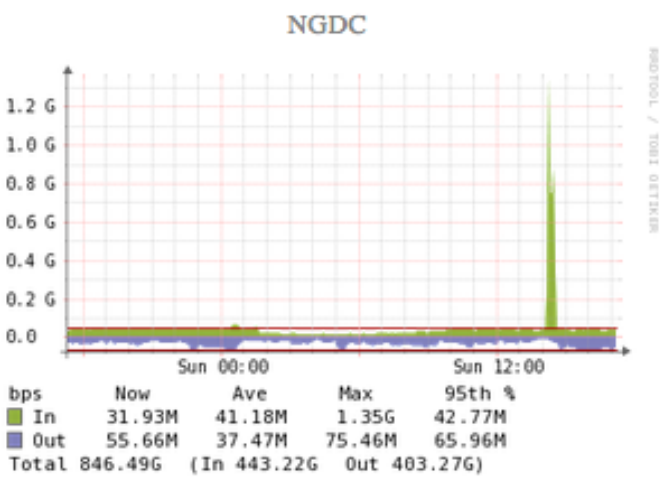


Defense in depth - multiple layers of security



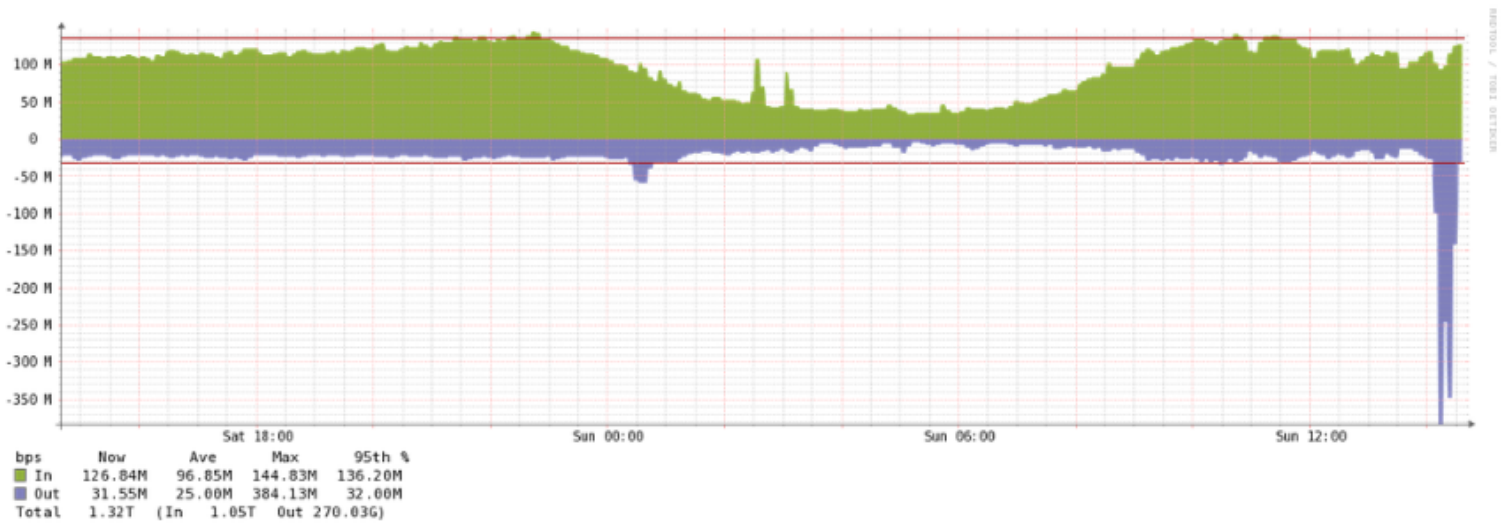
DDoS traffic before filtering





Only two links shown, at least 3Gbit incoming for this single IP

DDoS traffic after filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

Knowing what it going on, is half the battle

How to get started

How to get started searching for security events?

Collect basic data from your devices and networks

- Netflow data from routers
- Session data from firewalls
- Logging from applications: email, web, proxy systems

Centralize!

Process data

- Top 10: interesting due to high frequency, occurs often, brute-force attacks
- *ignore*
- Bottom 10: least-frequent messages are interesting

