

Unix/Linux centralized Access Control Systems

Issue

Many enterprises maintain populations of Unix and/or Linux based servers. Centralized user and access management for such systems turns out to be non-trivial as standard products which do not provide appropriate mechanisms. Most enterprises therefore use a generic user and role management system and on a further service which deploys such users and roles to the target system. For a secure operation of the servers care must be taken that the intended segregation of rights is correctly implemented from the generic role model down to the actual setting of the target operating system parameters.

Cnlab Services

Cnlab analyze the abstract role models and the supporting applications, as well all tools which are used for deploying to the targets. The goal is to identify potential **vulnerabilities**, to identify the potential **damage** which can incur if a vulnerability is exploited, and to assess the related **risk** for the organizations. Further, suggestions for **improvements** are worked out where this seems necessary.

The Cnlab methodology is based on our own experience from more than 10 years in the field, and on the common standards (such as ISO 17799, BSI, OWASP, OSSTMM).

Project Sketch

The project starts with the analysis of the abstract role model and the mechanisms which are used to define rights on an abstract level. Based on this analysis, the critical roles are identified. For the critical roles the actual settings in the target systems are analyzed (e.g. root access, SU configurations, Sudo configurations). Finally, the correct setup of the target system platforms are analyzed (hardening).

Work depends on role model complexity and on the size of the population. Typical projects start from 5 days, and can go up to 20 and more days for large and diverse server populations.

Success Stories

Our main experience is based on large Swiss banking setups, where some of the generic roles are planned to be granted to staff in foreign countries. Based on the Swiss banking secrecy regulations, special care must be taken that such persons cannot obtain high (root) privileges on the target servers. Our investigations have shown that such arrangements are possible, if appropriate precautions are observed.

Cnlab contacts

Detail Information on Unix Access Control reviews can be obtained from the following Cnlab representatives:

Thomas Lüthi Tel +41 55 214 33 41

Paul Schöbi Tel +41 55 214 33 33