



Módulo 4: Visão geral do Linux



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do módulo: Visão geral do Linux

Objetivo do módulo: Implementar segurança básica do Linux.

Título do Tópico	Objetivo do Tópico
Linux Básico	Explicar por que as habilidades do Linux são essenciais para o monitoramento e a investigação de segurança de rede.
Trabalhando no Linux Shell	Usar o Linux Shell para manipular arquivos de texto.
Servidores e clientes Linux	Explicar como funcionam as redes client-server.
Administração Básica do Servidor	Explicar como um administrador do Linux localiza e manipula arquivos de log de segurança.
O sistema de arquivos Linux	Gerenciar o sistema de arquivos e as permissões do Linux.
Trabalhando na GUI do Linux	Explicar os componentes básicos da GUI do Linux.
Trabalhando em um host Linux	Usar ferramentas para detectar malware em um host do Linux.

4.1 Noções básicas do Linux

O que é Linux?

- Linux é um sistema operacional criado em 1991.
- O Linux é de código aberto, rápido, confiável e pequeno. Ele requer muito poucos recursos de hardware para ser executado e é altamente personalizável.
- Linux faz parte de várias plataformas e pode ser encontrado em dispositivos de qualquer lugar, desde relógios de pulso a supercomputadores.
- O Linux foi projetado para ser conectado à rede, o que torna muito mais simples escrever e usar aplicativos baseados em rede.
- Uma distribuição Linux é o termo usado para descrever pacotes criados por diferentes organizações e incluir o kernel Linux com ferramentas personalizadas e pacotes de software.



do Linux O valor do Linux

O Linux é frequentemente o sistema operacional escolhido no Centro de Operações de Segurança (SOC). Estas são algumas das razões para escolher o Linux:

- **Linux é open source** - Qualquer pessoa pode adquirir Linux gratuitamente e modificá-lo para atender a necessidades específicas.
- **A CLI do Linux é muito poderosa** - A CLI (Command Line Interface) Linux é extremamente poderosa e permite que os analistas executem tarefas não apenas diretamente em um terminal, mas também remotamente.
- **O usuário tem mais controle sobre o sistema operacional** - O usuário administrador no Linux, conhecido como o usuário root, ou superusuário, pode modificar qualquer aspecto do computador com algumas teclas pressionadas.
- **Ele permite um melhor controle de comunicação de rede** - Controle é uma parte inerente do Linux.

Visão geral do Linux no SOC

- A flexibilidade fornecida pelo Linux é um ótimo recurso para o SOC. Todo o sistema operacional pode ser adaptado para se tornar a plataforma de análise de segurança perfeita.
- Sguil é o console de analistas de segurança cibernética em uma versão especial do Linux chamada Security Onion.
- O Security Onion é um conjunto de ferramentas de código aberto que trabalham juntas para análise de segurança de rede.

The screenshot displays the Sguil-0.9.0 interface, which is a network security monitoring tool. The top window shows a list of network events with columns for ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The bottom window shows a detailed view of a selected packet, including its source and destination IP addresses, ports, and the payload data.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	seconion...	5.1583	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion...	5.1584	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion...	5.1599	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoader ...
RT	1	seconion...	5.1600	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	7	seconion...	7.1896	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion...	7.1897	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion...	7.1912	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoader ...
RT	1	seconion...	7.1913	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	1	seconion...	5.1679	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	1	seconion...	7.1992	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	49	seconion...	7.1998	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	49	seconion...	5.1701	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	1	seconion...	5.1770	2020-05-10 21:41:13	209.165.201.17	38782	209.165.200.235	3306	6	ET SCAN Suspicious Inbound to ...

Sid	Net	Hostname	Type	Last
1	seconion-os...	seconion-os...	ossec	2020-05-12
2	seconion-en...	seconion-en...	pcap	2020-05-12
3	seconion-en...	seconion-en...	snort	2020-05-10
4	seconion-en...	seconion-en...	pcap	2020-05-12
5	seconion-en...	seconion-en...	snort	2020-05-10
6	seconion-en...	seconion-en...	pcap	2020-05-12
7	seconion-en...	seconion-en...	snort	2020-05-10

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	209.165.201.17	209.165.200.235	4	5	0	172	50175	2	0	63	16900
DATA	47 45 54 20 2F 31 31 20 48 54 54 50 2F 31 2E 31	0D 0A 48 6F 73 74 3A 20 32 30 39 2E 31 36 35 2E	32 30 30 2E 32 33 35 0D 0A 55 73 65 72 2D 41 67	65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30	20 28 63 6F 6D 70 61 74 69 62 6C 65 38 20 4D 53	GET /11 HTTP/1.1 ..Host: 209.165. 200.235..User-Ag ent: Mozilla/4.0 (compatible; MS					

do Linux no SOC (Condd.)

A tabela a seguir lista algumas ferramentas que são freqüentemente encontradas em um SOC:

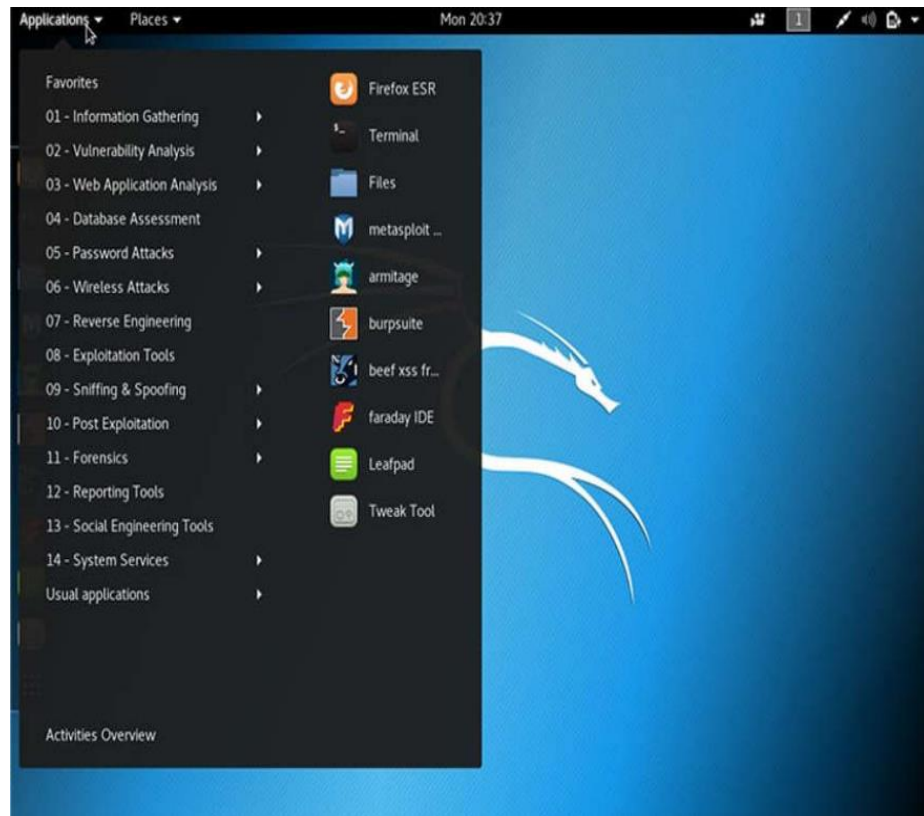
Ferramenta SOC	Descrição
Software de captura de pacotes de rede	<ul style="list-style-type: none">• Uma ferramenta crucial para um analista de SOC, pois permite observar e entender cada detalhe de uma transação de rede.• Wireshark é uma ferramenta popular de captura de pacotes.
Ferramentas de análise de malware	<ul style="list-style-type: none">• Essas ferramentas permitem que os analistas executem e observem com segurança a execução de malware sem o risco de comprometer o sistema subjacente.
Sistemas de detecção de intrusão (IDSs)	<ul style="list-style-type: none">• Essas ferramentas são usadas para monitoramento e inspeção de tráfego em tempo real.• Se qualquer aspecto do tráfego atualmente em fluxo corresponder a qualquer uma das regras estabelecidas, uma ação predefinida será executada.

do Linux no SOC (Cont.)

Ferramenta SOC	Descrição
Firewalls	<ul style="list-style-type: none">• Este software é usado para especificar, com base em regras predefinidas, se o tráfego tem permissão para entrar ou sair de uma rede ou dispositivo.
Gerenciadores de log	<ul style="list-style-type: none">• Os arquivos de log são usados para registrar eventos.• Como uma rede pode gerar um número muito grande de entradas de log, o software do gerenciador de logs é empregado para facilitar o monitoramento de log.
Segurança das informações e gerenciamento de eventos (SIEM)	<ul style="list-style-type: none">• Os SIEMs fornecem análise em tempo real de alertas e entradas de log geradas por dispositivos de rede, como IDSs e firewalls.
Sistemas de emissão de bilhetes	<ul style="list-style-type: none">• A atribuição de tíquetes de tarefa, edição e gravação é feita através de um sistema de gerenciamento de tíquetes. Os alertas de segurança são frequentemente atribuídos a analistas por meio de um sistema de emissão de bilhetes.

