

Activity: Get help in the command line

Activity overview

As a security analyst, you won't have all the answers all the time, but you can learn where to find them. One of the great things about Linux is that you can get help right through the command line.

In this lab activity, you'll use the `man` and `whatis` commands to get information on other commands and how they work. You'll also use the `apropos` command to search the manual page for a command with a specified string.

When working as a security analyst, you'll likely find it useful to know how to discover which command to use or information about what commands do.

With that in mind, let's explore your scenario.

Scenario

In this scenario, you have to find more information about commands that you need to use. You also need to discover which command to use to perform a certain task.

Here's how you'll do this task: **First**, you'll explore a few commands you can use in the shell to learn more about other commands. **Next**, you'll find an option you need to add to a command. **Third**, you'll use a command to get a brief description of commands so you can identify their differences. **Finally**, you'll identify the command you need to perform a task.

It's time to get ready to explore some of the Linux help resources!

Task 1. Learn more about commands

In this task, you need to explore a few commands you can use in the shell to learn more about the functionality of other commands.

First, imagine you can't quite remember what the `cat` command does and want a quick reminder.

1. Run the `whatis` command to get a short description of `cat`.

```
analyst@37394dfa1495:~$ whatis cat
cat (1)             - concatenate files and print on the standard output
analyst@37394dfa1495:~$ sudo mandb
Purging old database entries in /usr/share/man...
Processing manual pages under /usr/share/man...
Purging old database entries in /usr/share/man/pl...
Processing manual pages under /usr/share/man/pl...
```

Next, imagine that you want more details about `cat` and all of its options.

2. Use the `man` command to get more details about `cat`.

The man command returns a general description of cat and information about each of its options:

```
CAT(1) User Commands
NAME
    cat - concatenate files and print on the standard output
SYNOPSIS
    cat [OPTION]... [FILE]...
DESCRIPTION
    Concatenate FILE(s) to standard output.

    With no FILE, or when FILE is -, read standard input.

    -A, --show-all
        equivalent to -vET

    -b, --number-nonblank
        number nonempty output lines, overrides -n

    -e
        equivalent to -vE

    -E, --show-ends
        display $ at end of each line

    -n, --number
        number all output lines

    -s, --squeeze-blank
        suppress repeated empty output lines

    -t
        equivalent to -vT

    -T, --show-tabs
        display TAB characters as ^I

    -u
        (ignored)

    -v, --show-nonprinting
        use ^ and M- notation, except for LFD and TAB

    --help display this help and exit
--More--
```

Now, imagine you've remembered there's a command that prints just the first part of a file, but you can't remember the exact command. The apropos command is useful in these instances. You can use keywords with apropos to find a command.

4. Use apropos to find a command that returns the first part of a file:

```
analyst@37394dfa1495:~$ apropos -a first part file
head (1) - output the first part of files
analyst@37394dfa1495:~$
```

Task 2. Explore the useradd command

In this task, imagine that you want to set the expiration date for a temporary user account. You know that you need to use the useradd command for this, but you're not quite sure how to complete the task. You realize it might involve adding an option to the command.

1. Use the most appropriate Linux command to get help on the useradd command and learn more about all of its options.

```
--help display this help and exit
analyst@37394dfa1495:~$
analyst@37394dfa1495:~$ apropos -a first part file
head (1)          - output the first part of files
analyst@37394dfa1495:~$ man useradd
USERADD(8)          System Management Commands          USERADD(8)

NAME
    useradd - create a new user or update default new user information

SYNOPSIS
    useradd [options] LOGIN

    useradd -D

    useradd -D [options]

DESCRIPTION
    useradd is a low level utility for adding users. On Debian, administrators should usually use
    adduser(8) instead.

    When invoked without the -D option, the useradd command creates a new user account using the
    values specified on the command line plus the default values from the system. Depending on
    command line options, the useradd command will update system files and may also create the
    new user's home directory and copy initial files.

    By default, a group will also be created for the new user (see -g, -N, -U, and
    USERGROUPS_ENAB).

OPTIONS
    The options which apply to the useradd command are:

    --badname
        Allow names that do not conform to standards.

    -b, --base-dir BASE_DIR
        The default base directory for the system if -d HOME_DIR is not specified. BASE_DIR is
        concatenated with the account name to define the home directory. If the -m option is not
        used, BASE_DIR must exist.

    If this option is not specified, useradd will use the base directory specified by the
    HOME variable in /etc/default/useradd, or /home by default.
```

Task 3. Explore the rm and rmdir commands

In this task, you need to determine the difference between the rm and rmdir commands.

