Testing and Monitoring Grid Systems

Michal Procházka, Daniel Kouřil

CESNET SA1

Outline

- Network services
- Remote vulnerabilities
- System patching status
- Containing user jobs

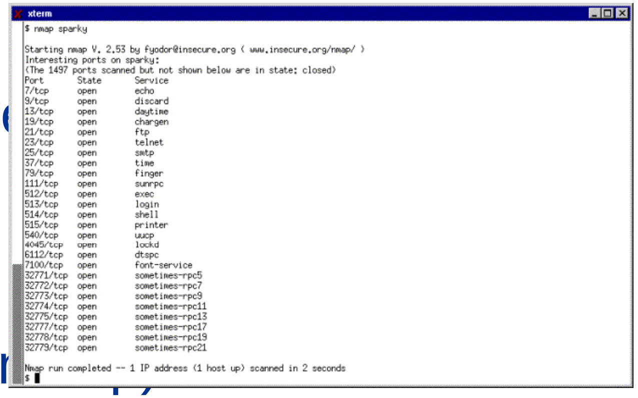
Network services

- **Network services**
  - Administrator should have an overview of running services on each host
  - Not all services are used and needed on a host
  - It is recommended to run only needed services
  - Test of the service presence can identify possible back-door
  - Useful to scan host remotely from local network and from outside the local network as well
  - Nmap for remote testing and netstat utility for local view on the listening services

http://insecure.org/nmap

Network services

- **Nmap**
  - Network exploration tool and security / port scanner
  - Common options:
    - -P0 - do not check wheter host is aliv
    - -oX - output in XML format
    - -p 1-65535 - range of ports to scan
    - -sR - test the RPC (same info as rpci p)
    - -sV - try to detect versions of listening programs
    - -sS - use TCP SYN scan - most popular
    - -sT - TCP Connect, -sU - UDP scan, -sA TCP ACK
    - -vv - level of verbosity
    - -O - try to detect OS



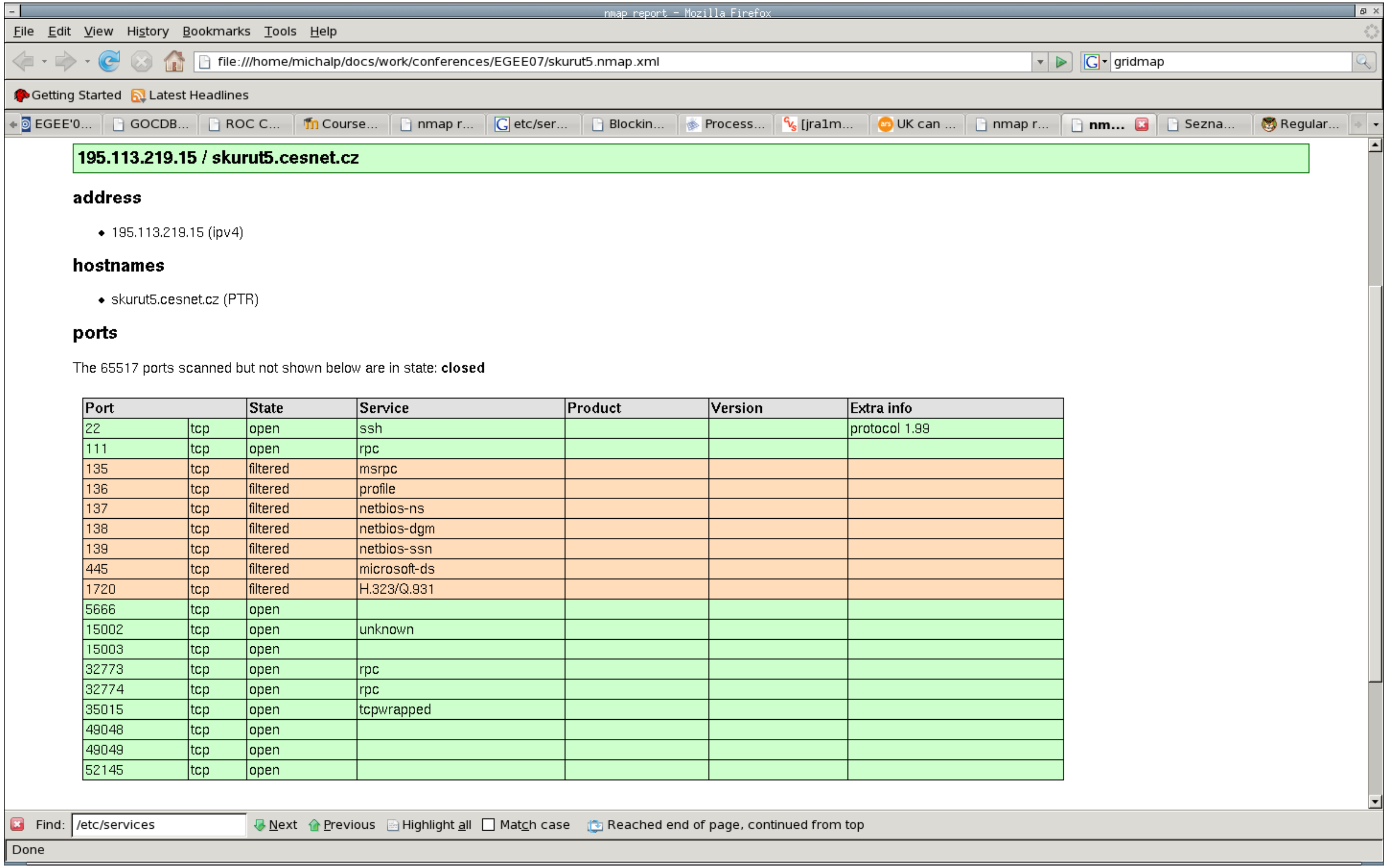
```
$ nmap sparky

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on sparky:
(The 1497 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
540/tcp    open        uucp
4045/tcp   open        lockd
6112/tcp   open        dtspc
7100/tcp   open        font-service
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7
32773/tcp  open        sometimes-rpc9
32774/tcp  open        sometimes-rpc11
32775/tcp  open        sometimes-rpc13
32777/tcp  open        sometimes-rpc17
32778/tcp  open        sometimes-rpc19
32779/tcp  open        sometimes-rpc21

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
$ ▌
```

