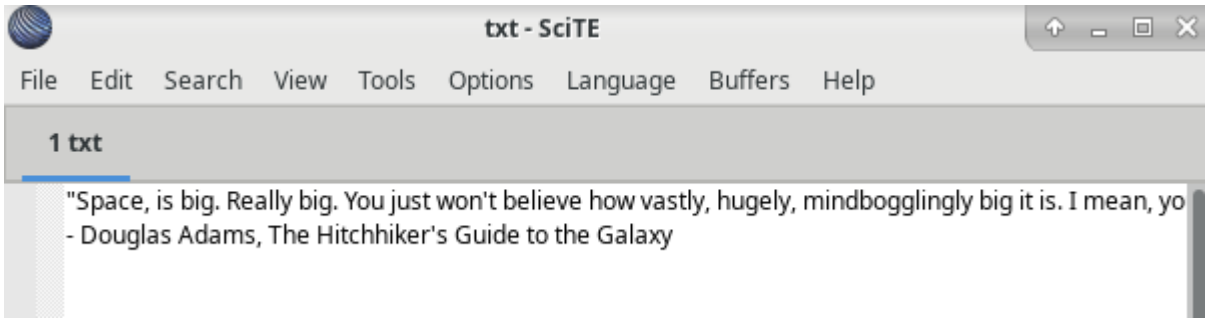
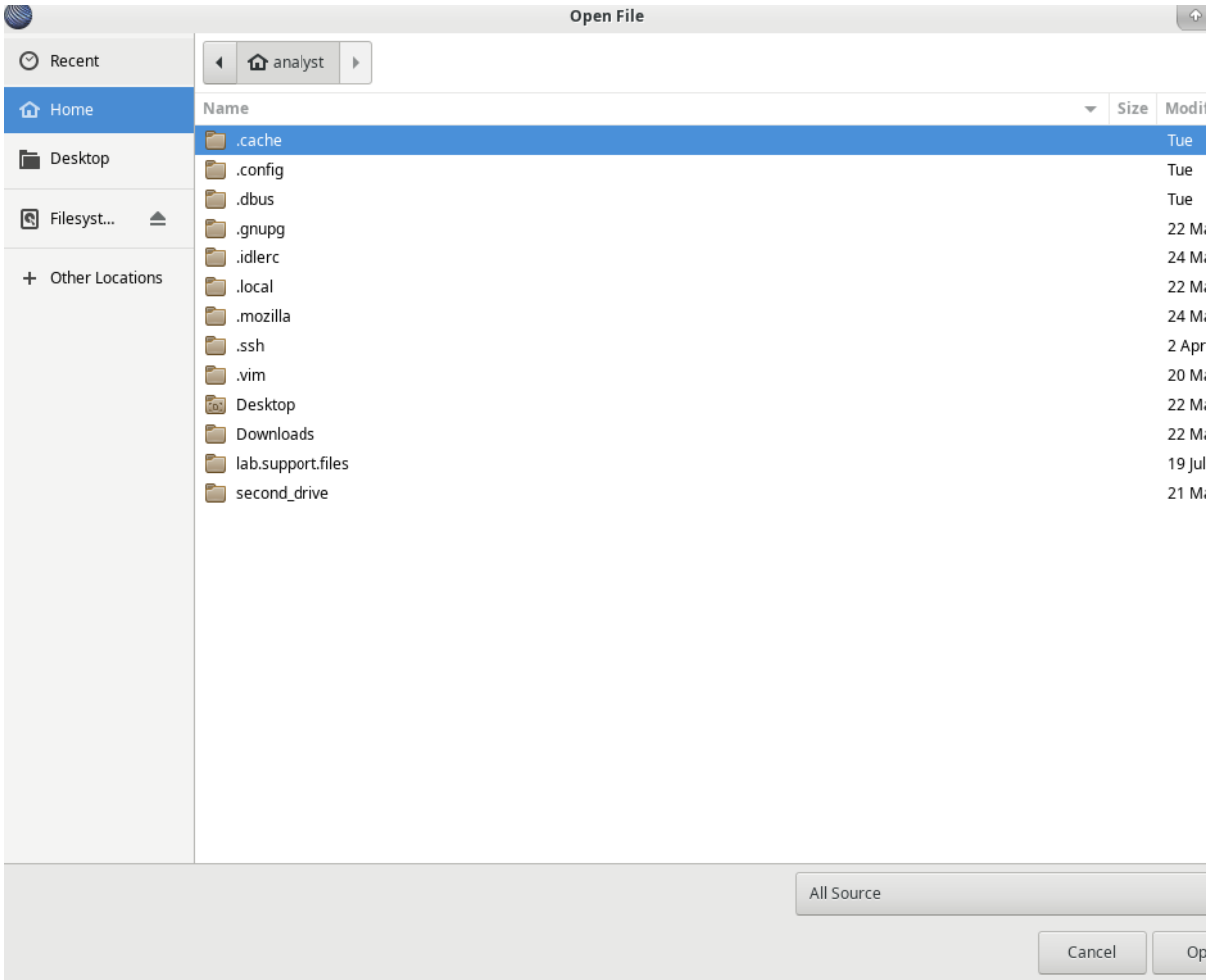
CYBEROPS - Working with Text Files in the CLI

