

THINK LIKE A HACKER

JENS MYRUP PEDERSEN
AAU CYBER SECURITY NETWORK



Think like a hacker!

Purpose:

- You will learn about cyber attacks – what they are, who conduct them, and why?
- You will learn about different kinds of vulnerabilities.
- Focus on **hands-on** to really **understand what the different attacks mean**.
- Have **fun** and discuss cyber security with your fellow students 😊

During the next 10-15 minutes, each team is welcome to register (one lab per team + ghost labs) at upc.ntp-event.dk



Program

TALK

11.00 - Who are the attackers, what are their motivations and abilities?

HANDS-ON

12.00 – Introduction to the virtual labs. We will look at some basic security problems at websites, and we will use some basic tools (Wireshark and nmap).

13.00 -



The different attackers

- In order to efficiently prevent and detect attacks – and to minimize their impact – it is important to understand who the enemy is.
 - Motivations
 - Abilities
 - Resources available
- We can categorize the different attackers into the following groups (this is not an absolute science, and there are more groups, and different definitions):
 - Insiders
 - Cyber criminals
 - Script kiddies
 - Gray hats
 - Hacktivists
 - Nation states



Overview: Circumplex taxonomy

Insiders

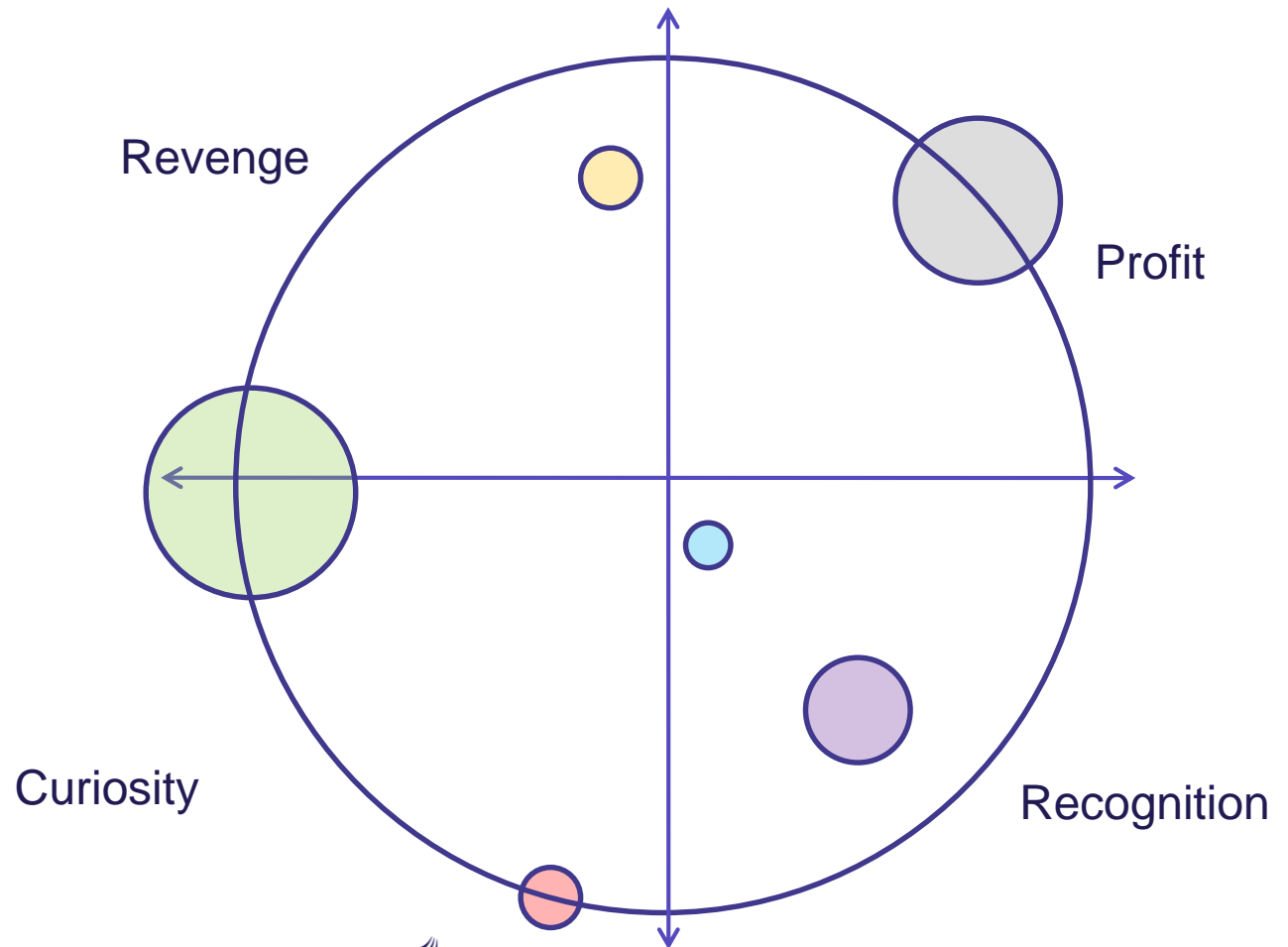
Cyber criminals

Script kiddies

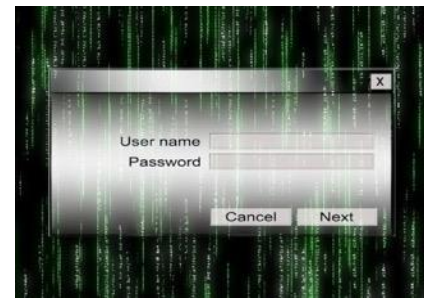
Gray hats

Hacktivists

Nation states



Insiders



- Insiders are trusted people, with malicious intent. They have privileged access and knowledge of relevant systems.
- Motivation: Insiders are often motivated by revenge, e.g. due to disagreements with employers. This can lead to sabotage. They can also be motivated by profit, e.g. by sharing or using data or knowledge available from the systems.
- Abilities: An insider can have extensive knowledge of the systems he is operating in, including knowledge of vulnerabilities. He might have the skills to hide his activities.
- Resources: Often working alone, but with access to system resources.

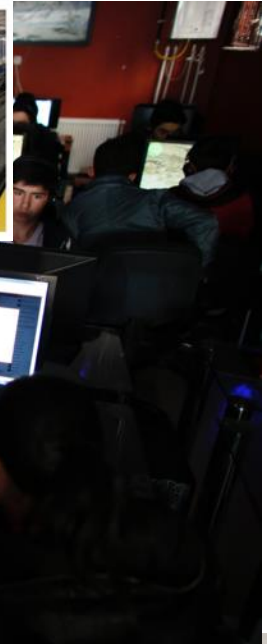


Cyber criminals (professionals)

