Security scan (gruppo Auditing)

Mini Workshop CCR
Trento, 16-18 Marzo 2016

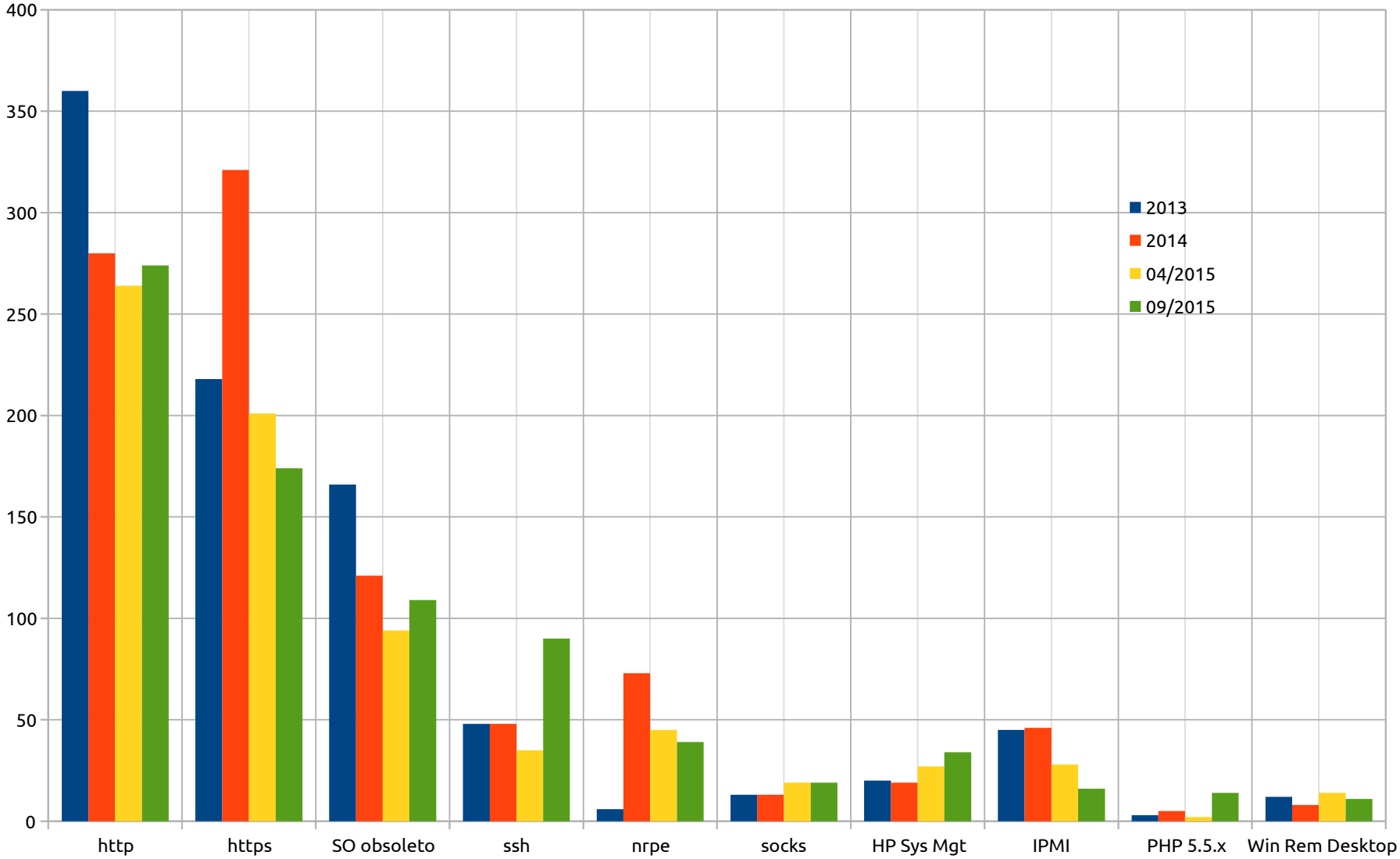
Gruppo Auditing

- Membri
  - Franco Brasolin
  - Roberto Cecchini
  - Leandro Lanzi
  - Michele Michelotto
  - Antonella Monducci
- Server web: **https://audiweb.infn.it/**

