

# Sessão 6 — Segurança básica e procedimentos operacionais



As atividades desta sessão serão realizadas na máquina virtual *Client\_Linux*.

## 1) Identificando senhas fracas

Uma das formas de verificar se o seu sistema atende às recomendações básicas de segurança é utilizar os programas "quebradores" de senha, ou *password crackers*. Neste exercício, utilizaremos um desses programas para mostrar seu funcionamento.

1. Obtenha e instale o *password cracker* John the Ripper, ou simplesmente `john`.
2. Crie o arquivo `/root/dicionario.txt` com uma lista de senhas. Caso considere necessário, acrescente palavras que julgue impróprias para uso em senhas. Por exemplo:
3. Rode o *password cracker* com o comando `# john -wordlist=/root/dicionario.txt -rules /etc/shadow`.
4. Veja o resultado da verificação com o comando `# john -show /etc/shadow`.

## 2) Descobrindo a funcionalidade do bit SGID em diretórios

A utilidade do SUID e SGID foi vista desde a sessão de aprendizagem 1. Execute a sequência de comandos e depois responda as seguintes perguntas:

1. Crie o grupo `corp` e defina-o como grupo secundário do seu usuário.
2. Entre no sistema a partir da sua conta e crie um diretório chamado `dir_corp`.
3. Verifique a qual grupo pertence o diretório criado no passo acima. Modifique-o para que passe a pertencer ao grupo `corp` e mude a sua permissão para `2755`.
4. Crie, no seu diretório *home* um arquivo chamado `arq1`. Em seguida, mude para o diretório criado no segundo item e crie um arquivo chamado `arq2`.
5. Verifique os grupos aos quais pertencem os arquivos criados no item anterior. Você saberia explicar por que os arquivos pertencem a grupos distintos, embora tenham sido criados pelo mesmo usuário?
6. Quais as vantagens desse esquema?

## 3) Obtendo informações sobre os recursos computacionais

1. Vimos, no texto teórico, que uma das importantes funções de um administrador de sistemas é acompanhar o uso dos recursos computacionais de sua instituição. Discuta com o seu colega quais comandos vistos em todo o módulo podem auxiliar na coleta desse tipo de informação.

## 4) Controlando os recursos dos usuários

Um dos grandes desafios de um administrador de sistema, nos tempos atuais, é controlar a ocupação do espaço em disco do seu sistema — aplicações do tipo P2P (*peer-to-peer*), por exemplo, são consumidoras vorazes desse tipo de recurso.

1. Que medidas podem ser tomadas para controlar a ocupação de disco de forma automática?