Network services

- **Nmap**
  - List of well-know ports used in grids is available from the gLite CVS:

    http://glite.cvs.cern.ch/cgi-bin/glite.cgi/org.glite.siteinfo.ports/doc/middleware-ports.txt?revision=HEAD&view=markup
  - Fill /etc/services with the entries from above link on machine which is used to scan other machines

- ## Example of Nmap output


nmap report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/michalp/docs/work/conferences/EGEE07/skurut5.nmap.xml
gridmap
Getting Started
Latest Headlines
EGEE'0... GOCDB... ROC C... Course... nmap r... etc/ser... Blockin... Process... [jra1m... UK can ... nmap r... nm... Sezna... Regular...
Find: /etc/services
Next
Previous
Highlight all
□ Match case
Reached end of page, continued from top
Done

195.113.219.15 / skurut5.cesnet.cz

address

- 195.113.219.15 (ipv4)

hostnames

- skurut5.cesnet.cz (PTR)

ports

The 65517 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra info
22	tcp	open	ssh			protocol 1.99
111	tcp	open	rpc			
135	tcp	filtered	msrpc			
136	tcp	filtered	profile			
137	tcp	filtered	netbios-ns			
138	tcp	filtered	netbios-dgm			
139	tcp	filtered	netbios-ssn			
445	tcp	filtered	microsoft-ds			
1720	tcp	filtered	H.323/Q.931			
5666	tcp	open				
15002	tcp	open	unknown			
15003	tcp	open				
32773	tcp	open	rpc			
32774	tcp	open	rpc			
35015	tcp	open	tcpwrapped			
49048	tcp	open				
49049	tcp	open				
52145	tcp	open				

Network services

- **Netstat**
  - Show network connections, interface statistics, ...
  - Common options:
    - -n show numerical address of host, do not perform name resolution
    - --numeric-hosts do not perform name resolution but show names of ports and usernames
    - -e show additional information like inodes and user IDs
    - -p show programs that belong to specific sockets
    - -l show only listening sockets
    - --inet reduce the output only on inet protocol

Remote vulnerabilities

- **Remote vulnerabilities**
  - Test known vulnerabilities of network serv
  - Scan ports on target host and perform the tests on open ports to check which service runs on it and then test the service for known vulnerabilities
  - It is recommended to test periodically all hosts
  - Results of the scan should be compared with the entries in the patch management

