Welcome to

Systems Security - 2

Intro to IT-security 2024

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Codeberg https://codeberg.org/kramse/
intro-to-it-security-system-security-2.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: xhek@kea.dk Mobile: +45 2026 6000

You are welcome to drop me an email

Goals for Today

- User accounts
- Authentication and Authorization
- Access Control Lists
- Confinement and isolation

Exercises

- Debian Linux exercises

Photo by Thomas Galler on Unsplash

Plan for part I: User accounts, Authentication and Authorization

Subjects

- What are user accounts – user ID
- Securing Administrative User Accounts
- Securing Normal User Accounts
- Databases: RDBMS, MariaDB

Exercises

- Databases - discussion about Relational Database Management System RDBMS Model and NoSQL
- RBAC on Github
- Password cracking
- SSH keys

Intrusion Kill Chains

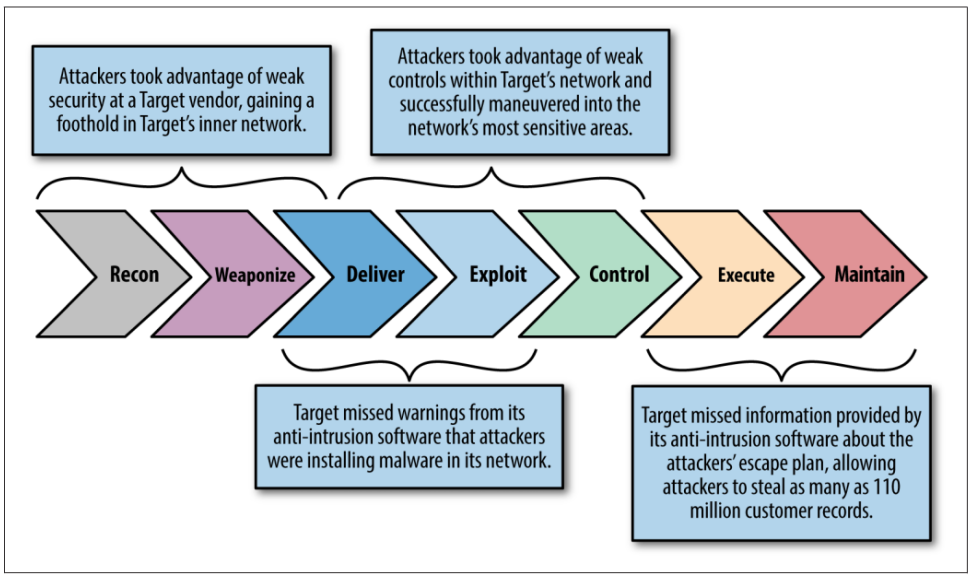


Figure 7-1. The kill chain

- 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, 2011

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

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/

Local vs. remote exploits

Local vs. remote angiver om et exploit er rettet mod en sårbarhed lokalt på maskinen, eksempelvis opnå højere privilegier, eller beregnet til at udnytter sårbarheder over netværk

Remote root exploit - den type man frygter mest, idet det er et exploit program der når det afvikles giver angriberen fuld kontrol, root user er administrator på Unix, over netværket.

Zero-day exploits dem som ikke offentliggøres – dem som hackere holder for sig selv. Dag 0 henviser til at ingen kender til dem før de offentliggøres og ofte er der umiddelbart ingen rettelser til de sårbarheder

Separation of duty ns function

> **Separation of duties** (SoD; also known as Segregation of Duties) is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.

Quote from https://en.wikipedia.org/wiki/Separation_of_duties

> **Separation of function**. Developers do not develop new programs on production systems because of the potential threat to production data.

Computer Security, Matt Bishop, 2019

Danish: Funktionsadskillelse

Lipners Integrity Matrix Model

	OBJECTS							
SUBJECTS	**Production Data**	**Production Code**	**Develop. Code & Test Data**	**Develop. Sys. Prog.**	**S/W Tools**	**Sys. Prog.**	**Re-pair Code**	**Audit Data**
System Mgr.	R	R	R	R	R	R	R	RW
Prod. User	RW	R				R		W
App'n. Prog.			RW		R	R		W
Sys. Program				RW	R	R		W
Sys. Control	RW	RW	RW	RW	RW	RW	RW	W
Repair	RW	R				R	R	W

Figure 12. Effects of Commercial Lattice Model with Integrity

Non-Discretionary Controls for Commercial Applications, Steven B. Lipner, IEEE Symposium on Security and Privacy, and Fifth Seminar on the DoD Computer Security Initiative, 1982

MLSH Chapter 2: intro

Securing Administrative User Accounts
Managing users is one of the more **challenging** aspects of IT administration. You need to make sure that users can always **access their stuff** and that they can **perform the required tasks** to do their jobs. You also need to ensure that users' stuff is always **secure from unauthorized users** and that users **can't perform any tasks that don't fit their job description**.

Source: *Mastering Linux Security and Hardening* (MLSH), third edition

Can we spot the:

- Confidentiality, Integrity and Availability requirements
- Principle of Least Privilege

The dangers of logging in as the root user

> A huge advantage that Unix and Linux operating systems have over Windows is that Unix and Linux do a much better job of keeping privileged administrative accounts separated from normal user accounts. Indeed, one reason that older versions of Windows were so susceptible to security issues, such as drive-by virus infections, was the common practice of setting up user accounts with administrative privileges, without having the protection of the User Access Control (UAC) that's in newer versions of Windows.

Source: *Mastering Linux Security and Hardening* (MLSH), third edition

- Agreed, but I may be biased
- Mac OS X made it very simple to run administrative tasks, so you didn't need to run as root
- Modern Linux user interfaces make similar attempts with `pkexec`, `kdesudo`, `gksudo` etc.
- Windows is getting better, many organisations in DK are removing administrative access to regular users, even KEA

The advantages of using sudo

Used properly, the sudo utility can greatly enhance the security of your systems, and it can make an administrator's job much easier. With sudo , you can do the following:

- Assign certain users full administrative privileges, while assigning other users only the privi- leges they need to perform tasks that are directly related to their respective jobs.
- Allow users to perform administrative tasks by entering their own normal user passwords so that you don't have to distribute the root password to everybody and their brother.
- Make it harder for intruders to break into your systems. If you implement sudo and disable the root user account, would-be intruders won't know which account to attack because they won't know which one has admin privileges.
- Create sudo policies that you can deploy across an entire enterprise network, even if that network has a mix of Unix, BSD, and Linux machines.
- Improve your auditing capabilities because you'll be able to see what users are doing with their admin privileges.