Linux Ferramentas Linux

- Computadores Linux que são usados no SOC geralmente contêm ferramentas de teste de penetração.
- Um teste de penetração, também conhecido como Pentesting, é o processo de procurar vulnerabilidades em uma rede ou computador atacando-o.
- Geradores de pacotes, scanners de porta e explorações de prova de conceito são exemplos de ferramentas Pentesting.
- Kali Linux é uma distribuição Linux que contém muitas ferramentas de penetração juntas em uma única distribuição Linux.
- Observe todas as principais categorias de ferramentas de teste de penetração do Kali Linux.



4.2 Como trabalhar no Linux Shell

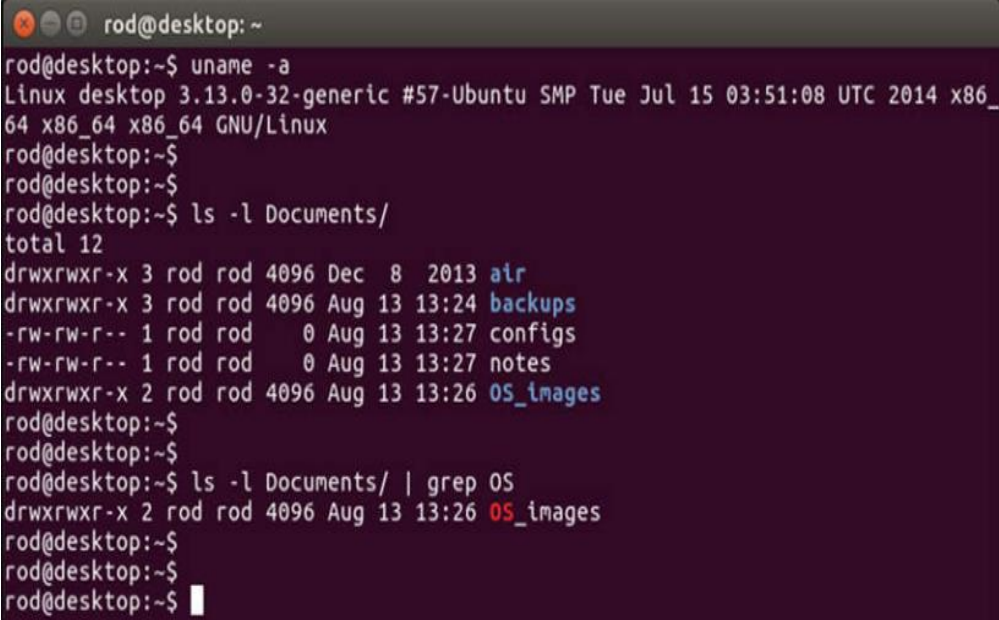
O Shell Linux

- No Linux, o usuário se comunica com o SO usando a CLI ou a GUI.
- O Linux geralmente inicia na GUI por padrão. Isso oculta a CLI do usuário.
- Uma maneira de acessar a CLI a partir da GUI é por meio de um aplicativo de emulador de terminal. Esses aplicativos fornecem acesso do usuário ao CLI e são nomeados como uma variação da palavra terminal.
- No Linux, emuladores de terminal populares são Terminator, eterm, xterm, konsole e gnome-terminal.
- Fabrice Bellard criou JSLinux que permite que uma versão emulada do Linux seja executada em um navegador.

Observação: *Os termos shell, console, janela do console, terminal da CLI e janela do terminal são frequentemente usados de forma intercambiável.*

O Shell Linux (Cont.)

A figura mostra o gnome-terminal, um emulador de terminal Linux popular.



```
rod@desktop: ~  
rod@desktop:~$ uname -a  
Linux desktop 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/  
total 12  
drwxrwxr-x 3 rod rod 4096 Dec  8 2013 air  
drwxrwxr-x 3 rod rod 4096 Aug 13 13:24 backups  
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 configs  
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 notes  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/ | grep OS  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$
```

Trabalhando nos Comandos Básicos do Shell do Linux

- Os comandos Linux são programas criados para executar uma tarefa específica.
- Como os comandos são programas armazenados no disco, quando um usuário digita um comando, o shell deve encontrá-lo no disco antes que ele possa ser executado.
- A tabela a seguir lista os comandos básicos do Linux e suas funções:

Comando	Descrição
mv	Move ou renomeia arquivos e diretórios.
chmod	Modifica as permissões do arquivo.
chown	Altera a propriedade de um arquivo.
dd	Copia os dados de uma entrada para uma saída.
pwd	Exibe o nome do diretório atual.
ps	Lista os processos que estão em execução no sistema.
su	Simula um login como outro usuário ou para se tornar um super usuário.

Trabalhando nos Comandos Básicos do Shell do Linux (Cont.)

Comando	Descrição
sudo	Executa um comando como um superusuário, por padrão, ou outro usuário nomeado.
grep	Usado para pesquisar cadeias de caracteres específicas em um arquivo ou outras saídas de comando.
ifconfig	Usado para exibir ou configurar informações relacionadas à placa de rede.
apt-get	Usado para instalar, configurar e remover pacotes no Debian e seus derivados.
iwconfig	Usado para exibir ou configurar informações relacionadas à placa de rede sem fio.
shutdown	Desliga o sistema e executa tarefas relacionadas ao encerramento, incluindo reiniciar, parar, colocar em suspensão ou expulsar todos os usuários conectados no momento.
passwd	Usado para alterar a senha.
cat	Usado para listar o conteúdo de um arquivo e espera o nome do arquivo como parâmetro.
man	Usado para exibir a documentação de um comando específico.

arquivo do shell do Linux e comandos de diretório

Muitas ferramentas de linha de comando estão incluídas no Linux por padrão. A tabela a seguir lista alguns dos comandos mais comuns relacionados a arquivos e diretórios:

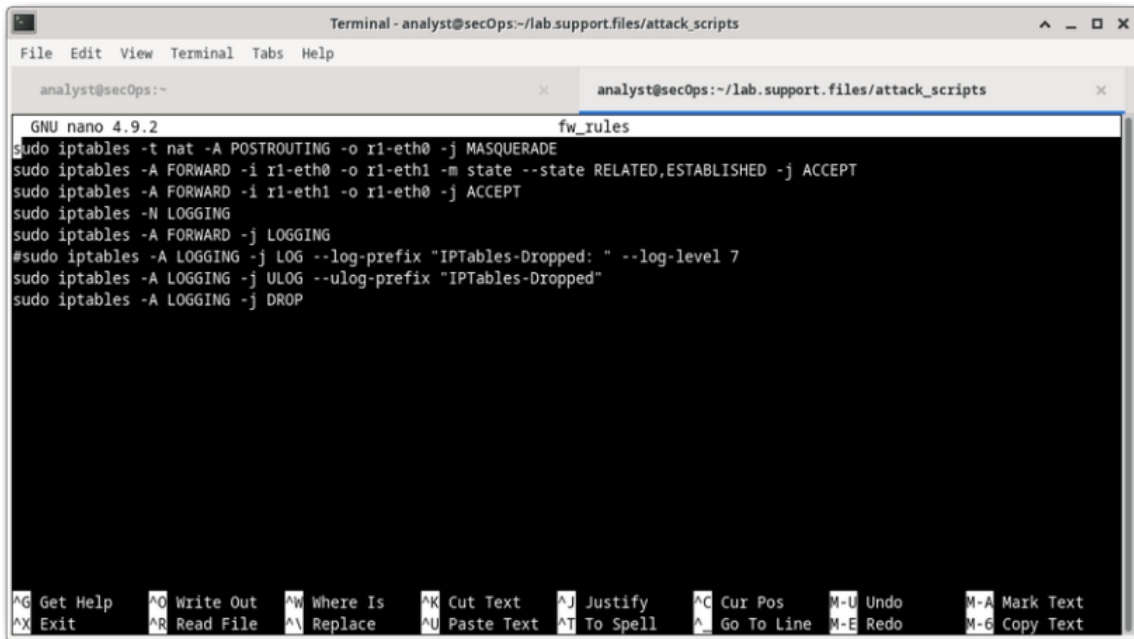
Comando	Descrição
É	Exibe os arquivos em um diretório.
cd	Altera o diretório atual.
mkdir	Cria um diretório dentro do diretório atual.
cp	Copia arquivos da origem para o destino.
mv	Move arquivos para um diretório diferente.
rm	Remove os arquivos.
grep	Pesquisa cadeias de caracteres específicas em um arquivo ou outras saídas de comandos.
cat	Lista o conteúdo de um arquivo e supõe o nome do arquivo como o parâmetro.

Trabalhando com Arquivos de Texto

- Linux tem muitos editores de texto diferentes, com vários recursos e funções.
- Alguns editores de texto incluem interfaces gráficas, enquanto outros são apenas ferramentas de linha de comando. Cada editor de texto inclui um conjunto de recursos projetado para suportar um tipo específico de tarefa.
- Alguns editores de texto se concentram no programador e incluem recursos como realce de sintaxe, verificação de parênteses e outros recursos focados na programação.
- Embora os editores de texto gráficos sejam convenientes e fáceis de usar, os editores de texto baseados em linha de comando são muito importantes para os usuários do Linux. O principal benefício dos editores de texto baseados em linha de comando é que eles permitem a edição de arquivos de texto a partir de um computador remoto.

