Security Training Experiences from Security Service Challenge 4

Ursula Epting

Karlsruher Institut für Technologie

Step 1 Acknowledge

2010-04-27 (timestamps UTC)

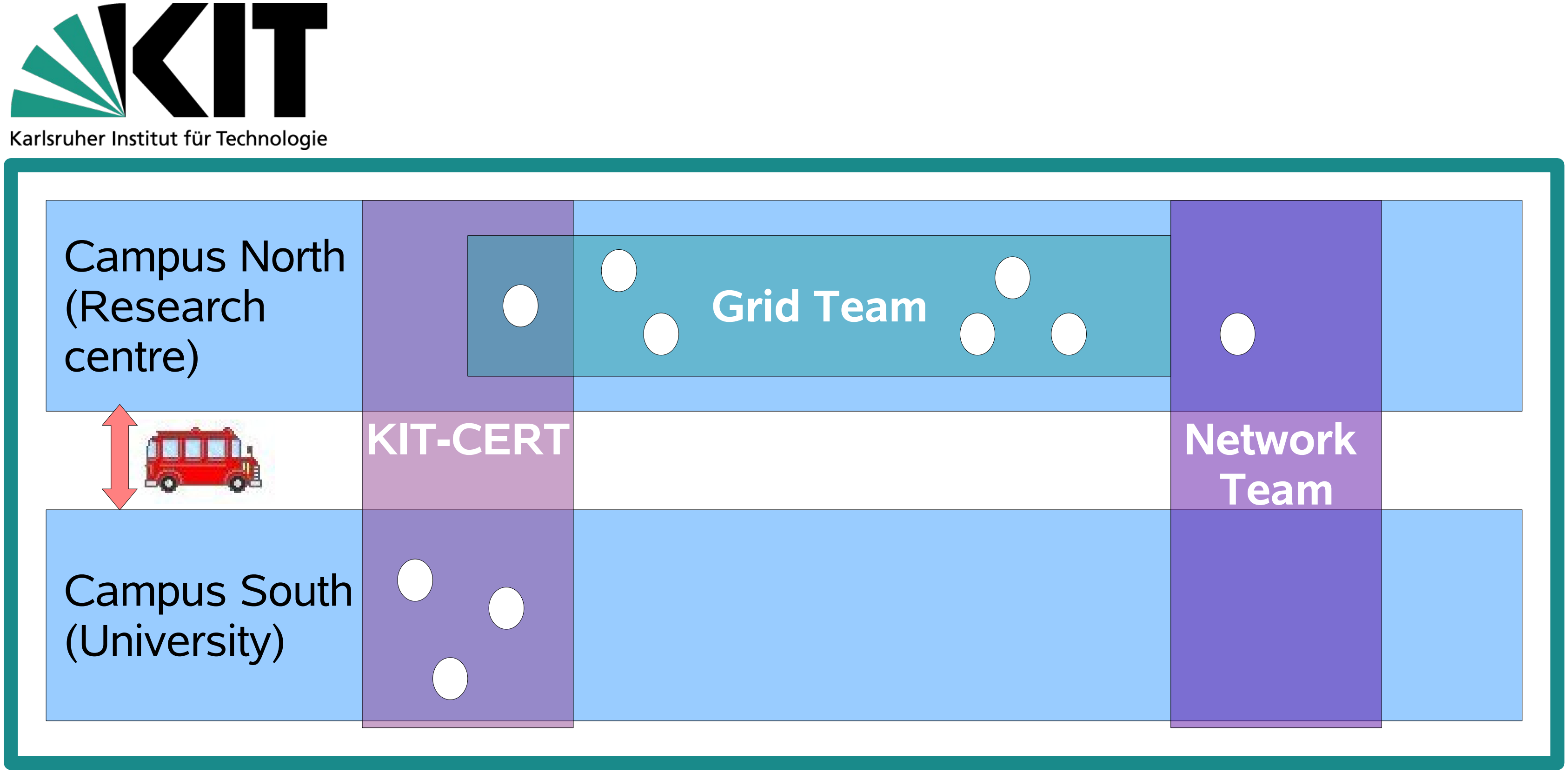
11:25 received alarm mail

11:36 sent Acknowledge, started investigation

- call on internal team consisting of GridMiddleware -, PBS-, Unix/Linux-, Network experts and KIT-CERT for a meeting
- until now Grid security coordination was not connected to KIT-CERT

Alarm

Involved Teams


Karlsruher Institut für Technologie
Campus North (Research centre)
Grid Team
KIT-CERT
Network Team
Campus South (University)

Step 2 confirm incident

11:40 Look at traffic between given Ips 192.108.46.24 (local NAT-GW address) and 195.140.243.2

11:44 found corresponding wn

11:47 found job running on wn

11:48 found user id - patlas33

11:53 set wn offline
for a real case mount home read-only to not disturb forensics!

Step 3 confirm and contain

12:03 saved home-directory of patlas33

12:05 stopped the Job, saved local information (processes, netstat,...)
Do not kill the job unless you have saved the home-dir!

12:22 found binary lutra_linux_64_rh5 with suspicious strings e.g. "Who shot the sheriff...", DN=/C=DE/ST=1337/L=H4x0rH0m3/O=I HaZ InternetZ/CN=Wunderbar

Binary was deeply analyzed (see next talk)

Step 4 communicate

12:56 Initial "Heads up" to csirt-list

Warn other sites to minimize damage globally! Follow the IR procedure!

13:35 banned user locally

Protect your resources!

13:39 Mail to Atlas-VO security list

Get information about user from the VO!

14:07 Answer from VO-management:

*job submitted by DN xy, with link to job details

Step 5 respond

14:27 asked VO-admin to contact the user to verify job submission
Misbehaving user or certificate compromised?

14:28 Analysis of Panda job information led to ui (difficult to understand Panda logs)

14:57 banned pilot job submitter
(just to be sure :)

Step 5 respond

15:35 sent update to SSC4-CSIRT list, including analysis job binary, ui, in parallel ongoing netflow and binary analysis
Keep others updated!

15:43 Mail to NIKHEF-CERT
ui - compromised?

16:33 Atlas-VO-management confirmed job not compatible with VO-Policy
=> user globally banned from pilot-job-framework – protect others!

Step 7

16:50 pilot job submitter unbanned

19:58 reply from NIKHEF-CERT ~ „we will take care of the user and ui…“

End of first day…

Step 8 dig further

During the next days 2010-04-28/29/30 we had more findings:

- job tried to install "at"-job
- user was also mapped to another local account atlas138
- globus-gridftp logs showed that file /etc/passwd of several nodes was read from another ui

Step 9 communicate

- Updates sent to VO-admins and NIKHEF-CERT regarding gridftp-transfers of user
- Update sent to NIKHEF-CERT regarding the used ui
- Sent updates to the csirt-List about deeper analysis of the binary, netflow analysis
- Mail to user himself asked to verify job submission (no answer received…)

Step 10 Close incident

2010-05-03 15:00 Sent final report to SSC4-CSIRT-list

Lessons learnt

wins

- combination of experience of grid- and cert-team
- team worked in one room, good communication
- improved internal procedures

fails

- NAT-Logs only held for short time ✓
- no access for non-griddies but cert-members to the nodes ✓
- little mess with timestamps on nodes and routers ✓

Next Step

Questions?