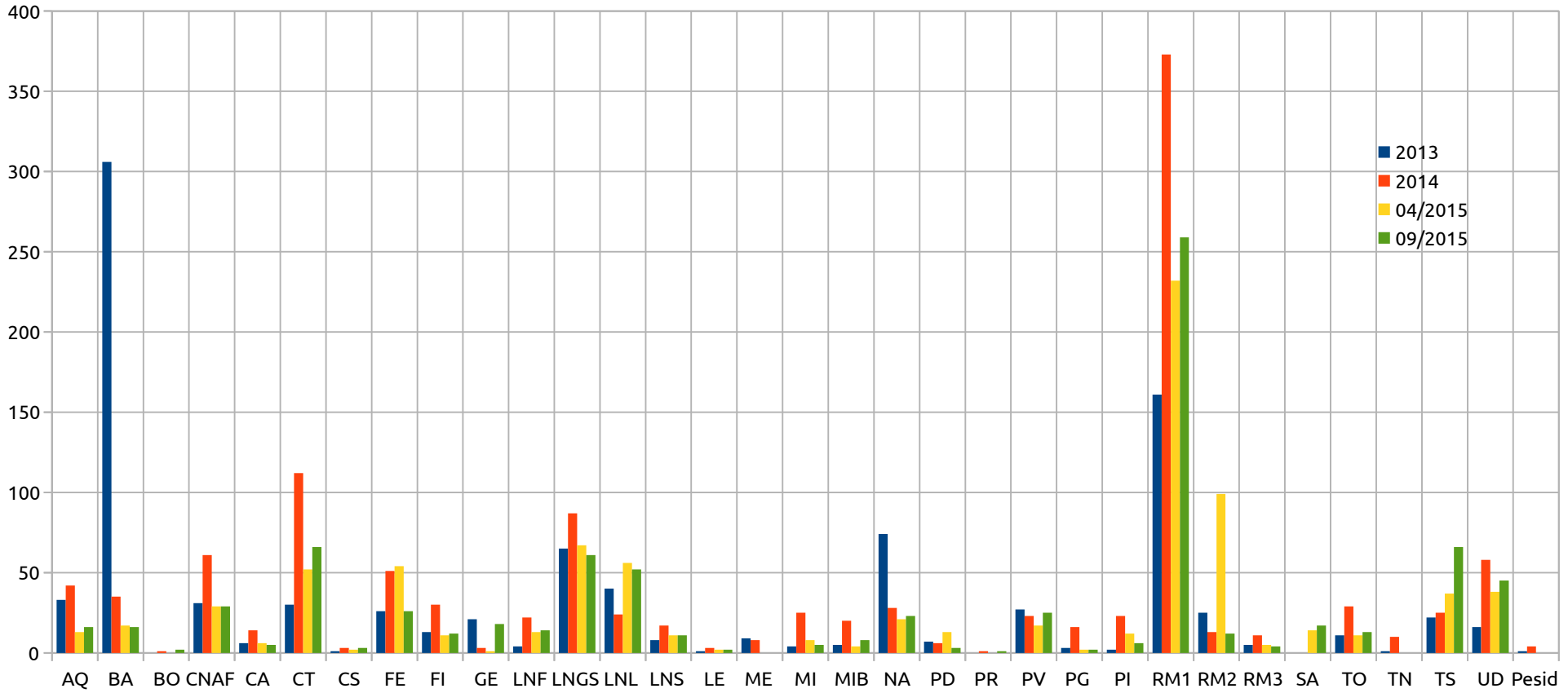
Scansioni periodiche

- Nessus (Professional Feed)
- Nodi:
  - 2013: 3137
  - 2014: 3928
  - 2015
    - aprile: 3647
    - **settembre: 3479**

Vulnerabilità gravi (per porta)

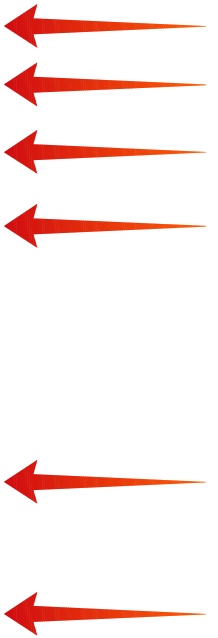


Vulnerabilita gravi (per Struttura)



