FACULDADE DE TECNOLOGIA SENAC GOIÁS

TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Alunos:
Cristhian Lopes de Souza
Matheus do Carmo
Matheus Oliveira
Pablo de Almeida

SISTEMAS OPERACIONAIS

Professor: Lucilia

Goiânia, 06 de Dezembro de 2016

O estudo para confeccionar esse trabalho teve como base o livro “Sistemas Operacionais, 3º edição, Deitel”, que aborda em um capítulo dedicado a segurança, 19, e outros dois que discute estudos de caso em sistemas operacionais Linux e Windows e pesquisas em sites da internet.

Segurança da informação tem seus pilares, CIDA, são eles: confidencialidade, integridade, disponibilidade e autenticidade. A confidencialidade garantindo que a informação não será lida por terceiros, integridade garantindo que não seja modificada, disponibilidade garantindo o acesso por usuários autorizados no momento requisitada e autenticação que garante a identificação do usuário.

O desafio proposto pela matéria de SO é que fosse feito um estudo dos sistemas operacionais Linux e Windows e definir qual o sistema é mais seguro para ser instalado os serviços IP, HTTP, SSH, DHCP e MSTP.

De um modo geral, considerando-se que diversos usuários estão compartilhando os mesmos recursos, como: memória, processador e dispositivos de E/S, faz-se então necessário existir mecanismos de proteção para garantir a confiabilidade e a integridade dos dados e programas dos usuários, além do próprio sistema operacional. Como vários programas ocupam a memória principal simultaneamente, cada usuário possui uma área reservada onde seus programas e dados são armazenados durante o processamento. O sistema operacional deve possuir mecanismos de proteção a essas áreas, de forma a preservar as informações nela contidas.

Por default, o Linux autentica seus usuários exigindo que forneçam um nome e senha de usuários via processo de login, as senhas sofrem hash usando algoritmos MD5 ou DES e então são armazenados em entradas correspondente ao ID dos usuários. Diferentemente de criptografia que podem reverter a operação de criptografia usando a chave criptográfica, os algoritmos de hash não são reversíveis. No Linux administradores possuem permissão para carregar módulos de autenticação conectáveis (***Pluggable Autentication Modules - PAMs***), Módulos que podem reconfigura o sistema durante a execução para incluir técnicas melhoradas de autenticação.

Diferente do Windows, usuários adicionados no Linux recebem permissões meninas do sistema limitando o seu acesso a setores mais críticos SO.

O Linux fornece segurança a recursos de sistemas controlando o acesso a arquivos, para controlar como os outros usuários acessam recursos, cada arquivo do sistema recebe atributos de controle de acesso que especificam permissões de segurança de arquivo, porem mesmo o sistema de autenticação com módulos PAMs não são suficientes para garantir segurança pois os módulos adicionais aperfeiçoam o método de autenticação do usuário no SO e não a nível de arquivo, para resolver esse problema o Linux permitir o administrador inserir LSM (***Liux Security Modules***) que são módulos instaláveis no núcleo similares aos PAMS porém fornecendo maior segurança a nível de acesso a arquivos, assim quando um arquivo é invocado após passar pelo controle de acesso é analisado pelo LSM. O LSM mais utilizado no Linux é o SELinux.

Um recurso que aumenta a segurança a nível de arquivo no Linux é o ***Journal*** funcionalidade de arquivos extendidos, ext3, antes dos metadados e os dados serem modificados em discos são armazenados no journal diminuindo a sim a necessidade de gravar mais de uma vez em disco. Enquanto em alguns contextos a falta de funções de sistemas de arquivos "modernos", como alocação dinâmica de inodes e estruturas de dados em árvore, poderia ser considerada uma desvantagem, em termos de "recuperabilidade" isso dá ao ext3 uma significante vantagem sobre sistemas de arquivos que possuem-nas. Os metadados do sistema de arquivos estão todos em locais fixos e bem conhecidos, e há certa redundância inerente à estrutura de dados, que permite que sistemas ext2 e ext3 sejam recuperáveis no caso de uma corrupção de dados significante, em que sistemas de arquivos em árvore não seriam recuperáveis.

Com os relatos acima concluímos que o Linux pode nos fornece melhor performance e segurança aos dados que serão fornecidos pelos serviços IP, um ponto muito discutido é o suporte caso necessário, porém além das comunidades que discutem problemas e soluções, grupos de pesquisas, algumas distribuições possuem suporte técnico.