Intro To System Administration - McCool Cheat Sheet

by cfmccool via cheatography.com/89679/cs/20414/

Popular Commands

ps - shows the status of running processes, supports more than 80 command-line options on Linux systems.

man - traditional "on-line" documentation

pwd - print working directory

cd - move to another directory

mkdir - to make a directory

rmdir - remove to directory

Useful Keys

Ctrl-U : Delete the line from the cursor to the beginning of the line.

Ctrl-C : Aborts execution.

Ctrl-Z : Suspends execution.

Ctrl-S : Stops the terminal output until you press Ctrl-Q.

Fix Key Commands

stty function key

Function is what you want to do:
erase, kill, intr, susp

Key is the key that you press. Put ⟨ in front of key i.e ⟨C

To generate list of current terminal settings:
stty a

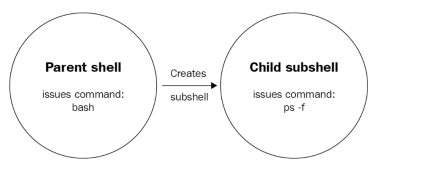
Command to bring shell to a reason and making it operate as expected if it doesn't:
stty sane

Manuel Pages

To find out about a command:
man *command*

Manual pages are divided into different

Diagram of Processes Forked From Shell



More Important Directories

/var/spool
Temporary storage for files being printed, sent by UUCP, and so on.

/usr/lib
Standard libraries, such as libc.a.

/usr/lib/X11
The X Window System distribution. Contains the libraries used by X clients, as well as fonts, sample resources files, and other important parts of the X package.

/usr/include
Standard location of include files used in C programs

/usr/src
Location of sources to programs built on the system.

Even More Important Directories

/usr/local
Programs and datafiles that have been added locally by the system administrator.

/etc/skel
Sample startup files you can place in home directories for new users

/dev
This directory contains the so-called device files, the interface between the filesystem and the hardware

/proc
The interface between the filesystem and the running processes, the CPU, and memory

Boot Process Tasks

Tasks:
Finding, loading, and running bootstrapping code

Finding, loading, and running the OS kernel

Running startup scripts and system daemons

Maintaining process hygiene and managing system state transitions

Shells on Linux

bash - Bourne Again shell. The most commonly used shell on Linux. Command-line editing, history substitution.

csh - Different interface for programming. No command-line editing, history substitution.

ksh - Korn shell. Command-line editing.

sh - Bourne shell. The original shell. No command-line editing.

tcsh - Enhanced C shell. Command-line editing.

zsh - Z shell. The newest of the shells. Command-line editing. Has very powerful completion features.

Remote Logins

ssh -1 accountname systemname

-1 specifies the account on the remote system

Another syntax with identical effects is:
ssh accountname@systemname

To suspend remote login:
~ followed by Ctrl-Z

To Copy Stuff Over SSH

sections depending on their purpose. User commands are in section 1, Unix system calls in section 2, and so on. 1, 5 (file formats), and 8 (system administration commands).

Important Directories

/bin
The most essential Unix commands, such as ls.

/usr/bin
Other commands.

/sbin
Very common commands used by the superuser for system administration.

/usr/sbin
Commands used less often by the superuser for system administration.

/boot
Location where the kernel and other files used during booting are sometimes stored.

/etc
Files used by subsystems such as networking, NFS, and mail.

/var
Administrative files, such as log files, used by various utilities.

/opt
Directory is often used for larger software packages

What the test command can do

Check whether a file exists
Check whether a directory exists
Check whether a variable is not empty
Check whether two variables have the same values
Check whether FILE1 is older than FILE2
Check whether INTEGER1 is greater than INTEGER2

Transport Layer Security

Uses public key cryptography and PKI to secure messages between nodes on a network. TLS runs as a separate layer that wraps TCP connections. Once a client and server have established a TLS connection, the contents of the exchange, including the URL and all headers, are protected by encryption.

To copy files in the SSH suite:
scp

Copies a file from your local system to remote system:
scp filepath accountname@systemname:
DO NOT FORGET COLON

Copies a file from the remote system to your own:
scp accountname@systemname:filepath

To copy a directory:
scp -r accountname@systemname:directoryname relative path.

Elements of Security

Confidentiality - Privacy of data

Integrity - Authenticity of Information

Availability - Must be accessible to authorized to users when they need it

Copying the Current Shell

ps -f
The current shell is copied including the environment variables.

Cheatography

Intro To System Administration - McCool Cheat Sheet

by cfmccool via cheatography.com/89679/cs/20414/

How Security Is Compromised

Social Engineering

Software Vulnerabilities

Distributed Denial-of-Service

Insider Abuse

Network, system, or application configuration errors

To Create A Temp File w/ Random Name

mktemp
This command is used to create a temporary file with a random name, which could be useful is we needed to have a place on disk for some temporary data. With the -d flag to mktemp, we would create a temporary directory with a random name. Because the random name is sufficiently long and we should always have write permissions in /tmp/, we would expect the mktemp command to almost always succeed and thus return an exit status of 0.

Basic Security Measures

Software Updates

Unnecessary Services - Disabling unnecessary services.

