SECURITY AUDITING OF MAIL SERVICES AT INFN

DIY AUDITING

HEPIX Umeå
May 25-29 2009

Ombretta Pinazza, on behalf of INFN Mailing and Security WG
Fulvia Costa, Francesco Ferrera, Diego Leanza, Alessia Spitaleri
Patrizia Belluomo , Franco Brasolin, Roberto Cecchini, Michele Michelotto

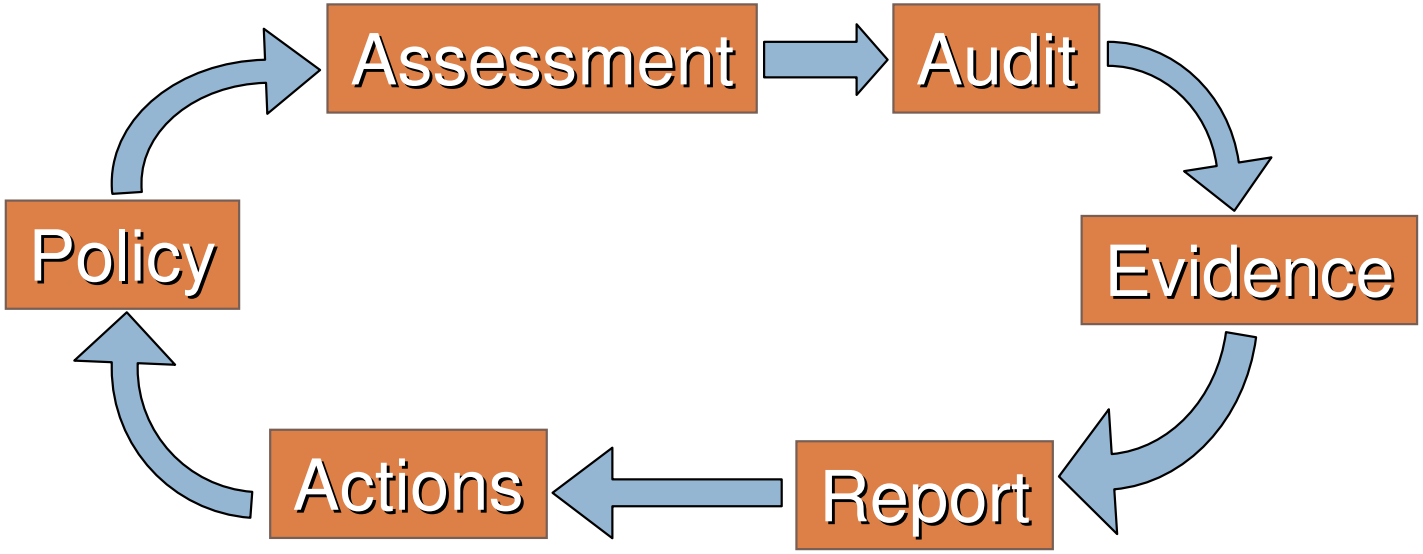
INFN

Contents

- Project description
  - Why security auditing
  - Contingencies and planning
- Methodology
  - From the first phase toward a regular procedure
- Results
  - Security overview
  - Feedback from the sites
- Conclusions

