

Session T1 – Audit and Security of Unix

By Rodney Kocot

Topic Summary

This session will cover a wide range of hands-on aspects of Unix security that an auditor should know. Topics include Physical Security, Security Utilities, User Administration Files and Programs (file formats and Unix programs used to manipulate them), User Attributes, Crack Programs, Resource Protection and Management (types of files, protections for types of files, and resource administration), Privileged Programs (setuid and setgid programs, programs executed at startup and in other privileged situations), Schedulers, System Startup and Shutdown, Network Security (file formats, services – their uses and abuses, and scanning software), Logging And Monitoring (common logs and their formats, reporting and review procedures), Common Findings, Audit Approach, Scripts and Utilities, as well as Sources Of Information.