Linux Tools

- Linux DD - Writing an iso file to an usb
- VIM
- SSH - Creating a keygen to automatically logon to remote servers
- Linux I/O Redirection
- linux files
- Samba
- SCP
- nmap

Linux DD - Writing an iso file to an usb

identify USB
─$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 465.8G 0 disk
├─sda1 8:1 0 512M 0 part /boot/efi
├─sda2 8:2 0 464.3G 0 part /
└─sda3 8:3 0 976M 0 part [SWAP]
sdb 8:16 1 14.6G 0 disk
└─sdb1 8:17 1 14.6G 0 part
sdc 8:32 0 1.8T 0 disk
└─sdc1 8:33 0 1.8T 0 part
nvme0n1 259:0 0 953.9G 0 disk
├─nvme0n1p1 259:1 0 16M 0 part
└─nvme0n1p2 259:2 0 953.9G 0 part

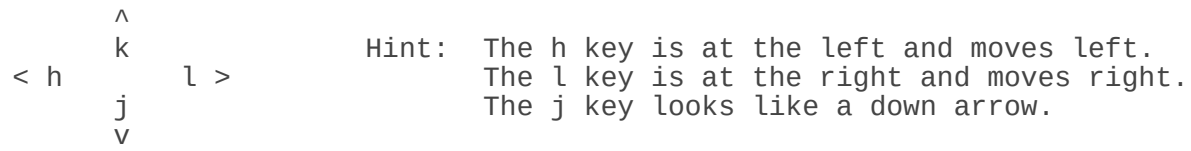
our USB is /dev/sdb

dd bs=4M if=/home/csr/Downloads/VMware-VMvisor-Installer-7.0U3g-20328353.x86_64.iso of=/dev/sdb status=progress oflag=sync

398458880 bytes (398 MB, 380 MiB) copied, 73 s, 5.5 MB/s
95+1 records in
95+1 records out
401446912 bytes (401 MB, 383 MiB) copied, 73.36 s, 5.5 MB/s

finished

VIM



Exiting VIM

to Exit VIM without saving press <ESC> then :q! <Enter>

Useful commands in Normal mode (press <ESC>)

i	Insert mode
x	Delete the character under the cursor
A	To append text
wq	To save a file and exit
ESC	Will place you in normal mode or will cancel an unwanted and partially completed command
dw	To delete until the start of the next word, Exluding its first character
d$	To delete to the end of the line (depends on where the cursor is at) Including the last character
de	To the end of the current word Including the last character.
2w	To move two words forward (you can use any combination, 3w will move you 3 words forward.
3e	To move the cursor to the end of the third word forward (you can use any combination 2e will move you 2 words forward.
0	Zero - to move to the start of the line
u	to undo the last command
U	to fix a whole line

CTRL-R	to redo the commands

Operations and Motions

Multiple combinations can be achieved

d2w will begin the next 2 words beginning at the cursor, d4w will delete the next 4 words.

in the example below we will place our cursor at *A* (first capital A) and type d2w

---> this ABC DE line FGHI JK LMN OP of words is Q RS TUV cleaned up.

after typing d2w cursor at A

---> this line FGHI JK LMN OP of words is Q RS TUV cleaned up.

now place cursor at *F* and type d4w

---> this line of words is Q RS TUV cleaned up.

now with our cursor at *of* type 3w to move 3 words forwward with our cursor at Q type d3w

---> this line of words is cleaned up.

/ to search after you hit enter press e to move/search to the next line

G G to go to the beginning of the file

Shift G to go to the end of the file

DD to delete a whole line you can also use 2dd to delete 2 lines \

Shift Z Z to exit VIM (this saves changes)

Shift Z Q to exit vim without saving

vim Command	Explanation
Esc	Switches from input mode to command mode. Press this key before typing any command.
i, **a**	Switches from command mode to input mode at (**i**) or after (**a**) the current cursor position.