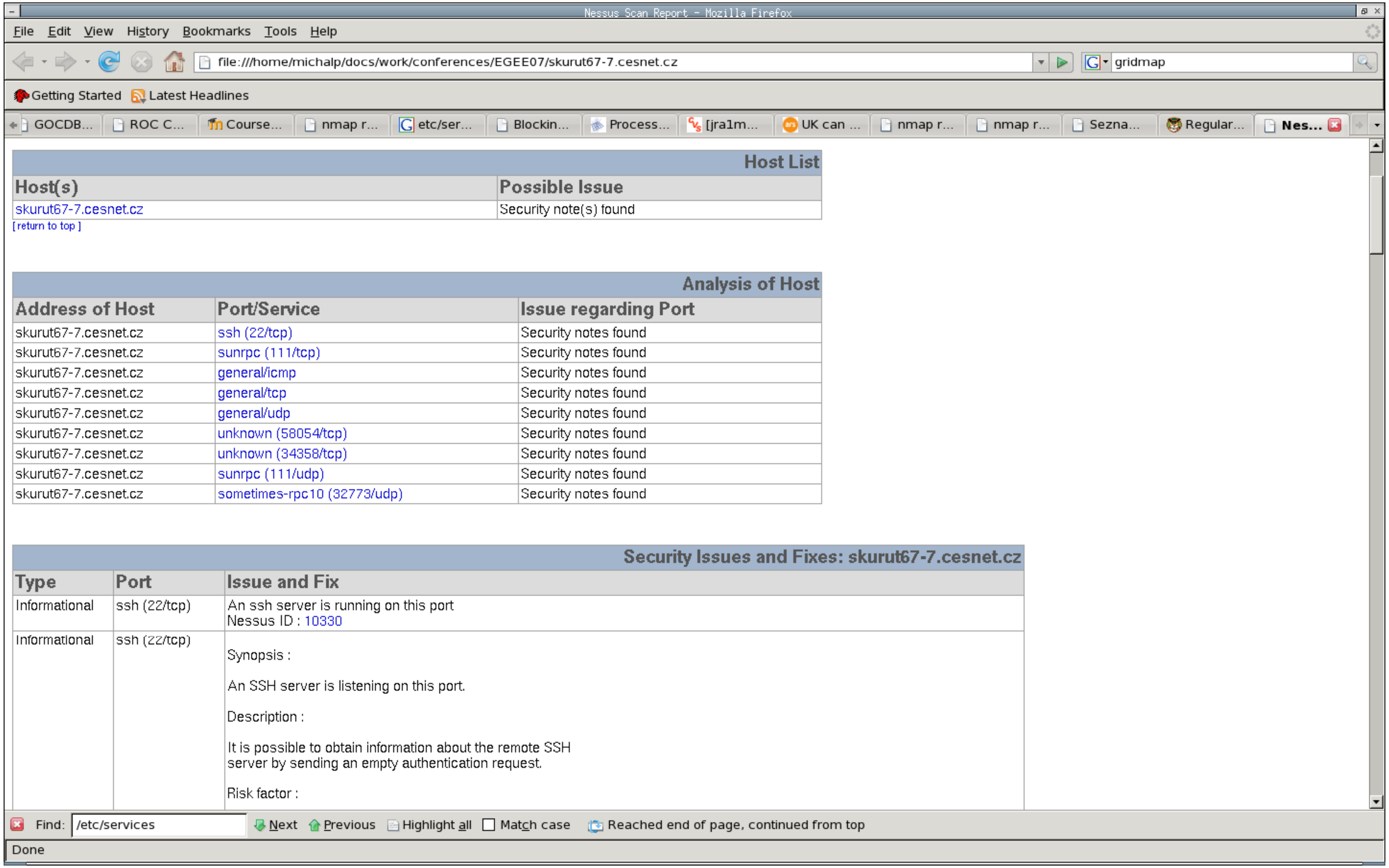
Remote vulnerabilities

- **Nessus**
  - Security auditing software
  - 21.9.2007: 15523 registered plugins
  - It is difficult to select appropriate plugins
  - Client-server architecture – GUI and CLI clients
  - All tests are run from the server
  - Good practise is to run two instances – one on internal network and second one on the external network
  - Nessus produces a lot of warnings => difficult to read the results in case of high number of hosts => make diffs on the results

http://www.nessus.org/nessus

Remote vulnerabilities

- ## Example of Nessus output


Nessus Scan Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/michalp/docs/work/conferences/EGEE07/skurut67-7.cesnet.cz
gridmap
Getting Started Latest Headlines
GOCDB... ROC C... Course... nmap r... etc/ser... Blockin... Process... [jra1m... UK can ... nmap r... nmap r... Sezna... Regular... Nes...