Source: *Mastering Linux Security and Hardening* (MLSH), third edition

Why use Sudo conclusion

Main thing about sudo is that you do NOT give out the root password to anybody! They will use their own credentials and can be limited to single commands, scripts and even parameters. You could have a single sudoers file for your own organisation, that includes groups of servers, user groups etc.

Sidenote: sudo also has a number of CVEs unfortunately

Configure Sudo in the Lab – no passwd

Not in sudoers file, cannot run sudo command. This can be fixed quite easily.

If you use the su command first, to switch user to root and run the visudo command:

```
$ su -
# visudo
```

You will get an editor, where you enter below the root line, your username and a similar line:

```
# User privilege specification
root ALL = (ALL:ALL) ALL
hlk ALL = (ALL:ALL) NOPASSWD: ALL
```

Then use ctrl-x if using Nano, and exit the editor - saving this configuration file.

Logging in

We did a small exercise last time: Investigate /etc

Objective:
We will investigate the /etc directory on Linux

We need a Kali Linux and a Debian Linux VM, to compare

Purpose:
Start seeing example configuration files, including:

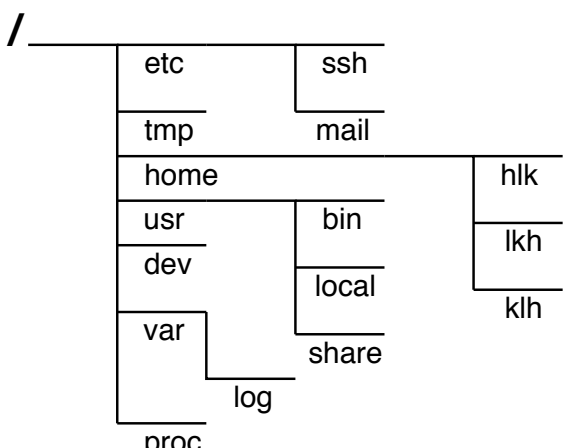
- User database `/etc/passwd` and `/etc/group`
- The password database `/etc/shadow`

This database of users is checked everytime someone logs into the system. Everything is tied up to users on Unix

Linux configuration in /etc

.

- Command line is a requirement in the *studieordningen* ☺
- Linux and Unix uses a single virtual file system
  https://en.wikipedia.org/wiki/Unix_filesystem
- No drive letters like the ones in MS-DOS and Microsoft Windows
- Everything starts at the root of the file system tree / - NOTE: *forward slash*
- One special directory is `/etc/` and sub directories which usually contain a lot of configuration files



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

Unix permissions

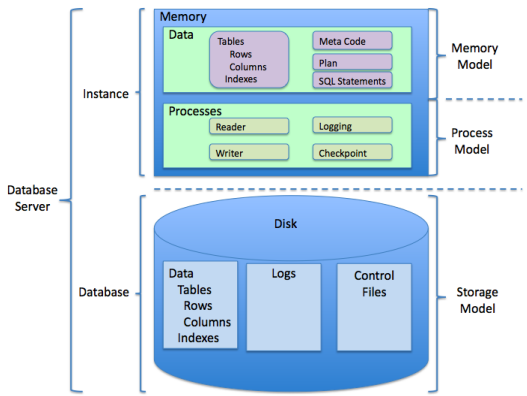
```
chown -R librenms:librenms /opt/librenms
chmod 771 /opt/librenms
setfacl -d -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/
setfacl -R -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/
```

Source: Install instructions for LibreNMS
https://docs.librenms.org/Installation/Install-LibreNMS/

- Ownership of files – who owns the files, owner and group
  `chown` – change owner
- Permissions – read, write and execute
  `chmod` – change file mode bits
- setfacl - set file access control lists

Microsoft Windows usually have the advanced file access control lists from NTFS, allowing named users access to files and directories

Relational Database Management System RDBMS



Relational Database Management System RDBMS is a common database architecture

Common examples MS-SQL, MySQL/MariaDB, PostgreSQL

Picture: By Scifipete - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=11506013

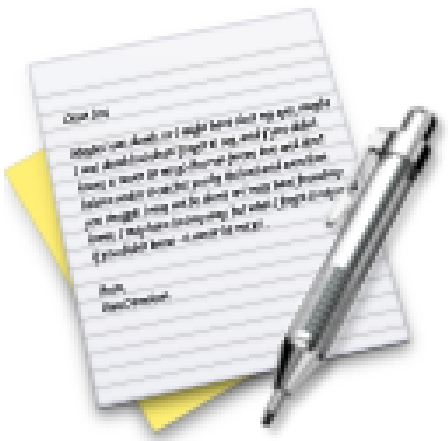
https://en.wikipedia.org/wiki/Relational_database#RDBMS

PostgreSQL security

	11	10	9.6	9.5	9.4
Channel binding for SCRAM authentication	Yes	No	No	No	No
Column level permissions	Yes	Yes	Yes	Yes	Yes
Default permissions	Yes	Yes	Yes	Yes	Yes
GRANT/REVOKE ON ALL TABLES/SEQUENCES/FUNCTIONS	Yes	Yes	Yes	Yes	Yes
GSSAPI support	Yes	Yes	Yes	Yes	Yes
Large object access controls	Yes	Yes	Yes	Yes	Yes
Native LDAP authentication	Yes	Yes	Yes	Yes	Yes
Native RADIUS authentication	Yes	Yes	Yes	Yes	Yes
Per user/database connection limits	Yes	Yes	Yes	Yes	Yes
ROLES	Yes	Yes	Yes	Yes	Yes
Row-Level Security	Yes	Yes	Yes	Yes	No
SCRAM-SHA-256 Authentication	Yes	Yes	No	No	No
Search+bind mode operation for LDAP authentication	Yes	Yes	Yes	Yes	Yes
security_barrier option on views	Yes	Yes	Yes	Yes	Yes
Security Service Provider Interface (SSPI)	Yes	Yes	Yes	Yes	Yes
SSL certificate validation in libpq	Yes	Yes	Yes	Yes	Yes
SSL client certificate authentication	Yes	Yes	Yes	Yes	Yes
SSPI authentication via GSSAPI	Yes	Yes	Yes	Yes	Yes

Feature overview security features in PostgreSQL
https://www.postgresql.org/about/featurematrix/#security

Exercise

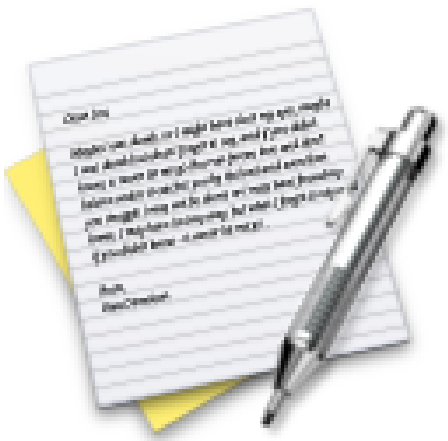


Now lets do the exercise

⚠ Configure a Database - 20 min

which is number **13** in the exercise PDF.