Remote Event Logging

Backups - Regular, tested system backups are an essential part of any site security plan. Protect your backups by limiting (and monitoring) access and by encrypting backup files.

Viruses and Worms

More Basic Security Measures

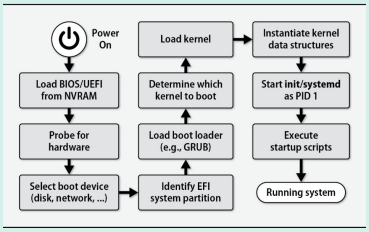
Root Kits - Programs and patches that hide important system information such as process, disk, or network activity.

Packet Filtering - Passes only traffic for services that you specifically want to offer

OpenSSH Essentials

Commands:
ssh : the client
sshd : the server daemon
ssh-keygen : for generating public/private key pairs
ssh-add and ssh-agent : tools for managing authentication keys
ssh-keyscan : for retrieving public keys from servers
sftp-server : the server process for file transfer over SFTP
sftp and scp : file transfer client utilities

Linux & Unix Boot Process



Viewing Files

xemacs - editor

cat - used to scan a file, rather than edit it.

vi - text editor

more - prints a screenful at a time and waits for you to press the spacebar before printing more. Can search for a string in the file: press the slash key (/), type the string, and press Return.

less - variation of more

nano - simple and low-impact starter editor

Linux login

Password:
- means you are at root level
$ - means you are at the user level
To set a password use the "passwd" command.

Filename Expansion

Startup Files

.bashrc - Startup file

.bash_profile - Runs only when you log in

.zshrc - .bashrc but for zsh

.zprofile - .bash_profile, but for zsh

.cshrc - For the C shell or tcsh

.login - .bash_profile for the C shell or tcsh.

.emacs - For Emacs editor

.exrc - For vi editor

.newsrc - For news readers

.xinitrc - For X Window System

.kde/share/config - Directory with configuration files for the K Desktop Environment

.gnome - Directory with configuration files for the GNOME

Cryptographic Message Properties

Confidentiality - messages are impossible to read for everyone except the intended recipients.

Integrity - it is impossible to modify the contents without detection.

Non repudiation - the authenticity of the message can be validated.

Symmetric Key Cryptography

Alice and Bob share a secret key that they use to encrypt and decrypt messages. They must find a way to exchange the shared secret privately. Once they both know the key, they can reuse it as long as they wish. Symmetric keys are relatively efficient in terms of CPU usage and the size of the encrypted payloads.
The need to distribute the shared key in advance is a serious impediment to many

from that system.

Passwords and Multifactor Authentication

Vigilance

Application penetration testing

Security Power Tools

Nmap - Network Port Scanner

Nessus - Next generation network scanner

Metasploit - Penetration testing software

Lynis - On-box security auditing

John the Ripper - Finder of insecure passwords

Bro - The programmable network intrusion detection system

Snort - the popular network intrusion detection system

OSSEC - Host-based intrusion detection

Fail2Ban - Brute-Force attack response system

ls - lists files.

ls text?text - lists files containing digits in a position if the difference in file names is just a digit.

ls text[13]text - lists files with the digits 1 and 3 in that position.

ls text[1-3]text - lists all files from 1-3 inclusive in that position. Also works with alphabetical characters [a-zA-Z]

ls text*text - lists all files that match the structure including a numbers and full words between the text.

use cases.

Public Key Cryptography

Alice generates a pair of keys. The private key remains a secret, but the public key can be widely known. Bob similarly generates a key pair and publishes his public key. When Alice wants to send Bob a message, she encrypts it with Bob's public key. Bob, who holds the private key, is the only one who can decrypt the message.
Alice can also sign the message with her private key. Bob can use Alice's signature and her public key to validate its authenticity.
Asymmetric ciphers.

Public Key Infrastructure

A network of entities who trust each other to varying degrees. By following indirect chains of trust outside your personal network, you can establish that a public key is trustworthy with a reasonable degree of confidence.
The Public Key Infrastructure, used to implement TLS on the web, addresses this problem by trusting a third party known as a Certificate Authority (CA) to vouch for public keys.
The CA signs certificates for Alice and Bob's public keys with its own private key.

Cryptographic Hash Functions

Properties:
Entanglement: every bit of the hash value depends on every bit of the input data. On average, changing one bit of input should cause 50% of the hash bits to change.

Pseudo-randomness: hash values should be indistinguishable from random data.

Non reversibility: given a hash value, it should be infeasible to discover another input that generates the same hash value.

NFS (Network File System)

The NFS protocol has been refined to increase platform independence, to improve performance over wide area networks such as the Internet, and to add strong, modular security features.

NFS Drawbacks

- NFS has no built-in provisions for synchronizing with backup servers.
- The sudden disappearance of an NFS server from the network can result in clients holding stale file handles that can be cleaned up only with a reboot.
- Strong security is possible but is overly complex.

Common Security Flavors for NFS Protocol

AUTH_NONE - no authentication
AUTH_SYS - UNIX-style user and group access control
RPCSEC_GSS - a stronger flavor that enables flexible security schemes