vim Command	Explanation
o	Opens a new line below the current cursor position and goes to input mode.
:wq	Writes the current file and quits.
:q!	Quits the file without applying any changes. The **!** forces the command to do its work. Add the **!** only if you really know what you are doing.
:w filename	Writes the current file with a new filename.
dd	Deletes the current line and places the contents of the deleted line into memory.
yy	Copies the current line.
p	Pastes the contents that have been cut or copied into memory.
v	Enters visual mode, which allows you to select a block of text using the arrow keys. Use **d** to cut the selection or **y** to copy it.
u	Undoes the last command. Repeat as often as necessary.
Ctrl-r	Redoes the last undo. (Cannot be repeated more than once.)
gg	Goes to the first line in the document.
G	Goes to the last line in the document.
/text	Searches for *text* from the current cursor position forward.
?text	Searches for *text* from the current cursor position backward.
^	Goes to the first position in the current line.
$	Goes to the last position in the current line.
!ls	Adds the output of **ls** (or any other command) in the current file.
:%s/old/new/g	Replaces all occurrences of *old* with *new*.

SSH - Creating a keygen to automatically logon to remote servers

```
csr@MainPC:~/Downloads$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/csr/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/csr/.ssh/id_rsa
Your public key has been saved in /home/csr/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:LAkXcDEfDYkzGq/aWJoL0ViHPvwsbxg9NOfeujAgyMg csr@MainPC
The key's randomart image is:
+---[RSA 3072]----+
|    ..=oo+       |
|   ...++...      |
|  o o+.o.        |
|=* .+ooo         |
|*E*o =o S        |
| o.== ..         |
|. .X=o .         |
| .*ooo. .        |
|  .o. oo         |
+----[SHA256]-----+
csr@MainPC:~/Downloads$ ssh-key
ssh-keygen   ssh-keyscan
csr@MainPC:~/Downloads$ ssh-key
ssh-keygen   ssh-keyscan
csr@MainPC:~/Downloads$ ssh-copy-id csr@192.168.10.218
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/csr/.ssh/id_rsa.pub"
```

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
csr@192.168.10.218's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'csr@192.168.10.218'"
and check to make sure that only the key(s) you wanted were added.

csr@MainPC:~/Downloads$ ssh 192.168.10.218
Web console: https://rhel-lab1.htf.com.mx:9090/ or https://192.168.10.218:9090/

Last login: Tue Apr 9 16:00:47 2024 from 192.168.10.209
[csr@rhel-lab1 ~]$

Linux I/O Redirection

Standard Input, Output, and Error Overview

Name	Default Destination	Use in Redirection	File Descriptor Number
STDIN	Computer keyboard	< (same as 0<)	0
STDOUT	Computer monitor	> (same as 1>)	1
STDERR	Computer monitor	2>	2

Common Bash Redirectors

Redirector	Explanation
> (same as 1>)	Redirects STDOUT. If redirection is to a file, the current contents of that file are overwritten.
>> (same as 1>>)	Redirects STDOUT in append mode. If output is written to a file, the output is appended to that file.
2>	Redirects STDERR.
2>&1	Redirects STDERR to the same destination as STDOUT. Notice that this has to be used in combination with normal output redirection, as in **ls whuhiu > errout 2>&1**.
< (same as 0<)	Redirects STDIN.

Exercise 2-2 Using I/O Redirection and Pipes

1. Open a shell as user **student** and type **cd** without any arguments. This ensures that the home directory of this user is the current directory while working on this exercise. Type **pwd** to verify this.
2. Type **ls**. You'll see the **ls** command output onscreen.

3. Type **ls > /dev/null**. This redirects STDOUT to the null device, with the result that you will not see it.
4. Type **ls ilwehgi > /dev/null**. This command shows a “no such file or directory” message onscreen. You see the message because it is not STDOUT, but rather an error message that is written to STDERR.
5. Type **ls ilwehgi 2> /dev/null**. Now you will no longer see the error message.
6. Type **ls ilwehgi /etc 2> /dev/null**. This shows the contents of the /etc folder while hiding the error message.
7. Type **ls ilwehgi /etc 2> /dev/null > output**. In this command, you still write the error message to /dev/null while sending STDOUT to a file with the name output that will be created in your home directory.
8. Type **cat output** to show the contents of this file.
9. Type **echo hello > output**. This overwrites the contents of the output file. Verify this by using **cat output** again.
10. Type **ls >> output**. This appends the result of the **ls** command to the output file. Type **cat output** to verify.
11. Type **ls -R /**. This shows a long list of files and folders scrolling over your computer monitor. (You might want to press Ctrl-C to stop [or wait some time]).
12. Type **ls -R /. | less**. This shows the same result, but in the **less** pager, where you can scroll up and down using the arrow keys on your keyboard.
13. Type **q** to close **less**. This will also end the **ls** program.
14. Type **ls > /dev/tty1**. This gives an error message because you are executing the command as an ordinary user, and ordinary users cannot address device files directly (unless you were logged in to tty1). Only the user root has permission to write to device files directly.

