

# Vulnerability handling

## DK-CERT

TF-CSIRT, Heraklion, 21. May 2010

**Shehzad Ahmad, DK-CERT**

Email: [shehzad.ahmad@uni-c.dk](mailto:shehzad.ahmad@uni-c.dk)

# Agenda

- Introduction of DK-CERT
  - Background, today and the future
  
- DK-CERT Services
  
- Vulnerability Handling
  - Vulnerability database
    - Our own database
  
  - Scanning report
    - How is the scanning done?
    - How is the result presented in the report

# Who is DK-CERT?

- DK-CERT is an organization of UNI•C, Danish IT Center for Education and Research - an agency under the Ministry of Education.
- UNI•C created DK-CERT in 1991 in connection with one of the first hacker cases in Denmark.
- The inspiration came from CERT/CC (1988) and US-CERT (1990).
- Our main task is to work as an Academic CERT.

# DK-CERT and GovCERT

”team update”

- Have agreed to deliver “National CERT” services.
  - Services for the citizens
    - Security information, alerts, vulnerabilities -> on website borger.dk
    - Mailing list -> allows us to send out information directly to the citizens
    - 1881 (public free number for citizens) IT-security calls in office hours
    - FAQ (approx 100 questions/answers)
    - (will be using facebook and twitter as well)
  - Services for SME
    - Security information, alerts, vulnerabilities, on website virk.dk
    - Mailing list for companies
  - Continue working with the ISP’s
  - Media, Police and other important partners...



# DK-CERT activities -> Incident Handling.

- DK•CERT receives reports of security incidents (**Incident Handling**), from outside and from the networks we monitor: Danish network for Research and Education (**Forskningsnettet**), and the network of UNI•C.