Sounds easy, but is complex in practice

Collect Network Evidence from the network

Network Flows introduced by Cisco around 1996

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

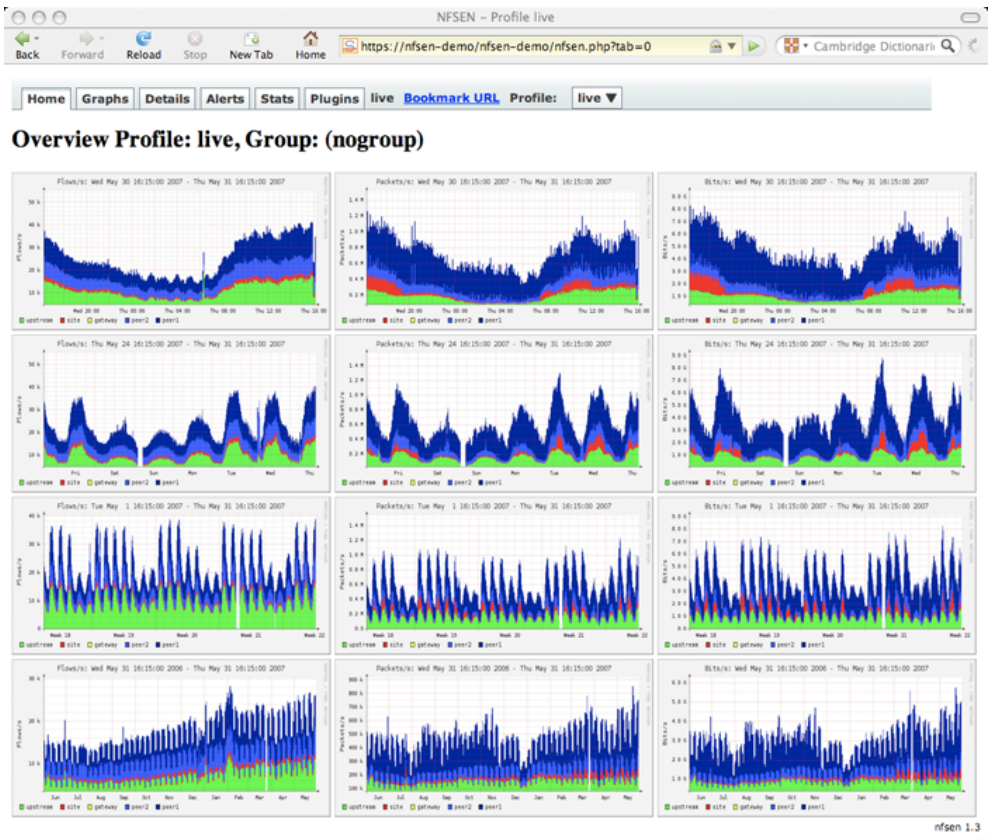
Netflow

- 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

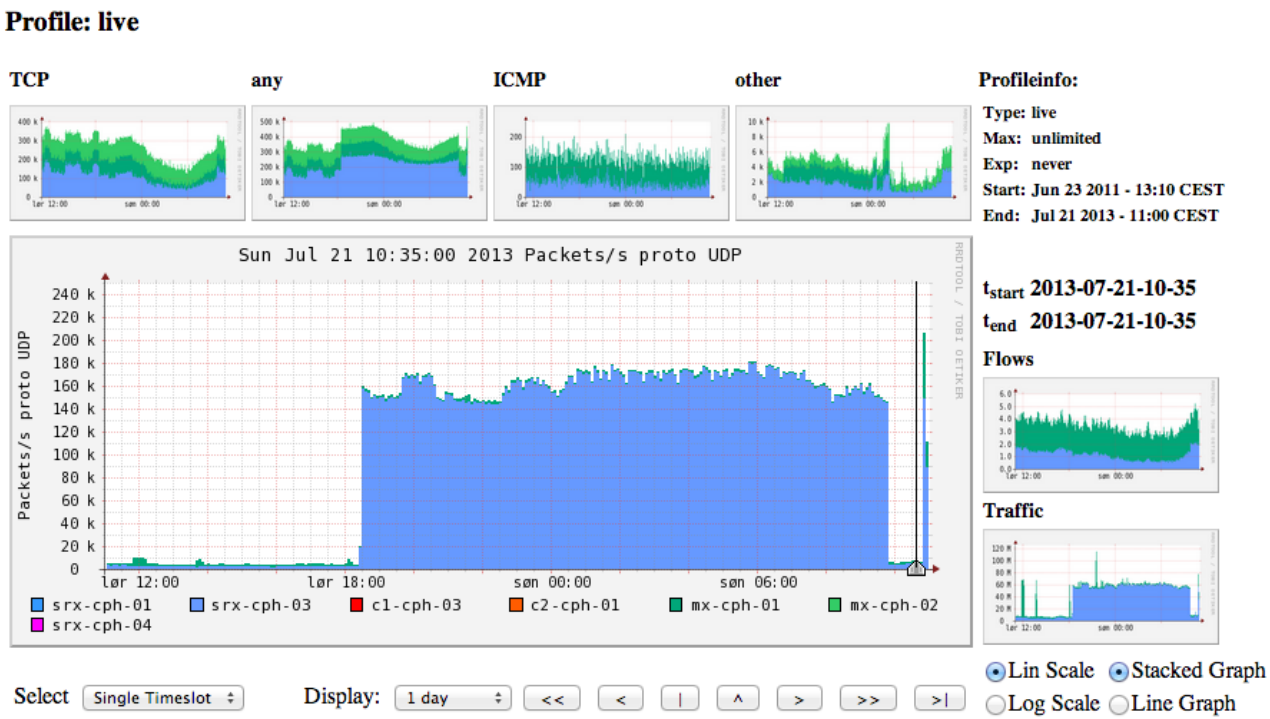
Netflow is often from routers, we dont have any here

Also look into Elastiflow! https://github.com/robcowart/elastiflow

Netflow using NFSen

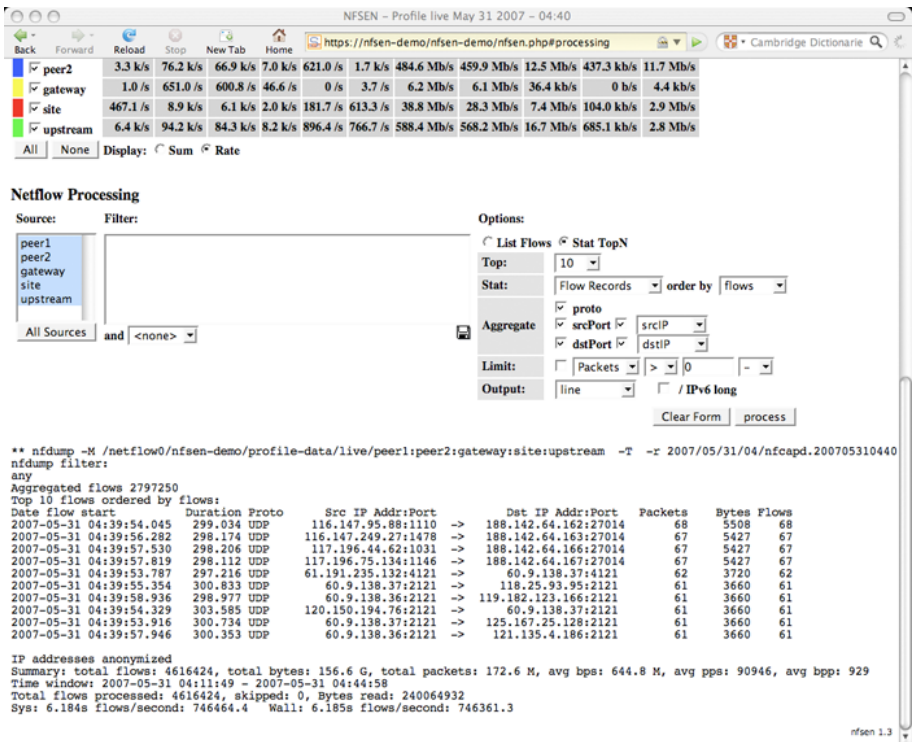


Netflow NFSen



An extra 100k packets per second from this netflow source (source is a router)

