


Welcome to

9. Breaking Out

KEA Kompetence Computer Systems Security 2023

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

Slides are available as PDF, kramse@Github 
9-breaking-out.tex in the repo security-courses

Goals for today



Today's goals:

- Photo by Thomas Galler on Unsplash

Plan for today

Subjects

- Exercises

MLSH 11: Kernel Hardening and Process Isolation

DSH chapter 16: Vulnerability Management

Browse: Using Memory Errors to Attack a Virtual Machine paper, An Experimental Study of DRAM Disturbance Errors, Exploiting the DRAM rowhammer bug to gain kernel privileges https://en.wikipedia.org/wiki/Row_hammer

An availability policy ensures that a resource or service can be accessed in some way in a timely fashion

Often expressed as *quality of service*

Denial of service occurs when this resource or service becomes unavailable

Fairness and starvation

Fairness policy prevents starvation, often rephrased as - process will make progress

If one process gets all resources, memory, cpu, network the others will starve - not have enough resources to progress

Compare to old operating systems Windows 3 / Mac OS 9

Cooperative multitasking vs pre-emptive multitasking

Availability and Network flooding attacks

- SYN flood is the most basic and very common on the internet towards 80/tcp and 443/tcp
- ICMP and UDP flooding are the next targets
- Supporting literature is TCP Synfloods - an old yet current problem, and improving pf's response to it, Henning Brauer, BSDCan 2017
- All of them try to use up some resources
- Memory space in specific sections of the kernel, TCP state, firewalls state, number of concurrent sessions/connections
- interrupt processing of packets - packets per second
- CPU processing in firewalls, pps
- CPU processing in server software
- Bandwidth - megabits per second mbps

There is a presentation about DDoS protection with low level technical measures to implement at

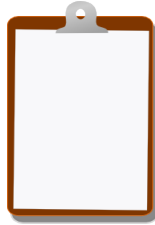
<https://github.com/kramse/security-courses/tree/master/presentations/network/introduction-ddos-testing>



Now lets do the exercise

i SYN flooding 101 - 60min

which is number **37** in the exercise PDF.



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