

ANAIS - XXII FÓRUM DE INICIAÇÃO CIENTÍFICA, III FÓRUM DE DESENVOLVIMENTO TECNOLÓGICO E INOVAÇÃO E II FÓRUM DE INICIAÇÃO CIENTÍFICA DO ENSINO MÉDIO.
n.1 (2015)

ANÁLISE DE VULNERABILIDADE EM SISTEMAS COMPUTACIONAIS UTILIZANDO FERRAMENTAS DE LIVRE DISTRIBUIÇÃO

Autores: PEREIRA, F.R.F.; SILVA, E.G.

Tipo de pesquisa: Trabalho de Conclusão de Curso de Graduação

Agência de fomento: Não se aplica

Área do conhecimento: Exatas – Ciência da Computação

Instituição de origem: USC

A redução dos preços dos computadores e a facilidade de conexão à internet tem causado grande aumento na popularidade dos dispositivos computacionais. O aumento da conectividade faz com que a segurança da informação seja um assunto cada vez mais recorrente no atual cenário computacional. Novas tecnologias são desenvolvidas a cada momento, da mesma forma, falhas são descobertas, exploradas e corrigidas enquanto estas tecnologias estão em uso. A evolução contínua da segurança e de novas tecnologias traduz-se, na prática, em uma impossibilidade de possuir ou desenvolver um sistema 100% seguro. Como alternativa a essa impossibilidade deve-se buscar vulnerabilidades, estudá-las e explorá-las, limitando-as ou corrigindo-as. Avaliações preventivas nos sistemas computacionais podem revelar falhas potenciais a serem consideradas e corrigidas antes que um usuário mal intencionado possa explorá-las. O objetivo principal do presente trabalho foi demonstrar as vulnerabilidades de acesso privilegiado em sistemas computacionais utilizando técnicas de invasão com o sistema operacional Linux e ferramentas de livre distribuição. O estudo foi desenvolvido em duas fases distintas: uma fase de investigação dos aspectos teóricos, e uma etapa prática de aplicação das técnicas de invasão, com o intuito de obter acesso a um sistema computacional. Dentre os diversos ataques pesquisados, o "Brute Force" foi o que se mostrou mais efetivo quando utilizado em conjunto com uma wordlist. Como exemplo deste processo pode-se citar um teste realizado com o servidor de e-mails - Gmail, o qual após 100 tentativas de senhas

**ANAIS - XXII FÓRUM DE INICIAÇÃO CIENTÍFICA, III FÓRUM DE DESENVOLVIMENTO TECNOLÓGICO E INOVAÇÃO E II FÓRUM DE INICIAÇÃO CIENTÍFICA DO ENSINO MÉDIO.
n.1 (2015)**

bloqueou o usuário por cerca de 3 minutos, além de que, para testar estas 100 senhas pode-se levar um tempo considerável, entretanto, se a senha estiver em uma posição bem alta na worlist, o processo pode levar de semanas a anos, tornando-se assim ineficiente. Espera-se com esse trabalho contribuir para melhoria da segurança dos sistemas computacionais.

Palavras-chave: Análise de vulnerabilidade. Sistemas computacionais. Ferramentas. Linux.