Trabalhando com Arquivos de Texto (Cont.)

- A figura mostra **nano**, um editor de texto de linha de comando popular.
- O administrador está editando regras de firewall. Editores de texto são frequentemente usados para configuração e manutenção do sistema no Linux.
- Devido à falta de suporte gráfico, nano (ou GNU nano) só pode ser controlado com o teclado.



```
Terminal - analyst@secOps:~/lab.support.files/attack_scripts
File Edit View Terminal Tabs Help
analyst@secOps:~
GNU nano 4.9.2 fw_rules
sudo iptables -t nat -A POSTROUTING -o r1-eth0 -j MASQUERADE
sudo iptables -A FORWARD -i r1-eth0 -o r1-eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i r1-eth1 -o r1-eth0 -j ACCEPT
sudo iptables -N LOGGING
sudo iptables -A FORWARD -j LOGGING
#sudo iptables -A LOGGING -j LOG --log-prefix "IPTables-Dropped: " --log-level 7
sudo iptables -A LOGGING -j ULOG --ulog-prefix "IPTables-Dropped"
sudo iptables -A LOGGING -j DROP
^G Get Help ^O Write Out ^M Where Is ^K Cut Text ^J Justify ^C Cur Pos ^U Undo ^A Mark Text
^X Exit ^R Read File ^\ Replace ^V Paste Text ^I To Spell ^_ Go To Line ^E Redo ^G Copy Text
```

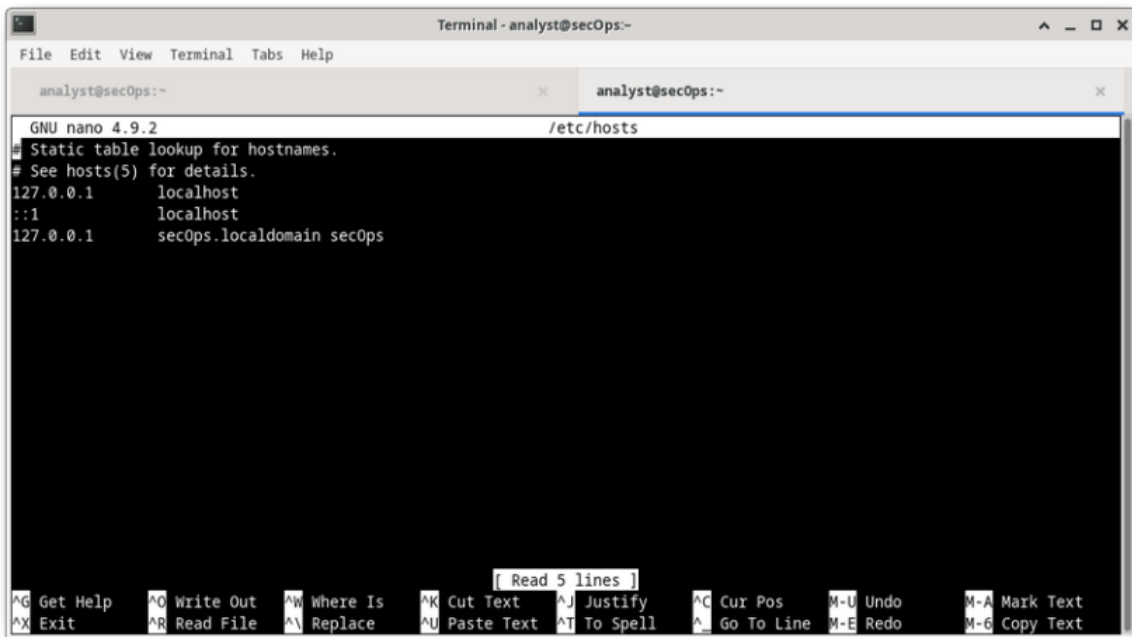
A Importância dos Arquivos de Texto no Linux

- No Linux, tudo é tratado como um arquivo. Isso inclui a memória, os discos, o monitor e os diretórios.
- Arquivos de configuração são arquivos de texto que são usados para armazenar ajustes e configurações para aplicativos ou serviços específicos.
- Os usuários com níveis de permissão adequados podem usar editores de texto para alterar o conteúdo dos arquivos de configuração.
- Depois que as alterações são feitas, o arquivo é salvo e pode ser usado pelo serviço ou aplicativo relacionado. Os usuários podem especificar exatamente como querem que qualquer aplicativo ou serviço se comporte. Quando iniciados, serviços e aplicativos verificam o conteúdo de arquivos de configuração específicos para ajustar seu comportamento de acordo.

Observação: O administrador usou o comando **`sudo nano /etc/hosts`** para abrir o arquivo. O comando **`sudo`** (abreviação de “superusuário do”) invoca o privilégio de superusuário para usar o editor de texto **`nano`** para abrir o arquivo **`host`**.

A Importância dos Arquivos de Texto no Linux (Cont.)

- Na figura, o administrador abriu o arquivo de configuração do host em **nano** para edição.
- O arquivo host contém mapeamentos estáticos de endereços IP do host para nomes.
- Os nomes servem como atalhos que permitem a conexão com outros dispositivos usando um nome em vez de um endereço IP. Somente o superusuário pode alterar o arquivo host.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
analyst@secOps:~
analyst@secOps:~
GNU nano 4.9.2 /etc/hosts
# Static table lookup for hostnames.
# See hosts(5) for details.
127.0.0.1    localhost
::1         localhost
127.0.0.1    secOps.localdomain secOps
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos  ^U Undo     ^M Mark Text
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line ^E Redo     ^G Copy Text
[ Read 5 lines ]
```

Laboratório — Trabalhando com arquivos de texto na CLI

Neste laboratório, você se familiarizará com editores de texto de linha de comando Linux e arquivos de configuração.

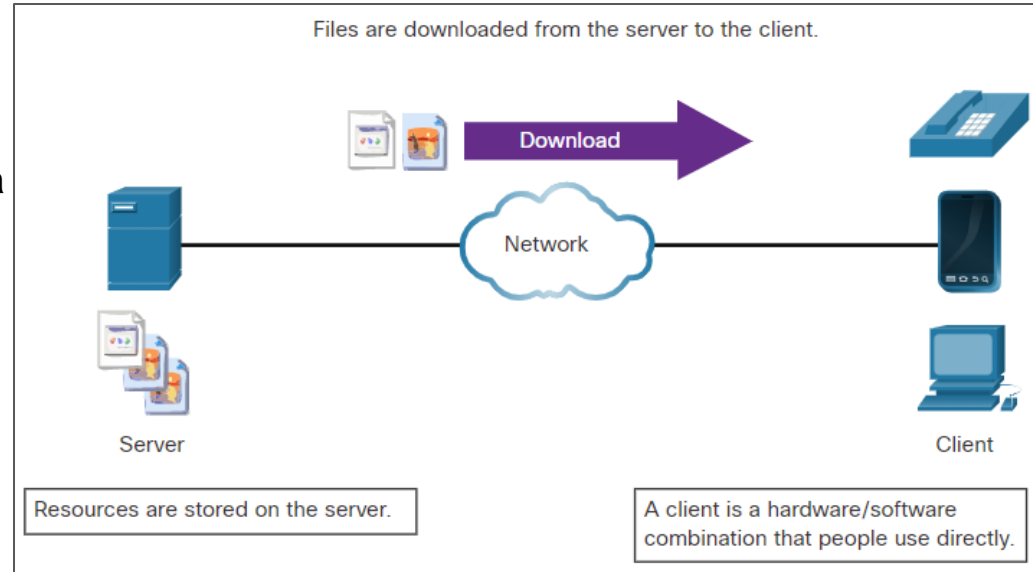
Lab — Familiarizando-se com o Linux Shell

Neste laboratório, você usará a linha de comando do Linux para gerenciar arquivos e diretórios e realizar algumas tarefas administrativas básicas.

4.3 Servidores e clientes do Linux

Uma Introdução às Comunicações Cliente-Servidor

- Os servidores são computadores com software instalado que lhes permite fornecer serviços aos clientes em toda a rede.
- Alguns fornecem recursos externos, como arquivos, mensagens de e-mail ou páginas da Web para clientes mediante solicitação.
- Outros serviços executam tarefas de manutenção, como gerenciamento de logs, varredura de disco e assim por diante.
- Cada serviço exige um software de servidor separado.
- O servidor na figura usa um software de servidor de arquivos para fornecer aos clientes a capacidade de recuperar e enviar arquivos.



Servidores e Clientes Linux, Servidores, Serviços e Suas Portas

- Uma porta é um recurso de rede reservado usado por um serviço.
- Embora o administrador possa decidir qual porta usar com qualquer serviço específico, muitos clientes são configurados para usar uma porta específica por padrão.
- A tabela a seguir lista algumas portas comumente usadas e seus serviços. Estes também são chamados de portas bem conhecidas.

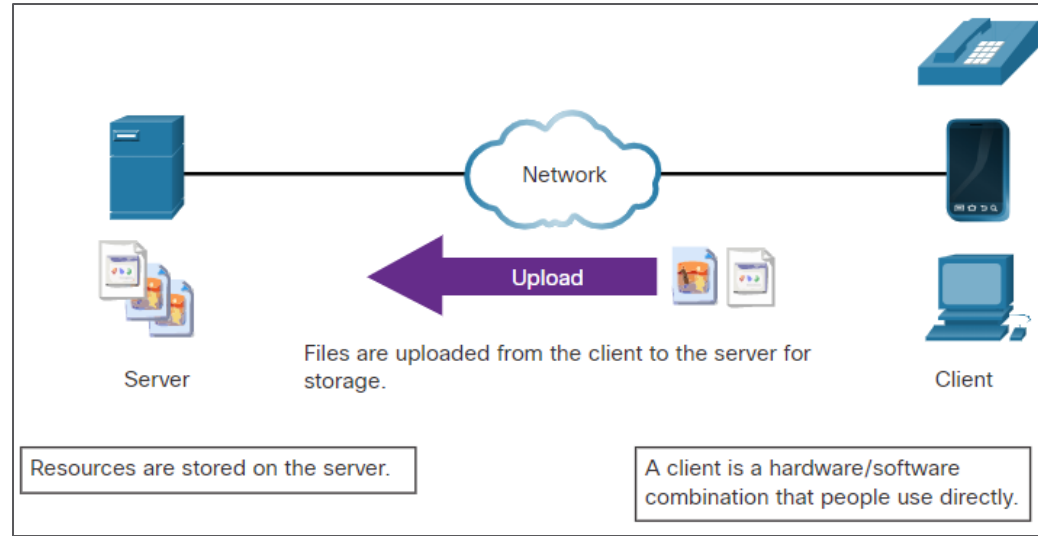
Porta	Descrição
20/21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Serviço de login remoto Telnet
25	Protocolo SMTP
53	Domain Name System (DNS)
67/68	Protocolo de Configuração Dinâmica de Host (DHCP)

Servidores e Clientes Linux, Servidores, Serviços e Suas Portas (Cont.)

Porta	Descrição
69	Protocolo de Transferência Trivial de Arquivo (TFTP)
80	Protocolo HTTP
110	Protocolo POP3 (Post Office Protocol - Protocolo dos Correios)
123	Network Time Protocol (NTP)
143	Protocolo IMAP
161/162	Protocolo de Gerenciamento Simples de Rede (SNMP)
443	HTTP seguro (HTTPS)

Clientes

- Os clientes são programas ou aplicativos projetados para se comunicar com um tipo específico de servidor.
- Os clientes usam um protocolo bem definido para se comunicar com o servidor.
- Os navegadores da Web são clientes da Web que são usados para se comunicar com servidores Web por meio do Hyper Text Transfer Protocol na porta 80.
- O cliente File Transfer Protocol é um software usado para se comunicar com um servidor FTP.
- A figura mostra um cliente fazendo upload de arquivos para um servidor.



Laboratório de servidores e clientes Linux - Servidores Linux

Neste laboratório, você usará a linha de comando do Linux para identificar servidores que estão sendo executados em um computador.

4.4 Administração básica do servidor

Arquivos de configuração do serviço de administração de servidor básico

- No Linux, os serviços são gerenciados usando arquivos de configuração.
- As opções comuns nos arquivos de configuração são o número da porta, a localização dos recursos hospedados e os detalhes da autorização do cliente.
- Quando o serviço é iniciado, ele procura seus arquivos de configuração, carrega-os na memória e se ajusta de acordo com as configurações nos arquivos.
- A saída do comando mostra uma parte do arquivo de configuração do Nginx, que é um servidor web leve para Linux.

