Update on Pakiti

Romain Wartel, CERN IT

EGEE Operational Security Coordination Team

OSCT5, 18-19 March 2008

www.eu-egee.org

Information Society and Media

Current version

Pakiti enables system administrators to monitor the patching status or a large number of systems.

- **It is hosted on SourceForge and maintained by CERN/EGEE OSCT**
- **See http://pakiti.sourceforge.net**

Limitation of the current version

- Client requires root access
- Client has several dependencies
- Client relies on the availability of Yum, APT, or up2date

This make the client unsuitable for grid monitoring. Also

- Difficult/impossible to categorise patches (bug fix, security, etc.)
- It is then more difficult to prioritise tasks and detect real problems

Wouldn't it be great to monitor the security patches on our grid services?

Main challenges

- Previous “security plugin” attempt was limited:
  - Security plugin works only for SL 3.x and SL 4.x (= no other RedHat flavor)
  - Security plugin is time-consuming to maintain
  - Security plugin significantly increases the load on the server (scalability problems)
  - Security plugin does not tell what is the vulnerability
  - Heavy client, hard to deploy on grid services

What we would need

To deploy Pakiti in EGEE we would need:

- On the client side:
  - No root access, lightweight client
  - No/little dependencies
  - Avoid relying on a package manager (Yum, APT, etc.)

  ==> simply send the list of installed packages?

- On the server side:
  - A clear list of security patches, in a standard format
  - No/little dependencies
  - Avoid relying on a package manager (Yum, APT, etc.)

  ==> OVAL data?

OVAL

- Open Vulnerability and Assessment Language (OVAL) is a MITRE standard:

"OVAL is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services."

http://oval.mitre.org/

- There are OVAL repositories for various vendors, including HP, Microsoft, SUN Solaris, NIST and Red Hat .

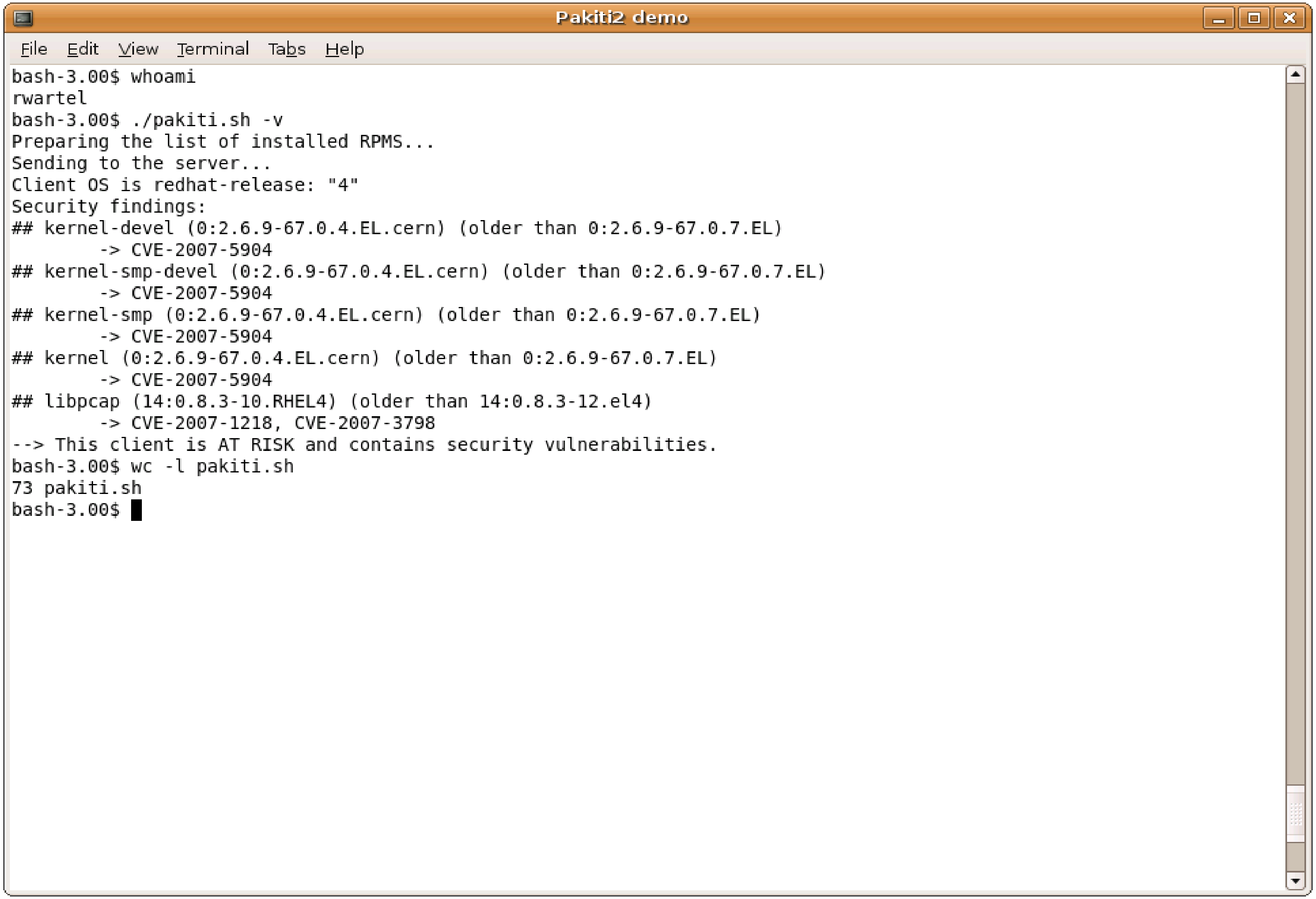
- It is then possible to merge OVAL information with the list of installed packages

