BRENO FARIAS DA SILVA, 2300516
FELIPE ARCHANJO DA CUNHA MENDES, 2252740
PAMELLA LISSA SATO TAMURA, 2254107

SISTEMAS OPERACIONAIS
LABORATÓRIO 11 - SEGURANÇA

Relatório técnico de atividade prática solicitado pelo professor Rodrigo Campiolo na disciplina de de Sistemas Operacionais do Bacharelado em Ciência da Computação da Universidade Tecnológica Federal do Paraná

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ - UTFPR
DEPARTAMENTO ACADÊMICO DE COMPUTAÇÃO - DACOM
CIÊNCIA DA COMPUTAÇÃO - BCC

CAMPO MOURÃO
JUNHO / 2022

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.

Resposta: Para configuração do nível de segurança da senha de usuários atendendo todos os requisitos do enunciado dado foi utilizado o comando ***apt install libpam-pwquality cracklib-runtime*** como sudo para instalação do programa e ***nano /etc/security/pwquality.conf*** para abrir o editor de texto. A primeira propriedade alterada **minlen** atende o mínimo de caracteres da senha. Em seguida, a **dcredit** para definir a quantidade mínima de dígitos. A propriedade **lcredit** e **ucredit** para indicar uma letra minúscula e minúscula, respectivamente. E, por fim, a última propriedade **ocredit** para designar a quantidade mínima de símbolos. As propriedades **lcredit, ucredit** e **ocredit** são definidas como -1 pela condição de se caso a quantidade da respectiva propriedade for menor que zero. Além disso, **minlen** é definido como 10, **dcredit** como -2. Por padrão, o arquivo de segurança está comentado. Assim, para o funcionamento das modificações impostas é necessário descomentar a linha de código descrito. O atributo **enforce_for_root** é usado para também obrigar o root a seguir as regras definidas.

Ao testar as modificações estabelecidas anteriormente, cumprindo corretamente todos os requisitos com o comando **passwd** e a senha "Aa843-891m" foi obtido a saída "*Password update successfully*". Realizando um teste induzido ao erro, com a senha "Pqowieurt", foi obtido o output "*The password contains less than 1 non-alphanumeric characters"* indicando a falta de um caractere numérico. Além disso, apesar de não estar explícito na saída, existe também a falta do símbolo (*other characters*).

b) Editar o arquivo /etc/adduser.conf e alterar a configuração GROUPHOMES para yes.

Resposta: Para a edição do arquivo o comando ***nano /etc/adduser.conf*** foi executado e a configuração GROUPHOMES foi modificada obtendo GROUPHOMES = yes.

c) Adicionar os grupos de usuários: alunos, professores.

Resposta: O comando geral para a adição de grupos é ***sudo addgroup <groupname>***. Assim, ***sudo addgroup alunos*** e ***sudo addgroup professores*** foram executados para a adição dos grupos "alunos" e "professores", respectivamente. Para a listagem dos grupos foi utilizado o comando ***cat /etc/group,*** assim, o valor resultante da saída correspondeu a: alunos:x:1001: e professores:x:1002:.

d) Cadastrar uma nova conta no grupo alunos e outra no grupo professores.

Resposta: Para cadastrar uma nova conta no grupo alunos a execução do comando ***adduser <username>*** foi necessário. Tomando como exemplo, o comando ***sudo adduser breno*** foi executado para o cadastro no grupo alunos com a senha Akjel31p-bj. E ainda, para o cadastro no grupo professores o comando ***adduser campiolo*** foi executado com a senha @n1me43-EB. Além disso, para adicionar as contas a um grupo o comando base usado foi ***usermod -a -G <groupName> <username>.*** Dessa forma, para incorporar contas ao grupo (alunos/breno e professores/campiolo) os respectivos comandos foram executados ***usermod -a -G alunos breno*** e ***usermod -a -G professores campiolo***. Também é possível criar um usuário e adicioná-lo automaticamente em um grupo usando o comando ***sudo adduser usernameHere –ingroup groupnameHere***

e) Remover os usuários do grupo alunos do sudo.