Imagine that you've used these commands before, but you can't remember how they're different.

- Use the most appropriate Linux command to quickly remind yourself what each command does.

```
as the field for the user's full name.
analyst@37394dfa1495:~$ whatis rm
rm (1)          - remove files or directories
analyst@37394dfa1495:~$ whatis rmdir
rmdir (1)       - remove empty directories
rmdir (2)       - delete a directory
analyst@37394dfa1495:~$
```

Task 4. Determine which command to use

In this task, imagine that you need to create a new group but you can't remember what command to use. You need to identify a command that will do this by searching for it through keywords. In this case, use the keywords create new group.

- Use the most appropriate Linux command with these keywords to identify what command to use.

```
analyst@37394dfa1495:~$ apropos "create new group"
create new group: nothing appropriate.
analyst@37394dfa1495:~$ apropos group
addgroup (8)      - add a user or group to the system
adduser (8)       - add a user or group to the system
adduser.conf (5)  - configuration file for adduser(8) and addgroup(8) .
cgroup_namespaces (7) - overview of Linux cgroup namespaces
cgroups (7)       - Linux control groups
chgpaswd (8)      - update group passwords in batch mode
chgrp (1)         - change group ownership
chown (1)         - change file owner and group
cpgr (8)          - copy with locking the given file to the password or group file
cppw (8)          - copy with locking the given file to the password or group file
delgroup (8)      - remove a user or group from the system
deluser (8)       - remove a user or group from the system
deluser.conf (5)  - configuration file for deluser(8) and delgroup(8) .
endgrent (3)      - get group file entry
endnetgrent (3)   - handle network group entries
exit_group (2)    - exit all threads in a process
fanotify_init (2)  - create and initialize fanotify group
fgetgrent (3)     - get group file entry
fgetgrent_r (3)   - get group file entry reentrantly
getegid (2)       - get group identity
getegid32 (2)     - get group identity
getgid (2)        - get group identity
getgid32 (2)      - get group identity
getgrent (3)      - get group file entry
getgrent_r (3)    - get group file entry reentrantly
getgrgid (3)      - get group file entry
getgrgid_r (3)    - get group file entry
getgrnam (3)      - get group file entry
getgrnam_r (3)    - get group file entry
getgrouplist (3)  - get list of groups to which a user belongs
getgroups (2)     - get/set list of supplementary group IDs
getgroups32 (2)   - get/set list of supplementary group IDs
getnetgrent (3)   - handle network group entries
getnetgrent_r (3) - handle network group entries
getpgid (2)       - set/get process group
getpgrp (2)       - set/get process group
getresgid (2)     - get real, effective and saved user/group IDs

systemd-sysusers (8) - Allocate system users and groups
systemd-sysusers.service (8) - Allocate system users and groups
sysusers.d (5)      - Declarative allocation of system users and groups
tcgetpgrp (3)       - get and set terminal foreground process group
tcsetpgrp (3)       - get and set terminal foreground process group
update-passwd (8)    - safely update /etc/passwd, /etc/shadow and /etc/group
vigr (8)            - edit the password, group, shadow-password or shadow-group file
vipw (8)            - edit the password, group, shadow password or shadow group file
analyst@37394dfa1495:~$ apropos -a "create new group"
create new group: nothing appropriate.
analyst@37394dfa1495:~$
```

Lab Summary: Get Help in the Command Line

In this lab I practiced using Linux help tools to quickly learn about commands and their options. I used `whatis` and `man` to get short and detailed descriptions of commands like `cat`. I used `apropos` with keywords to find commands such as `head` for displaying the first

part of a file. I explored the `useradd` command with `man` to identify the `-e` option for setting an account expiration date. I also compared `rm` and `rmdir` with `whatis` to understand their differences. Finally, I used `apropos` to confirm that the correct command to create a new group is `groupadd`.