Security Service Challenge

SSC_2 Challenging Storage Elements

An update for the OSCT, 26 January 2007

Pål S. Anderssen
CERN - IT

Objective

The goal of the LCG/EGEE Security Service Challenge (SSC), is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available.

SSC_2 Challenges Grid Storage Elements (SE)

SSC_2 Progression

SSC_2 Time-line

- Stage_1
  - Principal site of each ROC challenged: October 2006
    - 11/11 ROCs responded
  - Debriefing input from ROCs November 2006
    - 8/11 ROCs provided input
  - Debriefing Report Circulated December 2006
- Stage_2
  - Challenge passed over to the ROCs January 2007
    - 6 Sites in CERN ROC challenged
      - 2 responses filed
      - 4 first level escalations
        - » 1 site followed with response
        - » 2 sites pleaded for indulgence
        - » 1 site needs second level escalation

SSC_2 Stage_1: Status December 2006

Stage_1: ROCs challenged in October 2006

	ROC	Responded	Debriefing Input
1.	AsiaPacific	√	√
2.	CentralEurope	√	√
3.	CERN	√	√
4.	France	√	√
5.	GermanySwitzerland	√	
6.	Italy	√	√
7.	NorthernEurope	√	
8.	Russia	√	√
9.	SouthEasternEurope	√	√
10.	SouthWesternEurope	√	√
11.	UKI	√	
		100%	73% (8/11)

SSC More Information

- Follow-up information:

  Available in the GGUS tickets

- More on the LCG/EGEE TWiki pages:

  https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge

  (Contains pointers to more detail information about the SSC execution).

SSC_2 issues from the debriefing

- Some specific SSC_2 points raised in the debriefing:
  - The exercise was considered useful
  - It did not require too much resources
  - The GGUS ticketing worked satisfactorily
    - Issues raised about confidentiality, escalation paths, bridging to local ticketing systems.
  - “Fact sheet” for each challenge job
    - Particulars from Stage_1 are now on the WEB site
  - Recipe for resolution of the challenge
    - Awaiting volunteers
  - Additional explanatory text in the ticket to provide some guidance (not all sites log sufficient info for complete resolution)
    - Slightly modified proposal in the debriefing report

Suggestions for future SSC

- Some suggestions for future came out in the debriefing:
  - Targeting specific types of storage (some types are phased out)
  - Exhaustive testing, challenging all storage elements at a Site
  - Multi Site scenarios where RB, CE and SE are selected from different Sites, or even ROCs

From the OSCT June 2006 meeting

- **Proposals for SSC3**
  - **From OSCT June 2006 ➔**

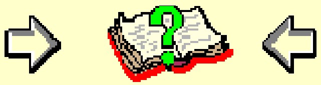
SSC_3 Proposals: Jens' Identity Dual-Play

Test OPerator (TOP)

- Submits the job targeting the challenged site

Identity A

- Writes file:
  - Protects file against **B**;



Identity B

- Tries to access the file:
  - read; write; delete;

TOP

- Issues the alert, escalates as required and checks the response:
  - Who did what and when?

SSC_3 Proposals: Ian’s “Block that Identity”

Test OPerator (TOP)

- Logs in to Grid under a test identity
- Starts repeating job submitting challenge to the site, using this id.
- Asks security of challenged site to block that id.
- Purges the repeating job when blockage has become effective
- Logs the time of the events
- An over-riding time-out is set to 72 hours

SSC_3 Proposals: Space for your proposal here

- Do you have a good idea?
  - Mail it to:

    project-egee-security-challenge@cern.ch

I thank you for the attention…