Exercise



Now lets do the exercise

⚠ RBAC Access permissions on GitHub up to 30min

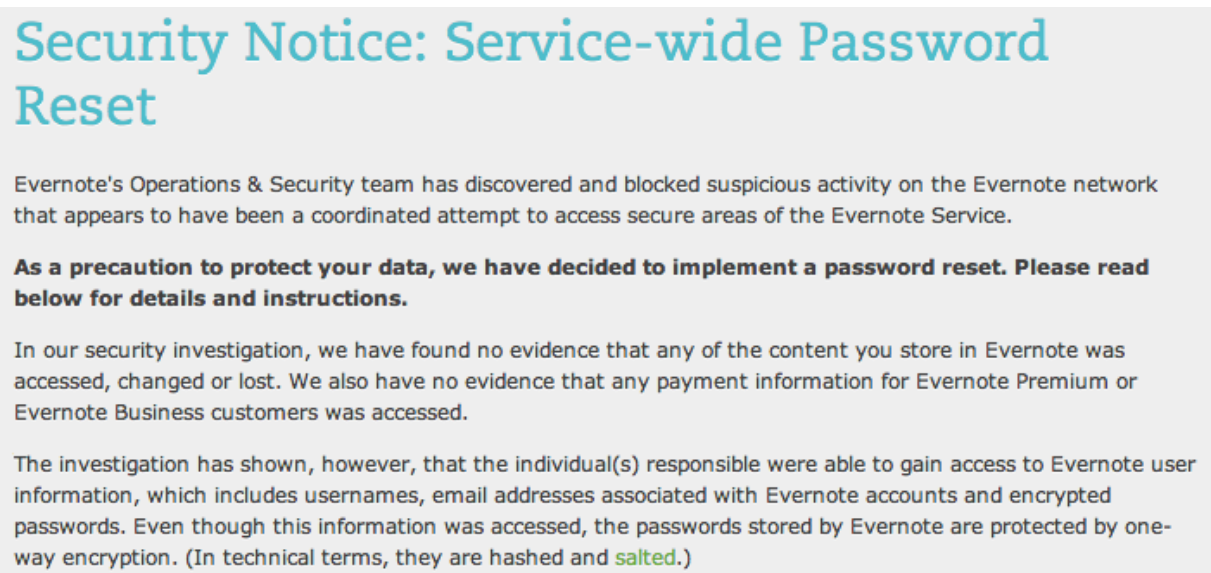
which is number **14** in the exercise PDF.

Passwords vælges ikke tilfældigt

Source: https://wpengine.com/unmasked/

Evernote password reset

What happens when security breaks?



Security Notice: Service-wide Password Reset

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

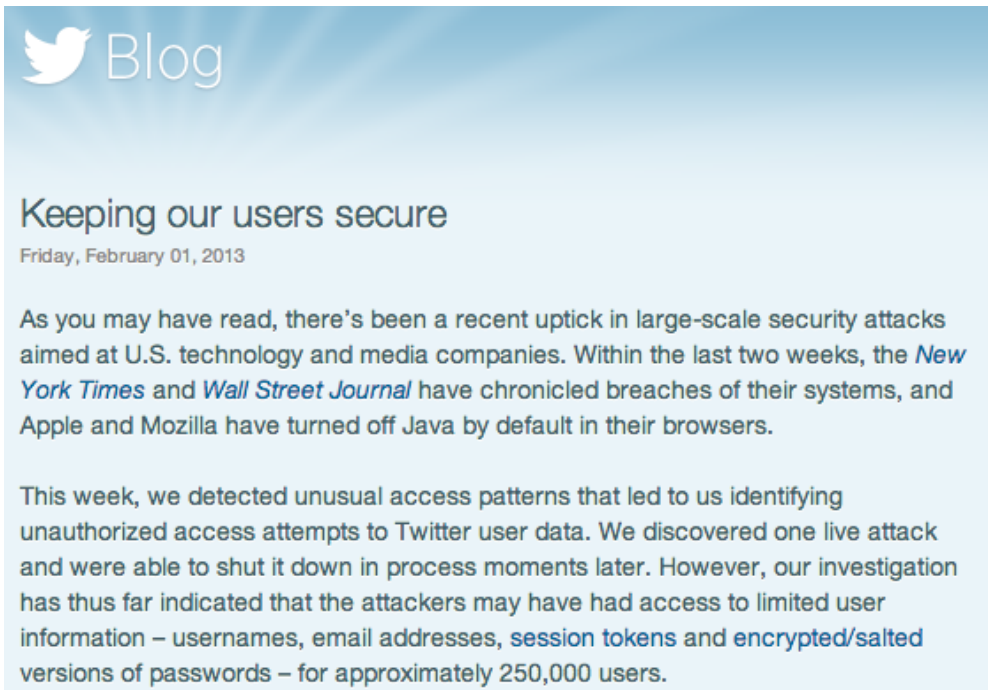
As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, changed or lost. We also have no evidence that any payment information for Evernote Premium or Evernote Business customers was accessed.

The investigation has shown, however, that the individual(s) responsible were able to gain access to Evernote user information, which includes usernames, email addresses associated with Evernote accounts and encrypted passwords. Even though this information was accessed, the passwords stored by Evernote are protected by one-way encryption. (In technical terms, they are hashed and salted.)