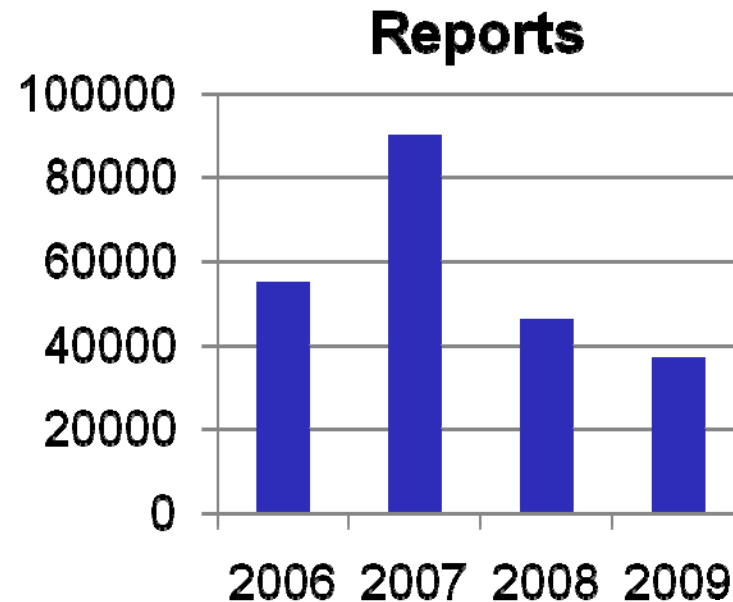
2006: **55.000**

2007: **90.000**

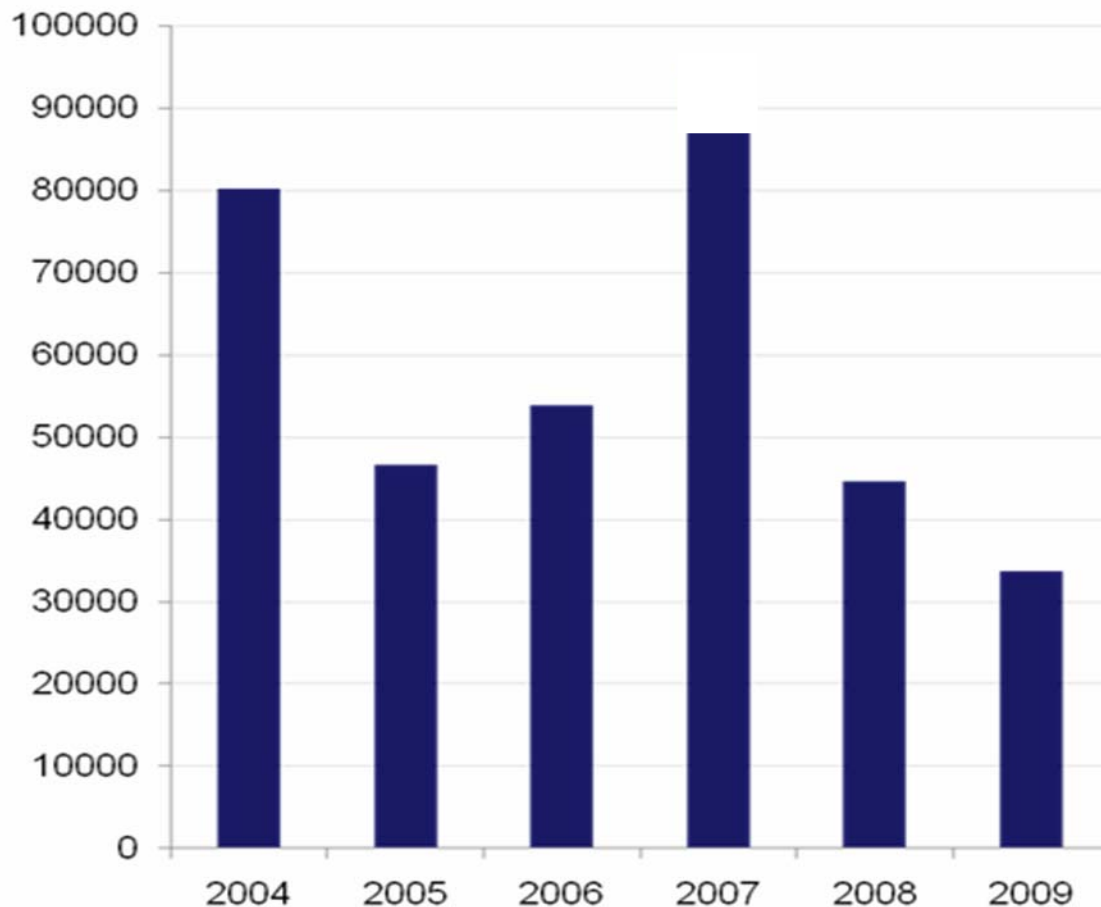
2008: **46.000**

2009: **37.000**

- (Standard incident reports as: phishing sites, port-scans, hacking incidents, spam etc.)



# Type of cases handled by DK-CERT



Type	2008	2009
Phishing	279	446
Denial of Service	5	5
Hacking	331	1217
Portscan	44666	33761
Root compromise	1	1
Spam	84	178
Trojan	42	105
Virus	5	15
Warez (copyright)	580	1649

← Port scan

# DK-CERT services

- Security scans
  - Normal vulnerability (port & service) scan
  - Deep application (WEB-servers, SQL-databases) scan
  - Wireless network scan (routers, encryption status, configuration etc. (coming up))
  
- Vulnerability database.
  - Mainly for Danish network for Research and Education (**Forskningsnettet**)
  
- Reverse engineering on malware (on hold at the moment).
  
- Awareness campaigns
  - Weekly newsletters, columns, articles, interviews etc....
  - We use Facebook (since 2008) and we are “testing” Twitter
  - Trend report 2009 (available in danish and english) (and new Q1 2010 report)

## Reactive Services



- + Alerts and Warnings
- + Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- + Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- + Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

## Proactive Services



- ⦿ Announcements
- ⦿ Technology Watch
- ⦿ Security Audit or Assessments
- ⦿ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ⦿ Development of Security Tools
- ⦿ Intrusion Detection Services
- ⦿ Security-Related Information Dissemination

## Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

# DK-CERT's Vulnerability database



## How will the customer use the Vulnerability database?

- The **customer chooses** what **applications** and **operating systems**, he/she will receive alerts on.
- Vulnerability **database collects warnings and information** on vulnerabilities from the Internet
- **Customer receives regular lists** of updates to the applications and systems he/she has chosen.