Netflow processing from the web interface



Bringing the power of the command line forward

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

Hændelseslog og Økonomi

Tag et stykke papir eller en computer

- Vi er lige blevet afbrudt i vores vigtige arbejde med CIS kontroller
- Vi skal udfylde en Hændelseslog og der er nogle økonomiske aspekter
- Når der sker en sikkerhedshændelse skal den helst håndteres effektivt
- Hvis man ikke har sikkerhedsprocedurer på plads bliver det typisk længerevarende og dyrere

Det er en erkendelse i sig selv at vi skal være klar til at håndtere sikkerhedshændelser, for de kommer

March 2021: ProxyLogon/ProxyShell CVE-2021-26855 CVSS:3.0 9.1 / 8.4

In March 2021, both Microsoft and IT Professionals had a major headache in the form of an Exchange zero-day commonly known as ProxyLogon. The vulnerability, widely considered the **most critical to ever hit Microsoft Exchange**, was quickly exploited in the wild by suspected state-sponsored threat actors, with US government and military systems identified as the most targeted sectors. **Ransomware variants such as DoejoCrypt were soon actively exploiting unpatched Exchange instances**, attempting to monetise the vulnerability.

A follow-up exploit, dubbed ProxyShell, was evolutionary in nature and targeted on-premise Client Access Servers (CAS) in **all supported versions of Exchange Server.** Due to the **remotely accessible nature of Exchange CAS, any unpatched instances would be vulnerable to Remote Code Execution. High profile victims included the European Banking Authority and the Norwegian Parliament.**

Source - for this description:
https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/

ProxyLogon CVE-2021-26855 CVSS:3.0 9.1 / 8.4

ProxyLogon is the formally generic name for CVE-2021-26855, a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin. We have also chained this bug with another post-auth arbitrary-file-write vulnerability, CVE-2021-27065, to get code execution. All affected components are vulnerable by default!

As a result, **an unauthenticated attacker can execute arbitrary commands on Microsoft Exchange Server through an only opened 443 port!**

Sources: https://proxylogon.com/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

Incident Handling: ProxyLogon

Hvis jeres organisation har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Marts Proxylogin - nem oprydning, ingen nedetid
- Økonomi: Marts Proxylogin oprydning EUR 3.000

Hvis jeres organisation *IKKE* har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Marts Proxylogin – mailservere inficeret 3 steder, ekstern hjælp nødvendig, nedetid 2 dage
- Økonomi: Marts Proxylogin oprydning EUR 3.000
- Økonomi: Marts ProxyLogon hændelseshåndtering ekstern hjælp EUR 10.000

June 2021: PrintNightmare CVE-2021-34527 CVSS:3.0 8.8 / 8.2

In June, Microsoft released a critical security update to address weaknesses in the Printer Spooler service on Windows desktop and server platforms. Unfortunately, it was released out-of-band outside of the standard patch Tuesdays due to the severity. Microsoft even released patches for Windows 7, an supported operating system that does not normally receive updates.

Initially categorised by Microsoft as a local privilege escalation on Windows, security researchers subsequently identified an additional **Remote Code Execution (RCE)** vector resulting in an updated advisory from Microsoft. As ever, the ability to test and deploy patches in a time-sensitive manner is key to minimising the impact of such vulnerabilities.

Additionally, PrintNightmare had the additional horror factor of dropping during the **summer holiday season in the northern hemisphere**. Our consultants continue to see systems vulnerable to PrintNightmare on client engagements, which can be trivially leveraged to obtain privilege escalation on unpatched Windows systems.

Source - for this description:
https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/

See also https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Incident Handling: PrintNightmare

Hvis jeres organisation har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Juni PrintNightmare - nem oprydning, ingen nedetid
- Økonomi: Juni PrintNightmare oprydning EUR 3.000

Hvis jeres organisation *IKKE* har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Juni PrintNightmare – servere inficeret, geninstallation nødvendig, nedetid 3 dage
- Økonomi: Juni PrintNightmare oprydning EUR 3.000
- Økonomi: Juni PrintNightmare hændelseshåndtering ekstern hjælp EUR 10.000

Da denne skete i ferien er der desværre også brugt mere tid på at håndtere sagen, alle sætter ekstra EUR 3.000 på listen med teksten "Grundet ferie og manglende ressourcer 3.000"

November 2021: Log4Shell

It would not be possible to discuss 2021 in the context of vulnerabilities without the mention of Log4Shell. **A widely used Java-based logging library caused headaches for Security professionals worldwide**. Many scrambled to quantify their use of Log4j within their estates.

A zero-day exploit quickly followed, confirming the worst - **Remote Code Execution (RCE) was indeed possible.** However, what made the nature of the vulnerability even more challenging was the ability to exploit a backend logging system from an unaffected front end host. For example, an attacker can craft a weaponised log entry on a mobile app or webserver not running Log4j. The attacker could make their way through to backend middleware itself running Log4j, which significantly extends the attack surface of the vulnerability.

The NCSC even took the step of recommending the update was immediately applied, whether or not Log4Shell was known to be in use. As is commonly the case with critical vulnerabilities, two successive Log4j patches were subsequently released in the week following the original addressing Denial of Service (DoS) and a further RCE. This further increased workloads of Security and IT teams just as they thought the worst of 2021 had been and gone.

Source - for this description:
https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/

See also https://en.wikipedia.org/wiki/Log4Shell

Incident Handling: Log4Shell

Hvis jeres organisation har implementeret CIS Control 1+2 og ingen Java har, noter følgende:

- Hændelseslog: November Log4Shell - nem oprydning, ingen nedetid
- Økonomi: November Log4Shell oprydning EUR 3.000

Hvis jeres organisation *IKKE* har implementeret CIS kontroller, noter følgende:

- Hændelseslog: November Log4Shell – mailservere inficeret 3 steder, ekstern hjælp nødvendig, nedetid 2 dage
- Økonomi: November Log4Shell oprydning EUR 3.000
- Økonomi: November Log4Shell hændelseshåndtering ekstern hjælp EUR 10.000

Hvis jeres organisation har et stort netværk uden segmentering og filtrering:
afsæt EUR 100.000 til fremtidige sikkerhedsproblemer nu

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/

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.

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

Ransomware

Defition 23-21 *Ransomware* is malware that inhibits the use of resources until a ransom usually monetary, is paid.