Sources:
http://evernote.com/corp/news/password_reset.php

Twitter password reset



Blog

Keeping our users secure

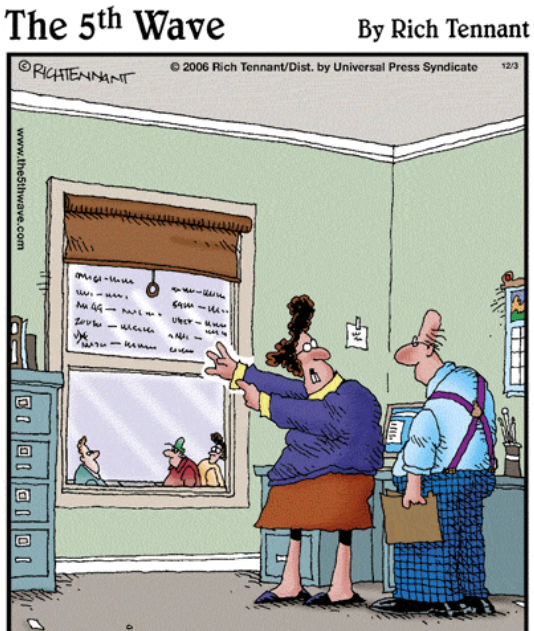
Friday, February 01, 2013

As you may have read, there's been a recent uptick in large-scale security attacks aimed at U.S. technology and media companies. Within the last two weeks, the *New York Times* and *Wall Street Journal* have chronicled breaches of their systems, and Apple and Mozilla have turned off Java by default in their browsers.

This week, we detected unusual access patterns that led to us identifying unauthorized access attempts to Twitter user data. We discovered one live attack and were able to shut it down in process moments later. However, our investigation has thus far indicated that the attackers may have had access to limited user information – usernames, email addresses, session tokens and encrypted/salted versions of passwords – for approximately 250,000 users.

Sources:
http://blog.twitter.com/2013/02/keeping-our-users-secure.html

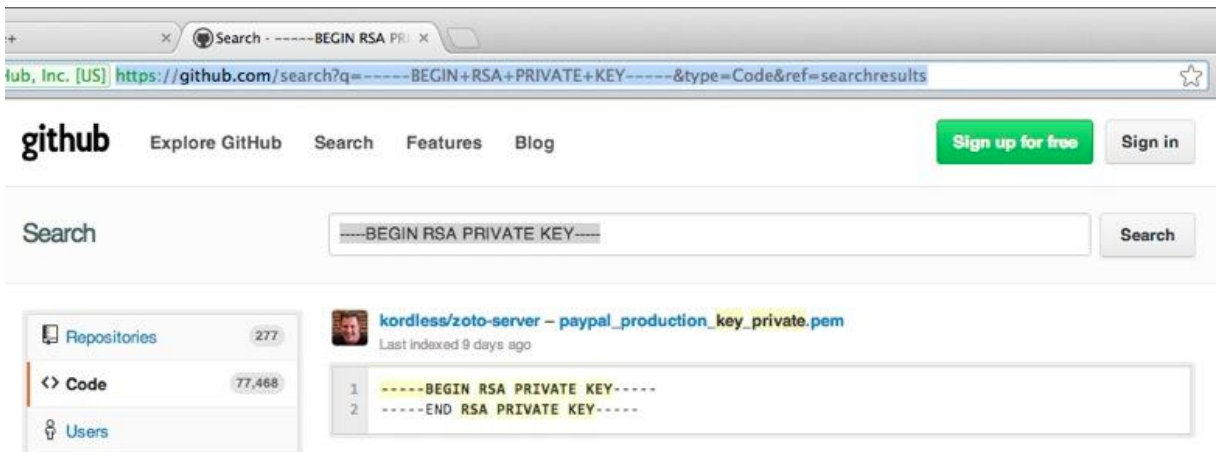
Saving passwords



"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

Use some kind of Password Safe program

January 2013: Github Public passwords?



Sources:

https://twitter.com/brianaker/status/294228373377515522

http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-details/

http://www.leakedin.com/

http://www.offensive-security.com/community-projects/google-hacking-database/

TwoFactor authentication: Example Duosecurity

Push Notification
Quickly view login or transaction details and tap "Approve" on your iOS or Android device.
Learn more at duosecurity.com/duo-push

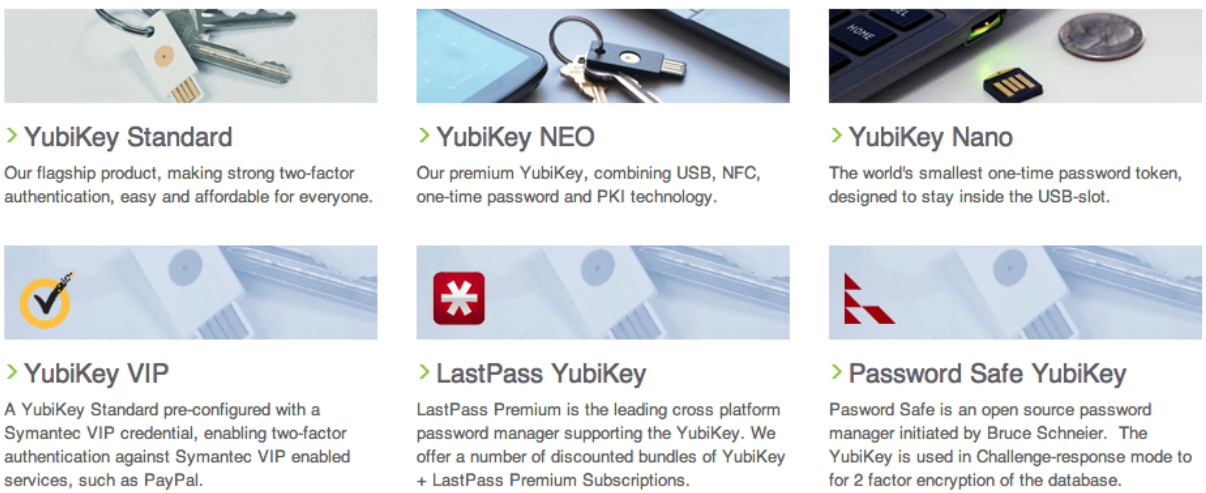
Smartphone Passcodes
Easily generate login passcodes — no cell service required. Duo Mobile is available for free on all smartphone platforms.

Text Message
Login passcodes sent via text message. Works on all phones with SMS support.

Phone Call
Simply answer a phone call and press a key to authenticate.