Pakiti 2

Pakiti 2 is being developed:

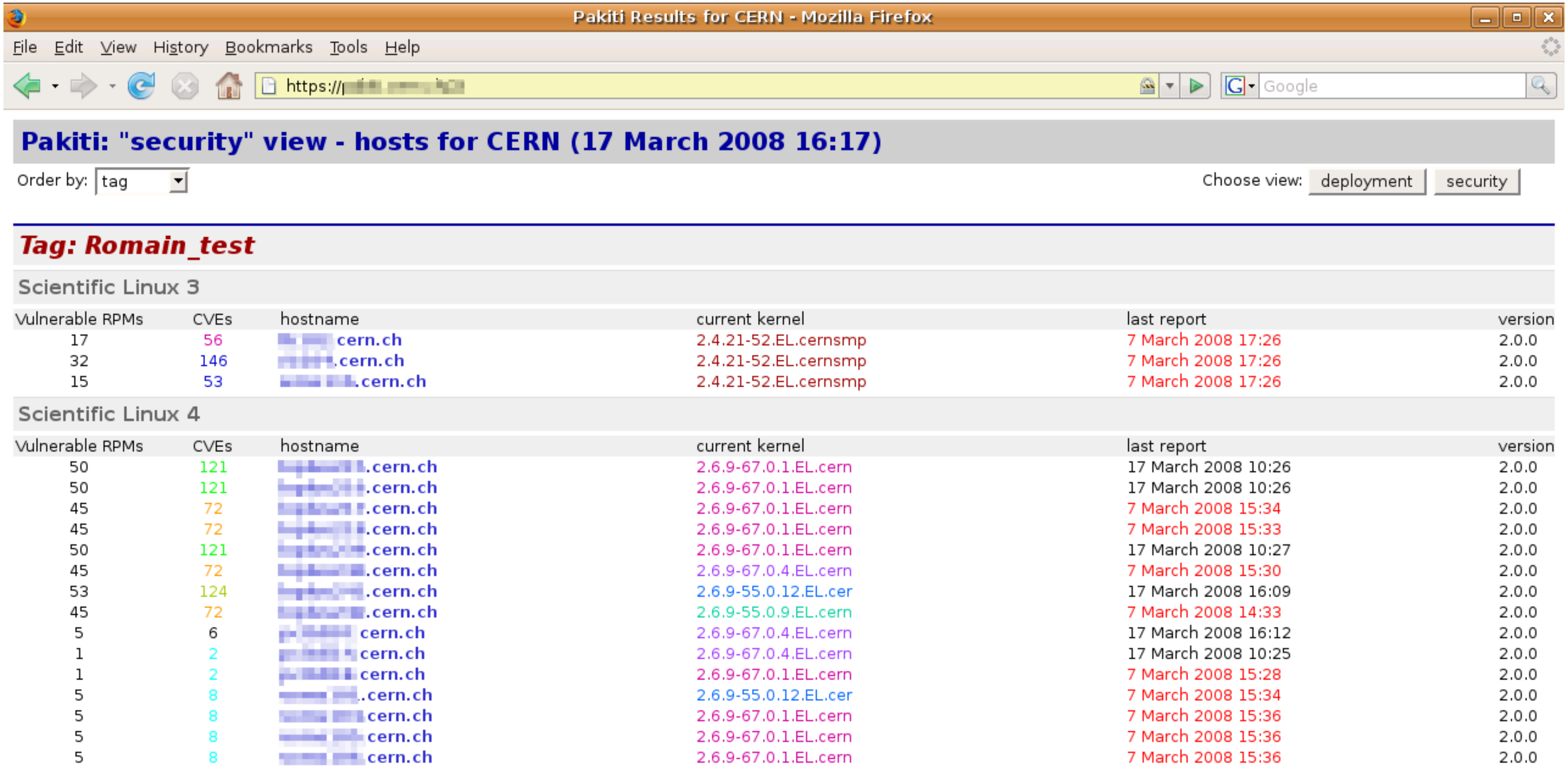
- **It uses OVAL data from Red Hat (other vendors can be supported)**
- **It includes a lightweight shell script on the clients**
- **It is not backward compatible**