Host List	
Host(s)	**Possible Issue**
skurut67-7.cesnet.cz	Security note(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
skurut67-7.cesnet.cz	ssh (22/tcp)	Security notes found
skurut67-7.cesnet.cz	sunrpc (111/tcp)	Security notes found
skurut67-7.cesnet.cz	general/icmp	Security notes found
skurut67-7.cesnet.cz	general/tcp	Security notes found
skurut67-7.cesnet.cz	general/udp	Security notes found
skurut67-7.cesnet.cz	unknown (58054/tcp)	Security notes found
skurut67-7.cesnet.cz	unknown (34358/tcp)	Security notes found
skurut67-7.cesnet.cz	sunrpc (111/udp)	Security notes found
skurut67-7.cesnet.cz	sometimes-rpc10 (32773/udp)	Security notes found

Security Issues and Fixes: skurut67-7.cesnet.cz		
Type	**Port**	**Issue and Fix**
Informational	ssh (22/tcp)	An ssh server is running on this port Nessus ID : 10330
Informational	ssh (22/tcp)	Synopsis : An SSH server is listening on this port. Description : It is possible to obtain information about the remote SSH server by sending an empty authentication request. Risk factor :

System patches status

- **System patches status**
  - Applying the security patches is necessary
  - Different types of packages systems to control (apt, yum, up2date)
  - Hard to recognize which updates are security updates
  - Hard to maintain security patches on all hosts (error prone, e.g. when a machine is in maintenance during patches installation, update process crashes on the host, ...)
  - Monitor state of patches on registered hosts and compare against released ones

System patches status

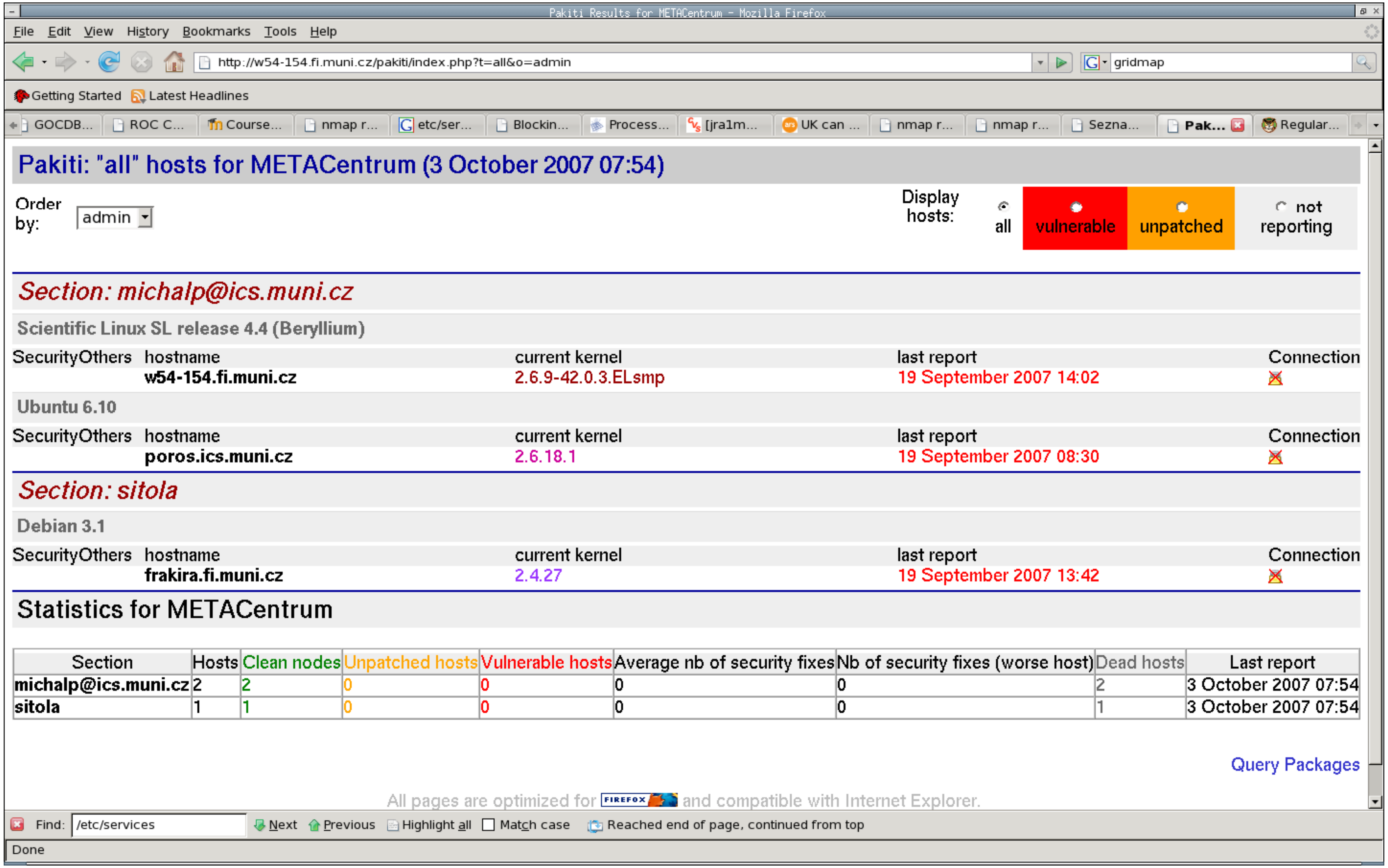
- **Pakiti**
  - Support of packages systems apt, yum, up2date
  - Client-server architecture
  - Server receives messages from the clients as a http POST request
  - Only monitor state of packages, do not install any package
  - Server supports web based output with various views on state of hosts and packages
  - Minimal installation requirements on the client (curl, perl), script is run every day by cron
  - Communication could be secured by HTTPs
  - Pakiti server can send its statistics to other trusted Pakiti server