```
[analyst@secOps ~]$ cat /etc/nginx/nginx.conf
#user html;

worker_processes 1;

#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;
#pid logs/nginx.pid;

events {
    worker_connections 1024;
}

http {
    include mime.types;
    default_type application/octet-stream;
    #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
    #                '$status $body_bytes_sent "$http_referer" '
    #                '"$http_user_agent" "$http_x_forwarded_for"';
    #access_log logs/access.log main;
```

Arquivos básicos de configuração do serviço de administração do servidor (Cont.)

A saída do comando mostra o arquivo de configuração para o protocolo de tempo de rede (NTP).

```
[analyst@secOps ~]$ cat /etc/ntp.conf
# Please consider joining the pool:
#
#       http://www.pool.ntp.org/join.html
#
# For additional information see:
# - https://wiki.archlinux.org/index.php/Network_Time_Protocol_daemon
# - http://support.ntp.org/bin/view/Support/GettingStarted
# - the ntp.conf man page
# Associate to Arch's NTP pool
server 0.arch.pool.ntp.org
server 1.arch.pool.ntp.org
server 2.arch.pool.ntp.org
server 3.arch.pool.ntp.org
# By default, the server allows:
# - all queries from the local host
# - only time queries from remote hosts, protected by rate limiting and kod
restrict default kod limited nomodify nopeer noquery notrap
restrict 127.0.0.1
restrict ::1
# Location of drift file
[analyst@secOps ~]$
```

Arquivos básicos de configuração do serviço de administração do servidor (Cont.)

- A saída do comando mostra o arquivo de configuração do Snort, um sistema de detecção de intrusões (IDS) baseado em Linux.
- Não há nenhuma regra para um formato de arquivo de configuração. É a escolha do desenvolvedor do serviço. No entanto, a **opção = formato de valor** é frequentemente usada.

```
[analyst@secOps ~]$ cat /etc/snort/snort.conf
#-----
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#   http://www.snort.org                Snort Website
#   http://vrt-blog.snort.org/          Sourcefire VRT Blog
#
#   Mailing list Contact:  snort-sigs@lists.sourceforge.net
#   False Positive reports: fp@sourcefire.com
#   Snort bugs:           bugs@snort.org
#
#   Compatible with Snort Versions:
#   VERSIONS : 2.9.9.0
#
#   Snort build options:
#   OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --
enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-react --enable-
flexresp3
<output omitted>
#####
# Step #1: Set the network variables.  For more information, see README.variables
#####
# Setup the network addresses you are protecting
##ipvar HOME_NET any
##ipvar HOME_NET [192.168.0.0/24,192.168.1.0/24]
ipvar HOME_NET [209.165.200.224/27]
# Set up the external network addresses.  Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

Dispositivos básicos de proteção da administração do servidor

- O endurecimento do dispositivo envolve a implementação de métodos comprovados de proteção do dispositivo e proteção de seu acesso administrativo.
- Alguns desses métodos envolvem a manutenção de senhas, a configuração de recursos avançados de login remoto e a implementação de login seguro com SSH.
- Dependendo da distribuição Linux, muitos serviços são habilitados por padrão. Parar esses serviços e garantir que eles não iniciem automaticamente no momento da inicialização é outra técnica de endurecimento do dispositivo.
- As atualizações do sistema operacional são extremamente importantes para manter um dispositivo reforçado. Os desenvolvedores de SO criam e emitem correções e patches regularmente.

Dispositivos básicos de proteção da administração do servidor (Condd.)

Seguem-se as práticas recomendadas básicas para o endurecimento do dispositivo:

- Garantir a segurança física
- Minimizar pacotes instalados
- Desativar serviços não utilizados
- Usar SSH e desabilitar o login da conta raiz por SSH
- Manter o sistema atualizado
- Desativar a detecção automática de USB
- Aplicar senhas fortes
- Forçar mudanças de senha periódicas
- Manter os usuários de reutilizarem senhas antigas

Logs do serviço de monitoramento de administração de servidor

- Arquivos de log são os registros que um computador armazena para manter o controle de eventos importantes. Kernel, serviços e eventos de aplicativos são todos registrados em arquivos de log.
- Ao monitorar arquivos de log do Linux, um administrador obtém uma visão clara do desempenho do computador, status de segurança e quaisquer problemas subjacentes.
- No Linux, os arquivos de log podem ser categorizados como:
 - Logs de aplicativos
 - Logs de eventos
 - Registros de serviço
 - Logs do sistema
- Alguns logs contêm informações sobre daemons que estão sendo executados no Linux. Um daemon é um processo em segundo plano que é executado sem a necessidade de interação do usuário.

Logs de serviço demonstrando de administração básica do servidor (Cont.)

A tabela a seguir lista alguns arquivos de log populares do Linux e suas funções:

Arquivo de log do Linux	Descrição
/var/log/mensagens	<ul style="list-style-type: none">• Este diretório contém logs genéricos de atividade do computador.• Ele é usado principalmente para armazenar mensagens informativas e não críticas do sistema.
/var/log/auth.log	<ul style="list-style-type: none">• Este arquivo armazena todos os eventos relacionados à autenticação em computadores Debian e Ubuntu.• Qualquer coisa que envolva o mecanismo de autorização do usuário pode ser encontrada neste arquivo.
/var/log/secure	<ul style="list-style-type: none">• Este diretório é usado por computadores RedHat e CentOS.• Ele também rastreia logins sudo, logins SSH e outros erros registrados pelo SSSD.
/var/log/boot.log	<ul style="list-style-type: none">• Este arquivo armazena informações relacionadas à inicialização e mensagens registradas durante o processo de inicialização do computador.