Pakiti 2 “client”



```
bash-3.00$ whoami
rwartel
bash-3.00$ ./pakiti.sh -v
Preparing the list of installed RPMS...
Sending to the server...
Client OS is redhat-release: "4"
Security findings:
## kernel-devel (0:2.6.9-67.0.4.EL.cern) (older than 0:2.6.9-67.0.7.EL)
        -> CVE-2007-5904
## kernel-smp-devel (0:2.6.9-67.0.4.EL.cern) (older than 0:2.6.9-67.0.7.EL)
        -> CVE-2007-5904
## kernel-smp (0:2.6.9-67.0.4.EL.cern) (older than 0:2.6.9-67.0.7.EL)
        -> CVE-2007-5904
## kernel (0:2.6.9-67.0.4.EL.cern) (older than 0:2.6.9-67.0.7.EL)
        -> CVE-2007-5904
## libpcap (14:0.8.3-10.RHEL4) (older than 14:0.8.3-12.el4)
        -> CVE-2007-1218, CVE-2007-3798
--> This client is AT RISK and contains security vulnerabilities.
bash-3.00$ wc -l pakiti.sh
73 pakiti.sh
bash-3.00$ 
```

Pakiti 2 “server” 1/5


Pakiti Results for CERN - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://[redacted]
Google

Pakiti: "security" view - hosts for CERN (17 March 2008 16:17)

Order by: tag

Choose view: deployment security

Tag: Romain_test

Scientific Linux 3

Vulnerable RPMs	CVEs	hostname	current kernel	last report	version
17	56	[redacted] cern.ch	2.4.21-52.EL.cernsmp	7 March 2008 17:26	2.0.0
32	146	[redacted].cern.ch	2.4.21-52.EL.cernsmp	7 March 2008 17:26	2.0.0
15	53	[redacted].cern.ch	2.4.21-52.EL.cernsmp	7 March 2008 17:26	2.0.0

