

Sessão 16

Redes de Computadores e Tolerância à Falhas

126**IDENTIFICAÇÃO DE *SCRIPTS* DANINHOS DURANTE A NAVEGAÇÃO NA INTERNET.***Clairton Cabreira* (Deptº de Ciência da Computação, UniLassale, Canoas-RS).

O uso crescente da internet como meio de comunicação, busca da informação - e, mais recentemente, como meio para execução de negócios não só por empresas, mas também por usuários domésticos (leigos) -, tem sido alvo de freqüentes ataques que exploram vulnerabilidades existentes em diferentes programas usados para esta finalidade (browser). Visando a facilidade de uso, estes softwares possibilitam a execução de *scripts*, em diferentes linguagens e situados em páginas (*sites*) remotas, os quais podem, de acordo com a necessidade, acessar diferentes recursos locais. Embora as restrições ao uso de recursos implementados pelos diferentes fabricantes de software possibilitem, num primeiro momento, um grau de segurança e confiabilidade, a existência e a exploração de eventuais falhas (vulnerabilidades) através de trechos de código daninhos vem causando transtornos e prejuízos crescentes para empresas, governos e usuários comuns. Os ataques mais explorados são aqueles baseados no chamado *buffer overflow* - que, em última análise, possibilitam ao intruso os mesmos privilégios do usuário local - e a negação de serviço (DOS), que visam diminuir o desempenho ou mesmo tornar inoperante o sistema local. Este trabalho tem como objetivo a elaboração de um programa para a identificação de páginas que contenha código que efetue este tipo de exploração durante a navegação na Web, bem como apresentar as principais técnicas envolvidas neste processo.