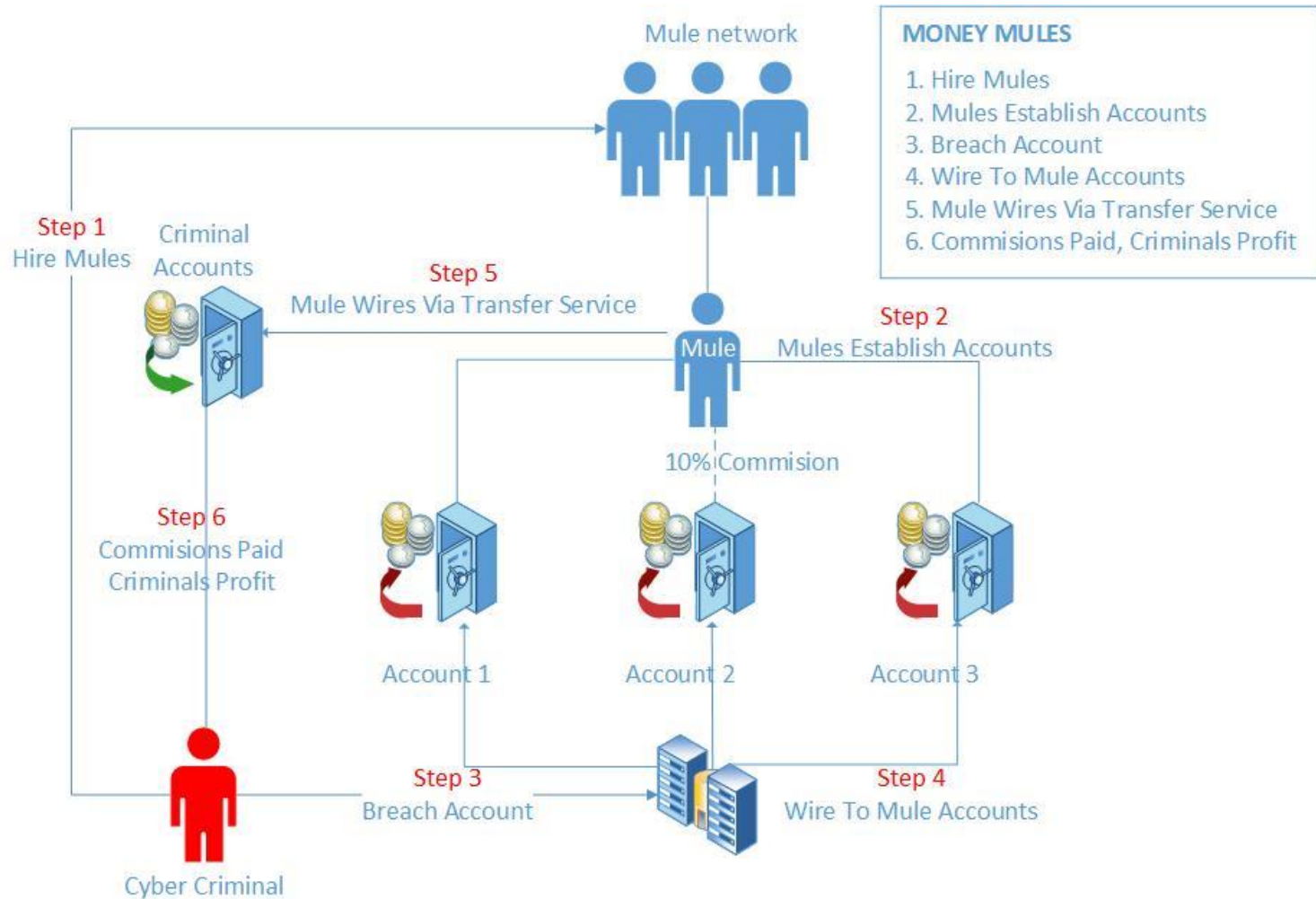
- Professional criminals are organised groups of hackers, with a strict business approach to attacks.
- Motivation: Financially motivated.
- Abilities: Professional criminals possesses a wide variety of technical skills and knowledge, and they are willing to recruit or hire people with additional competences – often through under-ground networks.
- Resources: Plenty of resources available in terms of money, equipment and manpower.



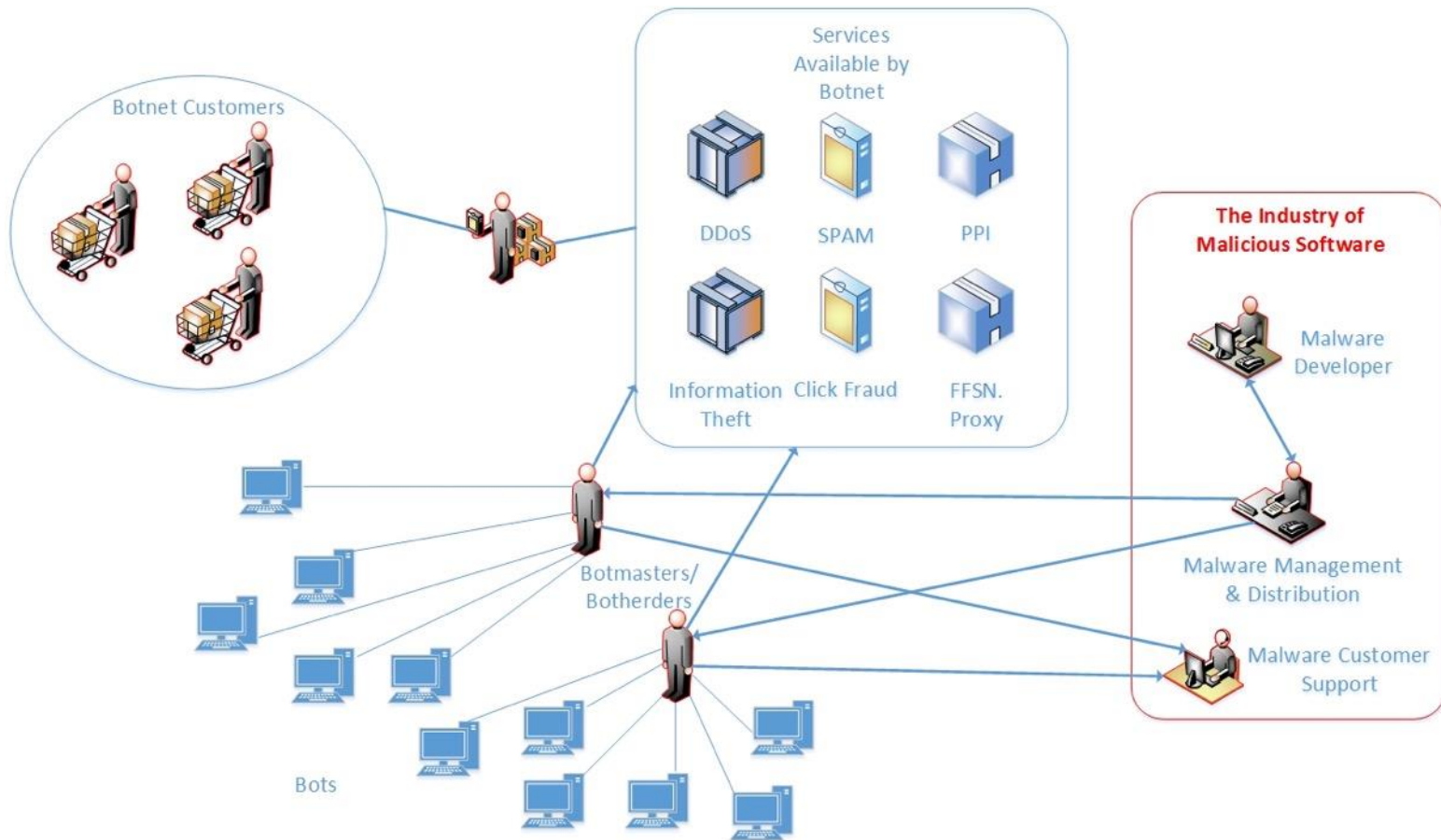
What cyber criminals are doing...



Based on well functioning markets...



The roles when operating a botnet



WHAT HAPPENS TO THE LAW WHEN THE LAW CANNOT BE ENFORCED?

You are alone in the trench.



Nation states

- Nation States or representatives hereof have been known to perpetrate everything from industrial espionage over military activities to devastating nationwide attacks in the cyber arena.
- Motivation: Many e.g. Revenge, intelligence or political and military gains.
- Abilities: Many Nation States have substantial presence in cyberspace and commands many highly skilled experts.
- Resources: Vast resources in terms of money, manpower, knowledge and intelligence, equipment.



Sabotage – Ukraine power grid



Advanced and targeted spear phishing

eea.grants2019@gmail.com

FeedBack on Review process in EEA GRANT (Estonia) 2019

To: Jens Myrup Pedersen,

Reply-To: eea.grants2019@gmail.com

archive 17 October 2019 at 14:51

Google Forms

Having trouble viewing or submitting this form?