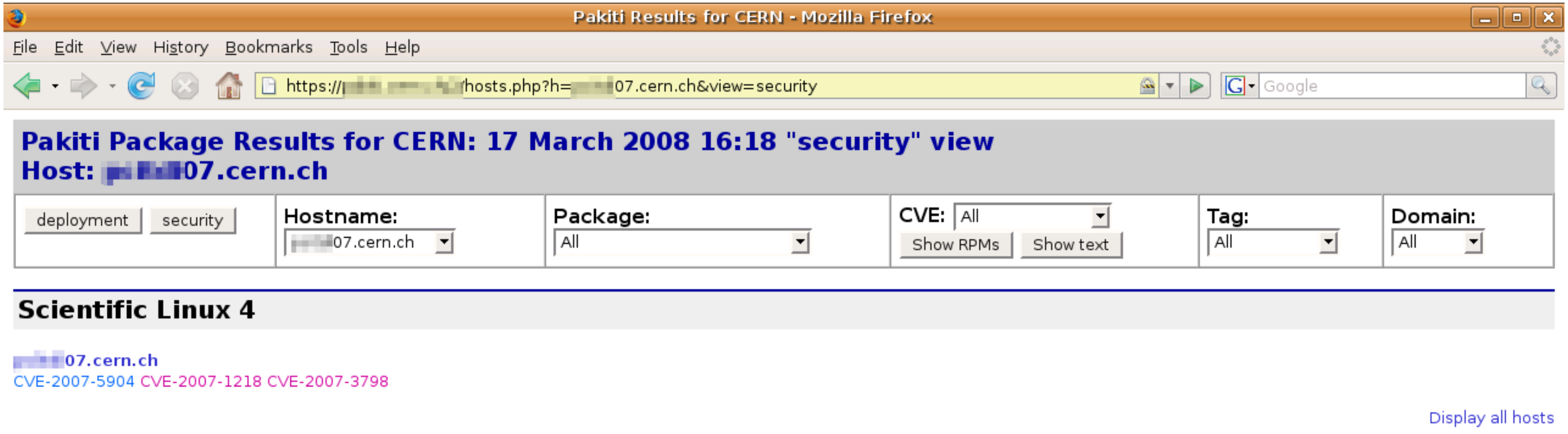
Scientific Linux 4

Vulnerable RPMs	CVEs	hostname	current kernel	last report	version
50	121	[redacted].cern.ch	2.6.9-67.0.1.EL.cern	17 March 2008 10:26	2.0.0
50	121	[redacted].cern.ch	2.6.9-67.0.1.EL.cern	17 March 2008 10:26	2.0.0
45	72	[redacted].cern.ch	2.6.9-67.0.1.EL.cern	7 March 2008 15:34	2.0.0
45	72	[redacted].cern.ch	2.6.9-67.0.1.EL.cern	7 March 2008 15:33	2.0.0
50	121	[redacted].cern.ch	2.6.9-67.0.1.EL.cern	17 March 2008 10:27	2.0.0
45	72	[redacted].cern.ch	2.6.9-67.0.4.EL.cern	7 March 2008 15:30	2.0.0
53	124	[redacted].cern.ch	2.6.9-55.0.12.EL.cer	17 March 2008 16:09	2.0.0
45	72	[redacted].cern.ch	2.6.9-55.0.9.EL.cern	7 March 2008 14:33	2.0.0
5	6	[redacted] cern.ch	2.6.9-67.0.4.EL.cern	17 March 2008 16:12	2.0.0
1	2	[redacted] cern.ch	2.6.9-67.0.4.EL.cern	17 March 2008 10:25	2.0.0
1	2	[redacted] cern.ch	2.6.9-67.0.1.EL.cern	7 March 2008 15:28	2.0.0
5	8	[redacted].cern.ch	2.6.9-55.0.12.EL.cer	7 March 2008 15:34	2.0.0
5	8	[redacted]cern.ch	2.6.9-67.0.1.EL.cern	7 March 2008 15:36	2.0.0
5	8	[redacted] cern.ch	2.6.9-67.0.1.EL.cern	7 March 2008 15:36	2.0.0
5	8	[redacted] cern.ch	2.6.9-67.0.1.EL.cern	7 March 2008 15:36	2.0.0

New Pakiti interface!

The “security view” displays the number of vulnerable RPMS installed, and the number of pending CVEs per node.

Pakiti 2 “server” 2/5


Pakiti Results for CERN - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google

https://[redacted]hosts.php?h=[redacted]07.cern.ch&view=security

Pakiti Package Results for CERN: 17 March 2008 16:18 "security" view
Host: [redacted]07.cern.ch

deployment security	Hostname: [redacted]07.cern.ch	Package: All	CVE: All Show RPMs Show text	Tag: All	Domain: All

