4451 – Linux Security SysAdmin in Cloud

Laboratório - Aula 03: Administração de Usuários II

Pré-Requisitos: Para iniciar o Laboratório 3 você precisará ficar atento aos Pré-Requisitos. É importante lembrar que o sucesso da correção automática depende obrigatoriamente dessa etapa.

- Você precisará estar logado com o Usuário root;
- Todas as etapas do Laboratório precisam ser executadas no mesmo terminal;
- É necessário executar o comando `# startdexterlab-3`
- Obrigatoriamente execute a limpeza do histórico antes de iniciar `# history -c`

Tarefas:

Execute as tarefas abaixo na máquina **4451 Practice Lab Debian** ou na máquina **4451 Practice Lab CentOS** do curso.

A empresa Dexter possue atualmente uma infraestrutura com compartilhamento em ambientes mistos através do Samba, e precisa ajustar as permissões corretas de acesso a usuários e grupos conforme os setores da empresa. Utilize seus conhecimentos em administração de usuários e execute as seguintes tarefas:

01 – **Altere o grupo dono** dos diretórios administrativo, pessoal, comercial e logística, armazenado em /DEXTER. O nome do grupo deve corresponder ao nome do diretório:

```
# chgrp administrativo /DEXTER/administrativo
```

```
# chgrp pessoal /DEXTER/pessoal
# chgrp comercial /DEXTER/comercial
# chgrp logistica /DEXTER/logistica
```

02 – **Defina a permissão 3770** para os diretórios administrativo, pessoal, comercial e logística, armazenado em /DEXTER:

```
# chmod 3770 /DEXTER/{administrativo,pessoal,comercial,logistica}
```

03 – **Altere o dono e grupo** dos diretórios armazenados em /LIXEIRAS. O nome do dono e grupo deve **corresponder a cada usuário que possuir UID maior ou igual a 1001**. Para isso crie um pequeno script em /dexter/scripts de nome **altera-permissoes.sh** com a estrutura em **For**:

```
# vim /dexter/scripts/altera-permissoes.sh
#!/bin/bash
for i in $(awk -F: '$3 >= 1001 {print $1}' /etc/passwd)
do
     chown $i.$i /LIXEIRAS/$i
done
```

04 – Crie um novo diretório em /DEXTER/Publico com **permissão especial "Stick BIT"**:

```
# mkdir /DEXTER/Publico
# chmod o+t /DEXTER/Publico ou chmod 1777 /DEXTER/Publico
# ls -ld /DEXTER/Publico
```

05 – **Pesquise** no sistema todos os arquivos e diretórios que possuem **permissão especial "Stick BIT"** (1777) e envie este resultado para /dexter/auditoria/lista_stickbit.txt:

```
# find / -perm 1777 > /dexter/auditoria/lista_stickbit.txt
# cat  /dexter/auditoria/lista_stickbit.txt
```

06 – Defina a **permissão especial SUID Bit** para o binário dexterlab-3:

```
# chmod g+s $(which dexterlab-3)
```

07 – **Pesquise** no sistema todos os arquivos que possuem **permissão especial "SUID bit"** (4755) e envie este resultado para /dexter/auditoria/lista_suid.txt:

```
# find / -perm 4755 > /dexter/auditoria/lista_suid.txt
```

08 – **Filtre** no sistema os nomes de todos usuários do sistema que possuem **UID menor ou igual a 999**, e envie este resultado para /dexter/auditoria/lista_usersystem.txt:

```
# awk -F: '$3 <= 999 {print $1}' /etc/passwd > /dexter/auditoria/lista_usersystem.txt
```

09 – **Pesquise** no sistema os nomes de todos os grupos do sistema que possuem **GID menor que 110**, e envie este resultado para /dexter/auditoria/lista_groupsystem.txt:

```
# awk -F: '$3 < 110 {print $1}' /etc/group > /dexter/auditoria/lista_groupsystem.txt
```

10 – Filtre os usuários validos do sistema (UID acima de 999) e envie a saída para o arquivo /dexter/auditoria/valid_users.txt:

```
# awk -F: '($3 > 999) {print $1}' /etc/passwd > /dexter/auditoria/valid_users.txt
```

Correção:

Assim que concluir todas as tarefas siga os passos abaixo para realizar a correção automática.

```
# history -w
# dexterlab-3
```

Para refazer o laboratório execute o comando: #recoverylab-3

Para cada tarefa correta será computado 1 ponto. Se não atingir a nota máxima, você pode repetir o laboratório e corrigir novamente, lembrando que é necessário executar os procedimentos de Pré-Requisitos toda vez que desejar recomeçar o Lab.