- **Part 1: Graphical Text Editors**

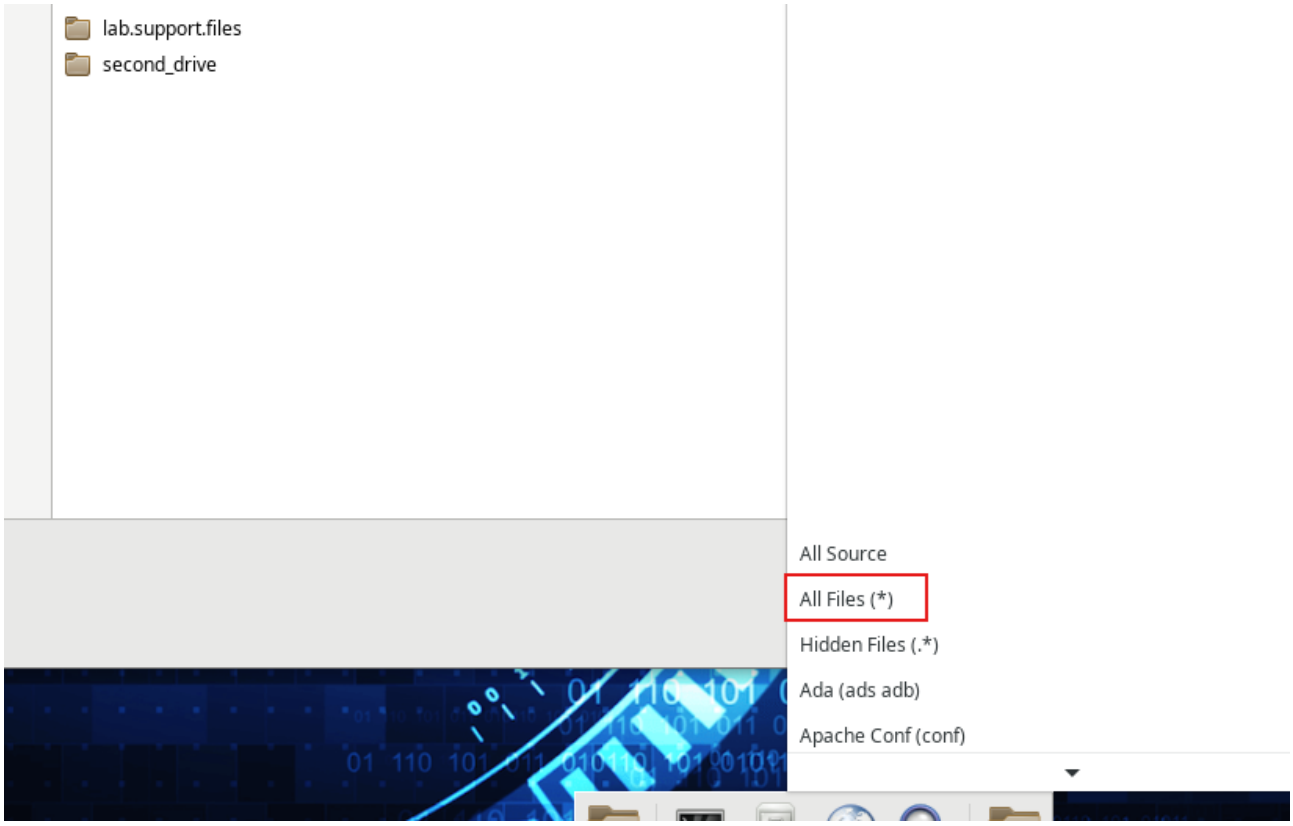
Salviamo il testo appena copiato su un file di nome **txt.**