Scientific Linux 4

[redacted]07.cern.ch
CVE-2007-5904 CVE-2007-1218 CVE-2007-3798

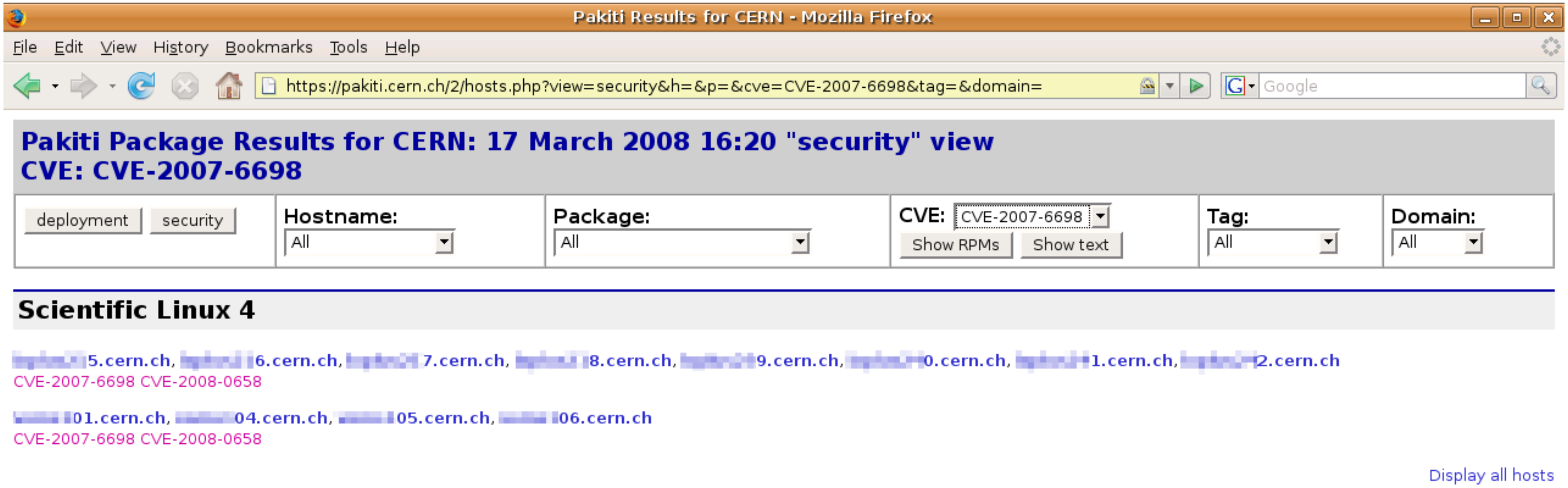
Display all hosts

As before, clicking on a hostname reveals more information on its patching status.

This time, we focus on vulnerabilities and CVEs

The colors DO NOT indicate a degree of severity

Pakiti 2 “server” 3/5


Pakiti Results for CERN - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
deployment
security
Show RPMs
Show text
Display all hosts

https://pakiti.cern.ch/2/hosts.php?view=security&h=&p=&cve=CVE-2007-6698&tag=&domain=

Pakiti Package Results for CERN: 17 March 2008 16:20 "security" view CVE: CVE-2007-6698