Logs de serviço demonstração de administração básica do servidor (Cont.)

Arquivo de log do Linux	Descrição
/var/log/dmesg	<ul style="list-style-type: none">• Este diretório contém mensagens de buffer do anel do kernel.• Informações relacionadas a dispositivos de hardware e seus drivers são registradas aqui.• É muito importante porque, devido à sua natureza de baixo nível, sistemas de registro como syslog não estão sendo executados quando esses eventos ocorrem e não estão disponíveis para o administrador em tempo real.
/var/log/kern.log	<ul style="list-style-type: none">• Este arquivo contém informações registradas pelo kernel.
/var/log/cron	<ul style="list-style-type: none">• Cron é um serviço usado para agendar tarefas automatizadas no Linux e este diretório armazena seus eventos.• Sempre que uma tarefa agendada (ou tarefa cron) é executada, todas as informações relevantes, incluindo status de execução e mensagens de erro, são armazenadas aqui.
/var/log/mysqld.log ou /var/log/mysql.log	<ul style="list-style-type: none">• Este é o arquivo de log do MySQL.• Todas as mensagens de depuração, falha e sucesso relacionadas ao processo mysqld e ao daemon mysqld_safe são registradas aqui.

Logs de serviço de monitoramento de administração básica do servidor (Cont.)

- A saída do comando mostra uma parte do arquivo de **log/var/log/messages**.
- Cada linha representa um evento registrado.
- Os carimbos de data/hora no início das linhas marcam o momento em que o evento ocorreu.

```
[analyst@secOps ~]$ sudo cat /var/log/messages
Mar 20 15:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1
20180312 (GCC)) #1 SMP PREEMPT Thu Mar 15 12:24:34 UTC 2018
Mar 20 15:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-
4ddf-bfd8-c169e8a877b2 rw quiet
Mar 20 15:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 15:28:45 secOps kernel: Intel GenuineIntel
Mar 20 15:28:45 secOps kernel: AMD AuthenticAMD
Mar 20 15:28:45 secOps kernel: Centaur CentaurHauls
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 20 15:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using
'standard' format.
Mar 20 15:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000ff000-0x00000000000fffff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000001000000-0x0000000003fffff] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000003ffff000-0x0000000003ffffff] ACPI data
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 20 15:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 15:28:45 secOps kernel: random: fast init done
Mar 20 15:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 15:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 15:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 15:28:45 secOps kernel: e820: last_pfn = 0x3ffff0 max_arch_pfn = 0x400000000
Mar 20 15:28:45 secOps kernel: MTRR: Disabled
Mar 20 15:28:45 secOps kernel: x86/PAT: MTRRs disabled, skipping PAT initialization too.
Mar 20 15:28:45 secOps kernel: CPU MTRRs all blank - virtualized system.
```

Laboratório básico de administração de servidor — localizando arquivos de log

Neste laboratório, você vai se familiarizar com a localização e manipulação de arquivos de log do Linux.

4.5 O sistema de arquivos Linux

Os Tipos de Sistema de Arquivos no Linux

- Existem muitos tipos diferentes de sistemas de arquivos, variando em propriedades de velocidade, flexibilidade, segurança, tamanho, estrutura, lógica e muito mais.
- O administrador decide o tipo de sistema de arquivos que é adequado para o sistema operacional.
- A tabela a seguir lista alguns tipos de sistema de arquivos comumente encontrados e

Sistema de arquivos Linux	Descrição
ext2 (segundo sistema de arquivos estendido)	<ul style="list-style-type: none">• ext2 era o sistema de arquivos padrão em várias distribuições Linux principais até ser suplantado pelo ext3.• O ext2 ainda é o sistema de arquivos escolhido para mídia de armazenamento baseada em flash, pois sua falta de um diário aumenta o desempenho e minimiza o número de gravações.• Como os dispositivos de memória flash têm um número limitado de operações de gravação, a minimização das operações de gravação aumenta a vida útil do dispositivo.

Os Tipos de Sistema de Arquivos no Linux (Cont.)

Sistema de arquivos Linux	Descrição
ext3 (terceiro sistema de arquivos estendido)	<ul style="list-style-type: none">• ext3 é um sistema de arquivo registrado projetado para melhorar o sistema de arquivo ext2 existente.• Um diário ou registro, o principal recurso adicionado ao ext3, é uma técnica usada para minimizar o risco de corrupção do sistema de arquivos no caso de perda repentina de energia.• Os sistemas de arquivos mantêm um registro de todas as alterações a serem feitas.• Se o computador falhar antes da conclusão da alteração, o diário pode ser usado para restaurar ou corrigir quaisquer problemas criados pela falha.• O tamanho máximo do arquivo em sistemas de arquivos ext3 é 32 TB.
ext4 (quarto sistema de arquivos estendido)	<ul style="list-style-type: none">• ext4 foi criado com base em uma série de extensões para ext3.• Enquanto as extensões melhoram o desempenho do ext3 e aumentam o tamanho dos arquivos suportados, os desenvolvedores estavam preocupados com problemas de estabilidade e se opuseram a adicionar as extensões ao ext3 estável.• O projeto ext3 foi dividido em dois; um mantido como ext3 e seu desenvolvimento normal e o outro, denominado ext4, incorporou as extensões mencionadas.

Os Tipos de Sistema de Arquivos no Linux (Cont.)

Sistema de arquivos Linux	Descrição
NFS (Network File System)	<ul style="list-style-type: none">• NFS é um sistema de arquivos baseado em rede, permitindo acesso a arquivos pela rede.• Do ponto de vista do usuário, não há diferença entre acessar um arquivo armazenado localmente ou em outro computador da rede.• O NFS é um padrão aberto, o que permite que qualquer pessoa o implemente.
CDFS (Compact Disc File System)	<ul style="list-style-type: none">• O CDFS foi criado especificamente para mídia de disco óptico.
Sistema de troca de arquivos	<ul style="list-style-type: none">• O sistema de arquivos de troca é usado pelo Linux quando fica sem RAM.• Quando isso acontece, o kernel move o conteúdo inativo da RAM para a partição de troca no disco.• Embora as partições de permuta possam ser úteis para computadores Linux com uma quantidade limitada de memória, elas não devem ser consideradas como uma solução primária.• A partição de permuta é armazenada no disco que tem velocidades de acesso muito mais baixas do que a RAM.

Os Tipos de Sistema de Arquivos no Linux (Cont.)

Sistema de arquivos Linux	Descrição
HFS Plus ou HFS+ (Sistema de Arquivos Hierárquico Plus)	<ul style="list-style-type: none">• Um sistema de arquivos usado pela Apple em seus computadores Macintosh.• O kernel Linux inclui um módulo para montar HFS+ para operações de leitura-gravação.
APFS (Sistema de Arquivos Apple)	<ul style="list-style-type: none">• Um sistema de arquivos atualizado que é usado por dispositivos Apple.• Ele fornece criptografia forte e é otimizado para unidades flash e de estado sólido.
Master Boot Record (MBR)	<ul style="list-style-type: none">• Localizado no primeiro setor de um computador particionado, o MBR armazena todas as informações sobre a forma como o sistema de arquivos é organizado.• O MBR entrega rapidamente o controle a uma função de carregamento, que carrega o sistema operacional.

Os Tipos de Sistema de Arquivos no Linux (Cont.)

- Montagem é o termo usado para o processo de atribuição de um diretório a uma partição.
- Após uma operação de montagem bem-sucedida, o sistema de arquivos contido na partição é acessível através do diretório especificado.
- A saída do comando mostra a saída do comando **mount** emitido na VM Cisco CyberOps.

```
[analyst@secops ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=494944k,nr_inodes=123736,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=11792)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

As funções Linux do sistema de arquivos Linux e permissões de arquivo

- O Linux usa permissões de arquivo para organizar o sistema e impor limites dentro do computador.
- Cada arquivo no Linux carrega suas permissões de arquivo, que definem as ações que o proprietário, o grupo e outros podem executar com o arquivo.
- Os direitos de permissão possíveis são Ler, Gravar e Executar.
- O comando **ls** com o parâmetro **-l** lista informações adicionais sobre o arquivo.

As Funções Linux do Sistema de Arquivos e Permissões de Arquivo (Cont.)

A saída do comando **ls -l** fornece muitas informações sobre o arquivo **space.txt**:

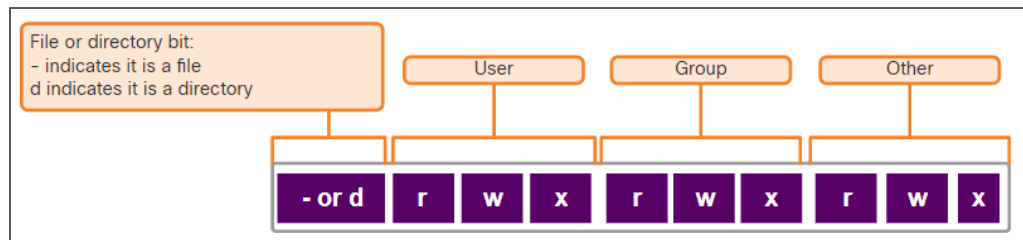
- O primeiro campo exibe as permissões com **space.txt(-rwxrw-r--)**.
- O segundo campo define o número de links rígidos para o arquivo (número **1** após as permissões).
- O terceiro e quarto campos exibem o usuário (**analista**) e o grupo (**staff**) que possui o arquivo, respectivamente.
- O quinto campo exibe o tamanho do arquivo em bytes. O arquivo **space.txt** tem 253 bytes.
- O sexto campo exibe a data e hora da última modificação.
- O sétimo campo exibe o nome do arquivo.

