Linux para Infraestrutura

Prof. André Nasserala

nasserala@gmail.com

Comando sudo

- Correspondente a SuperUser Do, sudo é um dos comandos básicos mais populares do Linux.
- Ele permite executar tarefas que exigem permissões administrativas ou de root.
- Ao usar o sudo, o sistema solicitará que os usuários se autentiquem com uma senha.
- Em seguida, o sistema Linux registrará um registro de data e hora como um rastreador.
- Por padrão, todo usuário root pode executar comandos sudo por 15 minutos/sessão.
- Se você tentar executar o sudo na linha de comando sem se autenticar, o sistema registrará a atividade como um evento de segurança.
- Aqui está a sintaxe geral:
- sudo [comando]

Comando sudo

- O arquivo /etc/sudoers precisa ser manipulado
- Utilize o comando visudo como root para fazer alterações no arquivo:
- # visudo

- ……
- ## Allow root to run any commands anywhere
- root ALL=(ALL) ALL
- nasserala ALL=(ALL) ALL
- ……

Comando su

- O comando switch user, ou su, permite executar um programa como um usuário diferente.
- Ele altera a conta administrativa na sessão de login atual.
- Esse comando é especialmente útil para acessar o sistema por meio de SSH ou usar o gerenciador de exibição da GUI quando o usuário raiz não está disponível.

- Esta é a sintaxe geral do comando:
- su [opções] [nome de usuário [argumento]]

- Quando executado sem nenhuma opção ou argumento, o comando su é executado com privilégios de root.
- Ele solicitará que você se autentique e use os privilégios sudo temporariamente.

Comando su

- Aqui estão algumas que você pode usar:

- -p ou –preserve-environment mantém o mesmo ambiente de shell, composto por HOME, SHELL, USER e LOGNAME.
- -s ou –shell permite especificar um ambiente de shell diferente para execução.
- -l ou –login executa um script de login para mudar para um nome de usuário diferente.
- Para executá-lo, é necessário digitar a senha do usuário.

Comandos alias e unalias

- O alias permite que você crie um atalho com a mesma funcionalidade de um comando, nome de arquivo ou texto.
- Quando executado, ele instrui o shell a substituir uma string por outra.
- Para usar o comando alias, digite a seguinte sintaxe:
- alias Name=String

- Por exemplo, você deseja tornar k o alias do comando kill:
- alias k=’kill’
- Por outro lado, o comando unalias exclui um alias existente.
- Veja a seguir como é a sintaxe geral:
- unalias [nome_do_alias]

Comando htop

- O comando htop é um programa interativo que monitora os recursos do sistema e os processos do servidor em tempo real.
- Ele está disponível na maioria das distribuições Linux e você pode instalá-lo usando o gerenciador de pacotes padrão.
- Em comparação com o comando top, o htop tem muitos aprimoramentos e recursos adicionais, como a operação com o mouse e indicadores visuais.
- Para usá-lo, execute o seguinte comando:
- htop [opções]

- Você também pode adicionar opções, como:
- -d ou –delay mostra o atraso entre as atualizações em décimos de segundos.
- -C ou –no-color ativa o modo monocromático.
- -h ou –help exibe a mensagem de ajuda e sai.

Comandos zip e unzip

- Use o comando zip para compactar seus arquivos em um arquivo ZIP, um formato universal comumente usado no Linux.
- Ele pode escolher automaticamente a melhor taxa de compactação.
- O comando zip também é útil para arquivar arquivos e diretórios e reduzir o uso do disco.
- Para usá-lo, digite a seguinte sintaxe:
- zip [opções] zipfile file1 file2….

- Por exemplo, se você tem um arquivo chamado note.txt que deseja compactar em archive.zip no diretório atual:
- zip archive.zip note.txt

Comandos zip e unzip

- Instalar:
- # yum install zip -y

- Por outro lado, o comando unzip extrai os arquivos compactados de um arquivo. Este é o formato geral:
- unzip [opção] nome_do_arquivo.zip

- Portanto, para descompactar um arquivo chamado archive.zip no diretório atual, digite:
- unzip archive.zip

Comando which

- O comando which no Linux recebe como argumento o nome de um comando e traz como resultado a localização no disco deste comando, nos diretórios referenciados na variável PATH.
- Ele é especialmente útil quando você estiver testando diversas versões de um comando e deseja ter certeza de que está executando a versão correta.

