Contribution ID: **26** Type: **not specified**

Cluster security tournament - Hands-on incident response and forensics in a realistic environment

In this workshop the participants will take on the role as security teams being responsible for the operational security of simulated grid sites running in a virtualized environment.

The sites will face attacks very similar to those seen in real life. The teams' task is to respond to these attacks and keep their services up and running as far as possible.

A running score will be kept, and at the end of the workshop the winners will receive fabulous prizes.

Maximum number of participants is 18.

Be prepared

A security incident always puts you in a challenging situation. You have to do many things correctly, quickly and in the correct order. What to do and when during incident response is usually formulated in an incident response procedure. We will start from the general Grid Incident Response Procedure available from EGI-CSIRT and discuss how to adapt it to local regulations.

Have a view of your site

Usually the information you initially get in a security incident will be relatively sparse and the amount of logs quite large. Therefore it is crucial to quickly get an initial overview of the problem, i.e. which systems are affected and which systems are at risk. Here we will discuss and use tools you can easily set up at your site as well, like a central syslog facility, a grid systems log analyzer and EGI CSIRT's vulnerability scanner Pakiti.

The heat is on

Now it is time to put your newly acquired knowledge to the test. As administrator of a simulated cluster, you will have to defend yourself against a determined attacker.

Hands-on forensics

Investigating a compromised system is a delicate situation. It is easy to lose crucial information if you are not careful enough. We will discuss several levels of volatile information and do and dont's in how to collect it. The creation and analysis of memory and disk images will be discussed.

Wrap-up, lessons learned

At the end of the work shop we will discuss the findings. The crucial point here is to find how the site was attacked and which steps could be taken to prevent this from happening again. This should result in some best practices on how to reduce the attack surface of your site.

Authors: VERSTEGEN, Aram; REESE, Heiko (KIT); NIXON, Leif (Linköping University); GABRIEL, Sven (Nikhef); DUSSA, Tobias (KIT); EPTING, Ursula (KIT)

Presenters: VERSTEGEN, Aram; NIXON, Leif (Linköping University); GABRIEL, Sven (Nikhef)