```
[analyst@secOps ~]$ ls -l space.txt
-rwxrw-r-- 1 analyst staff 253 May 20 12:49 space.txt
(1)(2)(3)(4)(5)(6)(7)
[analyst@secOps ~]$
```

As Funções Linux do Sistema de Arquivos e Permissões de Arquivo (Cont.)

A figura aqui mostra uma divisão das permissões de arquivo no Linux. O arquivo **space.txt** tem as seguintes permissões:

- O traço (-) significa que este é um arquivo.
- O primeiro conjunto de caracteres (**rw**x) é para permissão do usuário. O usuário (**analista**) que possui o arquivo pode **Ler**, **Escrever** e **Executar** o arquivo.
- O segundo conjunto de caracteres é para permissões de grupo (**rw**-). O grupo (**equipe**), equipe, que possui o arquivo pode **ler** e **gravar** no arquivo.
- O terceiro conjunto de caracteres é para quaisquer outras permissões de usuário ou grupo (**r**—) que possam somente **Read** o arquivo.



As Funções Linux do Sistema de Arquivos e Permissões de Arquivo (Cont.)

- Os valores octais são usados para definir permissões.
- Permissões de arquivo são uma parte fundamental do Linux e não podem ser quebradas.
- O único usuário que pode substituir a permissão de arquivo em um computador Linux é o usuário root.

Binário	Octal	Permissão	Descrição
000	0	---	Sem acesso
001	1	--x	Executar apenas
010	2	-w-	Somente escrita
011	3	-wx	Edição e execução
100	4	r--	Somente leitura
101	5	r-x	Ler e Executar
110	6	rw-	Leitura e Escrita
111	7	rwX	Ler, escrever e executar

os links rígidos do sistema de arquivos Linux e links simbólicos

- Um link rígido é outro arquivo que aponta para o mesmo local que o arquivo original.
- Use o comando **ln** para criar um link rígido.
- O primeiro argumento é o arquivo existente e o segundo argumento é o novo arquivo.
- Como mostrado na saída do comando, o arquivo **space.txt** está vinculado a **space.hard.txt** e o campo de link agora mostra 2.
- Ambos os arquivos apontam para o mesmo local no sistema de arquivos. Se você alterar um arquivo, o outro também será alterado.
- O comando **echo** é usado para adicionar algum texto a **space.txt**.

```
[analyst@secOps ~]$ ln space.txt space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.hard.txt
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "Testing hard link" >> space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.hard.txt
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ rm space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more space.txt
Space... The final frontier...
These are the voyages of the Starship Enterprise. Its continuing mission:
- To explore strange new worlds...
- To seek out new life; new civilizations...
- To boldly go where no one has gone before!
Testing hard link
[analyst@secOps ~]$
```

os links rígidos do sistema de arquivos Linux e links simbólicos (Cond.)

- Um link simbólico, também chamado de link simbólico ou link suave, é semelhante a um link rígido em que a aplicação de alterações ao link simbólico também mudará o arquivo original.
- Como mostrado na saída do comando, use a opção de comando **ln -s** para criar um link simbólico.
- Observe que adicionar uma linha de texto a **test.txt** também adiciona a linha a **mytest.txt**.

```
[analyst@secOps ~]$ echo "Hello World!" > test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ln -s test.txt mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "It's a lovely day!" >> mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more test.txt
Hello World!
It's a lovely day!
[analyst@secOps ~]$
[analyst@secOps ~]$ rm test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more mytest.txt
more: stat of mytest.txt failed: No such file or directory
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l mytest.txt
lrwxrwxrwx 1 analyst analyst 8 May  7 20:17 mytest.txt -> test.txt
[analyst@secOps ~]$
```

os links rígidos do sistema de arquivos Linux e links simbólicos (Cont.)

A tabela a seguir mostra vários benefícios de links simbólicos sobre links rígidos:

Links rígidos	Ligações suaves
Localizar links rígidos é difícil.	Links simbólicos mostram a localização do arquivo original no comando ls -l .
Links rígidos são limitados ao sistema de arquivos no qual eles são criados.	Links simbólicos podem ser vinculados a um arquivo em outro sistema de arquivos.
Links rígidos não podem se vincular a um diretório, pois o próprio sistema usa links rígidos para definir a hierarquia da estrutura de diretórios.	Links simbólicos podem ser vinculados a diretórios.

O

Laboratório do Sistema de Arquivos Linux - Navegando pelo Sistema de Arquivos Linux e Configurações de Permissão

Neste laboratório, você se familiarizará com sistemas de arquivos Linux.

4.6 Como trabalhar com a GUI do Linux

X Window System

- A interface gráfica presente na maioria dos computadores Linux é baseada no X Window System.
- X Window, também conhecido como X ou X11, é um sistema de janelas projetado para fornecer a estrutura básica para uma GUI.
- X inclui funções para desenhar e mover janelas no dispositivo de exibição e interagir com um mouse e teclado.
- X funciona como um servidor, o que permite que um usuário remoto use a rede para se conectar, iniciar um aplicativo gráfico e ter a janela gráfica aberta no terminal remoto.
- X não especifica a interface do usuário, deixando para outros programas, como gerenciadores de janelas, definir todos os componentes gráficos.

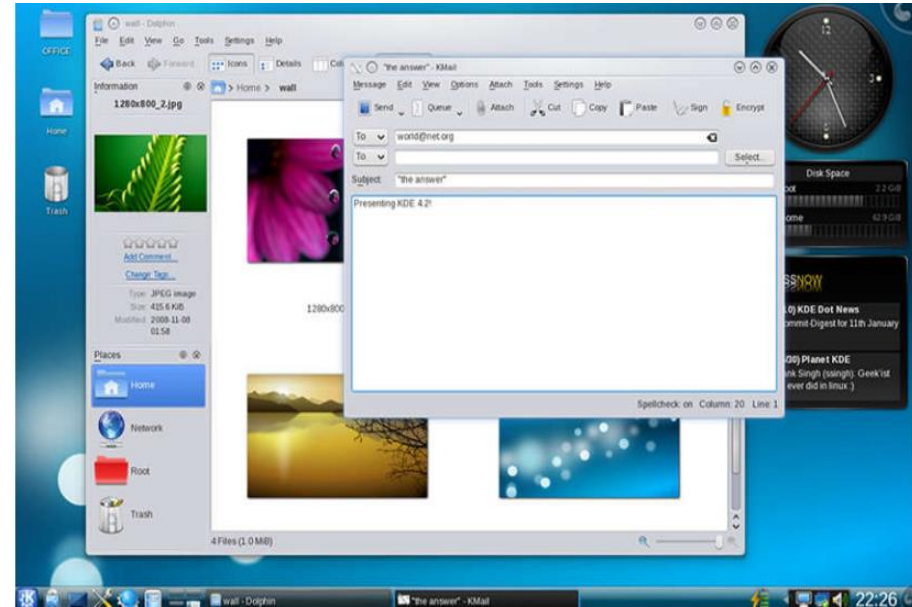
Trabalhando com o Linux GUI

X Window System (Condd.)

Exemplos de gerenciadores de janelas são o Gnome e o KDE.



O Gerenciador de Janelas do
Gnome

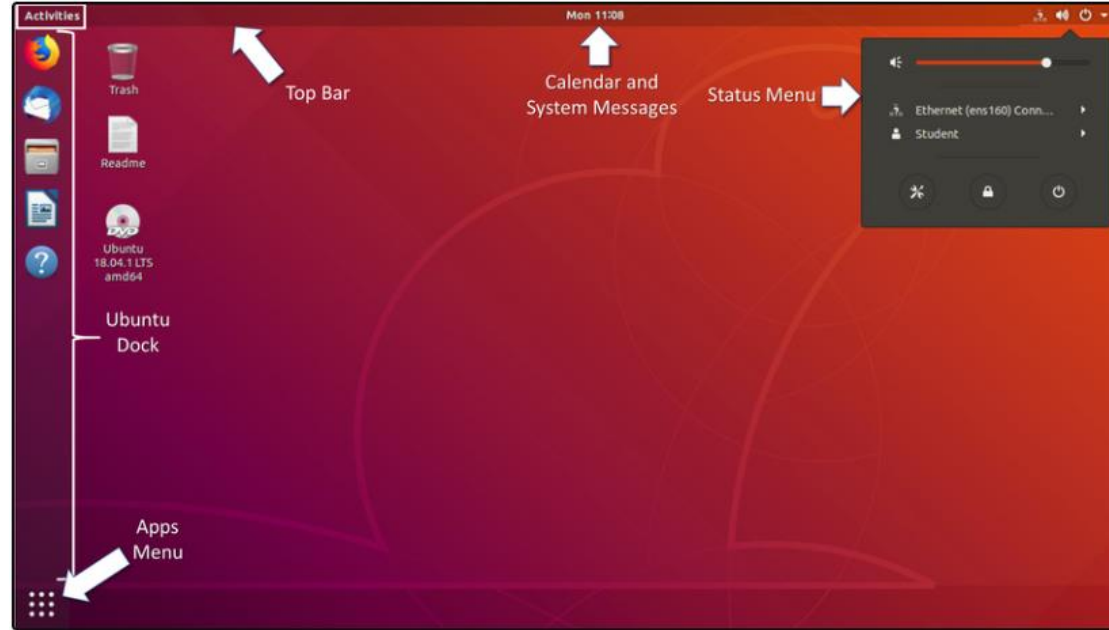


O Gerenciador de Janelas
KDE

Trabalhando com a GUI do Linux

A GUI do Linux

- Embora um sistema operacional não exija uma GUI para funcionar, as GUIs são consideradas mais fáceis de usar do que a CLI. A GUI Linux como um todo pode ser facilmente substituída pelo usuário.
- Ubuntu é uma distribuição Linux muito popular e amigável.
- Ubuntu Linux usa Gnome 3 como sua GUI padrão.
- A figura mostra a localização de alguns dos recursos do Ubuntu Gnome 3 Desktop.



do Linux A GUI do Linux (Cont.)

A tabela a seguir lista os principais componentes da interface do usuário do Unity:

Componente UI	Descrição
Menu Apps	<ul style="list-style-type: none">• O Menu Aplicativos mostra ícones para os aplicativos que estão instalados no sistema.• Um menu com o botão direito do mouse fornece atalhos que permitem iniciar ou configurar os aplicativos.• A caixa de pesquisa do sistema está disponível na Exibição de Atividades.
Dock do Ubuntu	<ul style="list-style-type: none">• Um dock no lado esquerdo da tela que serve como um inicializador de aplicativos e alternador para favoritos de aplicativos.• Clique para iniciar um aplicativo e, quando o aplicativo estiver em execução, clique novamente para alternar entre aplicativos em execução.• Se mais de um aplicativo estiver em execução, o iniciador exibirá todas as instâncias.• Clique com o botão direito do mouse em qualquer aplicativo no iniciador para ver detalhes sobre isso o aplicativo.
Barra superior	<ul style="list-style-type: none">• Esta barra de menus contém um menu para o aplicativo que atualmente tem o foco.• Ele exibe a hora atual e indica se há novas mensagens do sistema.• Ele também fornece acesso à visualização da área de trabalho Atividade e ao Menu Status do sistema.

do Linux A GUI do Linux (Cont.)

Componente UI	Descrição
Calendário e bandeja de mensagens do sistema	<ul style="list-style-type: none">• Clique no dia e na hora para ver o calendário de compromissos completo e as mensagens atuais do sistema.• Acesse o calendário de compromissos a partir daqui para criar novos compromissos.
Atividades	<ul style="list-style-type: none">• Alterne para a exibição de aplicativo para alternar ou fechar aplicativos em execução.• Uma poderosa ferramenta de pesquisa está disponível aqui que irá encontrar aplicativos, arquivos e valores dentro de arquivos.• Permite alternar entre espaços de trabalho.
Menu de Status	<ul style="list-style-type: none">• Permite a configuração do adaptador de rede e de outros dispositivos em execução.• O usuário atual pode fazer logoff ou alterar suas configurações.• Alterações de configuração do sistema podem ser feitas aqui.• A estação de trabalho pode ser bloqueada ou desligada a partir daqui.

4.7 Como trabalhar em um host do Linux

Instalando e executando aplicativos em um host Linux

- Muitos aplicativos de usuário final são programas complexos escritos em linguagens compiladas.
- Para auxiliar no processo de instalação, o Linux inclui programas chamados gerenciadores de pacotes.
- Usando um gerenciador de pacotes para instalar um pacote, todos os arquivos necessários são colocados no local correto do sistema de arquivos.
- Um pacote é o termo usado para se referir a um programa e todos os seus arquivos de suporte.
- A saída do comando mostra a saída de alguns comandos **apt-get** usados nas distribuições Debian.