Hostname: All

Package: All

CVE: CVE-2007-6698

Tag: All

Domain: All

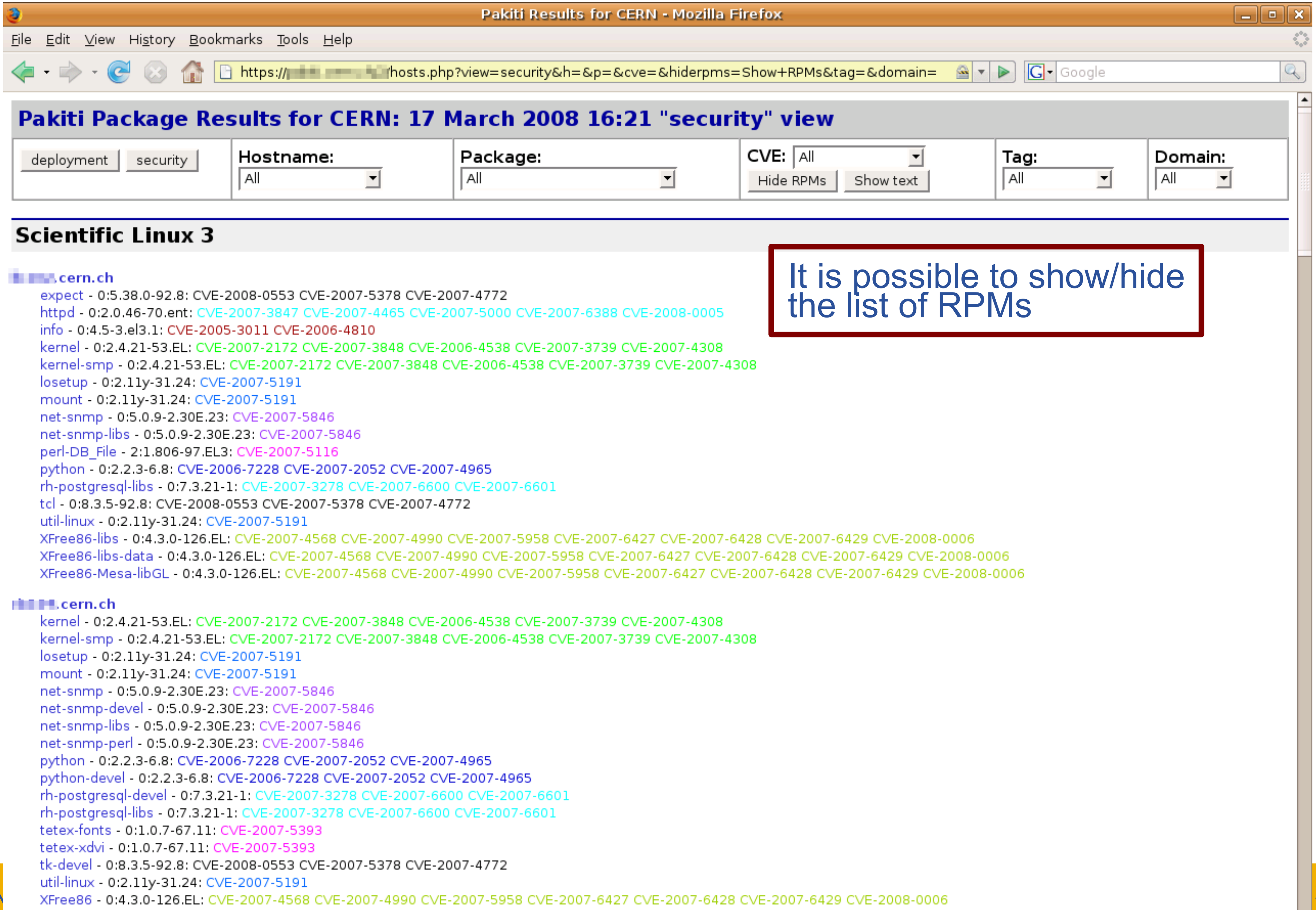
Scientific Linux 4

[redacted]5.cern.ch, [redacted]6.cern.ch, [redacted]7.cern.ch, [redacted]8.cern.ch, [redacted]9.cern.ch, [redacted]0.cern.ch, [redacted]1.cern.ch, [redacted]2.cern.ch
CVE-2007-6698 CVE-2008-0658

[redacted]01.cern.ch, [redacted]04.cern.ch, [redacted]05.cern.ch, [redacted]06.cern.ch
CVE-2007-6698 CVE-2008-0658

It is possible to search all hosts vulnerable to a given CVE.

Pakiti 2 “server” 4/5


Pakiti Results for CERN - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google

https://[redacted]hosts.php?view=security&h=&p=&cve=&hiderpms=Show+RPMs&tag=&domain=