Lab 2.1

1. Modify your shell environment so that on every subshell that is started, a variable is set. The name of the variable should be **COLOR**, and the value should be set to **red**. Verify that it is working.
2. Use the appropriate tools to find the command that you can use to change a user password. Do you need root permissions to use this command?
3. From your home directory, type the command **ls -al wergihl *** and ensure that errors as well as regular output are redirected to a file with the name /tmp/lsoutput.

1

```
[csr@rhel-lab1 ~]$ cat .bashrc
# .bashrc
```

```
# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]
then
    PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
if [ -d ~/.bashrc.d ]; then
        for rc in ~/.bashrc.d/*; do
                if [ -f "$rc" ]; then
                        . "$rc"
                fi
        done
fi

unset rc
COLOR=red
[csr@rhel-lab1 ~]$ echo $COLOR
red
[csr@rhel-lab1 ~]$
```

2 yes password needs root access

```
[csr@rhel-lab1 ~]$ sudo passwd student
Changing password for user student.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[csr@rhel-lab1 ~]$
```

3

```
[csr@rhel-lab1 tmp]$ sudo ls -la wergihi * > /tmp/lsoutput 2>&1
[csr@rhel-lab1 tmp]$ ls
hosts                                                systemd-private-fbeff084055846399d65d269a3a13921-
kdump.service-Hve1CF
lsoutput                                              systemd-private-fbeff084055846399d65d269a3a13921-
ModemManager.service-tvX68Q
systemd-private-fbeff084055846399d65d269a3a13921-chronyd.service-VtzKw9      systemd-private-
fbeff084055846399d65d269a3a13921-systemd-logind.service-lMEyTH
systemd-private-fbeff084055846399d65d269a3a13921-dbus-broker.service-mPKNBR
[csr@rhel-lab1 tmp]$ cat lsoutput
ls: cannot access 'wergihi': No such file or directory
-rw-r--r--. 1 csr  csr  209 Apr  9 17:15 hosts

systemd-private-fbeff084055846399d65d269a3a13921-chronyd.service-VtzKw9:
total 4
drwx------.  3 root root   17 Apr 11 17:23 .
drwxrwxrwt. 11 root root 4096 Apr 11 19:11 ..
drwxrwxrwt.  2 root root    6 Apr 11 17:23 tmp

systemd-private-fbeff084055846399d65d269a3a13921-dbus-broker.service-mPKNBR:
total 4
drwx------.  3 root root   17 Apr 11 17:23 .
drwxrwxrwt. 11 root root 4096 Apr 11 19:11 ..
drwxrwxrwt.  2 root root    6 Apr 11 17:23 tmp

systemd-private-fbeff084055846399d65d269a3a13921-kdump.service-Hve1CF:
total 4
drwx------.  3 root root   17 Apr 11 17:23 .
drwxrwxrwt. 11 root root 4096 Apr 11 19:11 ..
drwxrwxrwt.  2 root root    6 Apr 11 17:24 tmp

systemd-private-fbeff084055846399d65d269a3a13921-ModemManager.service-tvX68Q:
total 4
drwx------.  3 root root   17 Apr 11 17:23 .
```

```
drwxrwxrwt. 11 root root 4096 Apr 11 19:11 ..
drwxrwxrwt.  2 root root    6 Apr 11 17:23 tmp

systemd-private-fbeff084055846399d65d269a3a13921-systemd-logind.service-lMEyTH:
total 4
drwx------.  3 root root   17 Apr 11 17:23 .
drwxrwxrwt. 11 root root 4096 Apr 11 19:11 ..
drwxrwxrwt.  2 root root    6 Apr 11 17:23 tmp
```

linux files

Essential Tools for Managing Text File Contents
Command
Explanation
less
Opens the text file in a pager, which allows for easy reading
cat
Dumps the contents of the text file on the screen
head
Shows the top of the text file
tail
Shows the bottom of the text file
cut
Used to filter specific columns or characters from a text file
sort
Sorts the contents of a text file
wc
Counts the number of lines, words, and characters in a text file

Apart from their use on a text file, these commands

Samba

Mount a persistent drive on samba, here we're using fedora, same apply to other distros using different package manager.