Resposta: Para a remoção de usuários, nesse caso "breno", do grupo "sudo" do sudo o comando ***gpasswd --delete breno*** sudo foi executado. Como a ação foi finalizada com sucesso, o output obtido para esse comando foi "removing user breno from sudo group".

f) Testar a autenticação em novo console das contas criadas.

Resposta: Após a remoção dos usuários do grupo alunos do sudo, o teste da autenticação em um novo console das contas criadas foi realizado. Até então, o primeiro terminal está aberto e pode ser localizado com o atalho **ALT+F1**. Assim, ao autenticar mais consoles além do primeiro terminal, **ALT+F2** (Autenticou o user "breno") e **ALT+F3** (Autenticou o user "campiolo") fazem esse papel.

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).

Resposta: Para criar um arquivo "meuarquivo.txt", primeiramente, foi necessário acessar com a conta criada do grupo "alunos" e, em seguida, foi utilizado o comando base ***touch <nomeArquivo.txt>*** da qual atende esse propósito. Dessa maneira, ***touch meuarquivo.txt*** foi efetuado. Para a alteração das propriedades de acesso do dono, grupo e outros, o comando base é constituído por ***chmod.*** Assim, a propriedade de acesso do usuário dono foi modificado para somente modo escrita onde é definido por ***-u+rw-x*** ou, no formato numérico, usando o argumento ***chmod* 0200 *meuarquivo.txt,*** ou seja, essa ação pode ser resumida pelo comando ***chmod -u+rw-x meuarquivo.txt*** ou ***chmod* 0200 *meuarquivo.txt.*** Em seguida, o acesso do grupo foi alterado analogicamente ao processo anterior com a diferença de que, para o grupo, o acesso concedido corresponde à leitura (***-g+r-wx*** ou ***4***) definido pelo comando ***chmod -g+r-wx meuarquivo.txt*** ou ***chmod -g 6 meuarquivo.txt.*** Por fim, para outros o acesso de leitura, escrita e execução não é permitido (***-o-rwx*** ou ***7)***. Esse requisito é estabelecido pelo comando ***chmod -o-rwx meuarquivo.txt*** ou ***chmod -o 7 meuarquivo.txt***. Nota-se, então, que dependendo do

objetivo da propriedade de acesso (permissão) de cada comando, o número e o tipo alteram. Dessa forma, essa relação pode ser exibida na Tabela 1.

Tabela de relações entre permissões, número e tipo

Permissões	Número	Tipo
Retira todas as permissões	0	---
Permissão para execução	1	--x
Permissão para escrita	2	-w-
Permissão para escrita e execução	3	-wx
Permissão para leitura	4	r--
Permissão para leitura e execução	5	r-x
Permissão para leitura e escrita	6	rw-
Permissão para leitura, escrita e execução	7	rwx

Tabela 1: Permissões e seus números e tipo correspondentes

h) Altere o dono e o grupo do arquivo meuarquivo.txt para o usuário do grupo professores e do grupo professores.

Resposta: Para modificar o dono e o grupo do arquivo "meuarquivo.txt" para o usuário do grupo professores e do grupo professores foi necessário utilizar o comando base ***chown usuario[:grupo] arquivo(s),*** ou seja, ***chown campiolo:professores /home/alunos/breno/meuarquivo.txt***.

i) Liste os últimos usuários que autenticaram no sistema.

Resposta: Para obtenção da listagem dos últimos usuários que autenticaram no sistemas, foi preciso executar o comando ***lastlog.*** Assim, foi possível notar que o último usuário que autenticou no sistema foi "campiolo" às 16:59:55.

j) Desabilite a obrigatoriedade de autenticação do usuário root e faça um teste (depois habilite novamente).

Resposta: Para atender esse requisito foi preciso, primeiramente, abrir o arquivo com o comando ***nano /etc/passwd***. Ao abrir o arquivo, o campo de autenticação do usuário é dado por ***root:x:0:0:root :root:/bin/bash.*** Assim, para desabilitar a obrigatoriedade de autenticação do usuário root, o "x" deve ser desmarcado resultando em ***root::0:0:root :root:/bin/bash***. Após isso, foi necessário abrir um novo terminal, utilizando o atalho ALT+F5 visto anteriormente.