FILL OUT IN GOOGLE FORMS

We've invited you to fill out a form:

FeedBack on Review process in EEA GRANT (Estonia) 2019

(1 minute survey)




Dear Reviewer,

Your name had been involved in the Review process of EEA Grant Call 2019 in Estonia.
As following (https://www.etag.ee/wp-content/uploads/2019/09/Peitensendd_reviewers_2019-1.pdf).

So at EEA Grant organization, we would like to invite you to participate in this short survey to help us improving the future calls process.

Thank You for considering your time

Institutions

1. Have you been contacted and invited to review any proposal by ETAG (Estonian Research Council) ? *

☐ Yes

☐ No

If Yes, did you involve to review your corresponding proposal?

☐ Yes

☐ No

How did you see the general framework of call and proposals?

☐ weak

☐ moderate

☐ strong

The Guideline provided by ETAG (Estonian Research Council) was useful? (<https://drive.google.com/open?id=14HNDTAMVYtYisAEcUqKSNPbJPHj3ggT...>)

☐ Yes

☐ No

Please write proposal title which had been assigned to you?

How you have evaluated the proposal in general (1-5)

☐ Weak 1

☐ less Moderate 2

☐ Moderate 3

☐ Above Moderate 4

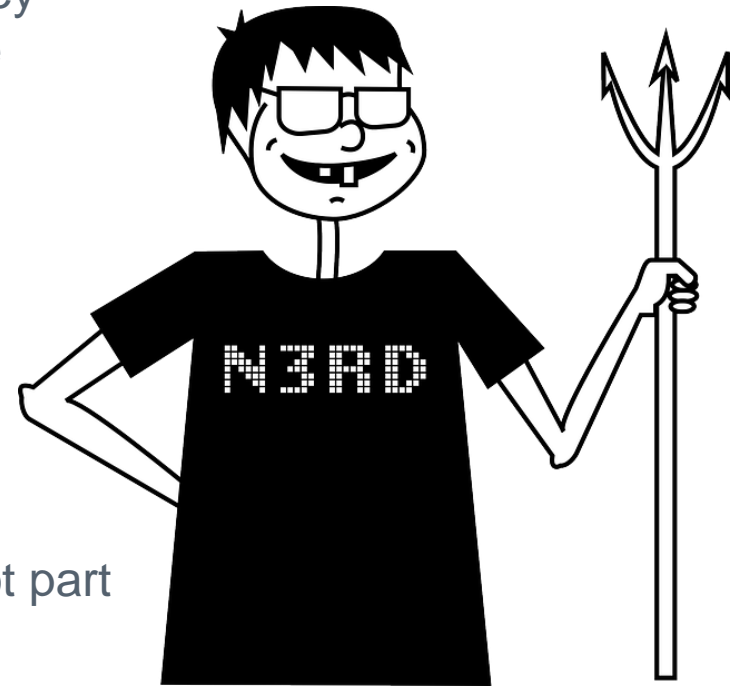
☐ Strong 5

If you have any comments to improve the process , please write below:



Script kiddies

- Script Kiddies are novices with low skills and limited understanding of technical consequences. They often use tools or scripts downloaded from the Internet.
- Motivation: Primarily curiosity, but can also be notirety.
- Abilities: Low technical competencies.
- Resources: Few resources, and most often not part of larger networks (i.e. they operate solo).



Gray hats

- Grey Hats are often skilful hackers with limited criminal intent.
- Motivation: Primarily curiosity, and unlikely to perpetrate sabotage.
- Abilities: This category often have very specialized technical skills, and an extensive exchange of information between them. As such they can be considered quite capable.
- Resources: Most work alone, despite of the knowledge exchange. But often they have skills and access to equipment.

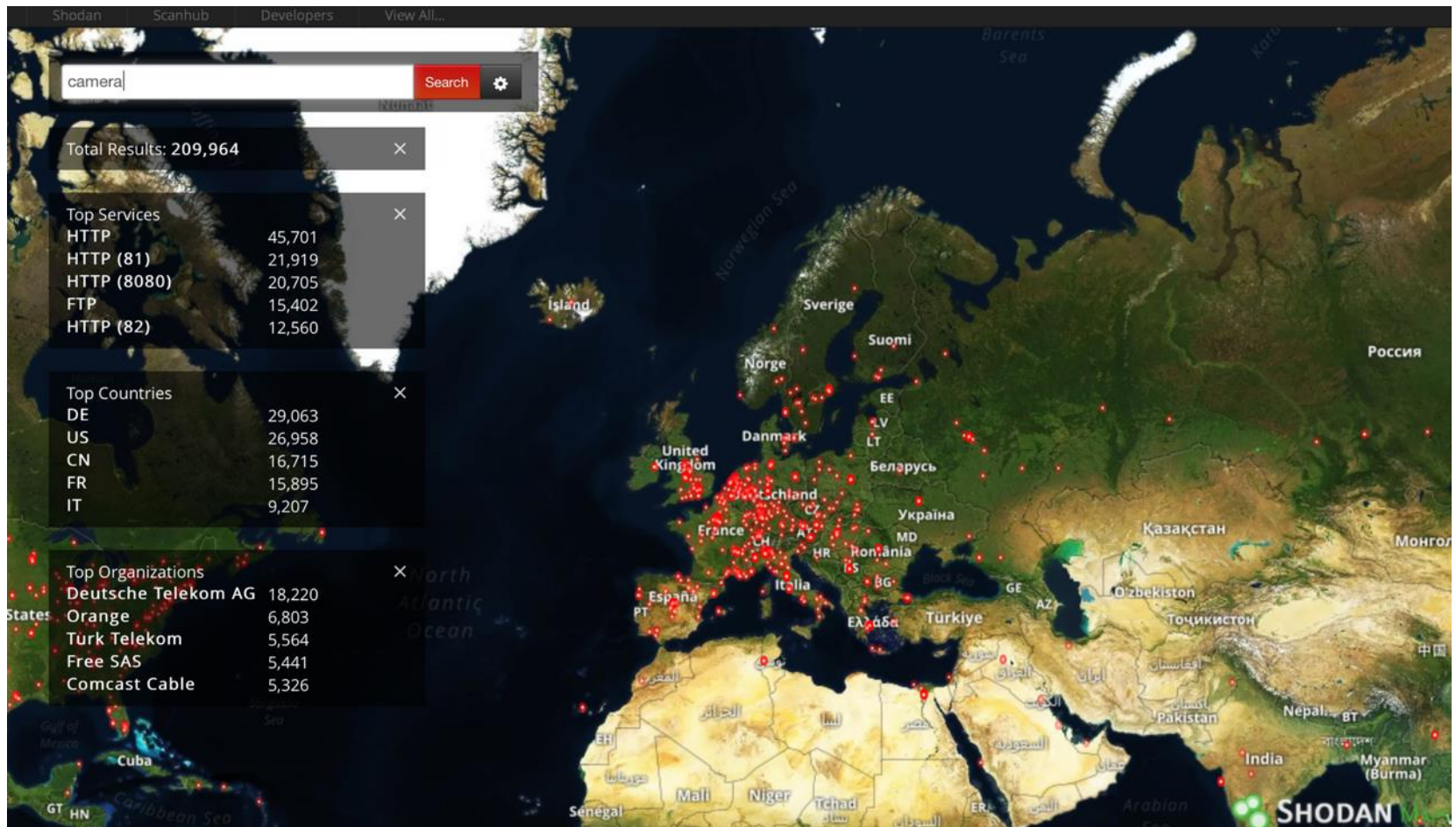


Hacktivists

- Hacktivists are often motivated by ideology and/or politics. They often operate in groups, with many and geographically distributed members with varying technical skills.
- Motivation: Often by ideology and/or political agendas. Revenge is not a common motivation in itself.
- Abilities: The members of hacktivist groups often have varying technical skills, but they usually have at least some highly skilled members.
- Resources: This varies a lot from group to group, but the larger groups (such as Anonymous) have a large geographical spread and plenty of manpower. Attack resources such as botnets might be available.