http://pakiti.sourceforge.net

Enabling Grids for E-sciencE

System patches status

- ## Pakiti example



Pakiti: "all" hosts for METACentrum (3 October 2007 07:54)

Order by: admin

Display hosts: ● all ○ vulnerable ○ unpatched ○ not reporting

Section: michalp@ics.muni.cz

Scientific Linux SL release 4.4 (Beryllium)

SecurityOthers	hostname	current kernel	last report	Connection
	w54-154.fi.muni.cz	2.6.9-42.0.3.ELsmp	19 September 2007 14:02	☒

Ubuntu 6.10

SecurityOthers	hostname	current kernel	last report	Connection
	poros.ics.muni.cz	2.6.18.1	19 September 2007 08:30	☒

Section: sitola

Debian 3.1

SecurityOthers	hostname	current kernel	last report	Connection
	frakira.fi.muni.cz	2.4.27	19 September 2007 13:42	☒

Statistics for METACentrum

Section	Hosts	Clean nodes	Unpatched hosts	Vulnerable hosts	Average nb of security fixes	Nb of security fixes (worse host)	Dead hosts	Last report
michalp@ics.muni.cz	2	2	0	0	0	0	2	3 October 2007 07:54
sitola	1	1	0	0	0	0	1	3 October 2007 07:54

Query Packages

All pages are optimized for FIREFOX and compatible with Internet Explorer.

Containing user jobs

- **Containing user jobs**
  - SEs, CEs, WNs and RBs all grant some level of user level access via a batch job or with gridftp
  - Avoid users to run unwanted software (by cron or by at)
  - User processes can survive the job termination, it is problem of parent processes and children orphans
  - Possible place for back-door

Containing user jobs

- **How to deal with this problem?**
  - Filter ssh connections from off-site (it is not necessary)
    - Only root is needed to login at WNs, RBs, SEs
      - sshd_config: `AllowUsers root michalp`
    - On CEs, do not allow to create authorized_keys file for users
      - sshd_config: `AuthorizedKeysFile /root/.ssh/authorized_keys`
      - DenyGroups directive in sshd_config
  - Disble cron and at for users
    - Create file /etc/at.allow and /etc/cron.allow on WNs, RBs, SEs, Ces containing:
    - root, edginfo, edguser, rgma on separeted line
  - Using Virtual Machines
    - Each user's job has its own VM
    - After job termination the VM is destroyed

Containing user jobs

- **How to protect on batch nodes?**
  - On Torque: PBS MOM epilogue script
    - Reconstruct the proces tree
    - Find all user jobs UID>99 that are running (option -u MIN_UID)
    - Substract legitimate jobs
    - Kill off the remainer jobs
  - Script independent on the type of the batch system
    - Kill all user jobs (UID > =500) belonging to SID trees whose first ancestor is init (PPID 1)
    - It can run only by root
  - More info: http://www.sysadmin.hep.ac.uk/wiki/ProcessesOnBatchNodes

Information Pointer

Thank you for your attention!