Logo em seguida, foi requisitado o nome do usuário pelo sistema. Diante disso, registra-se “root” e, assim, é possível notar que não foi necessário adicionar a senha do usuário root.

k) Acesse o arquivo /etc/shadow e explique o significado dos campos da entrada student.

Resposta: O arquivo ***/etc/shadow*** armazena as informações como o *hash* e o valor de ***salt***, por exemplo. Este arquivo consiste nove campos, sendo eles, o nome do usuário (*Username*), a senha criptografada (*Encrypted password*), a última modificação na senha (*Last password change*), o número mínimo de dias necessários para poder mudar novamente a senha (*Minimum password age*), o número de dias após o qual a senha deve ser alterada (*Maximum password age*), a quantidade de dias antes da senha expirar (*Warning period*), o número de dias de inatividade de uma conta, a data de quando uma conta foi desabilitada (*Expiration date*) e, por fim, um campo vazio que é reservado para uso futuro.

l) Acesse o arquivo /etc/passwd e explique o significado dos campos da entrada student.

Resposta: O campo “***x***” refere-se que a senha está no shadow. Shadow é um arquivo no Linux que armazena senhas encriptadas dos usuários e é acessível apenas a usuários root. Após isso, o primeiro valor “***1000***” refere-se ao *UID* (ou identificador de usuário), sendo o UID um número atribuído para cada usuário no sistema. O segundo valor “***1000***” consiste no *Group Identifier* (*GID* ou identificador de grupo), o qual consiste em um valor não negativo. Valores de 0 a 99 são reservados para o kernel, de 100 a 999 para administradores do sistema e de 1000 a 59999 para grupos de usuários do sistema. O campo que armazena a string “***Alunos SO***” refere-se ao nome do grupo que o usuário “***student***” pertence. Logo após tem-se o campo do diretório *home*, o qual é dado por “***home/student”***. Por fim, tem-se o campo do shell de login, o qual é o “***bash***”.

student:x:1000:1000:Alunos SO, , , :home/student:/bin/bash

m) Qual a finalidade dos arquivos do /var/log/: syslog, kern.log, auth.log e daemon.log

Resposta:

/var/log/:Syslog - Mostra mensagens gerais e informações sobre o sistema.

/var/log/:Kern.log - Guarda informações mantidas pelo kernel.

/var/log/:Auth.log - Armazena as informações relacionadas a eventos de autenticação do sistema.

/var/log/:Daemon.log - Mantém registro dos serviços que estão em execução em segundo plano, todavia não os representa de forma gráfica.

n) Configure o logrotate (/etc/logrotate.conf) para manter cópia trimestral dos logs e rotacionar diariamente.

Resposta: Para manter uma cópia trimestral dos logs, basta alterar o atributo “rotate = 4” para “rotate = 12”. O atributo diz o número de semanas em que uma cópia é mantida. Dessa forma, para manter uma cópia trimestral, basta pegar o número de meses (3) e multiplicar pela

quantidade de semanas contidas em um mês (4). Sendo assim, chegamos ao valor 12 a partir da conta 3*4.

o) Liste e identifique os serviços ativos no sistema.

Resposta: Para listar os serviços ativos no sistema é necessário executar o comando ***service --status-all | grep active***. De forma breve, basicamente é usando o argumento ***--status-all*** para listar todos os serviços e filtrar, com o comando ***grep***, pelos serviços ativos no sistema. Os serviços ativos no sistema são:

- Cryptdisks
- Hwclock.sh
- Kmod
- Mount-configfs
- Networking
- unmountnfs-alternative.sh

p) O que é o SELinux?

Resposta: SELinux, ou *Security-Enhanced Linux,* é uma arquitetura de segurança para sistemas Linux, a qual permite aos administradores ter mais controle sobre quem pode acessar o sistema, funcionando com base no controle de acesso a arquivos, processos e aplicações.

q) O que é o Pluggable Authentication Module (PAM) no Linux e qual sua localização?

Resposta: Pluggable Authentication Module consiste em permitir que seja possível integrar autenticações de baixo nível usando uma API. Este arquivo está disponível em **/etc/pam.conf**. No ***PAM*** é também possível alterar as políticas de autenticação de forma bem simples, apenas alterando os atributos dentro dos arquivos de configuração.