IX congresso interno de iniciação científica da unicamp
27 e 28 de setembro 2001

ANÁLISE FORENSE DE INTRUSÕES EM AMBIENTES UNIX

Guilherme Cesar Soares Ruppert (Bolsista FAPESP) e Prof. Dr. Paulo Lício de Geus (Orientador), Instituto de Computação - IC, UNICAMP

Com o aumento da importância das redes de computadores e da Internet, um assunto que tem se tornado cada vez mais preocupante é a invasão em sistemas computacionais de pessoas não autorizadas e maliciosas. Este trabalho visa o estudo de técnicas para identificação e reconstituição de intrusões em sistemas computacionais e redes de computadores sob plataforma Unix, visando identificar como se deu a invasão, quem seria o invasor e quais danos foram causados por ele durante o ataque. Com isso pode-se realizar laudos periciais para investigações desses crimes eletrônicos. Foram abordadas várias técnicas para se obter as evidências necessárias envolvendo: análise de segurança, análise de arquivos “log”, auditoria do sistema de arquivos, análise de processos e “core files”, recuperação de dados apagados e outros. Foram também abordados procedimentos que, aplicados a um sistema ainda não comprometido, viabilizem e facilitem uma eventual análise forense posterior.

Invasão de Computadores - Forense Computacional - Redes de Computadores