Laboratório 11: Segurança em Sistemas Operacionais Linux

1. Objetivos

- Compreender os princípios básicos de segurança em sistemas operacionais.
- Identificar arquivos importantes para configuração de segurança em Linux.
- Aprender comandos básicos de configuração de segurança em Linux.

2. Materiais

- Distribuição Linux.
- Virtualbox
- Comandos do sistema.

3. Procedimentos e Atividades

1. Obter a distribuição Linux no link informado pelo professor em aula.
2. Abrir o Virtualbox e importar o arquivo com a distro Linux.
3. Fazer autenticação no sistema. As credenciais (*login, password*) são (**student**, student) e (**root**, root).
4. Realizar e descrever a execução das atividades
   a) Configurar o nível de segurança da senha de usuários forçando ter no mínimo 10 caracteres, uma letra minúscula, uma maiúscula, dois caracteres numéricos e um símbolo. *(dicas: libpam-pwquality, /etc/security/pwquality.conf)*
   b) Editar o arquivo */etc/adduser.conf* e alterar a configuração *GROUPHOMES* para *yes*.
   c) Adicionar os grupos de usuários: *alunos*, *professores*. *(dicas:addgroup, /etc/group)*
   d) Cadastrar uma nova conta no grupo *alunos* e outra no grupo *professores*. *(dicas: adduser, groups)*
   e) Remover os usuários do grupo alunos do *sudo*. *(dicas: gpasswd, groups)*
   f) Testar a autenticação em novo console das contas criadas.
   g) Acessar com a conta criada do grupo alunos e criar um arquivo *meuarquivo.txt* e alterar as propriedades de acesso para o *dono* como leitura e escrita, para o *grupo* como somente leitura e para os *outros* nenhuma permissão. (Mostre como fazer usando o formato numérico e com opções). *(dicas: ls, chmod)*
   h) Altere o dono e o grupo do arquivo *meuarquivo.txt* para o *usuário do grupo professores* e do grupo *professores*. *(dicas: ls, chown)*
   i) Liste os últimos usuários que autenticaram no sistema. *(dicas: lastlog)*
   j) Desabilite a obrigatoriedade de autenticação do usuário *root* e faça um teste (depois habilite novamente). *(dicas: /etc/passwd)*
   k) Acesse o arquivo */etc/shadow* e explique o significado dos campos da entrada *student*.
   l) Acesse o arquivo */etc/passwd* e explique o significado dos campos da entrada *student*.
   m) Qual a finalidade dos arquivos do */var/log/*: *syslog*, *kern.log*, *auth.log* e *daemon.log*
   n) Configure o *logrotate* (*/etc/logrotate.conf*) para manter cópia trimestral dos logs e rotacionar diariamente.
   o) Liste e identifique os serviços ativos no sistema. *(dicas: service)*
   p) O que é o *SELinux?*
   q) O que é o *Pluggable Authentication Module (PAM)* no Linux e qual sua localização?