# How are warnings received by the user?

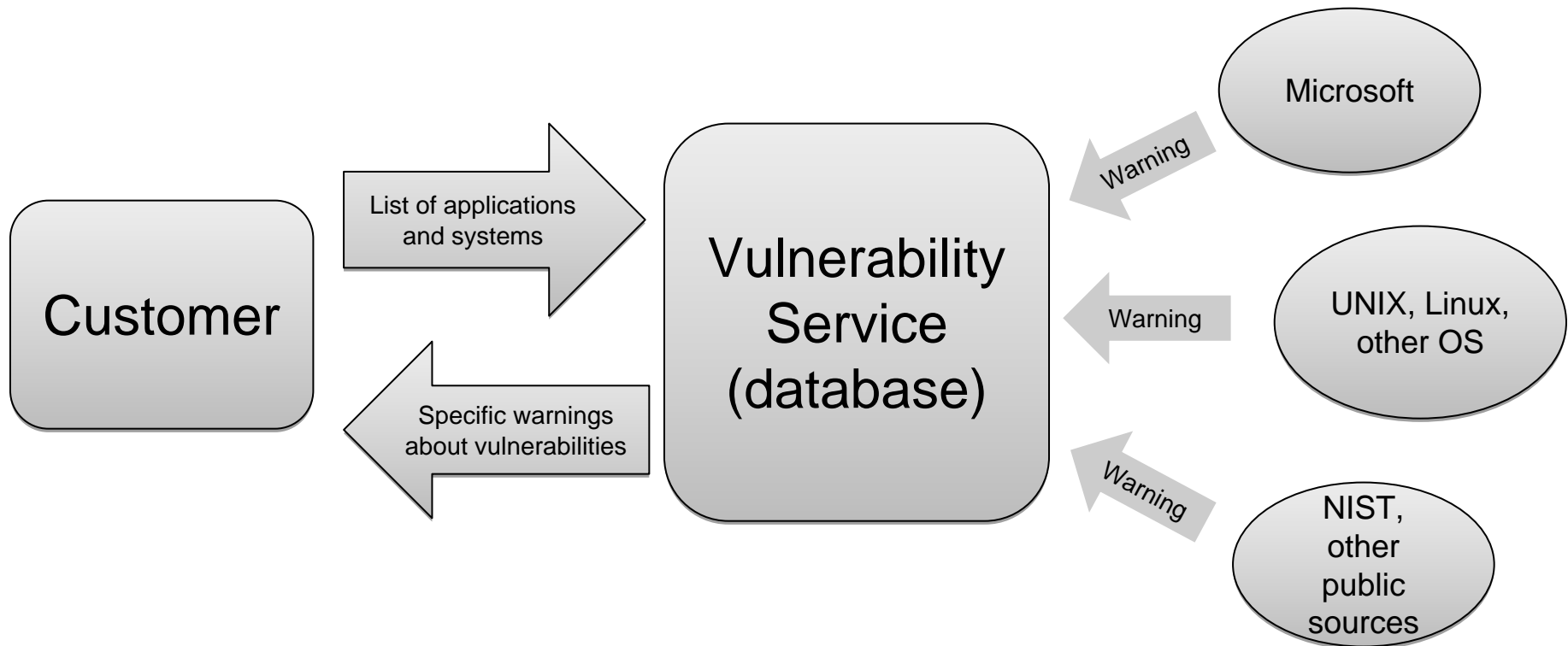
Warnings can be received in different ways:

- E-mail
- SMS\*
- DK-CERT's website
- RSS-feed - custom made\*
- Customers own site

# From where are the vulnerability information received?

- [nvd.nist.gov](http://nvd.nist.gov)
- OS-vendors – ex. Microsoft, Debian, Red Hat, Ubuntu, HP-UX
- The system can be extended - we can retrieve information from all those who publish vulnerabilities in a fairly fixed format.

# Vulnerability database



# Vulnerability

- One unique CVE id
- Short description
- Solution
- Vulnerable systems
- References (vendor-specific advisories)
- Possibility for specific vendor-related descriptions and features
- Different searchable dates
- CVSS-score, extendible

**Modified date:** 2010-05-14

**Publication date:** 2010-05-13

**CVE:** CVE-2010-1939

**CVSS-score:**

**High**



[More details on CVSS-score](#)

## Short description

Use-after-free vulnerability in Apple Safari 4.0.5 on Windows allows remote attackers to execute arbitrary code by using window.open to create a popup window for a crafted HTML document, and then calling the parent window's close method, which triggers improper handling of a deleted window object.

## Solution

For further details about a solution look under references.