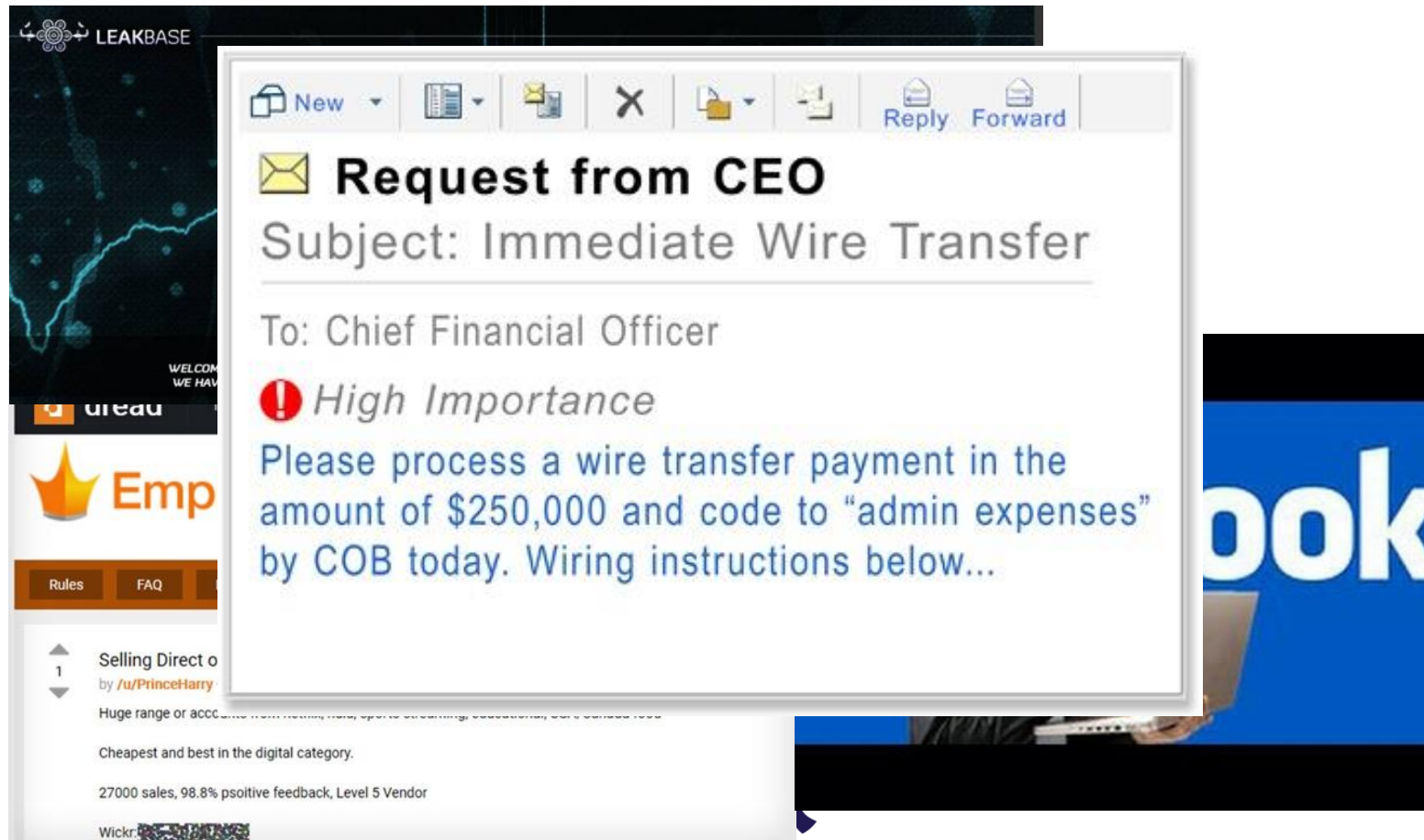
Observation 1: Plenty of tools – if flawed, it will be found...





Observation 2: Users are often “the weak link”, and they love to give away all their data in exchange for free wifi.

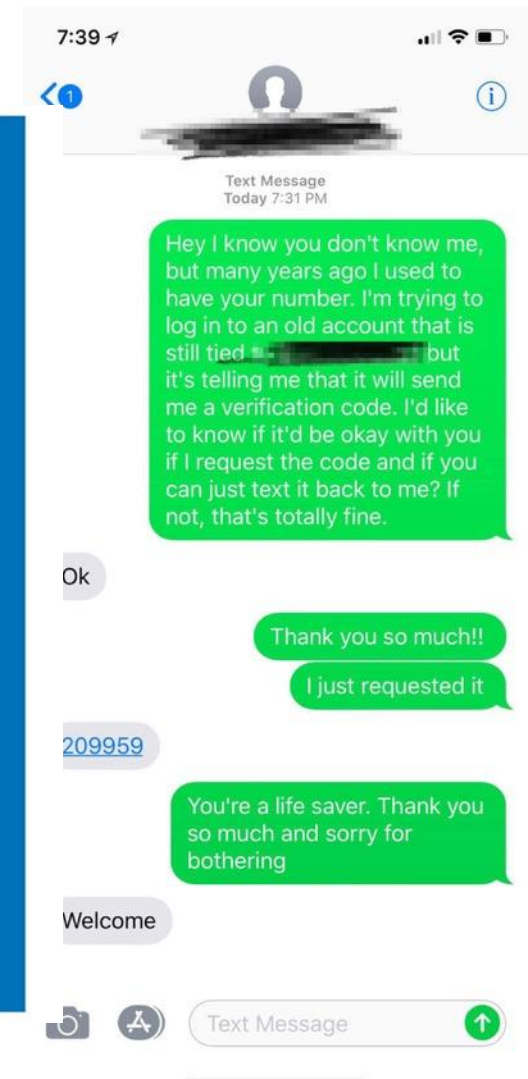
So we need technology to protect them...



The smart city with the not so smart citizen?



AALBORG UNIVERSITET



Observation 3: Machine learning is part of the solution

But it is not a magic tool, and ML algorithms can also be attacked.



What is a CTF?