```
analyst@cuckoo:~$ sudo apt-get update
[sudo] password for analyst:
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [534 kB]
<output omitted>
Fetched 4,613 kB in 4s (1,003 kB/s)
Reading package lists... Done
analyst@cuckoo:~$
analyst@cuckoo:~$ sudo apt-get upgrade
Reading package lists Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
linux-generic-hwe-16.04 linux-headers-generic-hwe-16.04
linux-image-generic-hwe-16.04
The following packages will be upgraded:
firefox firefox-locale-en glib2.0 javascriptcoregtk-4.0 glib2.0-webkit2-4.0 libjavascriptcoregtk-4.0-18
libwebkit2gtk-4.0-37 libwebkit2gtk-4.0-37-gtk2 libxext4 libxextstore3.0 linux-libc-dev logrotate
openssh-client
qemu-block-extra qemur-kvm qemu-system-common qemu-system-x86 qemu-utils
```

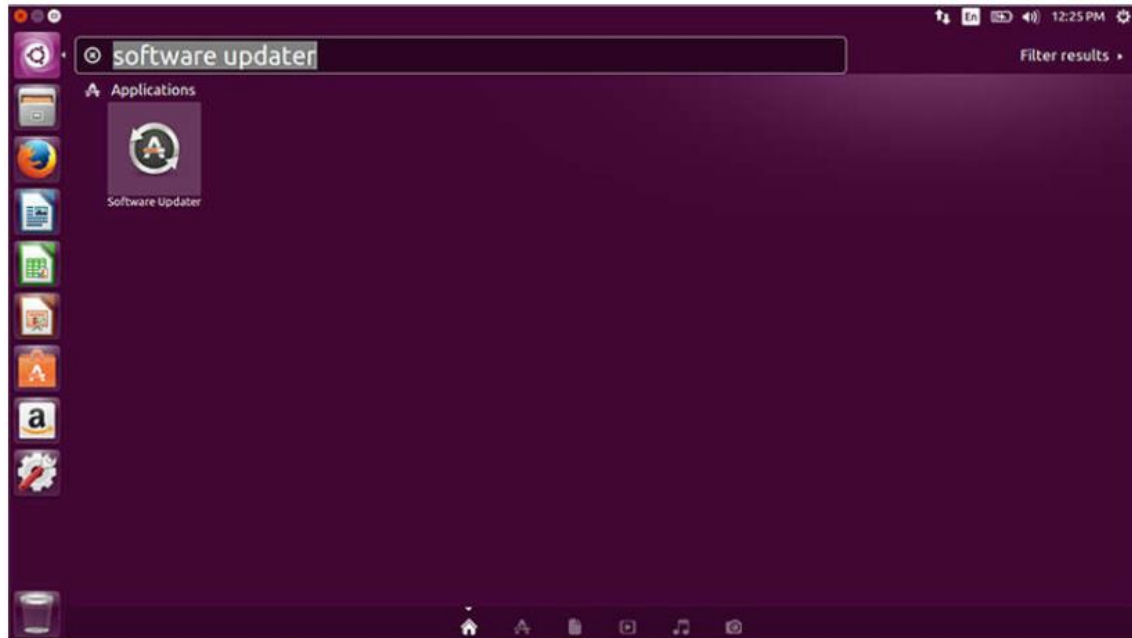
Mantendo o sistema atualizado

- As atualizações do sistema operacional, também conhecidas como patches, são lançadas periodicamente por empresas de sistema operacional para resolver quaisquer vulnerabilidades conhecidas em seus sistemas operacionais.
- Os sistemas operacionais modernos alertarão o usuário quando atualizações estiverem disponíveis para download e instalação, mas o usuário pode verificar as atualizações a qualquer momento.
- A tabela a seguir compara os comandos de distribuição Arch Linux e Debian/Ubuntu Linux para executar operações básicas do sistema de pacotes.

Tarefa	Arch	Debian/Ubuntu
Instalar um pacote pelo nome	pacman -S	apt install
Remover um pacote pelo nome	pacman -Rs	apt remove
Atualize um pacote local	pacman -Syy	apt-get update
Atualizar todos os pacotes atualmente instalados	pacman -Syu	atualização do apt-get

Mantendo o sistema atualizado (Cont.)

- Uma GUI do Linux também pode ser usada para verificar e instalar atualizações manualmente.
- No Ubuntu, por exemplo, para instalar atualizações, clique em **Dash Search Box**, digite **atualizador de software** e clique no ícone **Atualizador de Software**.



Processes e Garfos

- Um processo é uma instância em execução de um programa de computador.
- A bifurcação é um método que o kernel usa para permitir que um processo crie uma cópia de si mesmo.
- Os processos precisam de uma maneira de criar novos processos em sistemas operacionais multitarefa. A operação de fork é a única maneira de fazer isso no Linux.
- Quando um processo chama um fork, o processo chamador torna-se o processo pai e o processo recém-criado torna-se seu filho.
- Após o fork, os processos são, até certo ponto, processos independentes. Eles têm IDs de processo diferentes, mas executam o mesmo código de programa.

Processes e Garfos (Cont.)

A tabela a seguir lista três comandos que são usados para gerenciar processos.

Comando	Descrição
ps	<ul style="list-style-type: none">• Usado para listar os processos em execução no computador no momento em que ele é chamado.• Ele pode ser instruído a exibir processos em execução que pertencem ao usuário atual ou a outros usuários.
superior	<ul style="list-style-type: none">• Usado para listar processos em execução, mas ao contrário do ps, top continua exibindo processos em execução dinamicamente.• Pressione q para sair do topo.
Finaliza	<ul style="list-style-type: none">• Usado para modificar o comportamento de um processo específico.• Dependendo dos parâmetros, kill removerá, reiniciará ou pausará um processo.• Em muitos casos, o usuário executará ps ou top antes de executar kill.• Isso é feito para que o usuário possa aprender o PID de um processo antes de executar kill.

Processes e Garfos (Cont.)

A saída do comando mostra a saída do comando **superior** em um computador Linux.