Source: https://www.duo.com/

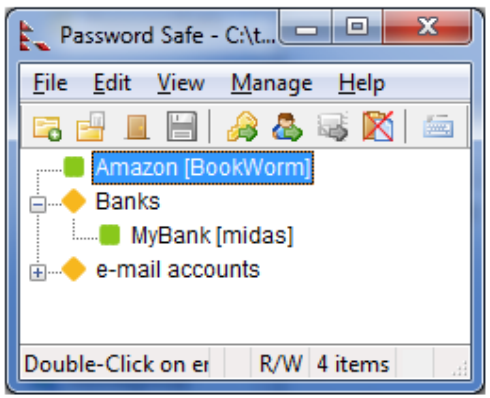
Yubico Yubikey



A Yubico OTP is unique sequence of characters generated every time the YubiKey button is touched. The Yubico OTP is comprised of a sequence of 32 Modhex characters representing information encrypted with a 128 bit AES-128 key

http://www.yubico.com/products/yubikey-hardware/ and also https://wiki.debian.org/Smartcards/YubiKey4

Storing passwords



Use password managers – even though they also have security issues the overall improvement is great

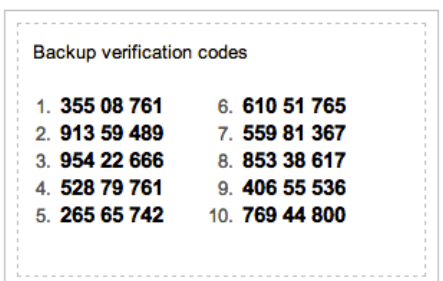
PasswordSafe https://pwsafe.org/ – Note: research for yourself which password manager to use!

Apple Keychain provides an encrypted storage

Browsere, Firefox Master Password, Chrome passwords, ... who do YOU trust

Low tech 2-step verification

Printing code on paper, low level pragmatic


Backup verification codes

1. 355 08 761
2. 913 59 489
3. 954 22 666
4. 528 79 761
5. 265 65 742
6. 610 51 765
7. 559 81 367
8. 853 38 617
9. 406 55 536
10. 769 44 800

Login from new devices today often requires two-factor - email sent to user

Google 2-factor auth. SMS with backup codes

Also read about S/KEY developed at Bellcore **in the late 1980s**
http://en.wikipedia.org/wiki/S/KEY

Conclusion passwords: integrate with authentication, not reinvent

John the ripper

> John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

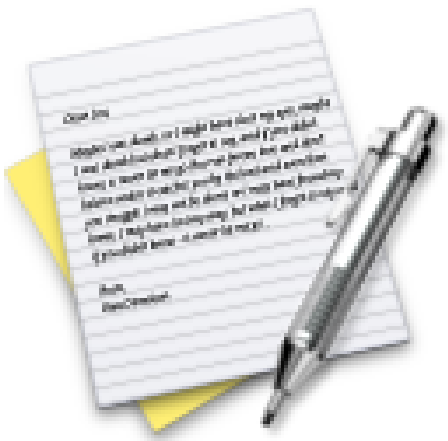
UNIX passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John The Ripper http://www.openwall.com/john/

Cracking passwords

- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:
http://hashcat.net/wiki/
http://www.openwall.com/john/

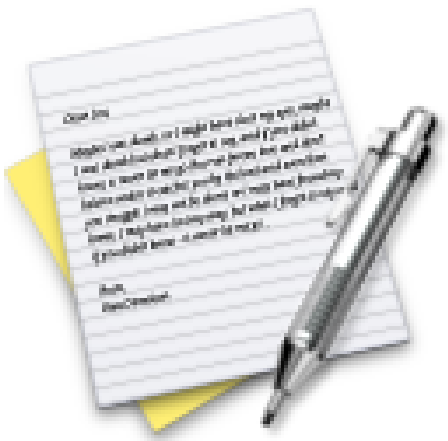
Exercise



Now lets do the exercise

⚠ Password Cracking 15min

which is number **15** in the exercise PDF.



Now lets do the exercise

Configure SSH keys for more secure access 30min

which is number **16** in the exercise PDF.

End of part I

Take a break!

Goals part II: ACLs, Confinement and Isolation

Access Control Lists, Confinement and isolation, Virtual Machines and Sandboxes'

- Identify the problem of keeping applications and data confined
- Discuss isolation - including sandboxes, virtual machines and capabilities

Virtual Machines

Definition 18-4 A *virtual machine* is a program that simulates the hardware of a (possibly abstract) computer system.

Also called hypervisor

Common technologies include VMware, Virtualbox, HyperV, Qemu, KVM

Qubes OS uses the Xen Project https://xenproject.org/

Also similarities to sandboxes implemented in Java Virtual Machine (JVM) and other places

Sandbox definition

Definition 18-6 A *sandbox* is an environment in which the actions of a process are restricted according to a security policy

Mentions firewall, which is why we also discuss these later today

Chroot, Jails and

Der findes mange typer *jails* på Unix

Ideer fra Unix chroot som ikke er en egentlig sikkerhedsfeature

- Unix chroot - bruges stadig, ofte i daemoner som OpenSSH
- FreeBSD Jails
- SELinux
- Solaris Containers og Zones
- VMware virtuelle maskiner, er det et jail?

Hertil kommer et antal andre måder at adskille processer - sandkasser

Husk også de simple, database som `_postgresql`, Tomcat som `tomcat`, Postfix postsystem som `_postfix`, SSHD som `sshd` osv. - simple brugere, få rettigheder

JVM security policies

```
// ========== WEB APPLICATION PERMISSIONS ====================================
// These permissions are granted by default to all web applications
// In addition, a web application will be given a read FilePermission
// and JndiPermission for all files and directories in its document root.
grant {
    // Required for JNDI lookup of named JDBC DataSource's and
    // javamail named MimePart DataSource used to send mail
    permission java.util.PropertyPermission "java.home", "read";
    permission java.util.PropertyPermission "java.naming.*", "read";
    permission java.util.PropertyPermission "javax.sql.*", "read";
...
};
// The permission granted to your JDBC driver
// grant codeBase "jar:file:${catalina.home}/webapps/examples/WEB-INF/lib/driver.jar!/-" \{
//      permission java.net.SocketPermission "dbhost.mycompany.com:5432", "connect";
// \};
```

Eksempel fra apache-tomcat-6.0.18/conf/catalina.policy

Apple sandbox named generic rules

```
;; named - sandbox profile
;; Copyright (c) 2006-2007 Apple Inc.  All Rights reserved.
;;
;; WARNING: The sandbox rules in this file currently constitute
;; Apple System Private Interface and are subject to change at any time and
;; without notice. The contents of this file are also auto-generated and not
;; user editable; it may be overwritten at any time.
;;
(version 1)
(debug deny)

(import "bsd.sb")

(deny default)
(allow process*)
(deny signal)
(allow sysctl-read)
(allow network*)
```

Apple sandbox named specific rules

```
;; Allow named-specific files
(allow file-write* file-read-data file-read-metadata
  (regex "^(/private)?/var/run/named\\pid$"
         "^/Library/Logs/named\\.log$"))

(allow file-read-data file-read-metadata
  (regex "^(/private)?/etc/rndc\\.key$"
         "^(/private)?/etc/resolv\\.conf$"
         "^(/private)?/etc/named\\.conf$"
         "^(/private)?/var/named/"))
```

Eksempel fra `/usr/share/sandbox` på Mac OS X

Capability-based security

Capability-based security is a concept in the design of secure computing systems, one of the existing security models. A capability (known in some systems as a key) is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure. Capability-based security is to be contrasted with an approach that uses hierarchical protection domains.

https://en.wikipedia.org/wiki/Capability-based_security

kea

Quick introduction

AppArmor is an effective and easy-to-use Linux application security system. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing both known and unknown application flaws from being exploited.