- Exemplos:
- $ which php
- /usr/bin/php

- $ which nginx
- /usr/sbin/nginx

Comando shred

- O comando shred nos permite excluir arquivos do computador com segurança, sobrescrevendo-o para esconder seu conteúdo.
- Ele pode sobrescrever o arquivo repetidamente, de modo a dificultar uma eventual tentativa de recuperação de arquivos, mesmo utilizando-se de equipamentos especializados nesta tarefa.

- Sintaxe:
- shred [opções] arquivos

Comando shred

- Exemplos de uso:
- Vamos usar um arquivo chamado confidencial em nossos exemplos. Esse arquivo consiste em um texto comum:

- 1. Sobrescrever o conteúdo do arquivo confidencial usando o método padrão:
- # shred confidencial

- 2. Veja o conteúdo do arquivo após a operação:
- # cat confidencial

- Veja que o arquivo continua existindo, porém com seu conteúdo brutalmente sobrescrito

Comando shred

- Sobrescrever e excluir o arquivo confidencial, liberando espaço em disco:
- # shred -u confidencial

- Sobrescrever todos os dados na partição /dev/sdb5:
- # shred /dev/sdb5

- Sobrescrever o arquivo confidencial, preenchendo-o com zeros:
- # shred -z confidencial

- Sobrescrever o arquivo 40 vezes e depois excluí-lo:
- # shred -n 40 -u confidencial

Comando whoami

- whoami imprime o nome de usuário associado ao ID do usuário efetivo atual.
- Executar whoami é o mesmo que executar o comando id com as opções -un .

- Sintaxe
- whoami [OPÇÃO]

- Comandos relacionados
- w – Mostra quem está conectado e o que está fazendo.
- who – Relata quais usuários estão conectados ao sistema.

Comando neofetch

- O Neofetch é um programa bem simples que nos permite a visualização de informações básicas sobre o hardware do PC via Terminal (Linha de Comandos).

- Para instalar:
- # yum install neofetch –y

- Exemplo:
- # neofetch

Comando wget

- O comando wget é um comando criado na linguagem C pela GNU Project e visa fazer download de conteúdos da Web, daí vem o nome, com o W fazendo referência a World Wide Web e o GET que é referente ao termo em inglês get ou pegar.
- Esse comando é categorizado com um comando não interativo, significa que ele pode desempenhar sua função independente do usuário estar logado ou não.

- Esse um exemplo básico da utilização desse comando, veja como você deve inserir o comando:
- wget https://seudominio.com.br/arquivo.txt

- Dessa forma o wget irá realizar o download do arquivo que estiver no diretório inicial do seu domínio.

Comando nmap

- Nmap é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker "Fyodor". (**yum install nmap –y**)
- É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.
- Os recursos do Nmap incluem:
  - Descoberta de hosts
  - Scanner de portas
  - Detecção de versão
  - Detecção do sistema operacional

Comando nmap

- -sP : Essa opção envia um pacote ICMP Ping Scan, que é usado para encontrar um host na rede.
- Exemplo:
- # nmap -sP 10.100.102.0/24

- -sU : Essa opção determina quais portas UDP estão ativas.
- Exemplo:
- # nmap -sU 10.100.102.39
- -sS : Essa opção já e mais aprimorada, além de mandar o pacote e esperar uma confirmação, no meio da conexão ele a interrompe, com isso ele consegue burlar algumas sistemas de proteção. O -sS procura por portas do tipo TCP.

Comando nmap

- Exemplo:
- # nmap -sS 10.100.102.39

- A saída deste comando irá lhe mostrar as portas abertas e os seus respectivos serviços que estão rodando.