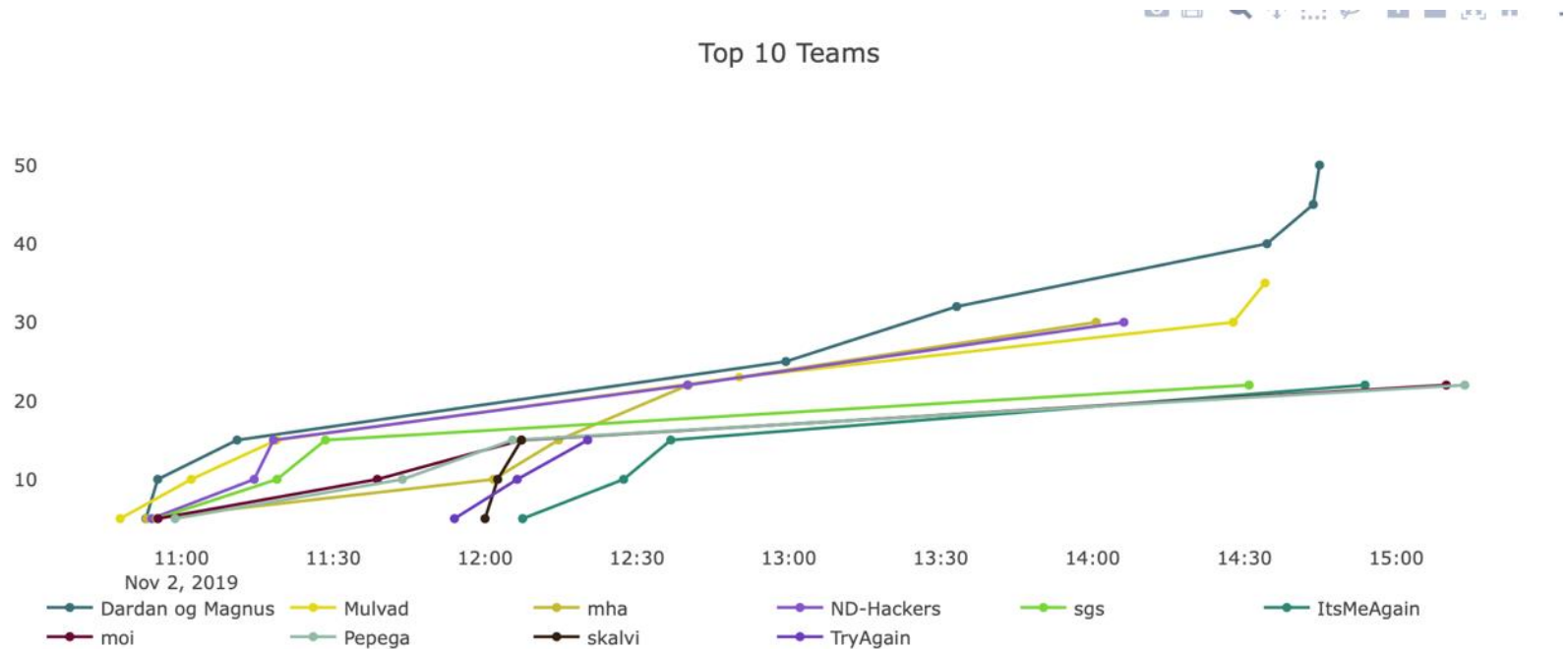
CTF = Capture The Flag

Basic idea is competition

Every flag gives a number of points

You can follow the teams on scoreboard...

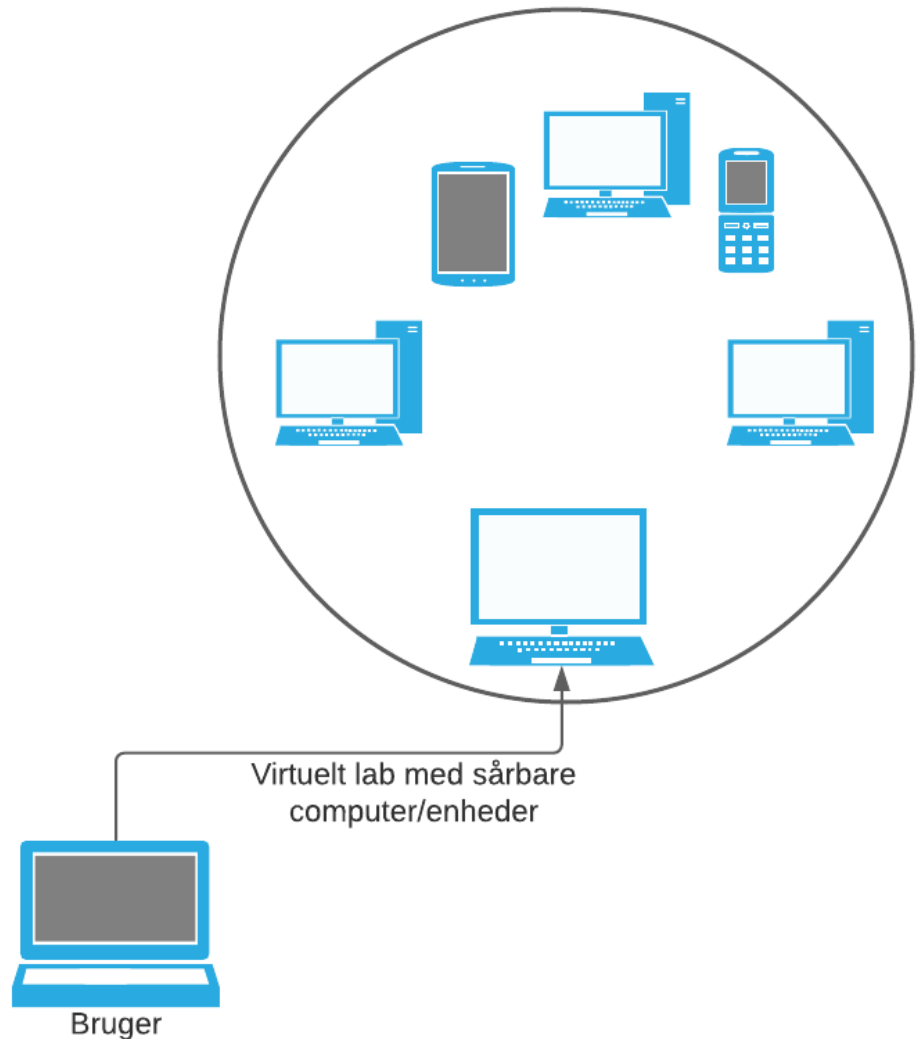
Most points win 😊



The virtual hacker lab

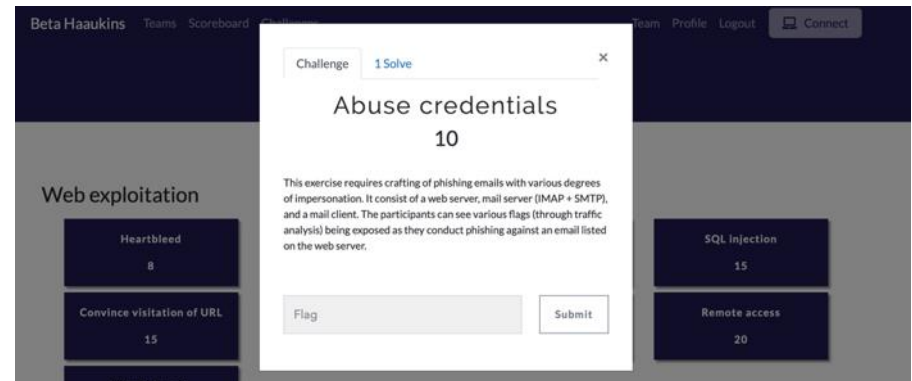
Start by registration at
happy42.haaukins.com

- Register as a **team** (NB: One lab access per team).
- Each team has their own **virtual lab**, with their own **devices/computers**.
- You might also create one or more "ghost teams", but their points do not count (so you need to solve them again as main teams). Flags and addresses are dynamic!
- Each computer has an **IP-address**, which is written A.B.C.D. Every letter represents 8 **bit**. In our case, A.B.C is the network address (fixed), while D is the address of the device itself.
- E.g. 192.168.1.4 – in this case 192.168.1 is common for the whole **network**, while "4" is specific to the **device**. Another device on the same network could be e.g. 192.168.1.17.