Book mentions 1989 example, PC CYBORG targetting PC/DOS computers

Uses cryptography to render data unreadable

Has become a huge problem for enterprises during the last 5-10 years

Often uses crypto-currencies today, like BitCoin (BTC) for payment

Often contains errors so decryption is impossible, or possible without payment!

Source: *Computer Security: Art and Science*, Matt Bishop ISBN: 9780321712332

https://www.pearson.com/us/higher-education/program/Bishop-Computer-Security-2nd-Edition/PGM25107.html

MITRE ATT&CK framework

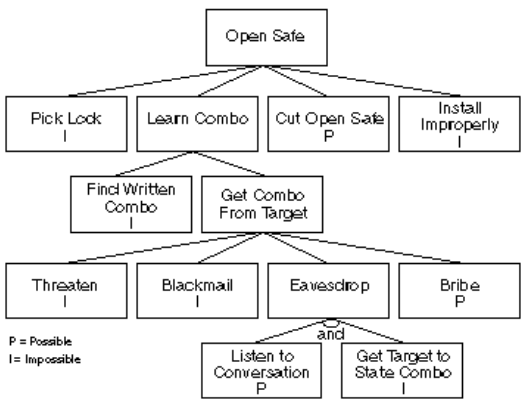
MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity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

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

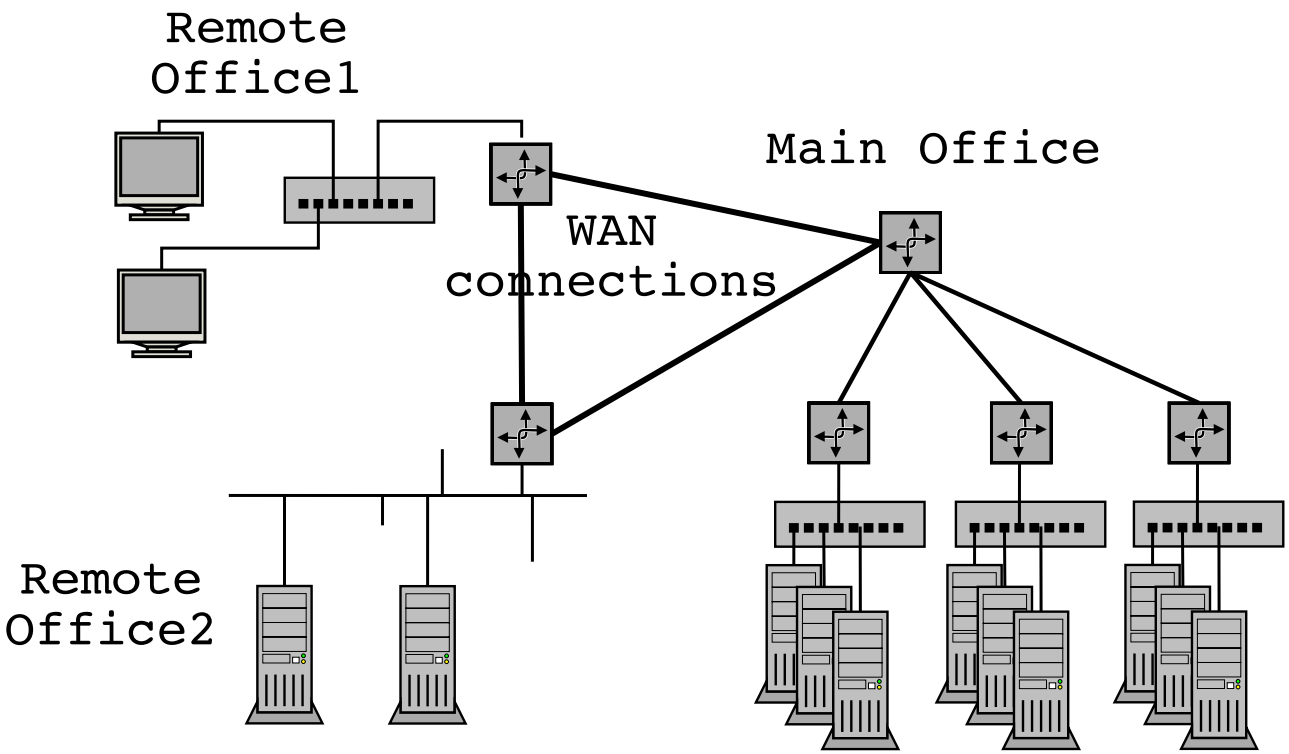
Attack trees



- Attacks can be said to be based on a chain of dependencies, or graphs
- To achieve goal, need to achieve sub goal x, y, and z – Break the chain and the attack fails!
- Simple example, installing updates remove a dependency for a vulnerability
- Attack trees, picture from Bruce Schneier Attack Trees article December 1999:

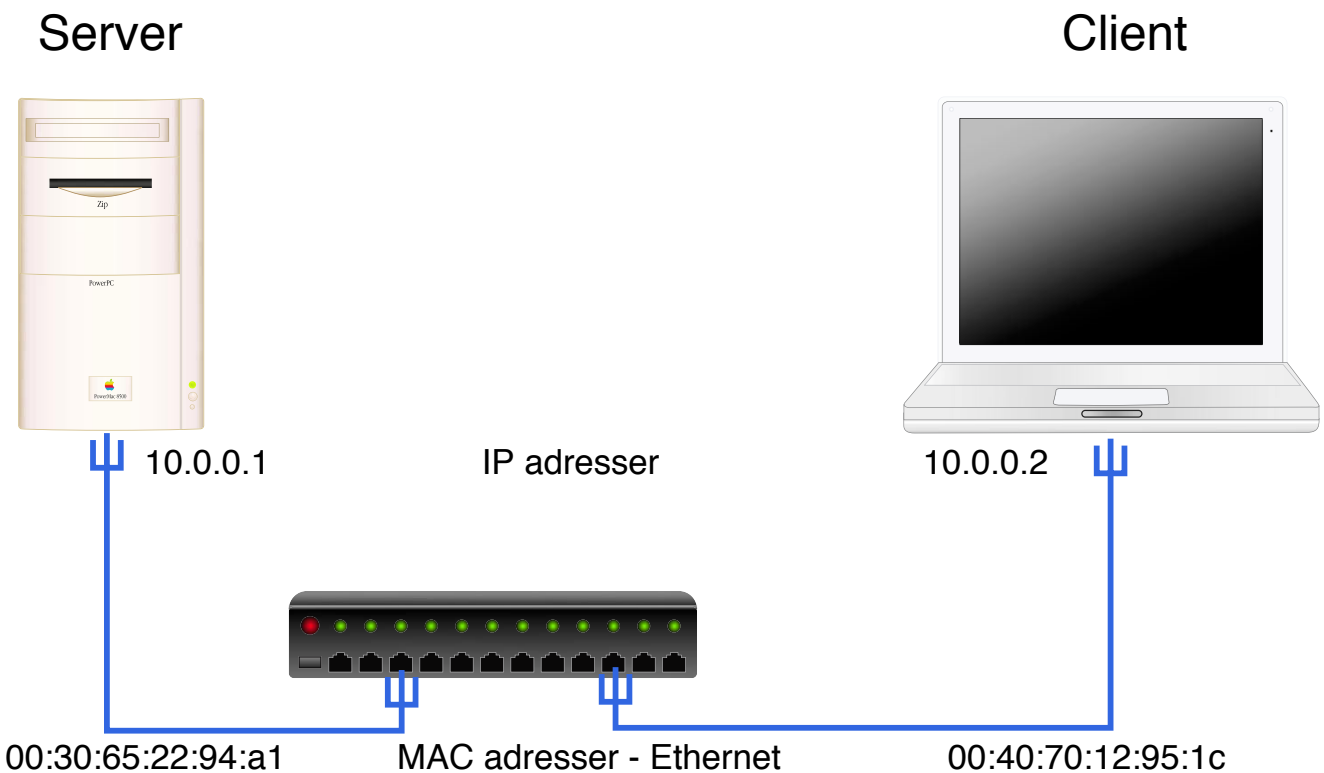
  https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Common Networks – spans multiple locations, regions, user bases



Fysisk er der en begrænsing for hvor lange ledningerne må være

Address Resolution Protocol (ARP)



Person in the middle attacks

ARP spoofing, ICMP redirects, the classics

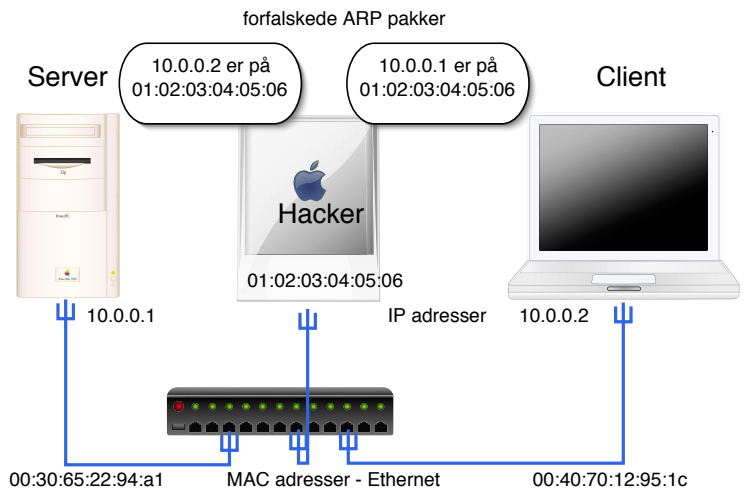
Used to be called Man in The Middle MiTM

- ICMP redirect
- ARP spoofing
- Wireless listening and spoofing higher levels like airpwn-ng https://github.com/ICSec/airpwn-ng

Usually aimed at unencrypted protocols

Today we only talk about getting the data, not how to perform higher level attacks

Hvordan virker ARP spoofing?



Hackeren sender forfalskede ARP pakker til de to parter

De sender derefter pakkerne ud på Ethernet med hackerens MAC adresse som modtager - som får alle pakkerne

Forsvar mod ARP spoofing

Hvad kan man gøre?

låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

Adskilte netværk - brug IEEE 802.1q VLANs

arpwatch er et godt bud - overvåger ARP

bruge protokoller som ikke er sårbare overfor opsamling

Security problems in the TCP/IP Suite

The title of a nice paper, and the rest of today

> The paper "Security Problems in the TCP/IP Protocol Suite" was originally pub- lished in Computer Communication Review, Vol. 19, No. 2, in April, 1989

Problems described in the original:

- sequence number spoofing
- routing attacks,
- source address spoofing
- authentication attacks

TCP sequence number prediction

> TCP SEQUENCE NUMBER PREDICTION One of the more fascinating security holes was first described by Morris [7] . Briefly, he used TCP sequence number prediction to construct a TCP packet sequence without ever receiving any responses from the server. This allowed him to spoof a trusted host on a local network.

tidligere baserede man login/adgange på source IP adresser, address based authentication

Er ikke en pålidelig autentifikationsmekanisme

Mest kendt er nok Shimomura der blev hacket på den måde,
måske af Kevin D Mitnick eller en kompagnon

I praksis vil det være svært at udføre på moderne operativsystemer

Se evt. http://www.takedown.com/ (filmen er ikke så god ;-))

Det er naturligvis fint med filtre så man kun kan tilgå services FRA bestemte IP

Routing attacks

Problems described in the original from 1989:

- IP Source routing attacks - angiv en rute for pakkerne
  Knapt så brugbar idag
- Routing Information Protocol Attacks
  The Routing Information Protocol [15] (RIP) - denne bruges ikke mere, outdated
- BGPv4 som bruges idag har kæmpe problemer, kludetæppe af kludges

Vi kommer til at snakke om https://github.com/tomac/yersinia

Solutions to TCP/IP security problems

Solutions:

- Use RANDOM TCP sequence numbers, Win/Mac/Linux - DO,but IoT?
- Filtrering, ingress / egress:
  "reject external packets that claim to be from the local net"
- Routers and routing protocols must be more skeptical
  Routing filtre everywhere, auth på OSPF/BGP etc.

Has been recommended for some years, but not done in all organisations

BGP routing Resource Public Key Infrastructure RPKI

DNS problems

> The Domain Name System (DNS) [32][33] provides for a distributed database mapping host names to IP addresses. An intruder who interferes with the proper operation of the DNS can mount a variety of attacks, including denial of service and password collection. There are a number of vulnerabilities.

