Security Monitoring

Daniel Kouřil, CESNET
OSCT meeting, EGEE’08 Conference
**Goals of monitoring**

- **Detecting potential problems**
  - known issues that can lead to incident
  - early alerts to the administrators
- **Detecting existing incident**
  - help to resolve existing incidents
- **Help stop spreading ongoing attacks, ...**
  - detecting sites with similar configuration problems, etc.
- **Traceability**
  - using existing monitoring data to found out information about users’ activities
Current status

- **SAM framework used**
  - two SAM tests, third one contributed by Eygene recently (file permissions)
  - in production use, results available to ROC security contacts

- **Pakiti**
  - system to monitor and evaluate status of installed packages
  - alerts when a vulnerable package is detected
  - only collects publicly available data

- **Standard syslog messages**
  - still not used by all gLite components
  - central logging server highly recommended
    - LB-based messaging to transport syslog messages
Job Monitoring & Traceability

- LB keeps complete history of jobs submitted via WMS
- useful information for tracking jobs
  - what CEs have been used during last X hours by particular user
- **OSCT/JRA1 is working on a CLI tool to ease the information retrieval**

```
trace_jobs.sh "/DC=cz/DC=cesnet-ca/O=Masaryk University/CN=Daniel Kouril" \
skurut1.cesnet.cz  2008-06-22
```

https://skurut1.cesnet.cz:9000/0CUi8_1eoBRavGkoAqSafQ (Submitted):
  submitted to skurut68-1 WMS on Thu Jul  3 14:32:36 2008

https://skurut1.cesnet.cz:9000/5QsEfMN7GIJoUPF5ew234f (Done):
  CE used: grid012.ct.infn.it:2119/jobmanager-lcglsf-auger

https://skurut1.cesnet.cz:9000/PaeU3rrS9j-XxDsAczA6-g (Cleared):
  CE used: grid012.ct.infn.it:2119/jobmanager-lcglsf-auger
golias25.farm.particle.cz:2119/jobmanager-lcgpbs-gridauger

- **Currently, only LB “super-users” can access the data**
Future plans

- **How to monitor?**
  - framework, sensors
  - two levels to cover separately
    - grid services (WMS, VOMS) – operated by sites, ROC, … on behalf of a VO, project
    - resources, services at individual sites
- **What to monitor?**
  - quite long list can be generated by looking at GSVG records, OSCT advisories, discussions, etc.
  - focus only on the most important patterns
- **How to process results?**
  - security test operator
  - visibility of sensitive information
    - some sensitive data can be gathered even by normal users!
    - sensitivity vs. their usefulness
• **SAM framework has limitations**
  - only WNs can be monitored from inside (CRLs, CAs, ..)
  - some sensors may require high-rate of invocation
  - no additional support needed from the component administrators

• **Operations automation planning (SA1)**
  - multi-site monitoring, to replace current SAM eventually
  - could also trigger security tests
  - based on Nagios
    - integrates with existing Nagios installations
    - inside monitoring grid components (other than WNs)
  - prototype expected by end of 2008
What to monitor

• Results of (other) project activities
  – GSVG “Extreme Criticial” vulnerabilities
  – Insecure configuration (OSCT advisories, …)
What to monitor

- **LCG Risk analysis**
  - ISSeG, OSG, EGEE risk assessment docs
- **(M1) Resources used to launch online attacks on other sites via DOS, Virus, Worms, SPAM etc**
  - detection on site level (number of opened connection, increased traffic, etc.)
  - on the grid level detection of similar sites (where the job has been sent to, or that contain the same vulnerability in site component – available from the outside)
- **(M2) Resources used to distribute or share non-LCG data, e.g. copyrighted, illegal, or inappropriate material**
- **(D1) Disruption via exploitation of security holes**
- **(D8) Damage caused by viruses, worms, trojans or back-doors**
- **(A2) Development process results in insecure middleware**
• **Who is able to access the results?**
  – primarily service owners/operators
  – result evaluation can be difficult and time-consuming
  – tests shouldn’t generate (many) false positives

• **Site’s “self-monitoring”**
  – performed using our tools by site administrators
  – they can decide to share the results with ROCs/…
  – aggregated information useful too
    ▪ indicating the tests are used, may reveal in sensors implementations, …
  – stand-alone monitoring package
    ▪ containing all relevant security sensors
    ▪ quick audit for smaller sites
Future steps

• **Consolidation of OSCT resources on monitoring**
  - Italy (6PM), France (2PM), CE (4-6PM), Russia?

• **Get more information about OAT**

• **Add some security-related tests**
  - probably port the SAM ones
  - simple, no controversy

• **Integrate them with the OAT pilot release**
  - result visibility

• **Present to the sites/ROCs**