Pakiti Package Results for CERN: 17 March 2008 16:21 "security" view

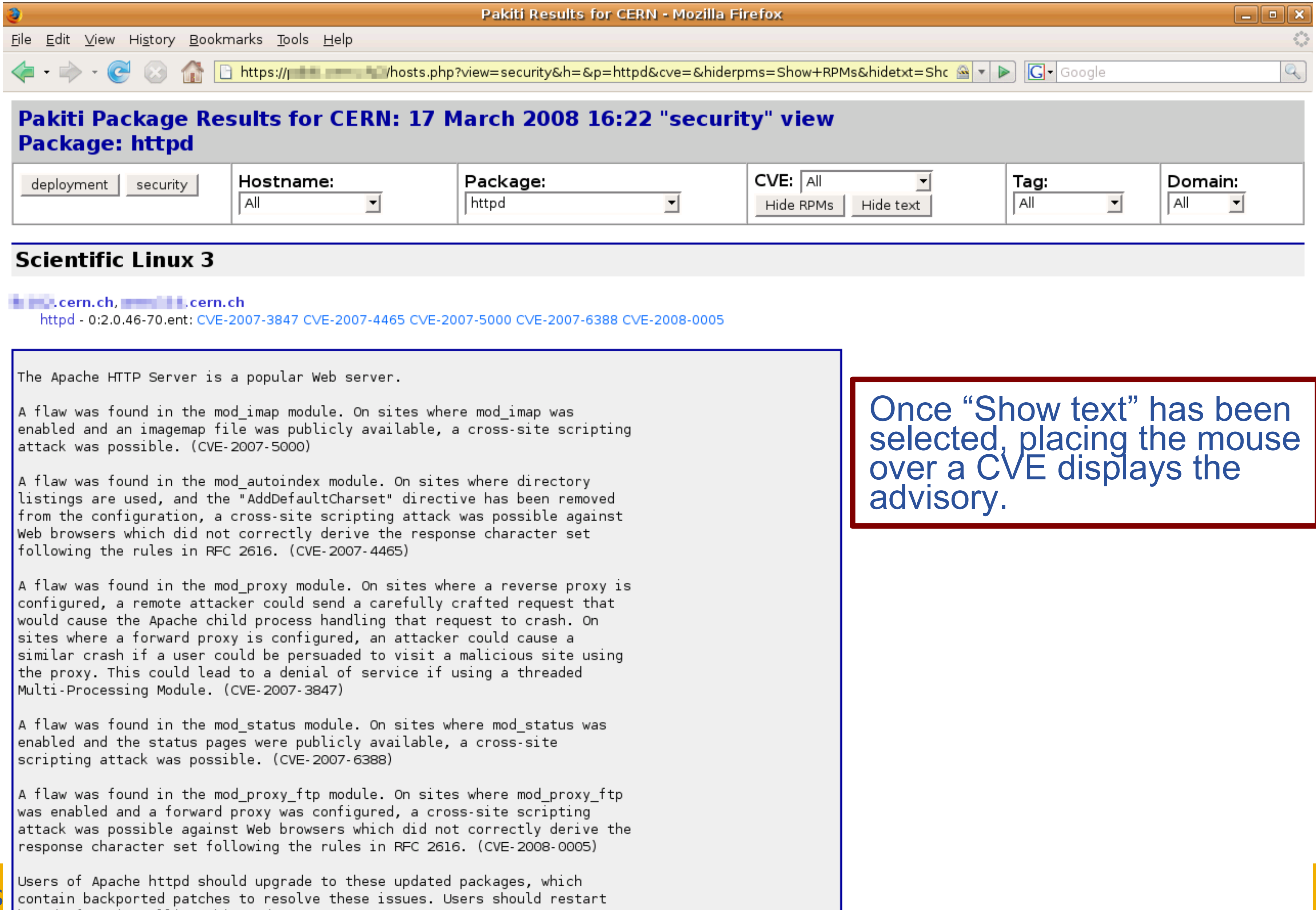
Scientific Linux 3

It is possible to show/hide the list of RPMs

```
[redacted].cern.ch
    expect - 0:5.38.0-92.8: CVE-2008-0553 CVE-2007-5378 CVE-2007-4772
    httpd - 0:2.0.46-70.ent: CVE-2007-3847 CVE-2007-4465 CVE-2007-5000 CVE-2007-6388 CVE-2008-0005
    info - 0:4.5-3.el3.1: CVE-2005-3011 CVE-2006-4810
    kernel - 0:2.4.21-53.EL: CVE-2007-2172 CVE-2007-3848 CVE-2006-4538 CVE-2007-3739 CVE-2007-4308
    kernel-smp - 0:2.4.21-53.EL: CVE-2007-2172 CVE-2007-3848 CVE-2006-4538 CVE-2007-3739 CVE-2007-4308
    losetup - 0:2.11y-31.24: CVE-2007-5191
    mount - 0:2.11y-31.24: CVE-2007-5191
    net-snmp - 0:5.0.9-2.30E.23: CVE-2007-5846
    net-snmp-libs - 0:5.0.9-2.30E.23: CVE-2007-5846
    perl-DB_File - 2:1.806-97.EL3: CVE-2007-5116
    python - 0:2.2.3-6.8: CVE-2006-7228 CVE-2007-2052 CVE-2007-4965
    rh-postgresql-libs - 0:7.3.21-1: CVE-2007-3278 CVE-2007-6600 CVE-2007-6601
    tcl - 0:8.3.5-92.8: CVE-2008-0553 CVE-2007-5378 CVE-2007-4772
    util-linux - 0:2.11y-31.24: CVE-2007-5191
    XFree86-libs - 0:4.3.0-126.EL: CVE-2007-4568 CVE-2007-4990 CVE-2007-5958 CVE-2007-6427 CVE-2007-6428 CVE-2007-6429 CVE-2008-0006
    XFree86-libs-data - 0:4.3.0-126.EL: CVE-2007-4568 CVE-2007-4990 CVE-2007-5958 CVE-2007-6427 CVE-2007-6428 CVE-2007-6429 CVE-2008-0006
    XFree86-Mesa-libGL - 0:4.3.0-126.EL: CVE-2007-4568 CVE-2007-4990 CVE-2007-5958 CVE-2007-6427 CVE-2007-6428 CVE-2007-6429 CVE-2008-0006

[redacted].cern.ch
    kernel - 0:2.4.21-53.EL: CVE-2007-2172 CVE-2007-3848 CVE-2006-4538 CVE-2007-3739 CVE-2007-4308
    kernel-smp - 0:2.4.21-53.EL: CVE-2007-2172 CVE-2007-3848 CVE-2006-4538 CVE-2007-3739 CVE-2007-4308
    losetup - 0:2.11y-31.24: CVE-2007-5191
    mount - 0:2.11y-31.24: CVE-2007-5191
    net-snmp - 0:5.0.9-2.30E.23: CVE-2007-5846
    net-snmp-devel - 0:5.0.9-2.30E.23: CVE-2007-5846
    net-snmp-libs - 0:5.0.9-2.30E.23: CVE-2007-5846
    net-snmp-perl - 0:5.0.9-2.30E.23: CVE-2007-5846
    python - 0:2.2.3-6.8: CVE-2006-7228 CVE-2007-2052 CVE-2007-4965
    python-devel - 0:2.2.3-6.8: CVE-2006-7228 CVE-2007-2052 CVE-2007-4965
    rh-postgresql-devel - 0:7.3.21-1: CVE-2007-3278 CVE-2007-6600 CVE-2007-6601
    rh-postgresql-libs - 0:7.3.21-1: CVE-2007-3278 CVE-2007-6600 CVE-2007-6601
    tetex-fonts - 0:1.0.7-67.11: CVE-2007-5393
    tetex-xdvi - 0:1.0.7-67.11: CVE-2007-5393
    tk-devel - 0:8.3.5-92.8: CVE-2008-0553 CVE-2007-5378 CVE-2007-4772
    util-linux - 0:2.11y-31.24: CVE-2007-5191
    XFree86 - 0:4.3.0-126.EL: CVE-2007-4568 CVE-2007-4990 CVE-2007-5958 CVE-2007-6427 CVE-2007-6428 CVE-2007-6429 CVE-2008-0006
```