The virtual hacker lab

- Each **challenge** contains a **description**. You need to find a flag, i.e. a code which will give you points. A flag looks like HKN{123ABC}, where 123ABC is different from flag to flag.
- When you insert the flag in the "flag"-field, you get your **points** 😊.
- Sometimes it is challenging to copy from the virtual environment. Hint: **Copy** to a **browser**, and from there to the outside.
- OBS: When you are in the virtual environment, you have a **Linux keyboard!**
- **Let's go there in a bit!**



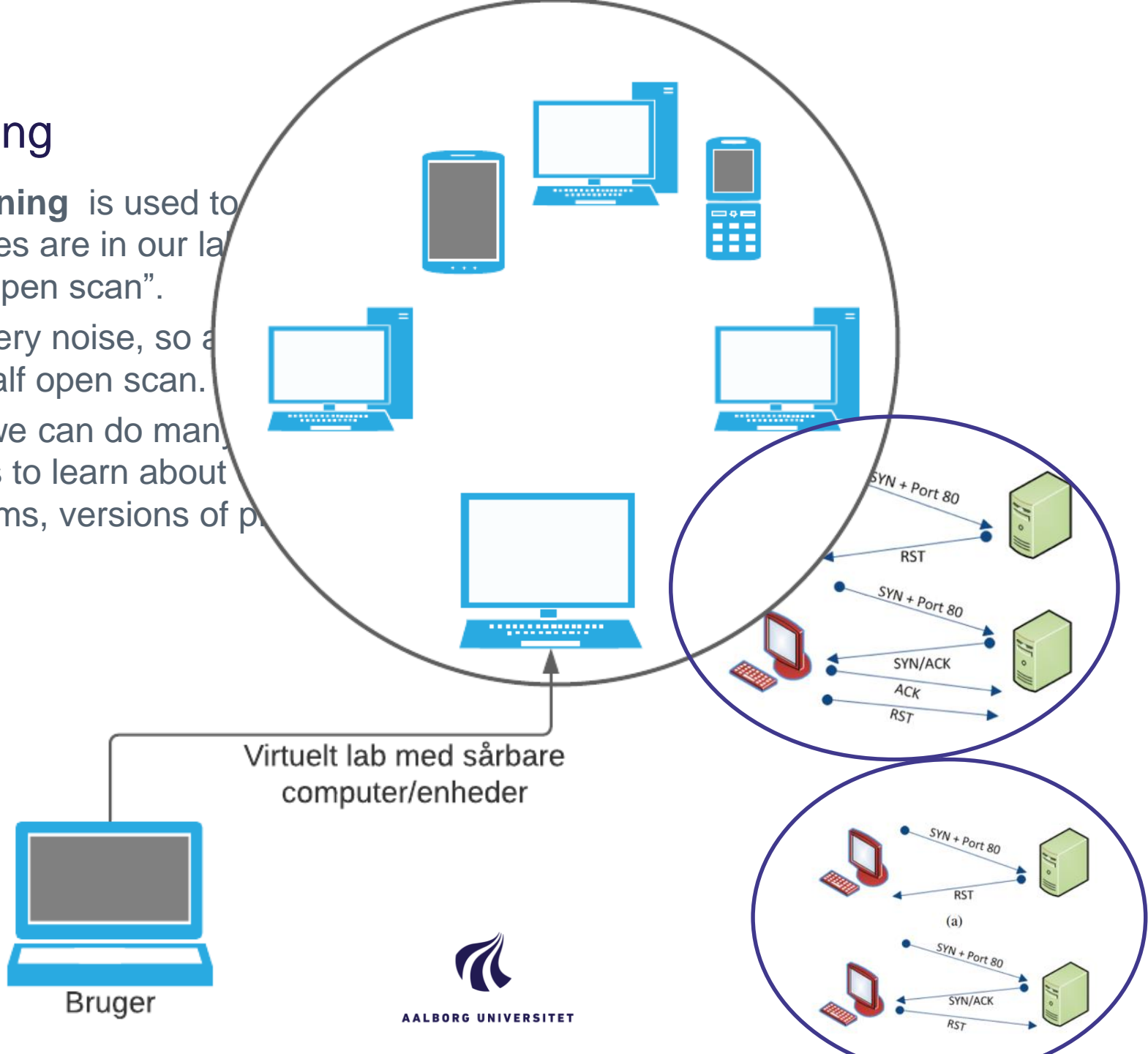
Some basic rules

- The main goal is learning, not competition 😊
- Remember to take breaks (10 min/hour)
- You are always welcome to move forward.
- **OBS – Telnet challenge – might need a reset once in a while...**
- If you finish all challenges, I will setup a new event for you with more. Do not worry 😊



Scanning

- **Scanning** is used to find out what devices are in our lab and what services they offer. This is the "open scan".
- It is very noisy, so we use a technique called the half open scan.
- And we can do many scans to learn about the systems, versions of protocols, etc.



Nmap and zenmap are super tools 😊

- De-facto standard network scanner.
- nmap → capable command line network scanning utility.
- zenmap → official Nmap Security Scanner GUI.
- nmap/zenmap offer:
 - Advanced techniques of mapping out networks: port scanning, OS detection, version detection, ping sweeps, etc.
 - Can be used to scan large networks.
 - Cross platform.
 - Free / code available with license.
 - Well documented and supported.

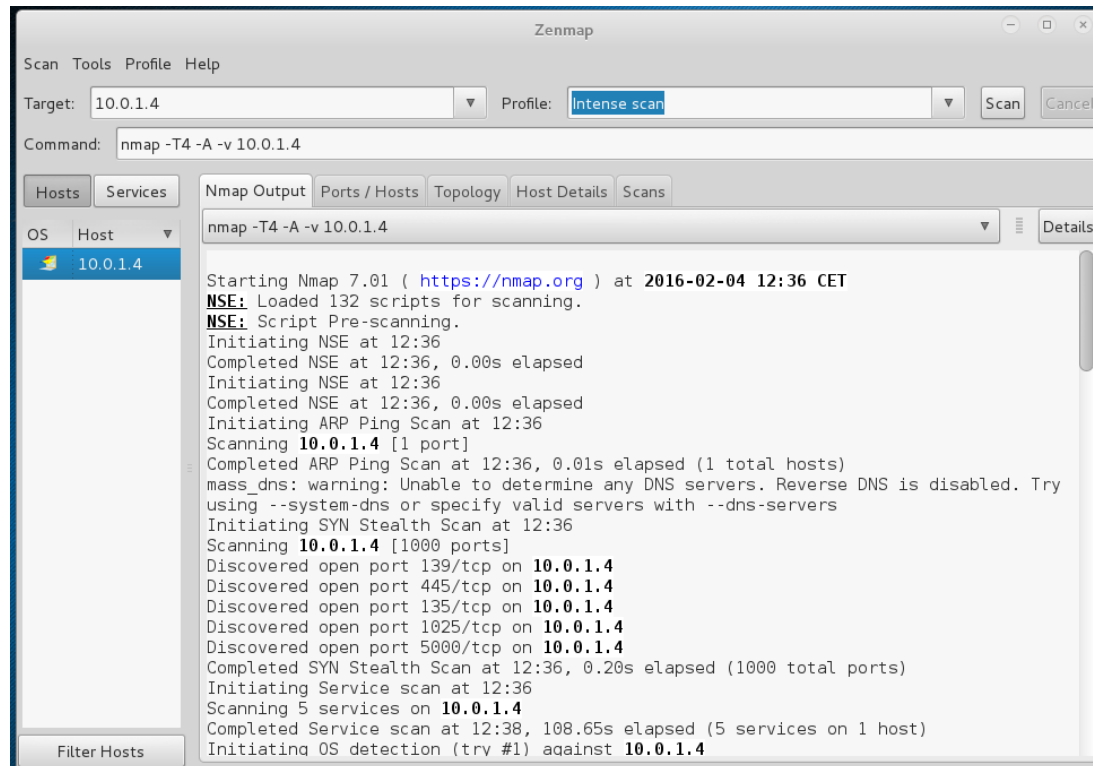


A few examples

- Ping sweep useful to identify targets and to verify rogue hosts.
 - Example:
 - – `nmap -v -sP 192.168.100.0/24`
 - `-sP` ping scan.
- Port scanning useful to identify active ports (services or daemons) that are running on the targets.
 - Example:
 - `nmap -v -sT 192.168.100.x`
 - `-sT` normal scan
 - `-sS` stealth scan
- `nmap 192.168.100.0-255`



Zenmap if you prefer the GUI



Let us try it out

- Open a terminal
- Use “ifconfig” command to find out what network and subnet you are at.
- Use nmap to find out which other computers are in your network (see previous commands). Try to use the command “nmap xx.xx.xx.00/24” (xx.xx.xx.00 is the network address), and then try to use “nmap -sP”. What is the difference?
- Use nmap to find out which operating system other computers are using (google how this is done).
- Remember to document your findings.
- Can you find a web server (that is only a web server – **running port 80?**)



Next Part – Monitoring!