We have a lot of the same problems in DNS today

Plus some more caused by middle-boxes, NAT, DNS size, DNS inspection

- DNS must allow both UDP and TCP port 53
- Your DNS servers must have updated software, see DNS flag day https://dnsflagday.net/ after which kludges will be REMOVED!

SNMP problems

> 5.5 Simple Network Management Protocol The Simple Network Management Protocol (SNMP) [37] has recently been defined to aid in network management. Clearly, access to such a resource must be heavily protected. The RFC states this, but also allows for a null authentication service; this is a bad idea. Even a ‘‘read-only’’ mode is dangerous; it may expose the target host to netstat-type attacks if the particular Management Information Base (MIB) [38] used includes sequence numbers. (T

True, and we will talk more about SNMP later in this course.

local networks

> 6.1 Vulnerability of the Local Network Some local-area networks, notably the Ethernet networks, are extremely vulnerable to eavesdropping and host-spoofing. If such networks are used, physical access must be strictly controlled. It is also unwise to trust any hosts on such networks if any machine on the network is accessible to untrusted personnel, unless authentication servers are used. If the local network uses the Address Resolution Protocol (ARP) [42] more subtle forms of host-spoofing are possible. In particular, it becomes trivial to intercept, modify, and forward packets, rather than just taking over the host's role or simply spying on all traffic.

Today we can send VXLAN spoofed packets across the internet layer 3 and inject ARP behind firewalls, in some cloud infrastructure cases ...

A Look Back at "Security Problems in the TCP/IP Protocol Suite" about 1989 + 15 years = 2004

Exposure, Attack surfaces, and reducing them

- Incident prevention
- Real-time intrusion detection systems (IDS/IPS)
- **Definition 27-7** An *attack surface* is the set of entry points and data that attackers can use to compromise a system.
- Reducing the chance of success also helps, randomization
- Use stack and heap protection
- Address space layout randomization (ASLR) is a host-level moving target defense.
- OpenBSD even randomizes the kernel on install – kernel address randomized link (KARL)
- Limit number of listening services, change insecure defaults, implement access control and firewalls
- Remove anything but the necessary request methods on web servers `GET`, `HEAD` and `POST`
- Restrict access to administrative interfaces
- Implement network segmentation

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: use the more updated list online http://cwe.mitre.org/top25/index.html

Principle of Least Privilege

Definition 14-1 The *principle of least privilege* states that a subject should be given only those privileges that it needs in order to complete the task.

Also drop privileges when not needed anymore, relinquish rights immediately

Example, need to read a document - but not write.

Database systems can often provide very fine grained access to data

Source: *Computer Security: Art and Science*, Matt Bishop ISBN: 9780321712332

https://www.pearson.com/us/higher-education/program/Bishop-Computer-Security-2nd-Edition/PGM25107.html

Principle of Fail-Safe defaults

Definition 14-3 The *principle of fail-safe defaults* states that, unless a subject is given explicit access to an object, it should be denied access to that object.

Default access *none*

In firewalls default-deny - that which is not allowed is prohibited

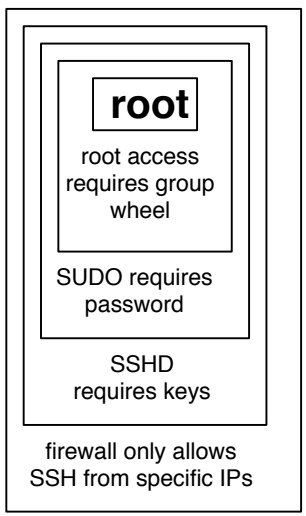
Newer devices today can come with no administrative users, while older devices often came with default admin/admin users

Real world example, OpenSSH config files that come with `PermitRootLogin no`

Source: *Computer Security: Art and Science*, Matt Bishop ISBN: 9780321712332

https://www.pearson.com/us/higher-education/program/Bishop-Computer-Security-2nd-Edition/PGM25107.html

Principle of Separation of Privilege – Defense in Depth



Definition 14-7 The *principle of separation of privilege* states that a system should not grant permission based on a single condition.

Company checks, CEO fraud

Programs like *su* and *sudo* often requires specific group membership and password

Firewallrollen idag

Idag skal en firewall være med til at:

- Forhindre angribere i at komme ind
- Forhindre angribere i at sende traffik ud
- Forhindre virus og orme i at sprede sig i netværk
- Indgå i en samlet løsning med ISP, routere, firewalls, switchede strukturer, intrusion detectionsystemer samt andre dele af infrastrukturen

Det kræver overblik!

Sample rules from OpenBSD PF Firewall

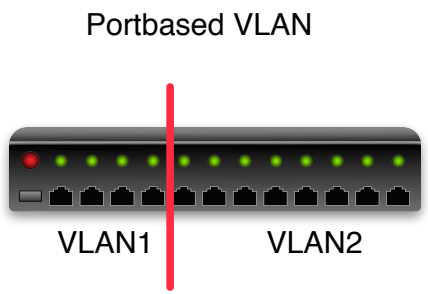
```
# hosts and networks
router="217.157.20.129"
webserver="217.157.20.131"
homenet=" 192.168.1.0/24, 1.2.3.4/24 "
wlan="10.0.42.0/24"
wireless=wi0
set skip lo0
# things not used
spoofed=" 127.0.0.0/8, 172.16.0.0/12, 10.0.0.0/16, 255.255.255.255/32 "

# default block anything
block in all
# egress and ingress filtering - disallow spoofing, and drop spoofed
block in quick from $spoofed to any
block out quick from any to $spoofed

pass in on $wireless proto tcp from { $wlan $homenet } to any port = 22
pass in on $wireless proto tcp from any to $webserver port = 80

pass out
```