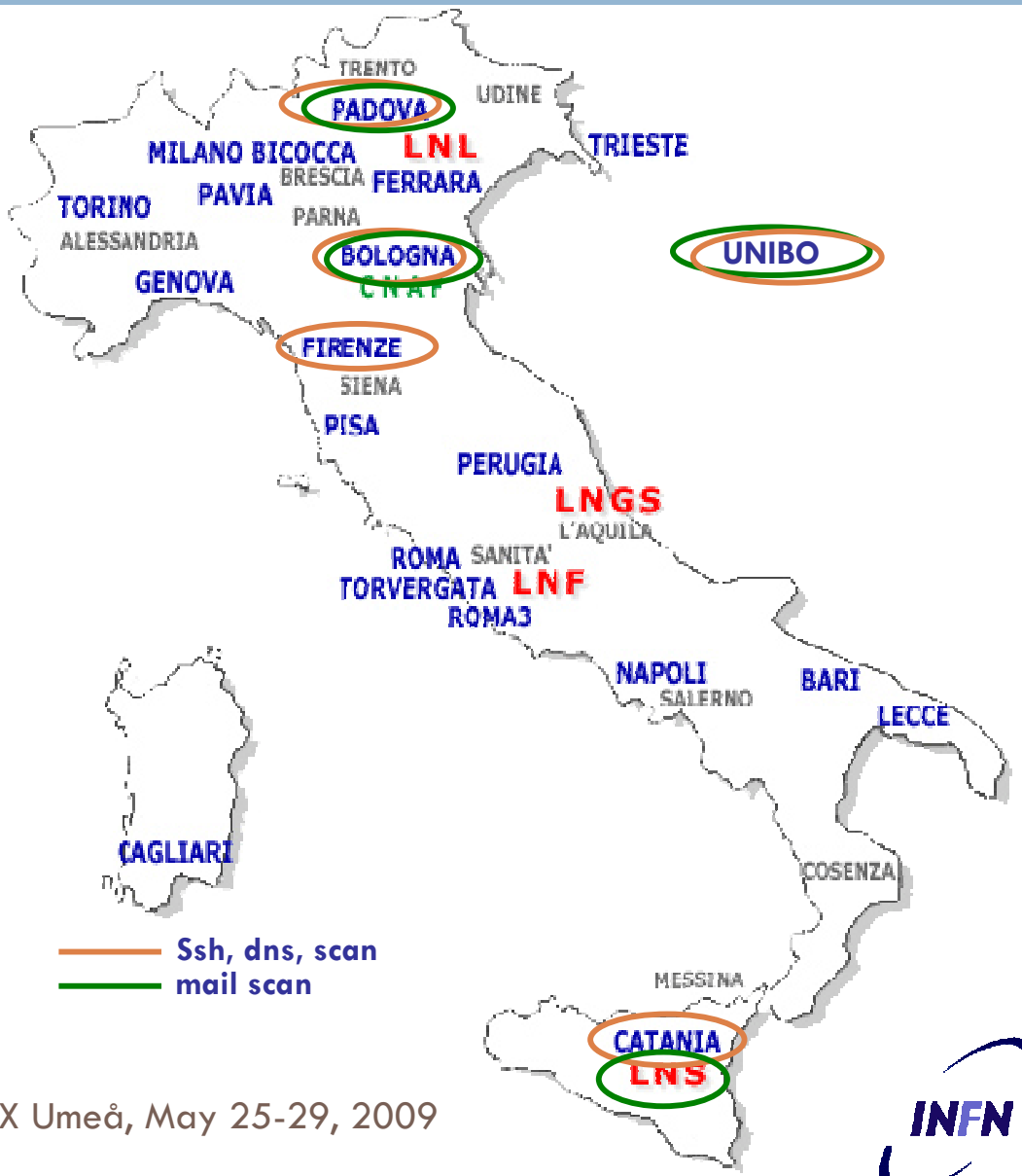
Why auditing? How?

- It's required by the italian laws for public organizations
- As a service for the INFN community
- As an opportunity for our working groups
- The overall procedure shall be systematic and well documented



External/Internal auditing

- Professional auditors are extremely expensive
- A cross-sites analysis using common parameters could be comparable to an external view
- Local admins take care of monitoring and internal auditing



Objectives - expectations

- Act in advance on emergencies: attacks to DNS, conficker worm, bugs and vulnerabilities
- A step toward a common security policy
- Feedback from site administrators
- First results
  - Screenshot of the publicly visible services
  - Identified several misconfigured and vulnerable services

Phase one

- SSH
  - Vulnerable versions
  - Filter policies (firewall, bastion hosts, …)
- HTTP and HTTPS
  - PHP and apache vulnerabilities
  - Several public servers
  - Unconfigured servers, open DBs, wikis, …
- DNS
  - Root queries
  - Recursive queries
  - Vulnerabilities (Debian, …)
- Conficker

Security Auditing WG

Mail services

- not only OS or software vulnerabilities
- check for misconfigured servers, open relays, explicit banners, unauthorized services
- dangerous ESMTP features
- SMTP AUTH

Mailing
Auditing
WG

Methodology 1

- Define the hosts subset to be analyzed
  - MX query to all DNS servers to build the list of official mail servers
  - Nmap scan of all INFN subnets to reveal open “mailing” services
  - Sys admin indication
- Analysis of the mailing services
  - TCL scripts managing the connection and saving the dialog in a file
  - Perl scripts handling ssl and starttls connections
  - Perl scripts parsing output files and recognizing problems
  - SMTP
    - Banner, exposed information, ESMTP features
    - SMTP/SSL: port 25 or 465, INFN CA or self cert., features
    - STARTTLS (587/tcp)
    - SMTP AUTH

Methodology 2

- The aim is to verify if multiple services are available on the same host
- Mailboxes
  - POP, POPS
  - IMAP, IMAPS
- Other services
  - HTTP, HTTPS
  - LDAP
  - POPPASSD