## Vulnerable systems:

[See list](#)

apple safari 4.0.5

## Advisory references and solutions

[Advisory from CERT-VN](#) [\(Original advisory\)](#)

[Advisory from VUPEN](#) [\(Original advisory\)](#)

[Advisory from BID](#) [\(Original advisory\)](#)

[Advisory from OSVDB](#) [\(Original advisory\)](#)

[Advisory from SECTRACK](#) [\(Original advisory\)](#)

[Advisory from SECUNIA](#) [\(Original advisory\)](#)

[Advisory from MISC](#) [\(Original advisory\)](#)

[Advisory from MISC](#) [\(Original advisory\)](#)

## Source

NIST

# Advisory

- Description
- Solution
- References to vulnerabilities
- Possibility for vendor-specific descriptions, solutions, and features

## 2010-05-02 squidguard -- buffer overflow

Source: DEBIAN

ID: DSA-2040

### Description

It was discovered that in squidguard, a URL redirector/filter/ACL plugin for squid, several problems in `src/sgLog.c` and `src/sgDiv.c` allow remote users to either:

```

cause a denial of service, by requesting long URLs containing many
slashes; this forces the daemon into emergency mode, where it does not
process requests anymore.
bypass rules by requesting URLs whose length is close to predefined
buffer limits, in this case 2048 for squidguard and 4096 or 8192 for squid
(depending on its version).

```

### Solution

For the stable distribution (lenny), this problem has been fixed in version 1.2.0-8.4+lenny1.

For the unstable distribution (sid), this problem has been fixed in version 1.2.0-9.

We recommend that you upgrade your squidguard package.

### Advisory from vendor

Advisory from DEBIAN

<http://www.debian.org/security/2010/dsa-2040>

### Vulnerabilities

The following vulnerabilities affect this advisory

[CVE-2009-3700](#)



Failure to Constrain Operations within the Bounds of a Memory Buffer

[CVE-2009-3826](#)



Failure to Constrain Operations within the Bounds of a Memory Buffer

# System

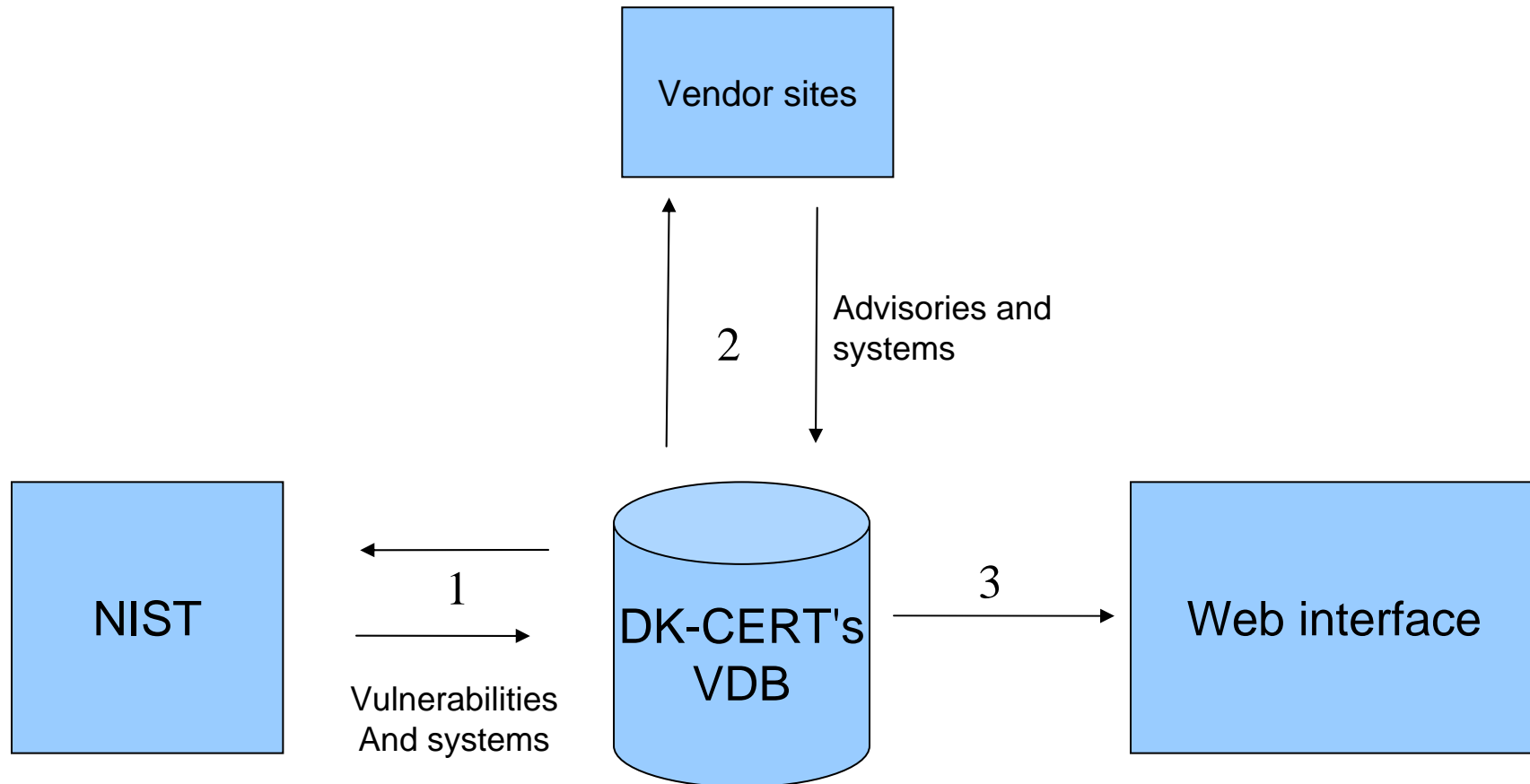
- Containers with name
- OS, application or hardware name with version
- Wildcards including not yet existing versions
- Systems can contain systems