Principali porte aperte (10/15)

Servizio	Porta	# Vuln.	# porte aperte
ssh	22	90 (35)	1951 (2187)
http	80	238 (238)	931 (927)
https	443 + 8443	146 (172)	738 (740)
mysql	3306		212 (233)
printer	631 + 515 + 9100		193 (247)
VNC	5900-3	6 (5)	132 (185)
ganglia	8649	(5)	151 (156)
nrpe (nagios)	5666	39 (45)	116 (126)
smtp	25	3 (3)	102 (92)
domain	53		83 (88)
sunrpc	111		25 (78)
netbios-ssn	139	- (62)	- (31)
IPMI	623/u	28	12 (19)
x11	6000	- (2)	32 (33)
ftp	21	1 (-)	15 (13)
tftp	69/u		1 (10)
shell / rsh	514	1 (1)	4 (8)

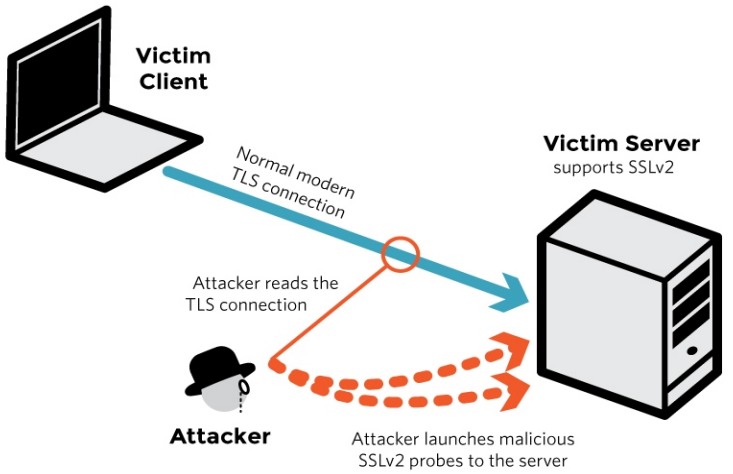


Vulnerabilità gravi web (3/16)

- 18 - OpenSSL Unsupported
- 5 - Apache 2.2.x < 2.2.15 Multiple Vulnerabilities
- 2 - Apache mod_proxy Content-Length Overflow
- 2 - OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities
- 2 - X11 Server Unauthenticated Access
- 2 - Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow
- 2 - X Server Unauthenticated Access: Screenshot
- 2 - HP System Management Homepage < 7.4.1 Single Sign On Buffer Overflow RCE
- 2 - ESXi 5.5 < Build 3568722 / 6.0 < Build 3568940 glibc DNS Resolver RCE
- 1 - Samba 'AndX' Request Heap-Based Buffer Overflow
- 1 - Nessus Unsupported Version Detection
- 1 - Tivoli Storage Manager Server Unsupported Product
- 1 - VMware ESXi 5.5 < Build 3029944 OpenSLP RCE (VMSA-2015-0007)

poodle, freak & DROWN

- **poodle**
  - vulnerabili al 3/16: **10**
- **freak**
  - vulnerabili al 3/16: **137**
- **DROWN**
  - vulnerabili al 3/16: **64**



Rimedi

- apache (**ssl.conf**)

  SSLProtocol all -SSLv3 -SSLv2

- postfix (**main.cf**)

  smtpd_tls_mandatory_protocols=!SSLv2, !SSLv3

- dovecot (**/etc/dovecot/conf.d/10-ssl.conf**)

  ssl_protocols = !SSLv3 !SSLv2

- **http://v.gd/gFhBHH**

TLS e CA

- SHA1 verso il fine vita
- Utilizzate il servizio **GARR TCS**!
- Verifica configurazioni:
  - server: **v.gd/YACdaO**
  - browser: **v.gd/TRPyiG**

AAI

- Ultime due campagne di phishing verso AAI
  - da dati netflow (campionati 10^{-3}) 60 connessioni (alcune ripetute molte volte)
  - il primo phishing non richiedeva la vecchia password, ma il secondo sì
  - quante password AAI sono state compromesse?
- Un sistema legato ad una sola password è inaccettabile
- **Indispensabile un meccanismo OTP**