Methodology 3

- Reporting
  - Global document with an evaluation of the security level, containing recommendations for the sites, based on common policies
  - Detailed modular reports on a web site with restricted access
  - Instructions, help and configuration documents
  - WIP
    - Needs of an organized database
    - Automatize data collection and analysis, and scan comparison

Results 1

- SSH
  - 3048 server open
  - High severity problems (Nessus):

34 sites (*.infn.it)
151 subnets
(B/C/trunks)
110.000 IPs
8.800 scanned

Scan date	Number
Nov 2008	89
Dec 2008	55
Jan 2009	59

Results 2

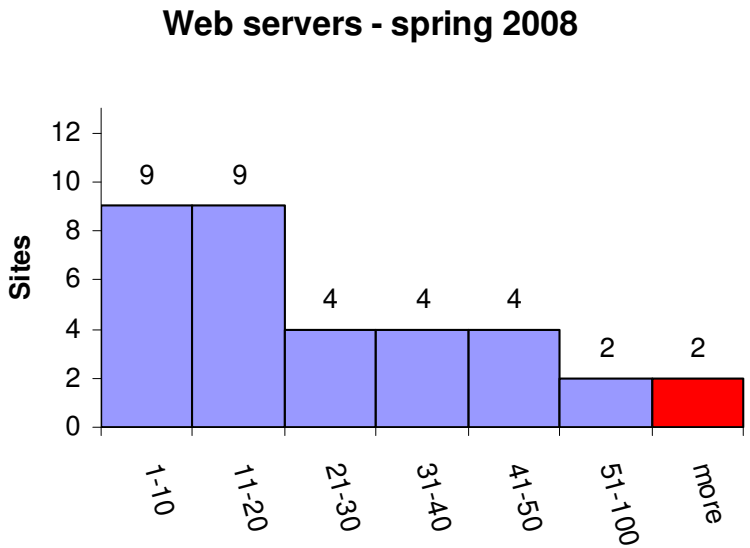
- DNS
  - 65 official servers per 34 sites

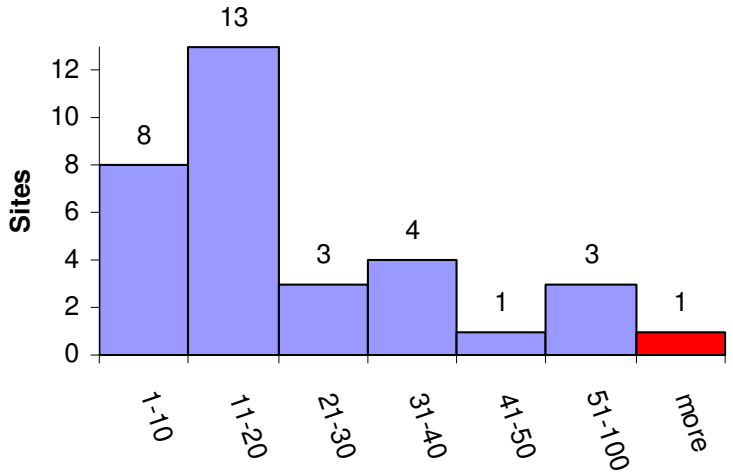
Date	Recursive queries		Root queries		off
	ok	no	ok	no	
Jan 2009	29	31	?	?	0
Feb 2009	43	18	37	24	4
Mar 2009	52	10	49	13	3

Results 3

- Web (HTTP and HTTPS)

Scan date	web servers total number	High severity problems	Medium severity problems	Low severity or no problems
Mar 2008	1193	218	576	399
May 2009	1252	199	557	496