## My systems

System	Saved applications, operating systems, and hardware devices	
Linux workstation	<i>ubuntu ubuntu * and later</i> <i>ubuntu ubuntu_linux * and later</i> <i>Debian debian_linux * and later</i>	<a href="#">Edit system</a>
Office PC	<i>Microsoft Corporation office 2003 sp2 and later</i>	<a href="#">Edit system</a>

# Vulnerabilities



# Future work

- Improve CVSS usage
- Use CPE (Common Product Enumeration) more
- More use of containers
- Integration with vulnerability scannings
- Improve registering of systems
- Better visualisation of systems, vulnerabilities and advisories
  - Statistics of vulnerabilities and advisories
  - Better overview of registered systems, vulnerabilities and advisories

# DK-CERT's Scanning and reporting system

# Vulnerability scanning

## Who are we scanning ?

- Organizations connected to the Danish Research Network (Forskningsnettet).
- Other organizations on request.

## What are we scanning ?

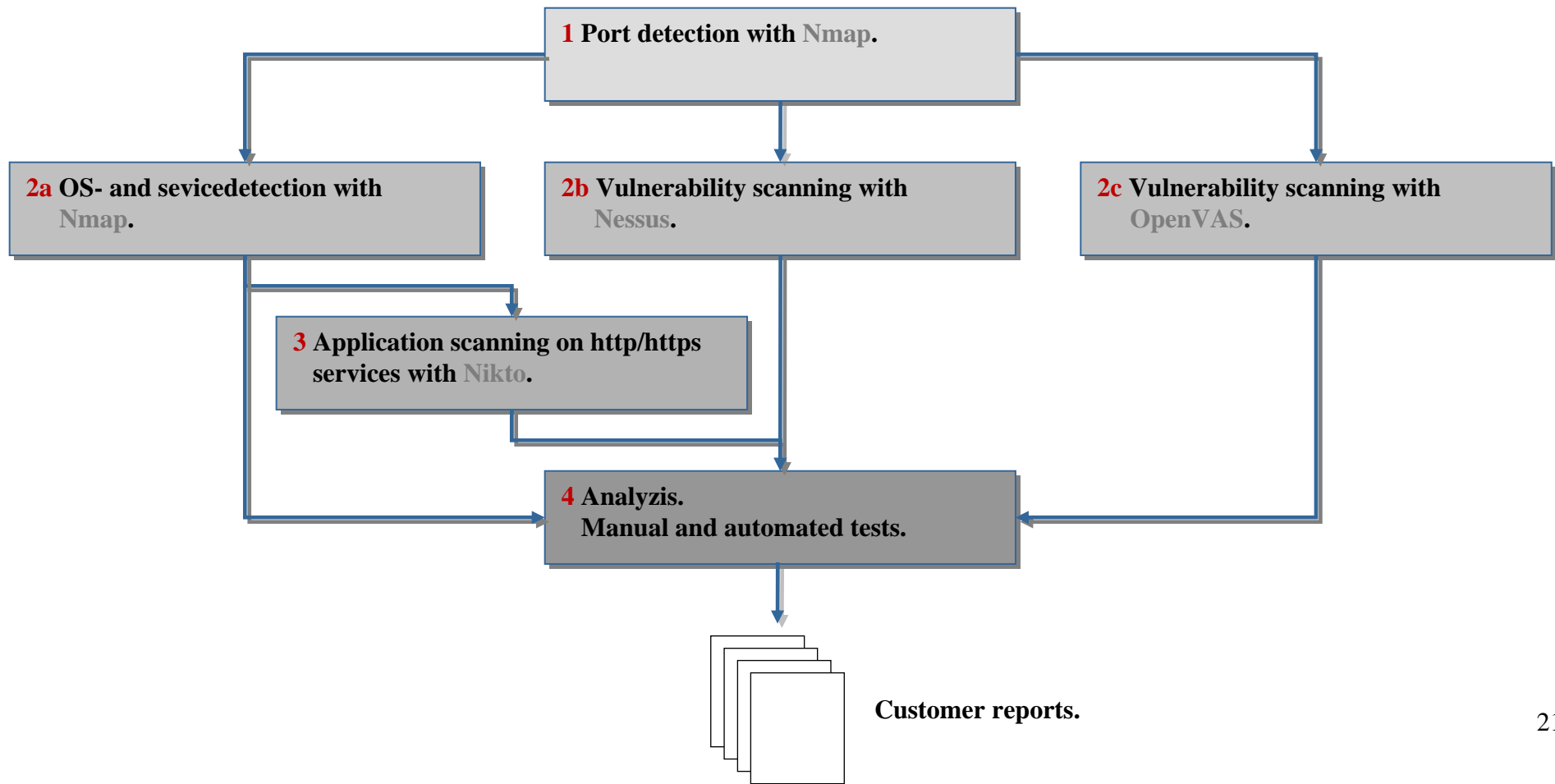
- Public ip-address spaces.
- TCP Ports 0-1024 and ports listed in nmap's list off well-known ports and ICMP.

## Why are we scanning ?

- To prevent compromise off data and systems in the scanned organizations.
- To assist the administrators in securing there systems.
- To assist in rendering visibility off risk management
- As a part off revision - and occasionally as part of analysis of compromised system.