- Wireshark – monitors everything that goes in and out of your interface
- In Wireless networks, monitor mode and promiscuous mode can be used to capture data traffic also to/from other hosts.
- So you can monitor all the traffic. In Haaukins, all traffic goes through your Kali machine!
- If traffic is unencrypted you can see everything. If it is encrypted? Well, then you need to work a little harder (depending on the encryption level).
- Now, let us try to find a login from a client to a webserver (http – not encrypted).
- And afterwards, let us see where we can use this login...



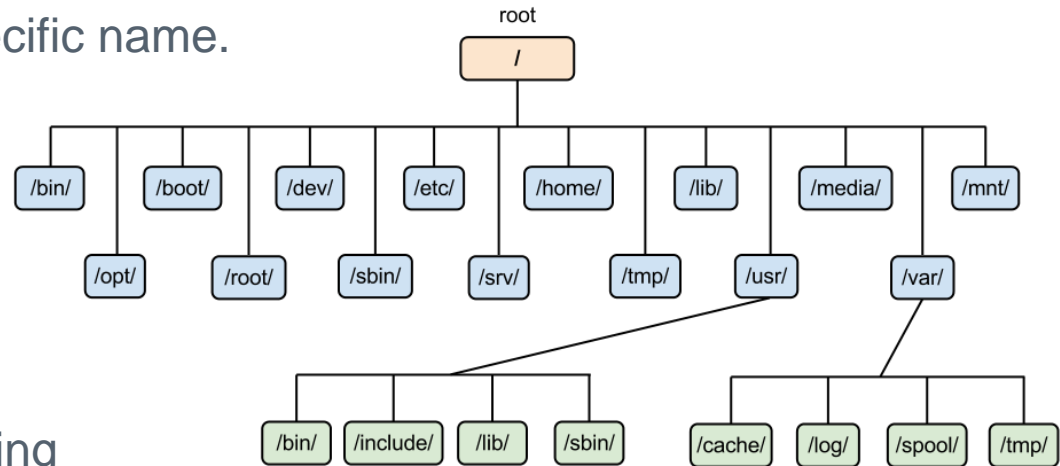
About bad websites – poor access control

- How well are *secret* informations protected? Microcms.com
- Is it access control, or are the informations really accessible, but just poorly hidden?
- And if there are hidden areas, is it possible to access these through a **qualified guess**? (Micro CMS URL). Or maybe you tell about it in **files for search engines**? (Micro CMS Robots)
- The first exercise with Micro CMS also include Cross-Site Scripting (XSS). For now we take the short version: XSS is about inserting **malicious code** into fields, which might be then hidden in e.g. data bases.
- Imagine you open a message on a dating website. Instead of a picture of your beloved one, malicious code has been uploaded – code that might open a pop-up message telling you that you have been hacked and need to pay in order to avoid having your data leaked.
- Can you find a place to inject such a script?
- OBS: Always "sanitise" input forms on websites!



The first challenges – intro session at 13.00!

- **List** content of a **folder (directory)**
- Read hidden files
- **Grab** lines with a specific content, using the grep command (for searching in files)
- **Find** files, e.g. files with a specific name.
- **Copy** files (cp)
- **Move** files
- Change **permissions** for files
- **Run executable** files



- Get a good Linux Understanding
- Don't be scared by the terminal
- We solve the challenges together
- Questions in the chat are most welcome!



The first challenges!

Forensics

List and read

1

Hidden files

2

Grabbing information

3

Find the file

4

Network scanning

5

Copying files

5

Moving files

6

Changing file/directory permissions

7

Follow Telnet stream

8

Telnet login

8

Executing custom binaries

8

Network sniffing

8



SQL Injections

In short: If input is not properly sanitised, and users can escape when inserting e.g. text in web forms. Small example from wikipedia with ' as escape character:

Imagine this line of code:

```
statement = "SELECT * FROM users WHERE name = '" + userName + "'";
```

Combined with this user input:

```
a';DROP TABLE users; SELECT * FROM userinfo WHERE 't' = 't
```

Be aware of also:

- Blind SQL injection
- Second order SQL injections (e.g. persistent)

Mitigation:

- Prevent: Pattern check, escaping
- Limit the damage: Database permissions



Password-cracking

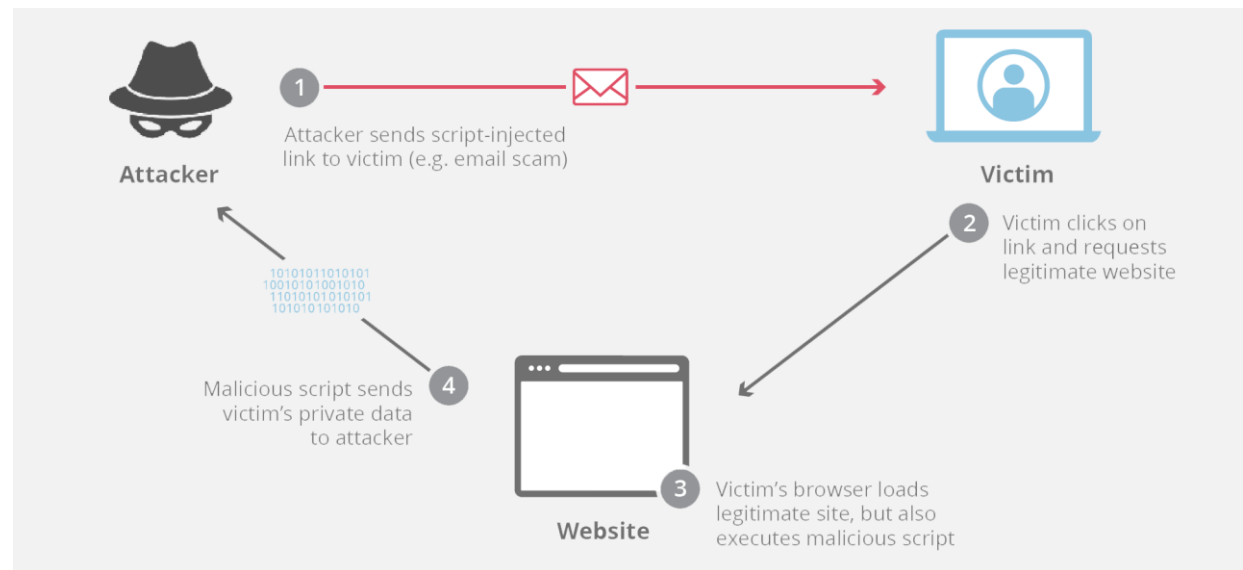
- Why is it important to choose passwords, which are:
 - Long
 - Contains numbers and letters
 - Are not used in multiple places?
- And why is it important to limit (or rate limit) the number of login attempts
- And to use **2-factor** authentication? (is this secure?)
- **Brute-force** attacks or **dictionary attacks!**
- We are looking at an **ftp-server**, and we can find the IP address because we know the server runs on **port 21**.
- We recommend to use a tool named **Hydra**
- We need to know the user name (or try to guess it) – any ideas?
- We also need to choose a **password-list** – go john?
- Google is always a big help 😊



Cross-site Scripting (XSS)

Reflected cross-site scripting.

- Here you use a link to an otherwise benign and trustworthy site for **executing** malicious code. The link could look like this: `http://legitimate-bank.com/index.php?user=<script>here is some bad code!</script>`
- Requires that the user presses the link.
- And that the page is vulnerable to XSS!
- Malicious code can be used to make the user e.g. install malware from another page, or send data to another page (usernames, passwords, **cookies**).



