

Host based intrusion detection with OSSEC

Monday, May 2, 2011 3:00 PM (30 minutes)

In this talk the open source host-based intrusion detection system OSSEC is described. Besides an overview of its features it will also be explained how to use it for non-security related monitoring and notifying. Furthermore several possible real life scenarios will be demonstrated and some of the current drawbacks will be elaborated.

Primary author: NEUBURGER, Bastian (GSI)

Presenter: NEUBURGER, Bastian (GSI)

Session Classification: Networking & Security

Track Classification: Security & Networking