AppArmor supplements the traditional Unix discretionary access control (DAC) model by providing mandatory access control (MAC). It has been included in the mainline Linux kernel since version 2.6.36 and its development has been supported by Canonical since 2009.

Source: https://apparmor.net/

Syscall restrictions seccomp

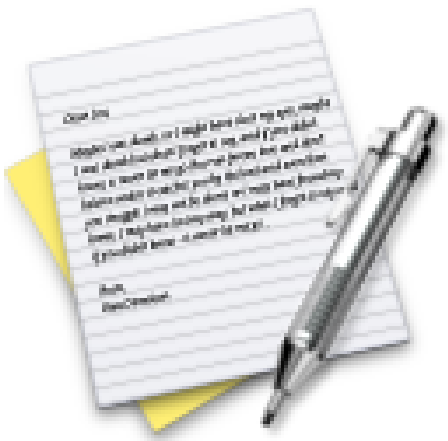
Restrict a Container's Syscalls with seccomp

FEATURE STATE: Kubernetes v1.19 [stable] Seccomp stands for secure computing mode and has been a feature of the Linux kernel since version 2.6.12. It can be used to sandbox the privileges of a process, restricting the calls it is able to make from userspace into the kernel. Kubernetes lets you automatically apply seccomp profiles loaded onto a node to your Pods and containers.

Identifying the privileges required for your workloads can be difficult. In this tutorial, you will go through how to load seccomp profiles into a local Kubernetes cluster, how to apply them to a Pod, and how you can begin to craft profiles that give only the necessary privileges to your container processes.

Source: https://kubernetes.io/docs/tutorials/security/seccomp/

Exercise

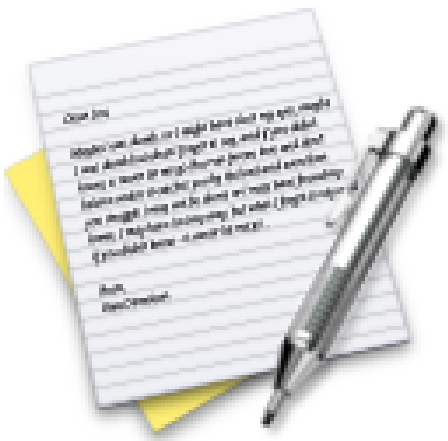


Now lets do the exercise

⚠ Research Virtual Machine Escapes 20min

which is number **17** in the exercise PDF.

Exercise

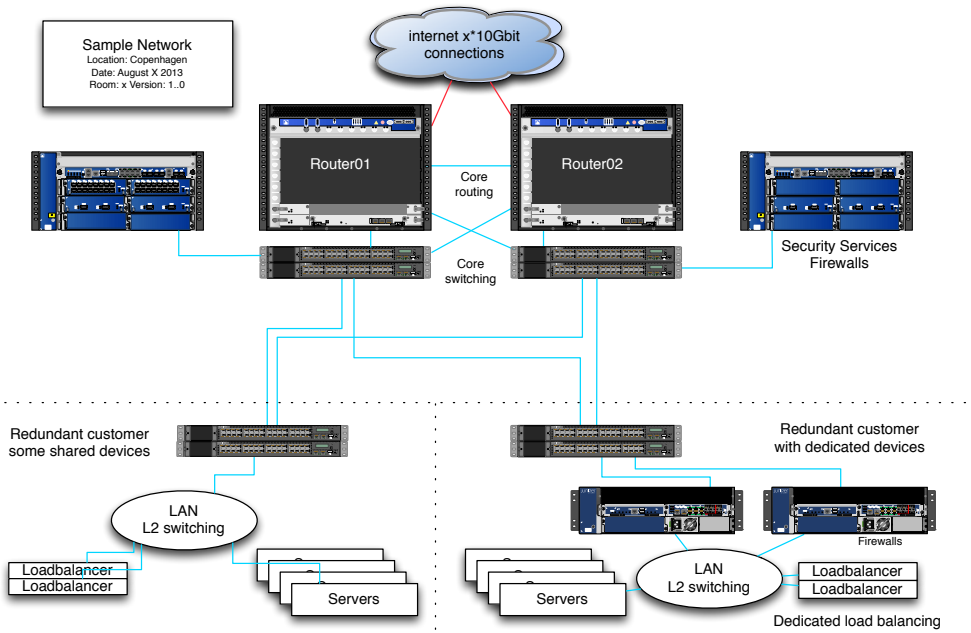


Now lets do the exercise

Try running a Docker container 20min

which is number **18** in the exercise PDF.

Firewall Flow Controls – *the firewall infrastructure*



Conclusion: Do as much as possible with your existing devices

Tuning and using features like stateless router filters works wonders

Firewalls and related issues

> In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.[2]

Source: Wikipedia

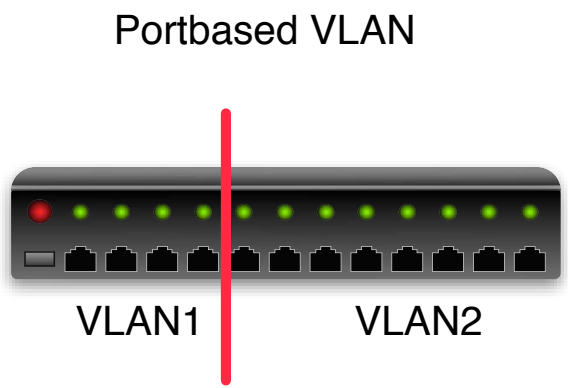
https://en.wikipedia.org/wiki/Firewall_(computing)

http://www.wilyhacker.com/ Cheswick chapter 2 PDF *A Security Review of Protocols: Lower Layers*

- Network layer, packet filters, application level, stateless, stateful

Firewalls are by design a choke point, natural place to do network security monitoring!