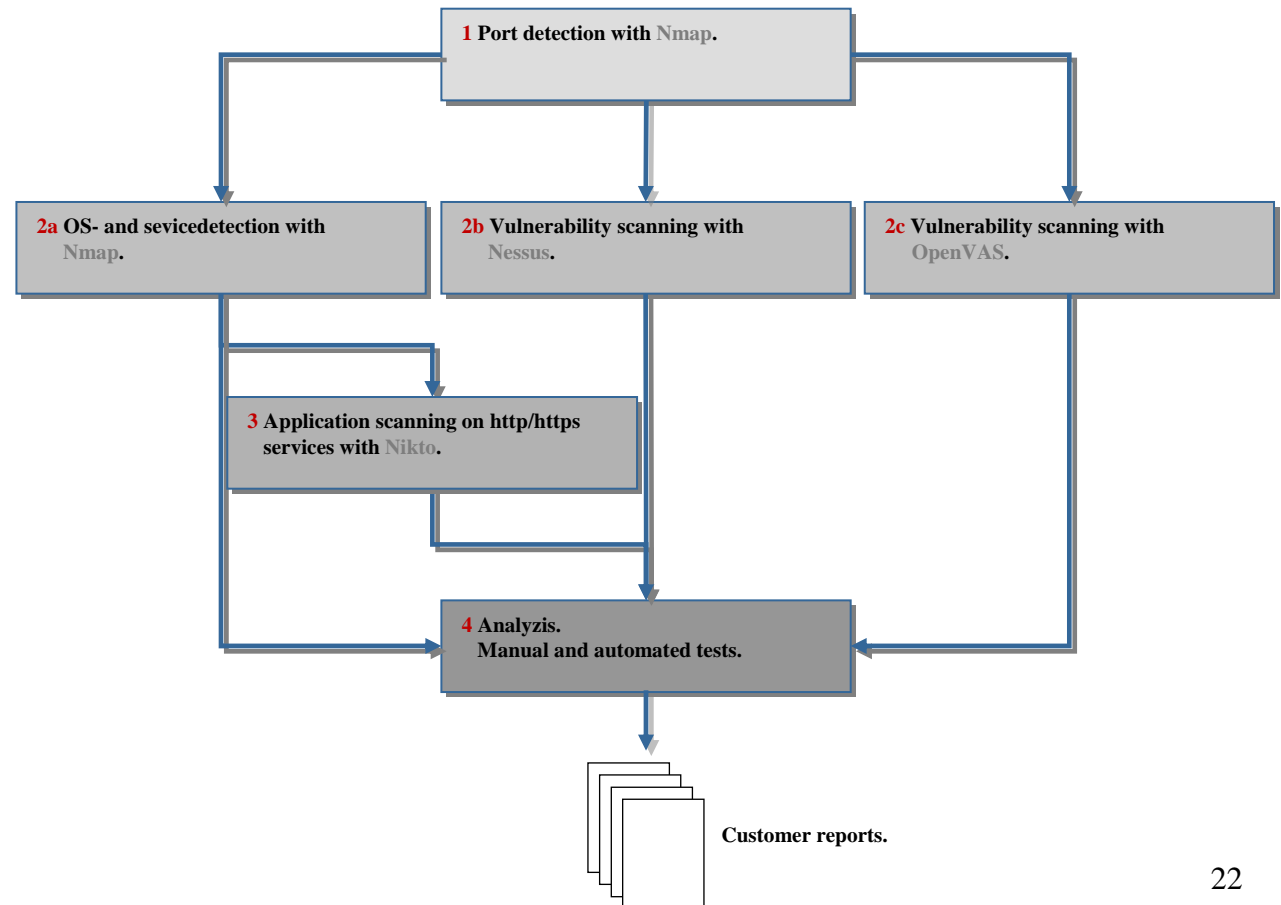
# Vulnerability scanning

## The scanning process:



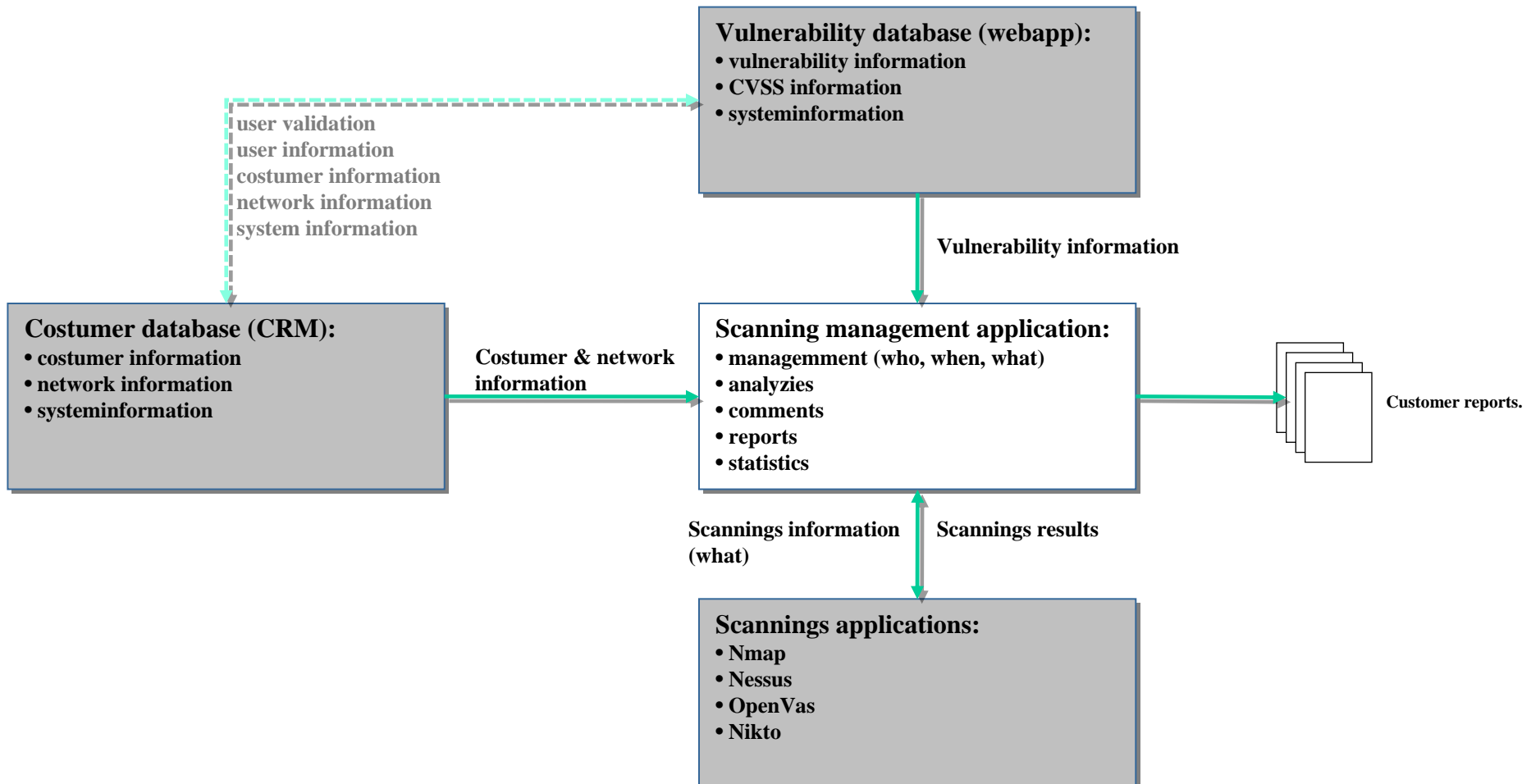
# Vulnerability scanning

- a) **initiate port scanning** from costume made web application.
- b) automated initiation of **vulnerability scanning's** with costume made scripts.
- c) automated initiation of **web application scanning's** with costume made scripts.
- d) automated **export of results** to costume made web application.
- e) **generation of report** in costume made web application.



# Vulnerability scanning

## System overview



# Vulnerability scanning

Reports are:

- generated from the scanning management application.
- costume made.
- the result of both the results, analysis, manual and automated tests.

The costume made reports:

- are in **html format** with pdf pages for print.
- has **functionality for managing the patch management** process.
- includes parts for both, management, it-security and it administrators.

# Vulnerability scanning

## The report

- How does it look?



# Vulnerability scanning

## The report (easy navigation):

[Forside](#)
[Resumé](#)
[Introduktion](#)
[Konklusion](#)
[IP-oversigt](#)
[Portoversigt](#)
[Sårbarheder](#)
[Bilag](#)



- overviews sorted on ip-adresses, ports & vulnerabilities.
- print management