```
[analyst@secOps ~]$ top
top - 11:29:16 up 0 min, 1 user, load average: 1.09, 0.31, 0.11
Tasks: 119 total, 1 running, 118 sleeping, 0 stopped, 0 zombie
%Cpu(s):  5.4 us,  2.0 sy,  0.0 ni, 87.4 id,  2.7 wa,  1.4 hi,  1.0 si,  0.0 st
MiB Mem :   982.8 total,   67.9 free,   765.8 used,   149.1 buff/cache
MiB Swap:    0.0 total,    0.0 free,    0.0 used.   39.3 avail Mem

   PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
  729 analyst   20   0 2652376 284472 61076 S   2.7   28.3   0:06.75 Web Cont+
  570 analyst   20   0 2691388 215728 62404 S   2.0   21.4   0:06.99 firefox
  357 root       20   0 267972  91960 18468 S   1.3    9.1   0:01.63 Xorg
  461 analyst   20   0 322208  21000 7480 S   1.3    2.1   0:00.67 xfce4-p+
  121 root       20   0      0      0      0 S    0.7    0.0   0:00.43 kswapd0
    1 root       20   0 174376   4196 1688 S    0.3    0.4   0:00.66 systemd
  294 root       20   0 245036  11876  868 S    0.3    1.2   0:00.34 python2+
  539 analyst   20   0 150824    660   0 S    0.3    0.1   0:00.02 VBoxCli+
  800 analyst   20   0 477768  18968 9800 S    0.3    1.9   0:00.30 xfce4-t+
    2 root       20   0      0      0      0 S    0.0    0.0   0:00.00 kthreadd
    3 root       0 -20      0      0      0 I    0.0    0.0   0:00.00 rcu_gp
    4 root       0 -20      0      0      0 I    0.0    0.0   0:00.00 rcu_par+
    5 root       20   0      0      0      0 I    0.0    0.0   0:00.00 kworker+
    6 root       0 -20      0      0      0 I    0.0    0.0   0:00.00 kworker+
    7 root       20   0      0      0      0 I    0.0    0.0   0:00.00 kworker+
    8 root       0 -20      0      0      0 I    0.0    0.0   0:00.00 mm_perc+
    9 root       20   0      0      0      0 S    0.0    0.0   0:00.02 ksoftir+
```

```
[analyst@secOps ~]$
```

malware de host Linux em um host Linux

- O malware do Linux inclui vírus, cavalos de Tróia, worms e outros tipos de malware que podem afetar o sistema operacional.
- Um vetor de ataque Linux comum é seus serviços e processos.
- A saída do comando mostra um invasor usando o comando Telnet para testar a natureza e a versão de um servidor Web (porta 80).
- O invasor descobriu que o servidor está executando o nginx versão 1.12.0. O próximo passo seria pesquisar vulnerabilidades conhecidas no código nginx 1.12.0.

```
analyst@secOps ~]$ telnet 209.165.200.224 80
Trying 209.165.200.224...
Connected to 209.165.200.224.
Escape character is '^]'.
<type anything to force an HTTP error response>
HTTP/1.1 400 Bad Request
Server: nginx/1.12.0
Date: Wed, 17 May 2017 14:27:30 GMT
Content-Type: text/html
Content-Length: 173
Connection: close
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.12.0</center>
</body>
</html >
Connection closed by foreign host.
analyst@secOps ~]$
```

Trabalhando em uma Verificação de Rootkit de Host Linux

- Um rootkit é um tipo de malware projetado para aumentar os privilégios de um usuário não autorizado ou conceder acesso a partes do software que normalmente não devem ser permitidas.
- Um rootkit é destrutivo à medida que muda o código do kernel e seus módulos, alterando as operações mais fundamentais do próprio sistema operacional.
- Os métodos de detecção de rootkit incluem a inicialização do computador a partir de uma mídia confiável.
- A remoção de rootkit pode ser complicada. A reinstalação do sistema operacional é a única solução real para o problema.
- **chkrootkit** é um popular programa baseado em Linux projetado para verificar o computador para rootkits conhecidos.
- A saída do comando mostra a saída do **chkrootkit** em um Ubuntu Linux.

```
analyst@cuckoo:~$ sudo ./chkrootkit
[sudo] password for analyst:
ROOTDIR is '/'
Checking 'amd'... not found
Checking 'basename'... not infected
Checking 'biff'... not found
Checking 'chfn'... not infected
Checking 'chsh'... not infected
Checking 'cron'... not infected
Checking 'crontab'... not infected
Checking 'date'... not infected
Checking 'du'... not infected
Checking 'dirname'... not infected
Checking 'echo'... not infected
Checking 'egrep'... not infected
Checking 'env'... not infected
Checking 'find'... not infected
Checking 'fingerd'... not found
Checking 'gpm'... not found
Checking 'grep'... not infected
Checking 'hdparm'... not infected
Checking 'su'... not infected
Checking 'ifconfig'... not infected
Checking 'inetd'... not tested
Checking 'inetdconf'... not found
```

Piping Comandos

- Embora as ferramentas de linha de comando geralmente sejam projetadas para executar uma tarefa específica e bem definida, muitos comandos podem ser combinados para executar tarefas mais complexas por uma técnica conhecida como tubulação.
- A tubulação consiste em encadear comandos juntos, alimentando a saída de um comando na entrada de outro.
- Os dois comandos, **ls** e **grep**, podem ser canalizado juntos para filtrar a saída de **ls**. Isto é mostrado na saída do comando **ls -l | grep host** e do comando **ls -l | grep file**.

```
[analyst@secOps ~]$ ls -l
total 40
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 April 2 14:44 Downloads
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
-rw-r--r-- 1 analyst analyst 19 May 20 10:53 mytest.com
-rw-r--r-- 1 analyst analyst 228844 May 20 10:54 rkhunter-1.4.6-1-any.pkg.tar.xz
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 257 May 20 10:52 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep host
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep file
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
[analyst@secOps ~]$
```

Trabalhando em uma demonstração de vídeo de host Linux - Aplicações, rootkits e comandos de tubulação

Assista ao vídeo para ver uma demonstração de instalação e atualização de aplicativos, verificação de um rootkit e uso de comandos de tubulação.



4.8 Resumo dos conceitos básicos do Linux

O que eu aprendi neste módulo?

- O Linux é um sistema operacional de código aberto rápido, confiável e pequeno.
- No Linux, o usuário se comunica com o sistema operacional por meio de uma GUI ou uma interface de linha de comando (CLI) ou shell.
- Servidores são computadores que possuem software instalado que lhes permite fornecer serviços a computadores cliente em toda a rede.
- No Linux, os servidores são gerenciados usando arquivos de configuração. Várias configurações podem ser modificadas e salvas em arquivos de configuração.
- O Linux suporta vários sistemas de arquivos diferentes que variam de acordo com velocidade, flexibilidade, segurança, tamanho, estrutura, lógica e muito mais. Alguns dos sistemas de arquivos suportados pelo Linux são ext2, ext3, ext4, NFS e CDFS.
- O sistema X Windows, ou X11, é uma estrutura de software básica que inclui funções para criar, controlar e configurar uma GUI do Windows em uma interface de apontar e clicar.
- Para instalar aplicativos em hosts Linux, programas chamados gerenciadores de pacotes são usados. Os pacotes são aplicativos de software e todos os seus arquivos de suporte.