- -sT :Similar a opção -sS, só que ela tem uma maior garantia de sucesso, ou seja, ela é melhor.mas de proteção.

Comando iperf

- O iperf3 é um programa gratuito baseado em linha de comando multiplataforma e de código aberto para realizar medições de throughput de rede em tempo real.
- É uma das ferramentas mais poderosas para testar a largura de banda máxima alcançável em redes IP (suporta IPv4 e IPv6).
- Com iperf, você pode ajustar vários parâmetros associados a tempo, buffers e protocolos como TCP, UDP e SCTP.
- Ele é útil para operações de ajuste de desempenho de rede.
- yum install iperf3 -y

Comando iperf

- Primeiro, conecte-se à máquina remota que você usará como o servidor e inicie o iperf3 no modo de servidor usando o sinalizador -s, ele irá escute a porta 5201 por padrão.

- Você pode especificar o formato (k, m, g para Kbits, Mbits , Gbits ou K, M, G para KBytes, Mbytes , Gbytes) para relatar, usando a opção -f conforme mostrado.
- $ iperf3 -s -f K

Comando iperf

- Se a porta 5201 estiver sendo usada por outro programa em seu servidor, você pode especificar uma porta diferente (por exemplo, 3000) usando a opção -p como mostrando.
- $ iperf3 -s -p 3000

- Opcionalmente, você pode executar o servidor como um daemon, usando o sinalizador -D e gravar mensagens do servidor em um arquivo de log, conforme a seguir.
- $ iperf3 -s -D > iperf3log

Comando iperf

- Em seguida, em sua máquina local, que trataremos como o cliente (onde ocorre o benchmark real), execute iperf3 no modo cliente usando -c sinalizar e especificar o host no qual o servidor está sendo executado (usando seu endereço IP ou domínio ou nome do host).
- $ iperf3 -c 192.168.10.1 -f K

- Após cerca de 18 a 20 segundos, o cliente deve encerrar e produzir resultados indicando a taxa de transferência média para o benchmark, conforme mostrado na captura de tela a seguir.

Comando iperf

```
[root@FWCasaNasser ~]# iperf3 -c 177.221.58.163 -f K
Connecting to host 177.221.58.163, port 5201
[  5] local 192.168.10.2 port 43862 connected to 177.221.58.163 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  7.50 MBytes  7682 KBytes/sec   61    109 KBytes
[  5]   1.00-2.00   sec  7.81 MBytes  7998 KBytes/sec    7    115 KBytes
[  5]   2.00-3.00   sec  7.81 MBytes  7998 KBytes/sec   33    120 KBytes
[  5]   3.00-4.00   sec  9.13 MBytes  9352 KBytes/sec    0    168 KBytes
[  5]   4.00-5.00   sec  9.37 MBytes  9598 KBytes/sec   31    163 KBytes
[  5]   5.00-6.00   sec  6.67 MBytes  6829 KBytes/sec   72   60.2 KBytes
[  5]   6.00-7.00   sec  7.39 MBytes  7567 KBytes/sec    0    120 KBytes
[  5]   7.00-8.00   sec  8.47 MBytes  8675 KBytes/sec    7    123 KBytes
[  5]   8.00-9.00   sec  8.29 MBytes  8490 KBytes/sec    2    138 KBytes
[  5]   9.00-10.00  sec  9.31 MBytes  9536 KBytes/sec   17    141 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  81.8 MBytes  8372 KBytes/sec  230             sender
[  5]   0.00-10.00  sec  81.3 MBytes  8321 KBytes/sec                  receiver

iperf Done.
```

Referências

- https://www.hostinger.com.br/tutoriais/comandos-linux
- https://www.certificacaolinux.com.br/comando-linux-which/
- http://www.bosontreinamentos.com.br/linux/comando-shred-excluindo-arquivos-e-limpando-discos-com-seguranca-no-linux/
- https://www.linuxforce.com.br/comandos-linux/comandos-linux-comando-whoami/
- https://pt.linux-console.net/?p=2347#gsc.tab=0