Together with Firewalls - Virtual LAN (VLAN)



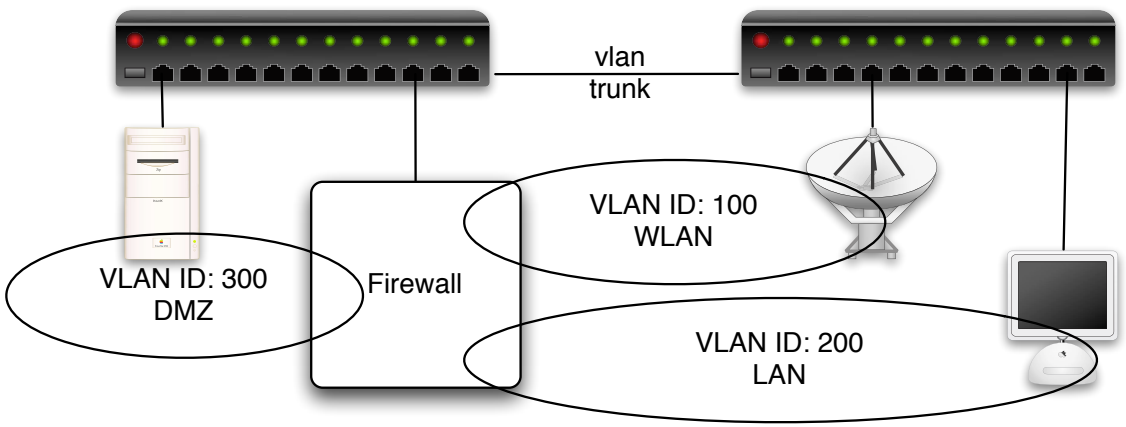
Managed switches often allow splitting into zones called virtual LANs

Most simple version is port based

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

Packets must traverse a router or firewall to cross between VLANs

Virtual LAN (VLAN) IEEE 802.1q



Using IEEE 802.1q VLAN tagging on Ethernet frames

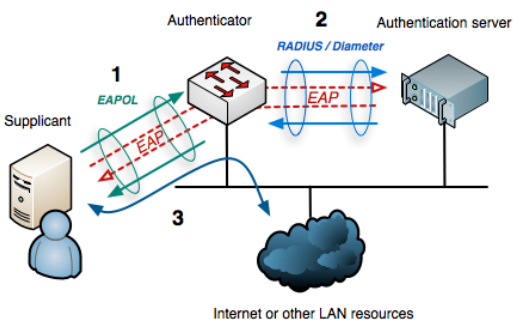
Virtual LAN, to pass from one to another, must use a router/firewall

Allows separation/segmentation and protects traffic from many security issues

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

Network Access Control – Connecting clients more securely

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



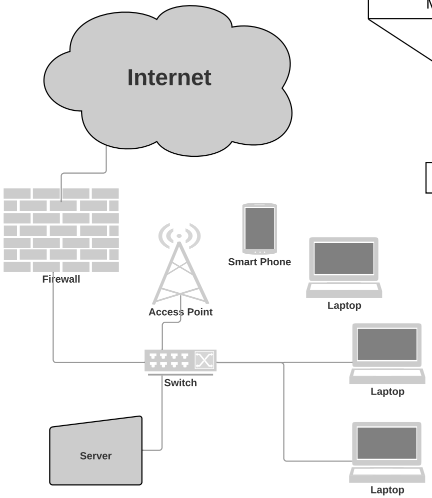
Authentication protocol ensures user validation before port access

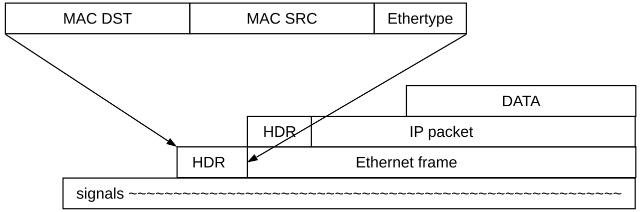
Can authenticate using username and then password or certificate