Pakiti 2 “server” 5/5


Pakiti Results for CERN - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://[redacted]/hosts.php?view=security&h=&p=httpd&cve=&hiderpms=Show+RPMs&hidetxt=Shc
Google

Pakiti Package Results for CERN: 17 March 2008 16:22 "security" view
Package: httpd

deployment
security
Hostname: All
Package: httpd
CVE: All
Hide RPMs
Hide text
Tag: All
Domain: All

Scientific Linux 3

[redacted].cern.ch, [redacted].cern.ch
httpd - 0:2.0.46-70.ent: CVE-2007-3847 CVE-2007-4465 CVE-2007-5000 CVE-2007-6388 CVE-2008-0005

```
The Apache HTTP Server is a popular Web server.

A flaw was found in the mod_imap module. On sites where mod_imap was
enabled and an imagemap file was publicly available, a cross-site scripting
attack was possible. (CVE-2007-5000)

A flaw was found in the mod_autoindex module. On sites where directory
listings are used, and the "AddDefaultCharset" directive has been removed
from the configuration, a cross-site scripting attack was possible against
Web browsers which did not correctly derive the response character set
following the rules in RFC 2616. (CVE-2007-4465)

A flaw was found in the mod_proxy module. On sites where a reverse proxy is
configured, a remote attacker could send a carefully crafted request that
would cause the Apache child process handling that request to crash. On
sites where a forward proxy is configured, an attacker could cause a
similar crash if a user could be persuaded to visit a malicious site using
the proxy. This could lead to a denial of service if using a threaded
Multi-Processing Module. (CVE-2007-3847)

A flaw was found in the mod_status module. On sites where mod_status was
enabled and the status pages were publicly available, a cross-site
scripting attack was possible. (CVE-2007-6388)

A flaw was found in the mod_proxy_ftp module. On sites where mod_proxy_ftp
was enabled and a forward proxy was configured, a cross-site scripting
attack was possible against Web browsers which did not correctly derive the
response character set following the rules in RFC 2616. (CVE-2008-0005)

Users of Apache httpd should upgrade to these updated packages, which
contain backported patches to resolve these issues. Users should restart
```

Once “Show text” has been selected, placing the mouse over a CVE displays the advisory.

Status and future work

- Current status: Testing/GUI improvements in progress
- Future work:
  - Packaging (one RPM for the client, one for the server)
  - Integration to SAM test
  - Integration on many CERN hosts being discussed (not only servers)
  - Check if gLite/GSVG could produce additional OVAL data

Feedback?