- management of responsebilities and updates.

172.20.57.17 (server17.iits.dk)							Ansvarlig:	Alle	
Port	I alt	H	M	L	Rettet	Ansvarlig	Print	Printet	
Port 21 (ftp) ▶	2	2					<input type="checkbox"/>	<input type="checkbox"/>	
Port 23 (telnet) ▶	1			1			<input type="checkbox"/>	<input type="checkbox"/>	
Port 25 (smtp) ▶	6	2	3	1		SA	<input type="checkbox"/>	<input type="checkbox"/>	
Port 80 (http) ▶	12	4	7		1/3 2010	SA	<input type="checkbox"/>	<input type="checkbox"/>	
Port 512 (exec) ▶	1	1				SA	<input type="checkbox"/>	<input type="checkbox"/>	
Port 513 (login) ▶	1	1					<input type="checkbox"/>	<input type="checkbox"/>	
Port 514 (shell) ▶	1	1					<input type="checkbox"/>	<input type="checkbox"/>	
Port 6112 (dtspc) ▶	1	1					<input type="checkbox"/>	<input type="checkbox"/>	
<b>Total</b>	<b>25</b>						<input type="button" value="Print"/>		

# Vulnerability scanning

## Presentation of the results for the customer with the report.

- The report is **presented remotely** to the customer(s) on an **Adobe Connect** installation on Danish Research Network.
- The customer can **download the report** from Adobe Connect.
- As a control for the security responsible, the customer can get a **rescan**.

[ Thank you for listening !]  
[Questions?]

Shehzad Ahmad

Email: [shehzad.ahmad@uni-c.dk](mailto:shehzad.ahmad@uni-c.dk)

DK-CERT