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

Protection, building secure and robust networks





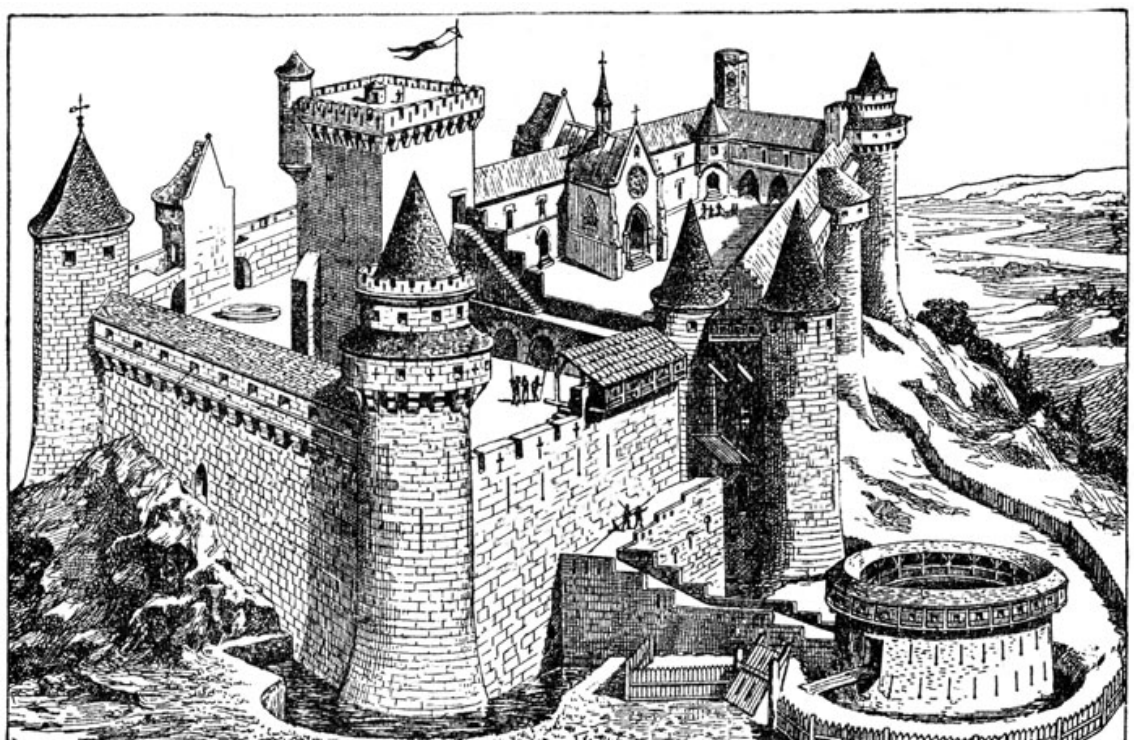
Ethernet frames contain packets

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

Example Internet IPv4 Packet Header

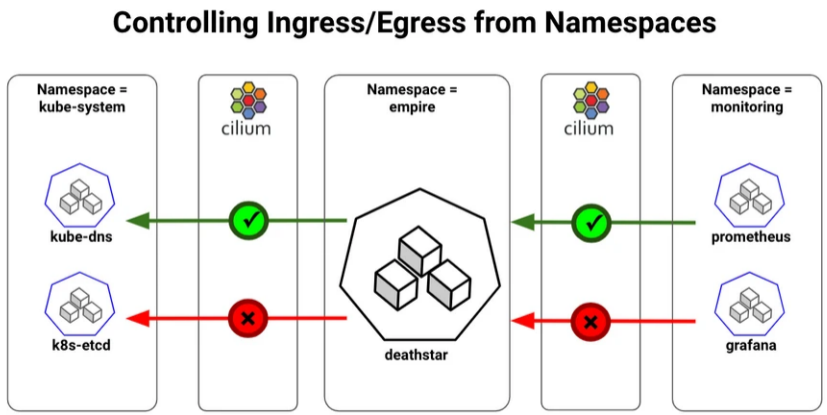
- We should prefer security mechanisms that does NOT require us to keep patching every month
- Can we change our networks to avoid this? Yes!

Defense in depth



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

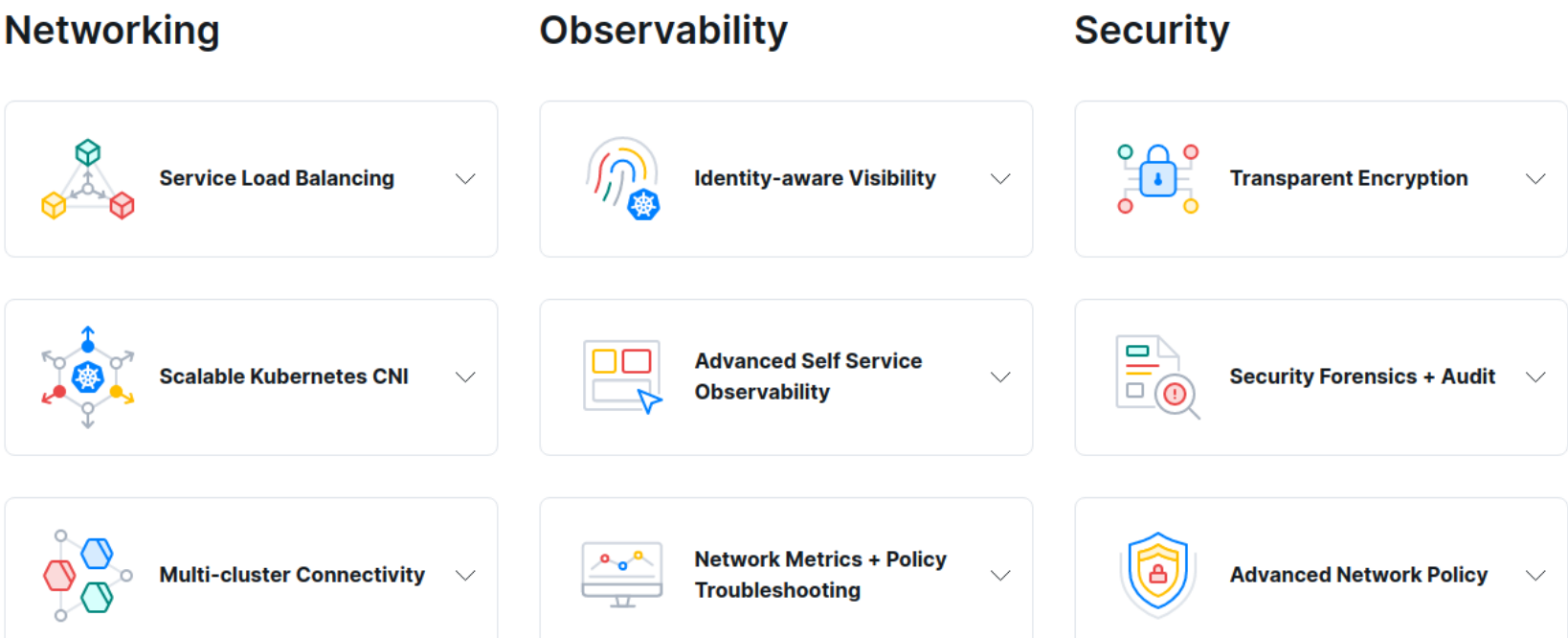
Cilium overview



Kubernetes provides Network Policies for controlling traffic going in and out of the pods. Cilium implements the Kubernetes Network Policies for L3/L4 level and extends with L7 policies for granular API-level security for common protocols such as HTTP, Kafka, gRPC, etc

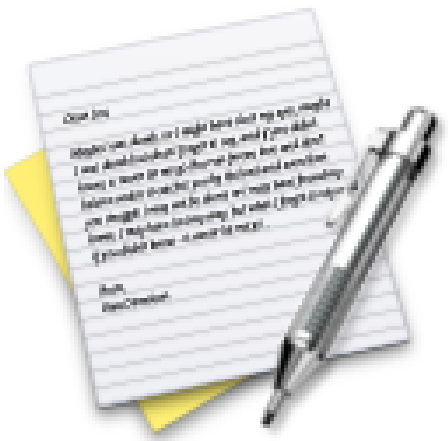
Source: picture and text from https://cilium.io/blog/2018/09/19/kubernetes-network-policies/

Security is more than blocking!



- A lot of features relate to *security*

Exercise

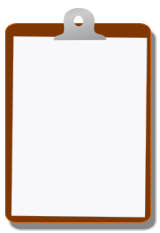


Now lets do the exercise

⚠ CIS Benchmarks teaser 30min

which is number **19** in the exercise PDF.

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools