Welcome to

# 2. Enterprise Attacks

## KEA Kompetence Computer Systems Security 2025

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

Slides are available as PDF, kramse@Codeberg

2-overview-enterprise-attacks.tex in the repo security-courses

# Goals


- Talk about vulnerabilities
- What are some examples
- How to find them, and find them in your networks
- Categories for attacks with Mitre ATT&CK

Photo by Thomas Galler on Unsplash

# Plan

## Subjects

- Get an idea of the MITRE ATT&CK framework
- Do a little hacking using Kali and Metasploit

## Exercises

- Port scan intro with Nmap

# Reading Summary

Read ATT&CK 101 Blog Post
https://medium.com/mitre-attack/att-ck-101-17074d3bc62

and browse MITRE ATT&CK web site
https://attack.mitre.org/

MSFT Hardware Security and Operating System Security

# layers of security enabled by default

> Windows 11 is designed with **layers of security enabled by default**, so you can focus on your work, not your security settings.
>
> Out-of-the-box features such as credential safeguards, malware shields, and application protection led to a reported 58% drop in security incidents, including a 3.1x reduction in firmware attacks.

Source: Windows 11 Security Book: Powerful security by design (MSFT), Microsoft 2023

- Nice quote, but how did they do it?!
- Just switching your app to a newer release of operating systems typically increase security
  Modern OpenBSD, Linux, FreeBSD, they all have more security features too
- Security by design and default – both properties we would like to see when selecting systems

# hardware and software work together

> In Windows 11, **hardware and software work together** to shrink the attack surface, protect system integrity, and shield valuable data.

Source: Windows 11 Security Book: Powerful security by design (MSFT), Microsoft 2023

Same goes for other operating systems

- A modern OS use special bits in the CPU
- A modern 64-bit architecture uses security aware memory management
- TPM chips are hardware devices with special properties
  https://en.wikipedia.org/wiki/Trusted_Platform_Module

# Hardware-enforced stack protection

> Hardware-enforced stack protection integrates software and hardware for a modern defense against cyberthreats like memory corruption and zero-day exploits. Based on Control- flow Enforcement Technology (CET) from Intel and AMD Shadow Stacks, hardware-enforced stack protection is designed to protect against exploit techniques that try to hijack return addresses on the stack.

Source: Windows 11 Security Book: Powerful security by design (MSFT), Microsoft 2023

- We will go deeper into buffer overflows and *stack protection* later

# System security: Trusted Boot

Trusted Boot (Secure Boot + Measured Boot) Windows 11 requires all PCs to use **Unified Extensible Firmware Interface (UEFI)'s Secure Boot** feature. When a Windows 11 device starts, Secure Boot and Trusted Boot work together to **prevent malware and corrupted components from loading**. Secure Boot provides initial protection, then Trusted Boot picks up the process. Secure Boot makes a safe and trusted path from the Unified Extensible Firmware Interface (UEFI) through the Windows kernel's Trusted Boot sequence. Malware attacks on the Windows boot sequence are blocked by the signature-enforcement handshakes throughout the boot sequence between the UEFI, bootloader, kernel, and application environments. To reduce the risk of firmware rootkits, **the PC verifies that firmware is digitally signed as it begins the boot process**. Then Secure Boot checks the **OS bootloader's digital signature** as well as all code that runs prior to the operating system starting to ensure the **signature and code are uncompromised and trusted by the Secure Boot policy.**

Source: Windows 11 Security Book: Powerful security by design (MSFT), Microsoft 2023

# Trusted Computing Base

> The trusted computing base (TCB) of a computer system is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system. By contrast, parts of a computer system that lie outside the TCB must not be able to misbehave in a way that would leak any more privileges than are granted to them in accordance to the system's security policy.

Source: https://en.wikipedia.org/wiki/Trusted_computing_base

- Trusted Computing Base is a term for the core part that ensures security
  https://en.wikipedia.org/wiki/Trusted_computing_base
- I often talk about the TCB of QubesOS which I use:
  *security-critical (i.e., trusted) code components in Qubes OS* https://www.qubes-os.org/doc/security-critical-code/

# Intrusion Kill Chains

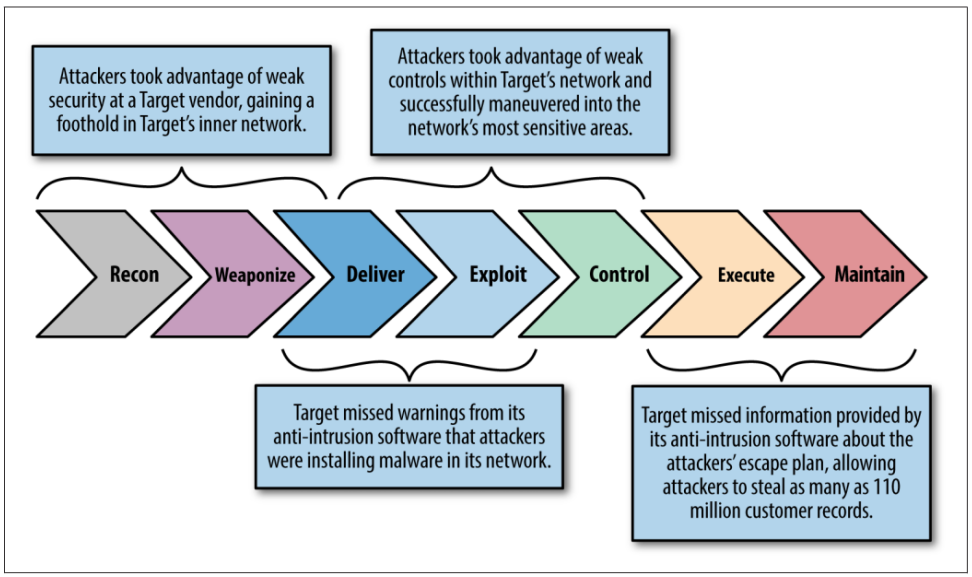



*Figure 7-1. The kill chain*

- 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

# Get an idea of the MITRE ATT&CK framework

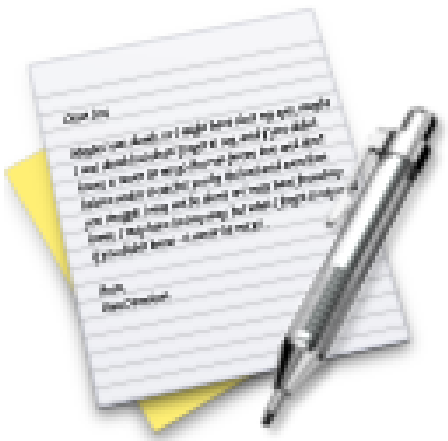
MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity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

https://attack.mitre.org/

# Exercise



Now lets do the exercise

## ⚠ Mitre ATT&CK Framework 25 min

which is number **9** in the exercise 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/

# Sample vulnerabilities

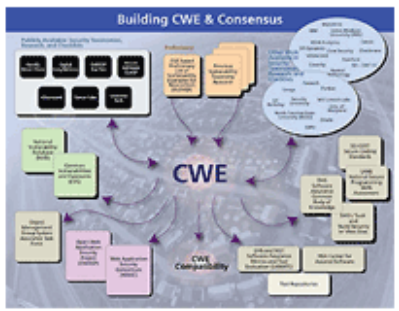
CVE-2000-0884
IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal"vulnerability.

CVE-2002-1182
IIS 5.0 and 5.1 allows remote attackers to cause a denial of service (crash) via malformed WebDAV requests that cause a large amount of memory to be assigned.

Source:
http://cve.mitre.org/-CVE

And updates from vendors reference these too! A closed loop

# CWE Common Weakness Enumeration




Enlarge

**CWE™** International in scope and free for public use, CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

## CWE in the Enterprise

- Software Assurance
- Application Security
- Supply Chain Risk Management
- System Assessment
- Training
- Code Analysis
- Remediation & Mitigation
- NVD (National Vulnerability Database)
- *Recommendation ITU-T X.1524 CWE,* ITU-T CYBEX Series

http://cwe.mitre.org/

# 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: http://cwe.mitre.org/top25/index.html

## Hacker tools

*Improving the Security of Your Site by Breaking Into it*
by Dan Farmer and Wietse Venema in 1993

Later in 1995 release the software SATAN
*Security Administrator Tool for Analyzing Networks*

Caused some commotion, panic and discussions, every script kiddie can hack, the internet will melt down!

> We realize that SATAN is a two-edged sword – like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

label Source: http://www.fish2.com/security/admin-guide-to-cracking.html

## Use hacker tools!

Port scan can reveal holes in your defense

Web testing tools can crawl through your site and find problems

Pentesting is a verification and proactively finding problems

Its not a silverbullet and mostly find known problems in existing systems

Combined with honeypots they may allow better security

# Agreements for testing networks

> Danish Criminal Code
> Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.

Hacking can result in:

- Getting your devices confiscated by the police
- Paying damages to persons or businesses
- If older getting a fine and a record – even jail perhaps
- Getting a criminal record, making it hard to travel to some countries and working in security
- Fear of terror has increased the focus – so dont step over bounds!

Asking for permission and getting an OK before doing invasive tests, always!

# ISC2 code of ethics

## Code of Ethics Preamble:

- The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

## Code of Ethics Canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession.

CISSP certified people sign papers to this extent.
https://www.isc2.org/ethics/default.aspx

# What happens today?

Think like a blue team member find vulnerable systems

Get basic tools running

- ping sweep, port scan
- OS detection – TCP/IP or banner grab
- Service scan – rpcinfo, netbios, ...
- telnet/netcat interact with services

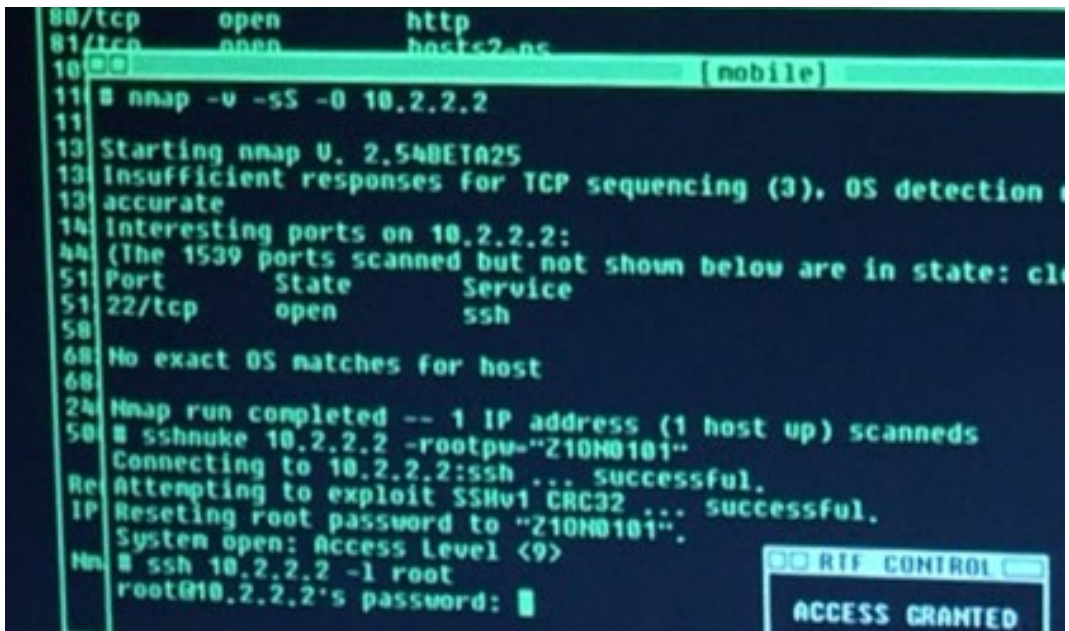
Exploit: Metasploit, Nikto, exploit programs

Cleanup/hardening not shown but in practice:

- Make a report
- Change and improve systems
- Follow up on critical vulnerabilities
- Change configuration, architecture etc.

Remember to document process, need to show others what you do

# Trinity breaking in




Very realistic:
https://nmap.org/movies/
https://youtu.be/51lGCTgqE_w

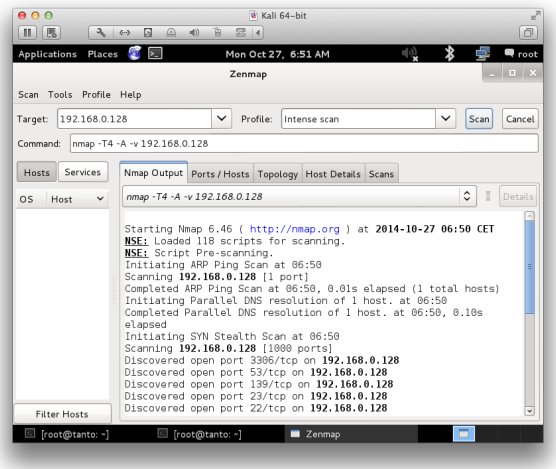
# Kali Linux the pentest toolbox


Kali http://www.kali.org/

100.000s of videos on youtube alone, searching for kali and $TOOL

Also versions for Raspberry Pi, mobile and other small computers

# Really do Nmap your world




- Nmap is a port scanner, but does more
- Finding your own infrastructure available from the guest network?
- See your printers having all the protocols enabled AND a wireless?

# Basal Portscanning

Hvad er portscanning

Afprøvning af alle porte fra 0/1 og op til 65535

Målet er at identificere åbne porte – sårbare services

Typisk TCP og UDP scanning

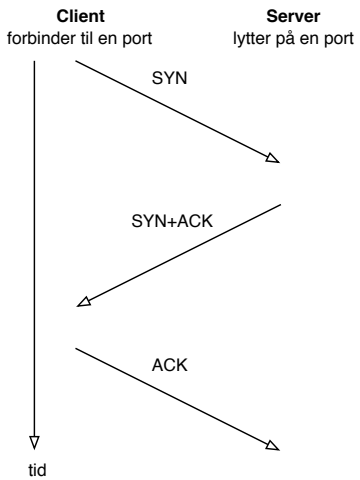
TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere, skal svare SYN

UDP applikationer svarer forskelligt – hvis overhovedet
Svarer på rigtige forespørgsler, uden firewall svares ICMP på lukkede porte

Brug GUI programmet Zenmap mens i lærer Nmap at kende

# TCP three-way handshake




- **TCP SYN half-open** scans
- Tidligere loggede systemer kun når der var etableret en fuld TCP forbindelse
  – dette kan/kunne udnyttes til *stealth*-scans
- Hvis en maskine modtager mange SYN pakker kan dette fylde tabellen over connections op – og derved afholde nye forbindelser fra at blive oprette – **SYN-flooding**

# Nmap port sweep efter webservere

```
root@cornerstone:~#  nmap -p80,443 172.29.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT    STATE    SERVICE
80/tcp  open     http
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

# Nmap port sweep efter SNMP port 161/UDP

```
root@cornerstone:~# nmap -sU -p 161 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:30 CET
Nmap scan report for 172.29.0.1
Host is up (0.00015s latency).
PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00011s latency).
PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 00:0C:29:46:22:FB (VMware)
...
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.18 seconds
```

# Nmap Advanced OS detection

```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).
PORT    STATE    SERVICE VERSION
80/tcp  open     http    Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
or iOS 4.1 - 7.1 (Darwin 10.0.0 - 14.0.0), Apple Mac OS X 10.8 - 10.8.3 (Mountain Lion)
or iOS 5.1.1 - 6.1.5 (Darwin 12.0.0 - 13.0.0)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```

- Lavniveau måde at identificere operativsystemer på, prøv også `nmap -A`
- Send pakker med *anderledes* indhold, observer svar
- En tidlig og detaljeret reference: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin, 2001

# Heartbleed CVE-2014-0160

## The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Source: http://heartbleed.com/

# Scan for Heartbleed and SSLv2/SSLv3

**Example Usage**

```
nmap -sV -sC <target>
```

**Script Output**

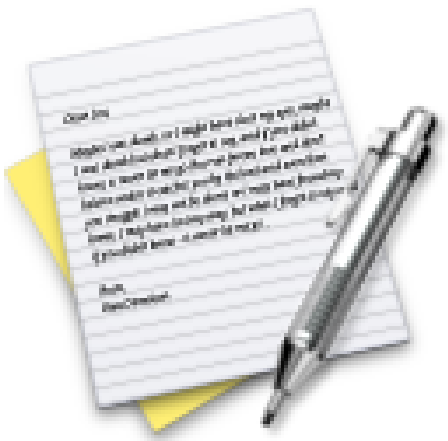
```
443/tcp open   https   syn-ack
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

`nmap -p 443 --script ssl-heartbleed <target>`
https://nmap.org/nsedoc/scripts/ssl-heartbleed.html

`masscan 0.0.0.0/0 -p0-65535  --heartbleed`
https://github.com/robertdavidgraham/masscan

Almost every new vulnerability will have Nmap recipe

# Exercise

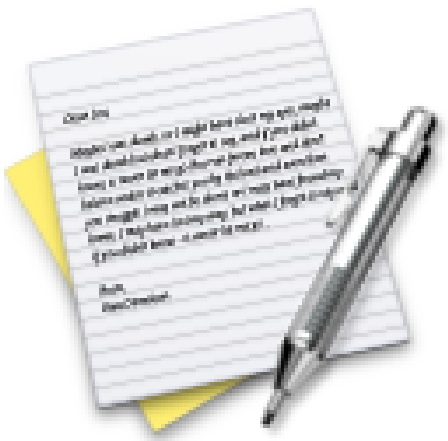


Now lets do the exercise

## ⚠ Create Lab network 15min

which is number **10** in the exercise PDF.

# Exercise

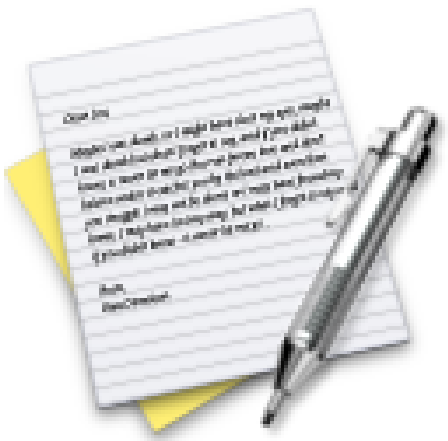


Now lets do the exercise

## ⚠ Discover active systems ping and port sweep 15min

which is number **11** in the exercise PDF.

# Exercise



Now lets do the exercise

## ⚠ Execute nmap TCP and UDP port scan 20 min

which is number **12** in the exercise PDF.

# Exercise

Now lets do the exercise

## ⚠ Perform nmap OS detection 15min

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

# Exercise

Now lets do the exercise

## ⚠ Perform nmap service scan 15min

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

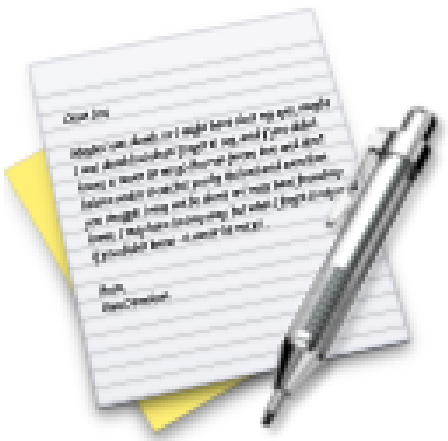
# Exercise

Now lets do the exercise

## ℹ Nmap full scan - 15min

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

# Exercise



Now lets do the exercise

## ℹ Reporting Nmap HTML 10min

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

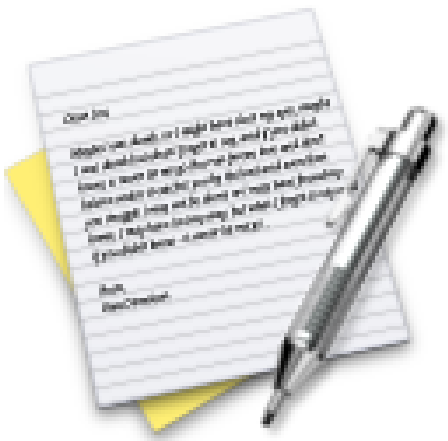
# Exercise

Now lets do the exercise

## ℹ Nping check ports 10min

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

# Exercise



Now lets do the exercise

## Nmap Scripting Engine NSE scripts 20min

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

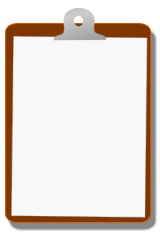
## Local vs. remote exploits

**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

# 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