Cross-site Scripting (XSS)

Let us see what a cookie is

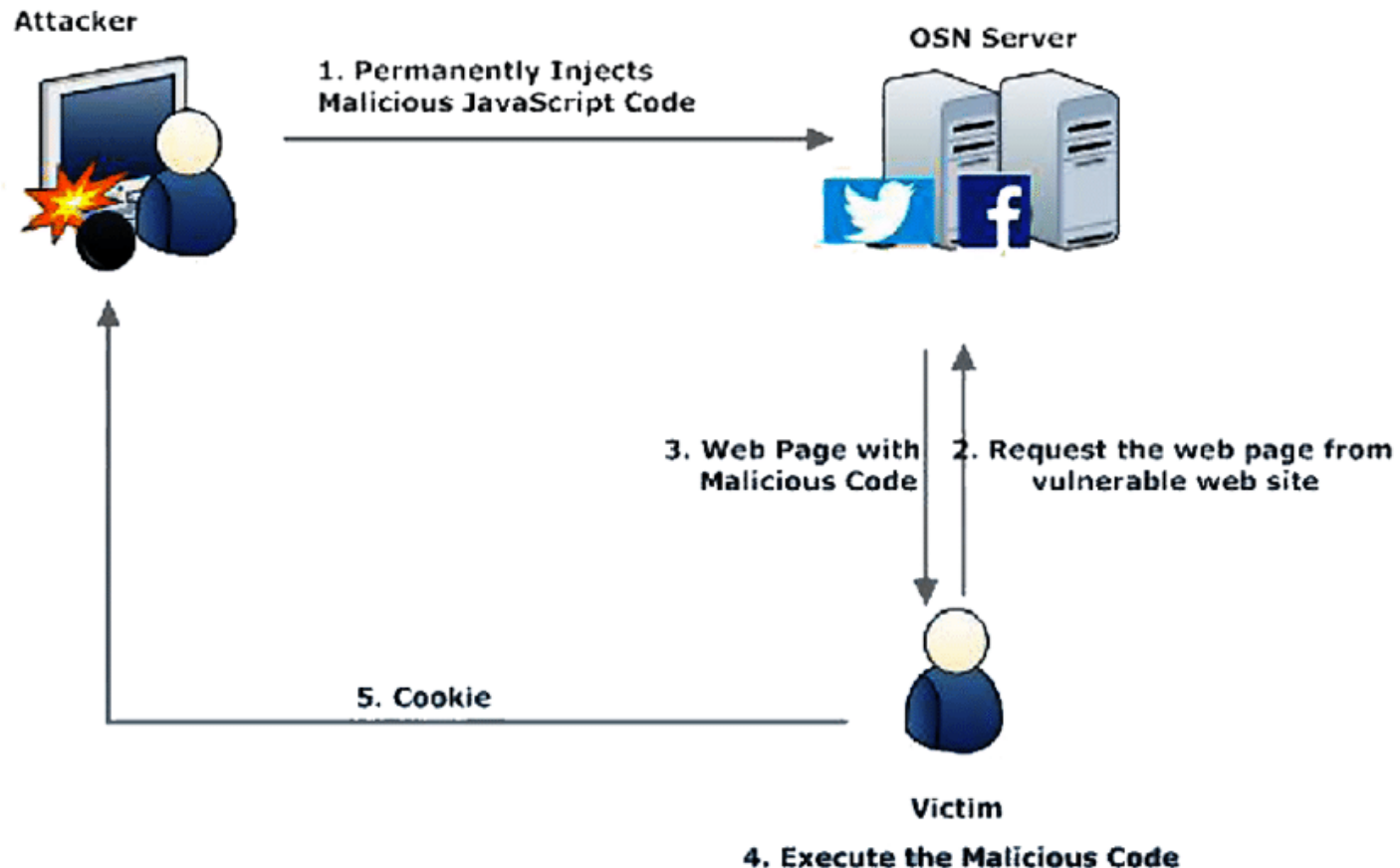
- When you visit a website, you will often be asked about cookies!
- Cookies are information, stored in your browser and related to the page you are visiting.
- This could be e.g. a webshop, where you put something in the shopping cart. When you come back the next day, the cookie is still set and therefore you can still see your goods in the shopping chart.
- But cookies are also used for massive surveillance.
- Or to keep track of your **authentication (session cookie)**. If it is possible to steal a session cookie, others might get access to your data.
- E.g. `<script>document.write('');</script>`



Cross-site Scripting (XSS)

Persistent cross-site scripting.

- Here, the malicious code is uploaded to a website, e.g. in a comments field, and so it remains on the server (as we saw in one of the first challenges).



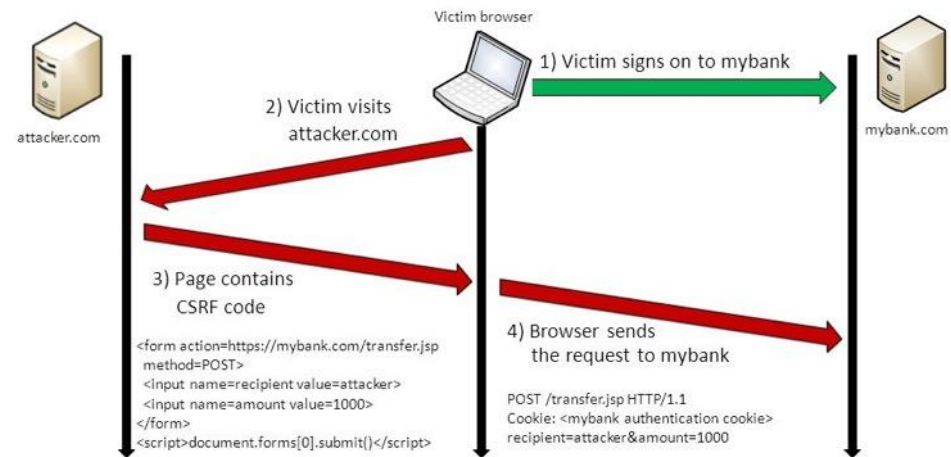
Cross-site Scripting (XSS)

- Let us see what we can do with <https://dogshare.com>.



Cross-site Request Forgery

- This time we are visiting **formalbank.com** in order to see if we can make other people transfer money to us. Bonusinfo:
- Everyone in the chat are logged in, and they will click on all links...
- OWASP: Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.
- Can be avoided using correct **authentication**, where it is not enough just to submit the request in a URL without additional verification from the server.
- Let's take a look at a Firefox feature before we start!



Program

TALK

10.00 - Who are the attackers, what are their motivations and abilities?

HANDS-ON

10.30-11.00 – Introduction to the virtual labs, including introduction to scanning and monitoring, broken access control.

11.00-11.50 Go hacking

11.50-12.00 SQL Injections

12.00-12.30 Go on hacking

12.30-13.00 Lunch

13.00-13.10 How easy it is to crack passwords

13.10-14.00 Go on hacking the FTP Server

14.00-14.10 Cross-Site Scripting

14.10-15.00 More hacking

15.00-15.10 Cross-Site Request Forgery

15.10-15.40 Hack harder

15.40-15.50 Session Hijacking: Steal the cookies

15.50-16.45 Last hacking

16.45-17.00 Final chance for questions, and round-off



Steal the cookie!

Welcome to the cookie factory, cookie-factory.com!

In this particular example it is about an attacker getting access to the contents of the session cookie, and being able to manipulate it to gain access to a company owners account which in theory would have elevated privileges.

This is possible because the Userid is incremented every time a new user is created. Therefore it is very easy to predict the number sequence and find out which Userid has the elevated privileges.

No more hints for this one – bon appetite!



Stay Secure!



AALBORG UNIVERSITET