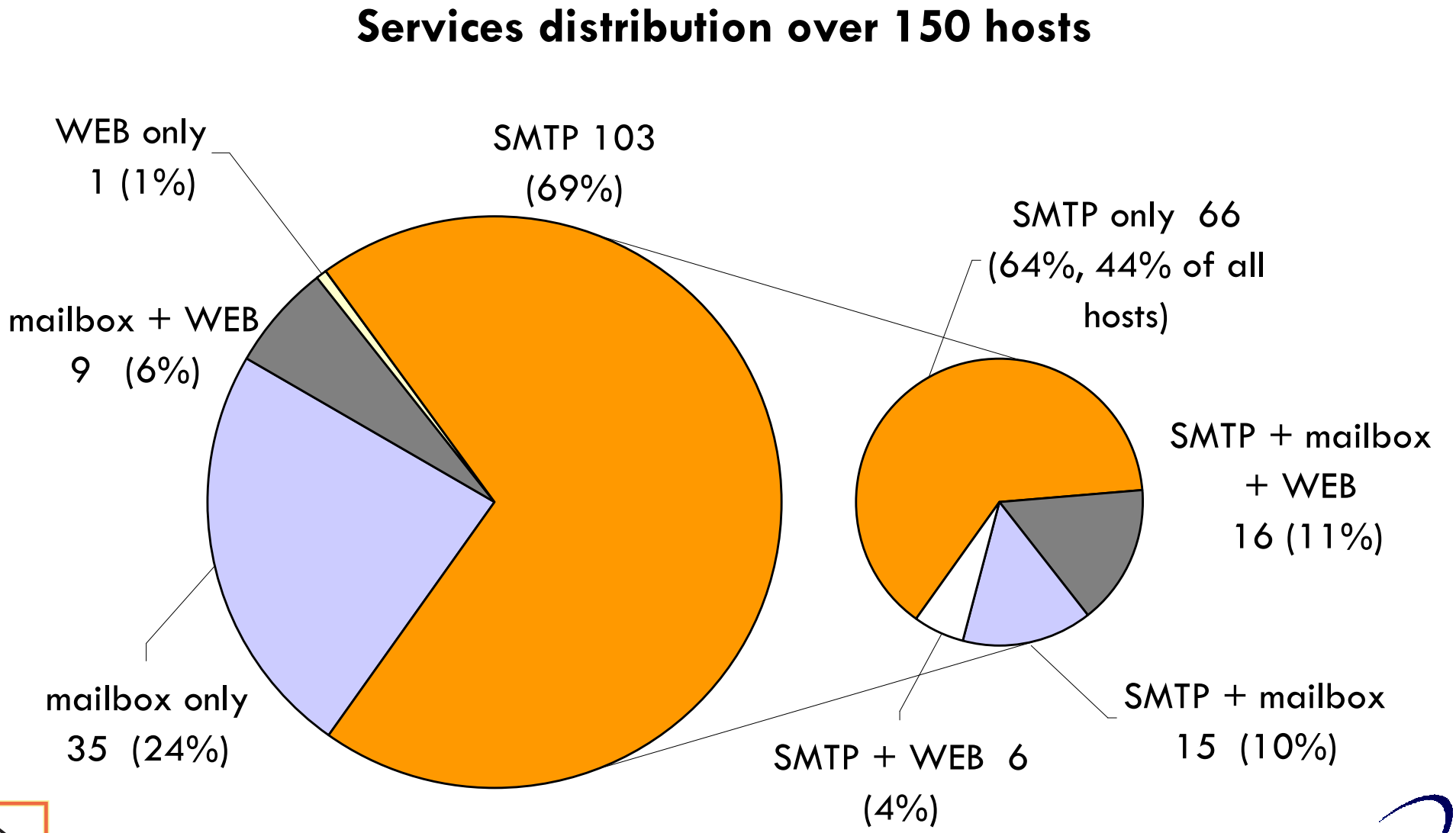
Results 4

- Mailing services

	Census 2007	Census 2008	Scan 2009
Hosts	71*	80*	150
Avg per site	2.7	3.1	4.4

* Census: declared by sites admins

Results 5


Services distribution over 150 hosts
WEB only
1 (1%)
SMTP 103
(69%)
SMTP only 66
(64%, 44% of all
hosts)
mailbox + WEB
9 (6%)
SMTP + mailbox
+ WEB
16 (11%)
mailbox only
35 (24%)
SMTP + mailbox
15 (10%)
SMTP + WEB 6
(4%)

Results 6

34	INFN sites	150	Hosts
22 (64%)	SMTP AUTH	55	MX
11 (32%)	SMTP/SSL on 465	77	SMTP
Security evaluation of mail services			
14 (41%)		35 (23%)	
7 (21%)		10 (7%)	
13 (38%)		4 (3%)	

- High severity problems (bugged version, open relay, clear text auth, …)
- Medium severity problems (unconf. web, dangerous ESMTP feat., …)
- not working (official MX off, wrong IP/name corresp. on DNS, …)
- ok

Conclusions

- Positive feedback from sites admins:
  - 74% sites have promptly checked their reports
  - Sent corrections, comments, requests
  - Several colleagues have intervened immediately to patch and protect their systems
- This self made analysis can represent a starting base for an organized auditing procedure
- INFN is trying to hire an IT graduate to carry on with the auditing activity

Thanks

- Security auditing group:
  - Roberto Cecchini, Franco Brasolin, Michele Michelotto, Patrizia Belluomo
- Mailing auditing group:
  - Fulvia Costa, Franco Ferrera, Diego Leanza, Alessia Spitaleri

Questions?