



# Haukins

A Highly Accessible and Automated Virtualization Platform for Security Education

Presentation for BlackHat Europe 2019

Ahmet Türkmen, Kaspar Hageman, Jens Myrup Pedersen

# How to get 50 high school students to start hacking in 5 minutes?



# How to get 50 university students to start hacking in 5 minutes?

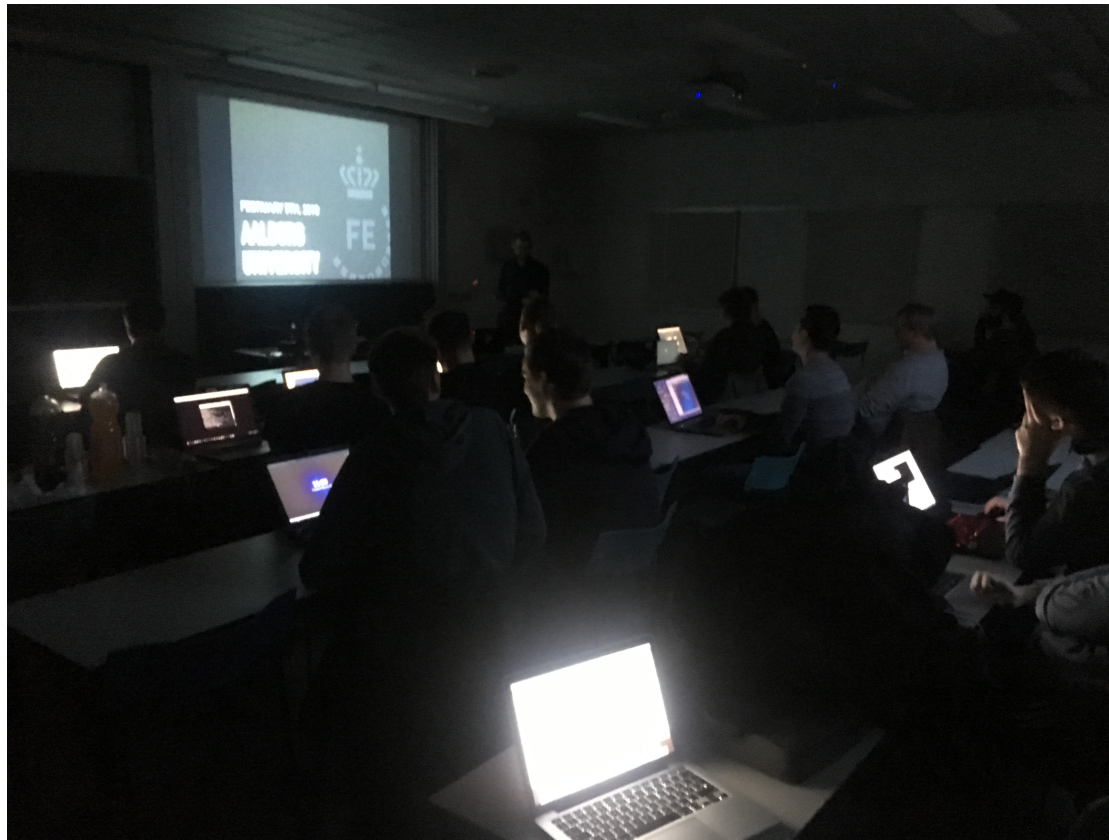




# How to get 50 software developers to start hacking in 5 minutes?

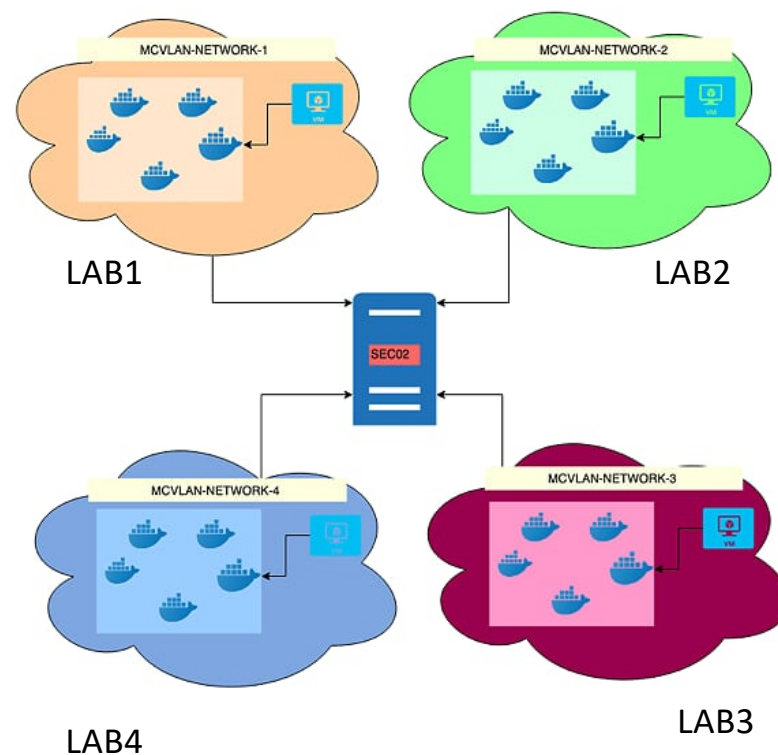


How to get 50 software developers to start hacking in 5 minutes? (for free)



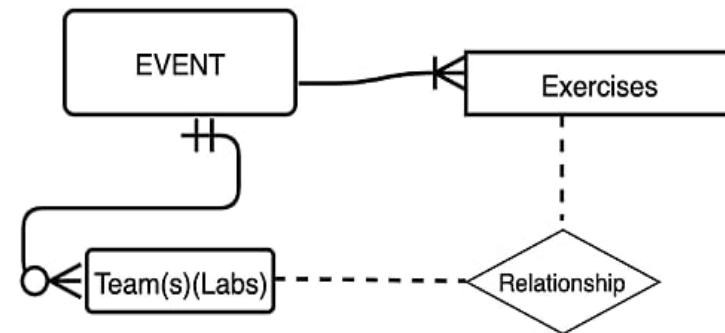
# Haaukins - Virtualized environment

- Kali Linux and virtual labs from a browser
- One lab per team
- Fully automated setup
- User registration: New lab is setup
- Open source for the benefit of everyone



# Step 1: Define an event

- A simple command line!
- Name of event
- Number of teams (max)
- Which challenges
- We are up running



# Step 2: Teams can register



[Beta Haukins](#) [Teams](#) [Scoreboard](#) [Challenges](#) [Register](#) | [Login](#)

Register

Team Name

Email

Password

Team Size

Technology Interest

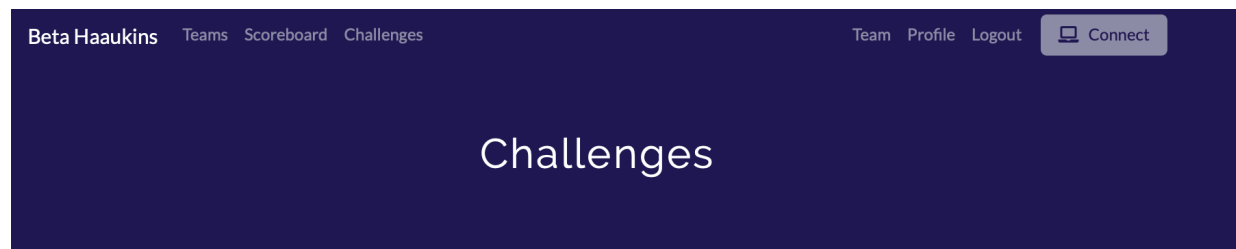
Hacking Experience (in total)

☒ I hereby declare that I understand and agree that (1) my activity (i.e. key presses and mouse clicks) on the platform is being monitored, (2) the data is anonymised and stored securely and (3) the raw data will NOT be shared with other parties and may be shared within the scientific community in a processed form.

Submit



# Step 3: See challenges (CTFd) – and connect



Network scanning 5	Network sniffing 5	Web server login 5	Heartbleed 8
Abuse credentials (phishing) 10	Vulnerability exploitation 10	Cross-site Request Forgery 12	Man in the middle 15
SQL injection 15	Convince visitation of URL (l 15	Impersonate colleague (phis 15	Cross-site scripting 15
Hijack domain (phishing) 20			

# Read about what to do...



Beta Haaukins

Teams

Scoreboard

Challenges

Team

Profile

Logout

Connect

Challenge

1 Solve

Abuse credentials

10

This exercise requires crafting of phishing emails with various degrees of impersonation. It consist of a web server, mail server (IMAP + SMTP), and a mail client. The participants can see various flags (through traffic analysis) being exposed as they conduct phishing against an email listed on the web server.

Flag

Submit

Web exploitation

Heartbleed

8

Convince visitation of URL

15

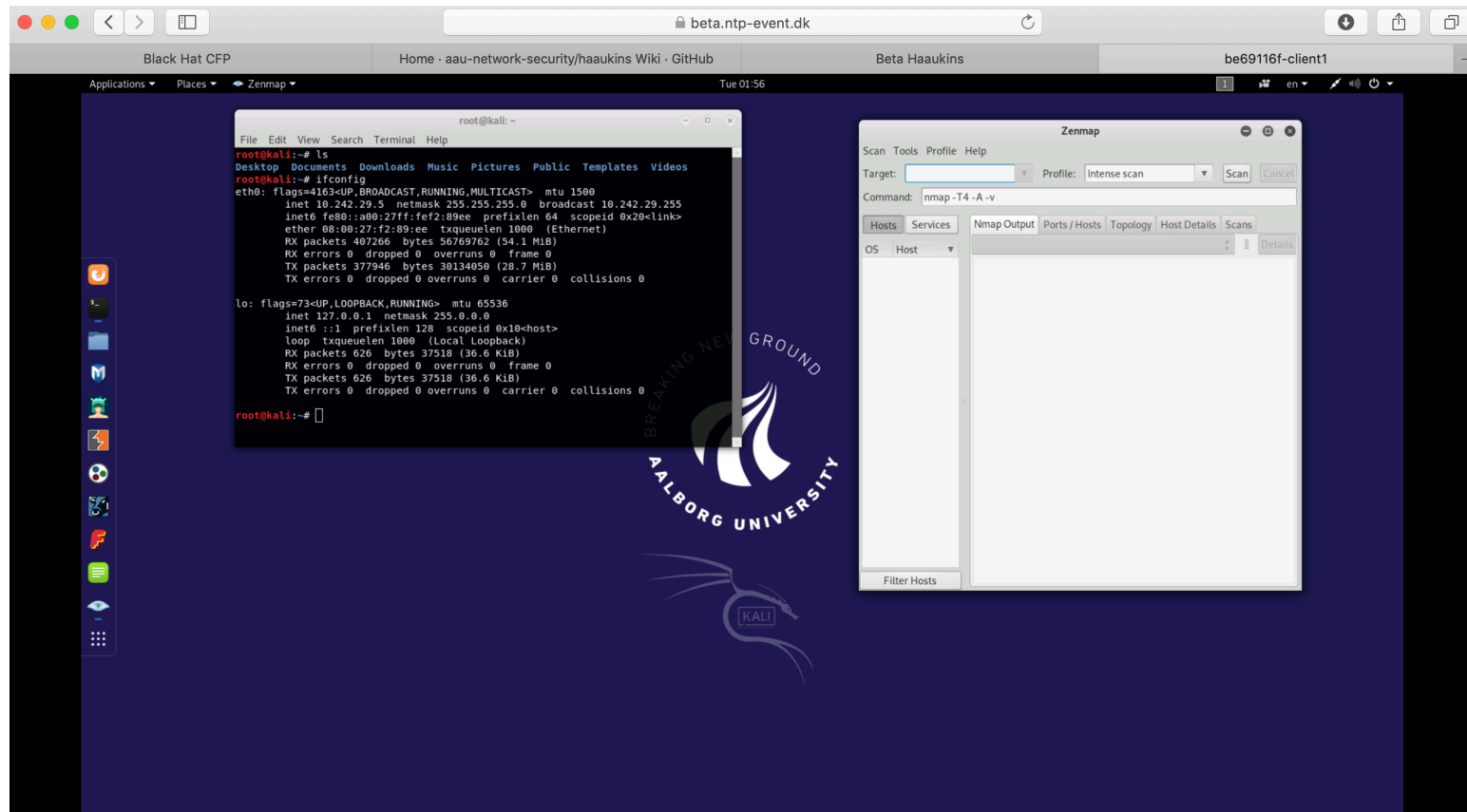
SQL injection

15

Remote access

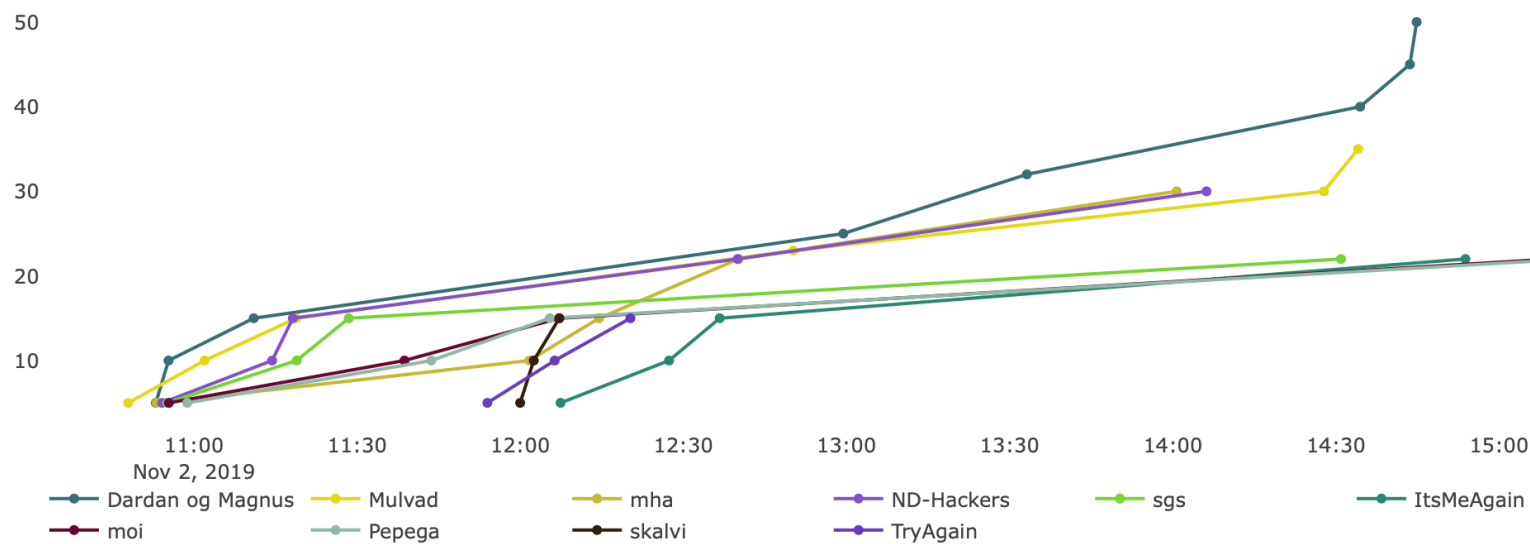
20

# Step 5: Start finding flags...



# Step 5: Follow the teams... (CTFd)

Top 10 Teams



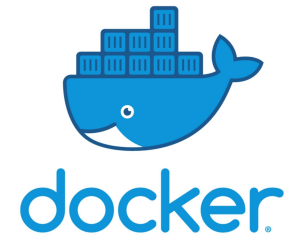
# Composed of :



- Kali
- Parrot
- Customized VMs



- Manages Docker and VM
- Creates Virtualized environment
- All actions in Haaukins managed by Go



- Training challenges
- CTFd
- Apache Guacamole





# Training challenges

cat\diff	Very Easy	Easy	Medium	Difficult	Very Difficult
Binary		<ul style="list-style-type: none"> <li>• Privilege Escalation</li> </ul>	<ul style="list-style-type: none"> <li>• <i>*Buffer overflow</i></li> </ul>		
Cryptopgraphy		<ul style="list-style-type: none"> <li>• Crypto JS Client</li> </ul>			
Forensics	<ul style="list-style-type: none"> <li>• Network Scanning</li> <li>• Network Sniffing</li> </ul>	<ul style="list-style-type: none"> <li>• Web Server Login</li> <li>• FTP Server Login 1/2</li> <li>• Vulnerability Explotation</li> </ul>			<ul style="list-style-type: none"> <li>• Man in the middle</li> </ul>
Reverse Engineering	<ul style="list-style-type: none"> <li>• Weird Code</li> </ul>	<ul style="list-style-type: none"> <li>• <i>* Debugger</i></li> </ul>			
Web Explotation	<ul style="list-style-type: none"> <li>• Micro CMS XSS</li> <li>• Micro CMS URL</li> </ul>	<ul style="list-style-type: none"> <li>• SQL Injection</li> <li>• Heart bleed</li> <li>• Abuse credentials</li> </ul>	<ul style="list-style-type: none"> <li>• CSRF</li> <li>• XSS</li> <li>• Convince visitation of URL</li> <li>• Impersonate colleague</li> </ul>	<ul style="list-style-type: none"> <li>• Joomla UARCE</li> </ul>	<ul style="list-style-type: none"> <li>• Web admin UARCE</li> <li>• Hijack Domain</li> </ul>

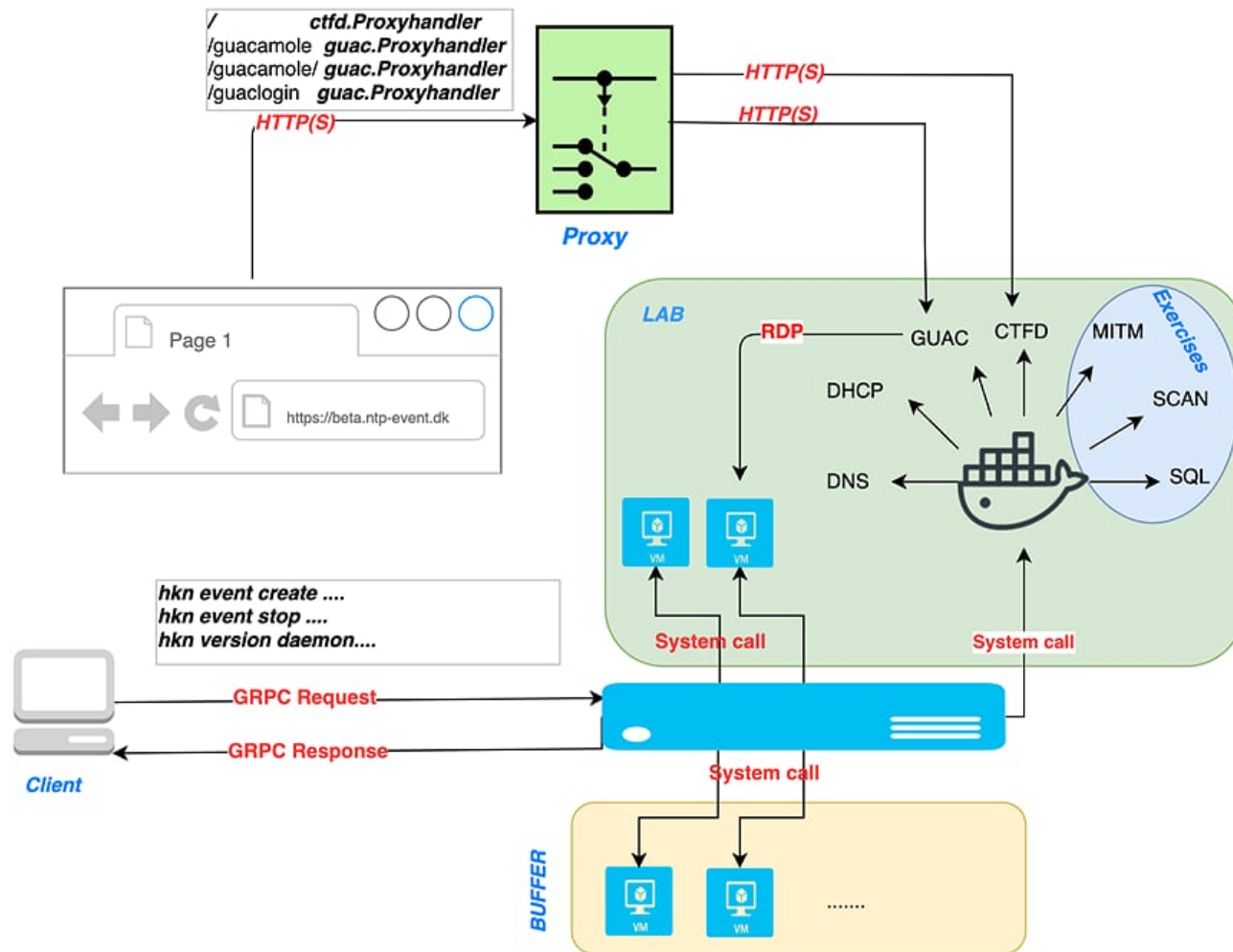




# Haukins – what is so special?

- Highly automatised - setup labs and events with one command line!
- Easy to get started for users - preparing for more prof. tools.
- Challenges focused on learning step-by-step
- Dynamic flags
- Randomization of e.g. IP addresses
- Open-source and offered free of charge to universities
- Near future: Cloud-based version, more advanced network setups.

# Internal Structure

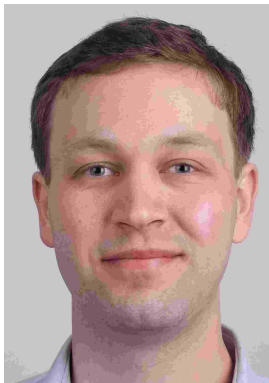


# Events: Hack with Central Bank of DK....



# Haaukins – the team

- Founders: Kaspar, Thomas, Jens.
- Developers: Gian, Ahmet
- Student helpers: Johan (and more)





See you on



<https://cybertraining.dk>

<https://github.com/aau-network-security/haaukins>

THANK YOU FOR YOUR ATTENTION