Query system make sure cifs utils and samba client are installed, if not run the install command for samba packages and cifs utils

```
sudo dnf install samba-client samba-common cifs-utils
```

```
csr@MainPC:/mnt$ sudo dnf list installed | grep -E 'cif*|samb'
cifs-utils.x86_64                          7.0-2.fc39                          @anaconda
cifs-utils-info.x86_64                     7.0-2.fc39                          @anaconda
cirrus-audio-firmware.noarch               20240312-1.fc39                     @System
crypto-policies.noarch                     20231204-1.git1e3a2e4.fc39          @fedora-
updates
crypto-policies-scripts.noarch             20231204-1.git1e3a2e4.fc39          @fedora-
updates
geolite2-city.noarch                       20191217-10.fc39                    @anaconda
libpciaccess.i686                          0.16-9.fc39                         @anaconda
libpciaccess.x86_64                        0.16-9.fc39                         @anaconda
mpdecimal.i686                             2.5.1-7.fc39                        @System
mpdecimal.x86_64                           2.5.1-7.fc39                        @anaconda
pciutils.x86_64                            3.11.1-1.fc39                       @System
pciutils-libs.i686                         3.11.1-1.fc39                       @updates
pciutils-libs.x86_64                       3.11.1-1.fc39                       @System
pcsc-lite-ccid.x86_64                      1.5.5-1.fc39                        @System
perl-Specio.noarch                         0.48-4.fc39                         @System
qemu-device-display-virtio-gpu-pci.x86_64          2:8.1.3-4.fc39
@updates
qemu-device-display-virtio-gpu-pci-gl.x86_64       2:8.1.3-4.fc39
@updates
samba-client.x86_64                        2:4.19.5-1.fc39                     @System
```

```
samba-client-libs.i686                  2:4.19.5-1.fc39                 @System
samba-client-libs.x86_64                2:4.19.5-1.fc39                 @System
samba-common.noarch                     2:4.19.5-1.fc39                 @System
samba-common-libs.x86_64                2:4.19.5-1.fc39                 @System
samba-common-tools.x86_64               2:4.19.5-1.fc39                 @System
samba-dcerpc.x86_64                     2:4.19.5-1.fc39                 @System
samba-ldb-ldap-modules.x86_64           2:4.19.5-1.fc39                 @System
samba-libs.x86_64                       2:4.19.5-1.fc39                 @System
samba-winbind.x86_64                    2:4.19.5-1.fc39                 @System
samba-winbind-clients.x86_64            2:4.19.5-1.fc39                 @System
samba-winbind-modules.x86_64            2:4.19.5-1.fc39                 @System
```

Create a credentials file to hide config from fstab config

```
sudo vim ~/.cred



# Enter credentials for SMB share
username=youruser
password=yourpassword

~

~

~

~

~

~

~
```

Set permisions to file

```
chmod 600 ~/.cred
```

edit /etc/fstab to add our smb drive

//192.168.3.100/zfs /mnt/zfs cifs credentials=/home/csr/.cred,_netdev,defaults 0 0 (optional add file_mode and dir_mode if remote server does not have cifs installed this will provide directory and file permissions if needed)

```
csr@MainPC:/mnt$ cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a device; this may
# be used with UUID= as a more robust way to name devices that works even if
# disks are added and removed. See fstab(5).
#
# <file system>             <mount point>  <type>  <options>  <dump>  <pass>
UUID=AA4E-9603                          /boot/efi      vfat    defaults,noatime 0 2
UUID=c67309b3-bb04-45fa-8cc6-a26d41301ba5 /boot          ext4    defaults,noatime 0 2
UUID=3822a8bd-6ffb-4834-8e9d-f753a4de704e /              btrfs   subvol=/@,compress=zstd:1,x-systemd.device-
timeout=0 0 0
UUID=3822a8bd-6ffb-4834-8e9d-f753a4de704e /home          btrfs   subvol=/@home,compress=zstd:1,x-
systemd.device-timeout=0 0 0
UUID=7062c1a3-df69-4877-b165-c3c9308afd8a swap           swap    defaults   0 0
tmpfs                                   /tmp           tmpfs   defaults,noatime,mode=1777 0

//192.168.3.100/zfs /mnt/zfs cifs credentials=/home/csr/.cred,_netdev,defaults,file_mode=0666,dir_mode=0777
0 0
```