Together with Firewalls - VLAN Virtual LAN



Nogle switche tillader at man opdeler portene

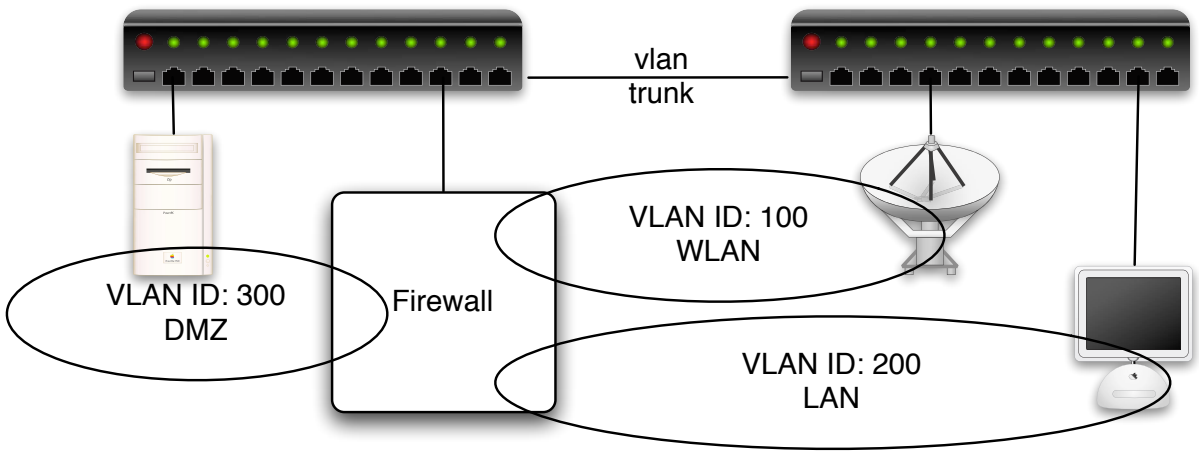
Denne opdeling kaldes VLAN og portbaseret er det mest simple

Port 1-4 er et LAN

De resterende er et andet LAN

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

IEEE 802.1q – virtual LAN



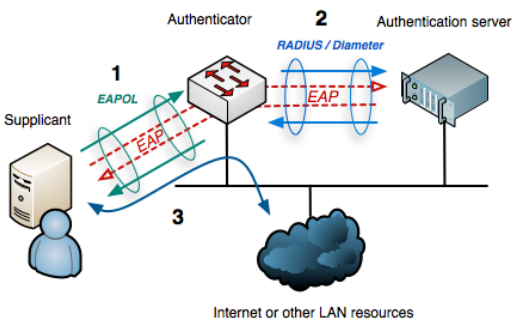
Med 802.1q tillades VLAN tagging på Ethernet niveau

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

VLAN trunking giver mulighed for at dele VLANs ud på flere switches

Network Access Control – Connecting clients more securely

IEEE 802.1x Port Based Network Access Control



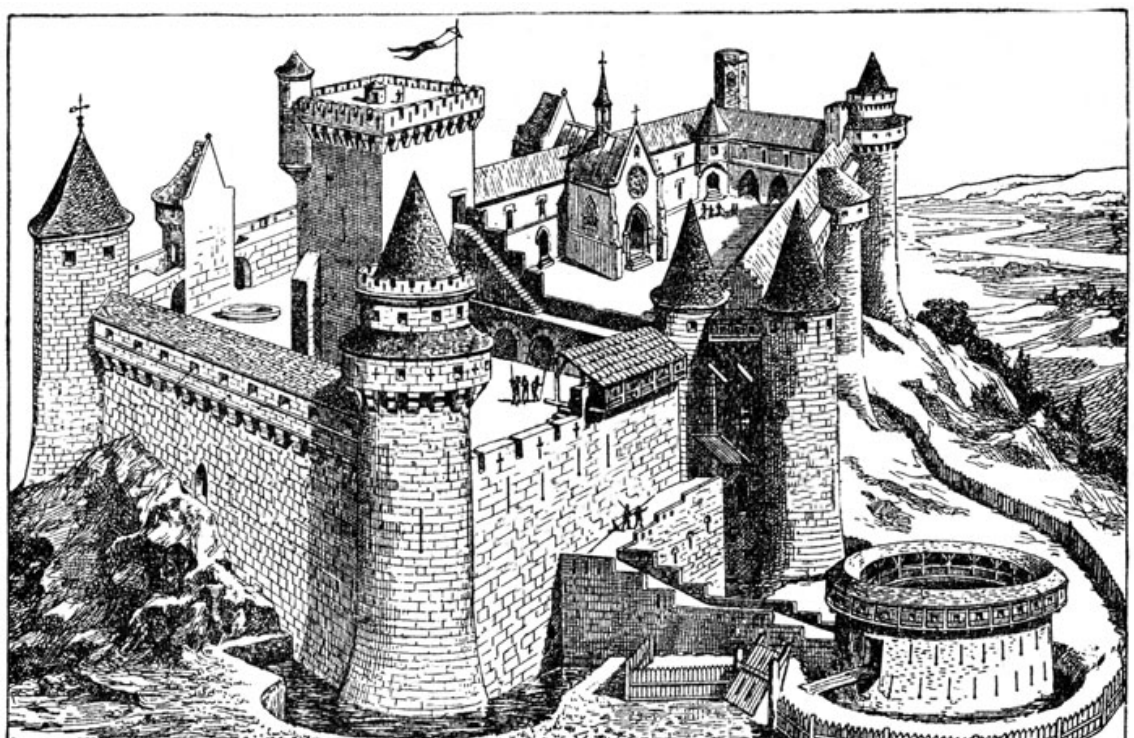
Denne protokol sikrer at man valideres før der gives adgang til porten

Når systemet skal have adgang til porten afleveres brugernavn og kodeord/certifikat

Typisk benyttes RADIUS og 802.1x integrerer således mod både LDAP og Active Directory

Bruges til Wi-Fi netværk

Defense in depth



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

Fokus 2022

- Brugerstyring
- Asset management
- Laptop sikkerhed
- VPN alle steder
- Penetration testing
- Firewalls og segmentering
- TLS og VPN indstillinger
- DNS og email
- Syslog og monitorering
- Incident Response og reaktion

Brug bogen *Defensive Security Handbook: Best Practices for Securing Infrastructure*

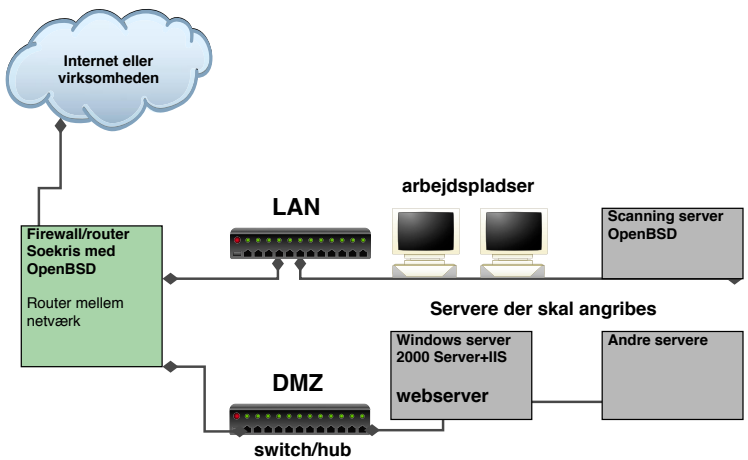
Design a robust network Isolation and segmentation

Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switche - der skal ARP spoofes og bedre performance
- Opdele med firewall til flere DMZ zoner for at holde udsatte servere adskilt fra hinanden, det interne netværk og Internet
- Overvåge, læse logs og reagere på hændelser

Husk du skal også kunne opdatere dine servere

Basic Network Security Pattern Isolate in VLANs



Du bør opdele dit netværk i segmenter efter trafik

Du bør altid holde interne og eksterne systemer adskilt!

Du bør isolere farlige services i jails og chroots

Brug port security til at sikre basale services DHCP, Spanning Tree osv.

Concrete advise for enterprise networks

- Have separation – anywhere, starting with organisation units, management networks, server networks, customers, guests, LAN, WAN, Mail, web, ...
- Use Web proxies - do not allow HTTP directly except for a short allow list,
  do not allow traffic to and from any new TLD
- Use only your own DNS servers, create a pair of Unbound servers,
  point your internal DNS running on Windows to these
  Create filtering, logging, restrictions on these Unbound DNS servers
  https://www.nlnetlabs.nl/projects/unbound/about/ and also https://pi-hole.net/
- Only allow SMTP via your own mail servers, create a simple forwarder if you must

Allow lists are better than block list, even if it takes some time to do it

Capture data and logs!

- Run DNS query logs – when client1 is infected with malware from domain malwareexample.com, then search for more clients infected
- Run Zeek and gather information about all HTTPS sessions – captures certificates by default, and we can again search for certificate related to malwareexample.com
- Run network logging – session logs in enterprise networks are GREAT
  (country wide illegal logging is of course NOT)

  Make sure to check with employees, inform them!

Indicators of Compromise and Signatures

An IOC is any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner. This could include a simple indicator such as the IP address of a command and control (C2) server or a complex set of behaviors that indicate that a mail server is being used as a malicious SMTP relay.

When an IOC is taken and used in a platform-specific language or format, such as a Snort Rule or a Bro-formatted file, it becomes part of a signature. A signature can contain one or more IOCs.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

Zeek is a framework and platform

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.

https://www.Zeek.org/ Does useful things out of the box using more than 10.000 script lines

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

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

Suricata, Zeek og DNS Capture – it a nice world, use it!

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

Default permit

One of the early implementers of firewalls Marcus J. Ranum summarized in 2005 The Six Dumbest Ideas in Computer Security https://www.ranum.com/security/computer_security/editorials/dumb/ which includes the always appropriate discussion about default permit versus default deny.

> **#1) Default Permit**
> This dumb idea crops up in a lot of different forms; it's incredibly persistent and difficult to eradicate. Why? Because it's so attractive. Systems based on "Default Permit" are the computer security equivalent of empty calories: tasty, yet fattening.
> The most recognizable form in which the "Default Permit" dumb idea manifests itself is in firewall rules. Back in the very early days of computer security, network managers would set up an internet connection and decide to secure it by turning off incoming telnet, incoming rlogin, and incoming FTP. Everything else was allowed through, hence the name "Default Permit." This put the security practitioner in an endless arms-race with the hackers.

- Allow all current networks today on all ports for all protocols *is* an allow list
  Which tomorrow can be split into one for TCP, UDP and remaining, and measured upon
- Measure, improve, repeat

We cannot do X

> We cannot block SMTP from internal networks, since we do not know for sure if vendor X equipment needs to send the MOST important email alert at some unspecific time in the future

Cool, then we can do an allow list starting today on our border firewall:

```
table <smtp-exchange> { $exchange1 $exchange2 $exchange3 }
table <smtp-unknown> persist file "/firewall/mail/smtp-internal-unknown.txt"
# Regular use, allowed
pass out on egress inet proto tcp from smtp-echange to any port 25/tcp
# Unknown, remove when phased out
pass out on egress inet proto tcp from smtp-internal to any port 25/tcp
```

Year 0 the unknown list may be 100% of all internal networks, but new networks added to infrastructure are NOT added, so list will shrink – evaluate the list, and compare to network logs, did networks send ANY SMTP for 1,2,3 years?

DROP SOME TRAFFIC NOW

- Drop some traffic on the border of everything
- Seriously do NOT allow Windows RPC across borders
- Border here may be from regional country office back to HQ
- Border may be from internet to internal networks
- Block Windows RPC ports, 135, 137, 139, 445
- Block DNS directly to internet, do not allow clients to use any DNS, fake 8.8.8.8 if you must internally
- Block SMTP directly to internet
- Create allow list for internal networks, client networks should not contact other client networks but only relevant server networks

You DONT need to allow direct DNS towards internet, except from your own recursive DNS servers

If you get hacked by Windows RPC in 2022, you probably deserve it, sorry for being blunt

Best would be to analyze traffic and create allow lists, some internal networks to not need internet at all

Example incident response procedures

> 5.4 Handling an Incident
>
> Certain steps are necessary to take during the handling of an incident. In all security related activities, the most important point to be made is that all sites should have policies in place. Without defined policies and goals, activities undertaken will remain without focus. The goals should be defined by management and legal counsel in advance.

- Quote from RFC2196 *Site Security Handbook* September 1997, IETF
  https://tools.ietf.org/html/rfc2196#section-5.4
- *Incident Handler's Handbook* by Patrick Kral, SANS Information Security Reading Room
  https://www.sans.org/reading-room/whitepapers/incident/paper/33901
- *Computer Security Incident Handling Guide*, NIST Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://cloud.google.com/security/incident-response/
- Microsoft Azure https://medium.com/@cloudyforensics/azure-forensics-and-incident-response-c13098a14d8d

Incident Handling Checklist from NIST.SP.800-61r2.pdf

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)	

Roundtable

- Lets discuss
- Are the proposed methods workable, why or why not
- Do you have time and skills
- Can't we just hire someone

Open mike night