run systemctl daemon-reload then sudo mount -a

```
csr@MainPC:/mnt$ mount -a
This program is not installed setuid root -  "user" CIFS mounts not supported.
mount: (hint) your fstab has been modified, but systemd still uses
       the old version; use 'systemctl daemon-reload' to reload.
csr@MainPC:/mnt$ systemctl daemon-reload
csr@MainPC:/mnt$ mount -a
This program is not installed setuid root -  "user" CIFS mounts not supported.
csr@MainPC:/mnt$ sudo mount -a
csr@MainPC:/mnt$ ls
zfs
csr@MainPC:/mnt$
```

to umount and mount to modify options

```
12:05:20 csr@MainPC ~ → sudo umount -t cifs /mnt/zfs/
12:06:44 csr@MainPC ~ → sudo mount -a
mount: (hint) your fstab has been modified, but systemd still uses
       the old version; use 'systemctl daemon-reload' to reload.
12:06:52 csr@MainPC ~ → systemctl daemon-reload
12:07:04 csr@MainPC ~ →
```

SCP

The syntax for `scp` is:

If you are on the computer from which you want to send file to a remote computer:

```
scp /file/to/send username@remote:/where/to/put
```

Here the `remote` can be a FQDN or an IP address.

On the other hand if you are on the computer wanting to receive file from a remote computer:

```
scp username@remote:/file/to/send /where/to/put
```

`scp` can also send files between two remote hosts:

```
scp username@remote_1:/file/to/send username@remote_2:/where/to/put
```

So the basic syntax is:

```
scp username@source:/location/to/file username@destination:/where/to/put
```

nmap

This uses the `nmap` tool to perform a detailed TCP port scan on the IP range `192.168.0.0/24`.

```
sudo nmap -sS -p- -PE -PP -PS80,443 -PA3389 -PU40125 -A -T4 -oA tcpscan-%D 192.168.0.0/24
```

- `sudo`: Runs the command with administrative privileges.
- `nmap`: The command-line tool used for network exploration and security auditing.
- `-sS`: Performs a TCP SYN scan, which is the default scan type for privileged users.
- `-p-`: Scans all 65,535 TCP ports.
- `-PE`: Sends ICMP echo requests (ping) to discover live hosts.
- `-PP`: Sends ICMP timestamp requests to discover live hosts.
- `-PS80,443`: Sends TCP SYN packets to ports 80 and 443 (default web server) to discover open ports.
- `-PA3389`: Sends TCP ACK packets to port 3389 (default RDP) to discover open ports.
- `-PU40125`: Sends UDP packets to port 40125 (unlikely to be in use) to discover open ports (some services such as the `chargen` protocol respond to empty UDP packets).
- `-A`: Enables aggressive scanning options, including OS detection, version detection, script scanning, and traceroute.
- `-T4`: Sets the timing template to "Aggressive" to speed up the scan (otherwise it can take quite a while, even on a /24 network).
- `-oA tcpscan-%D`: Specifies the output file name format. `%D` is a placeholder for the current date and time.
- `192.168.0.0/24`: Specifies the IP range to scan, in this case, all IP addresses from `192.168.0.0` to `192.168.0.255`.

For a simpler verbose scan,

```
sudo nmap -v -A -sS -p- -O target
```

- `sudo`: Runs the command with administrative privileges.
- `nmap`: The command-line tool used for network exploration and security auditing.
- `-v`: Enables **verbose output**, providing more detailed information during the scan.
- `-A`: Enables **aggressive scanning** options, including OS detection, version detection, script scanning, and traceroute.
- `-sS`: Performs a **TCP SYN** scan, which is the default scan type for privileged users.
- `-p-`: Scans **all 65,535 TCP ports**.
- `-O`: Enables **OS detection**, which attempts to determine the operating system running on the target.
- `target`: Specifies the target IP address, DNS name, or CIDR range to scan.