Appena proviamo a cercare il file per riaprirlo non lo si trova.

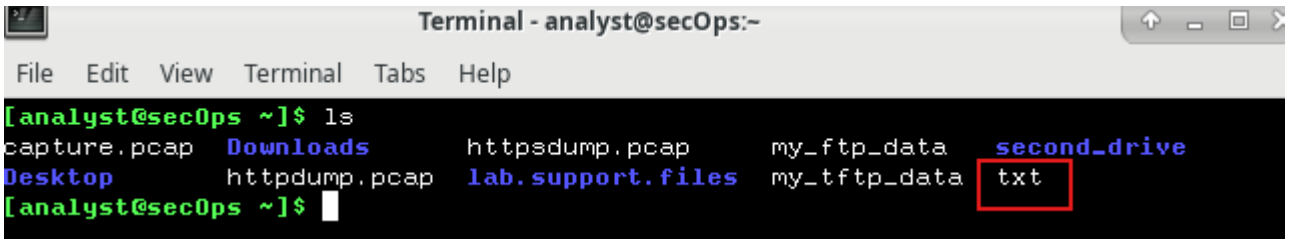


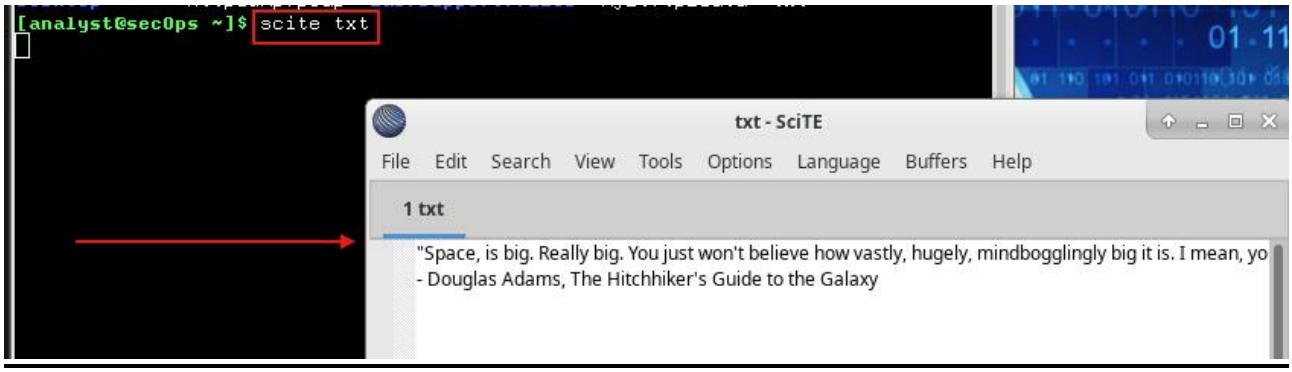
Serve infatti selezionare la tipologia di estensione da ricercare, in questo caso “**All Files(*)**”.



Step 2: Open SciTE from the Terminal

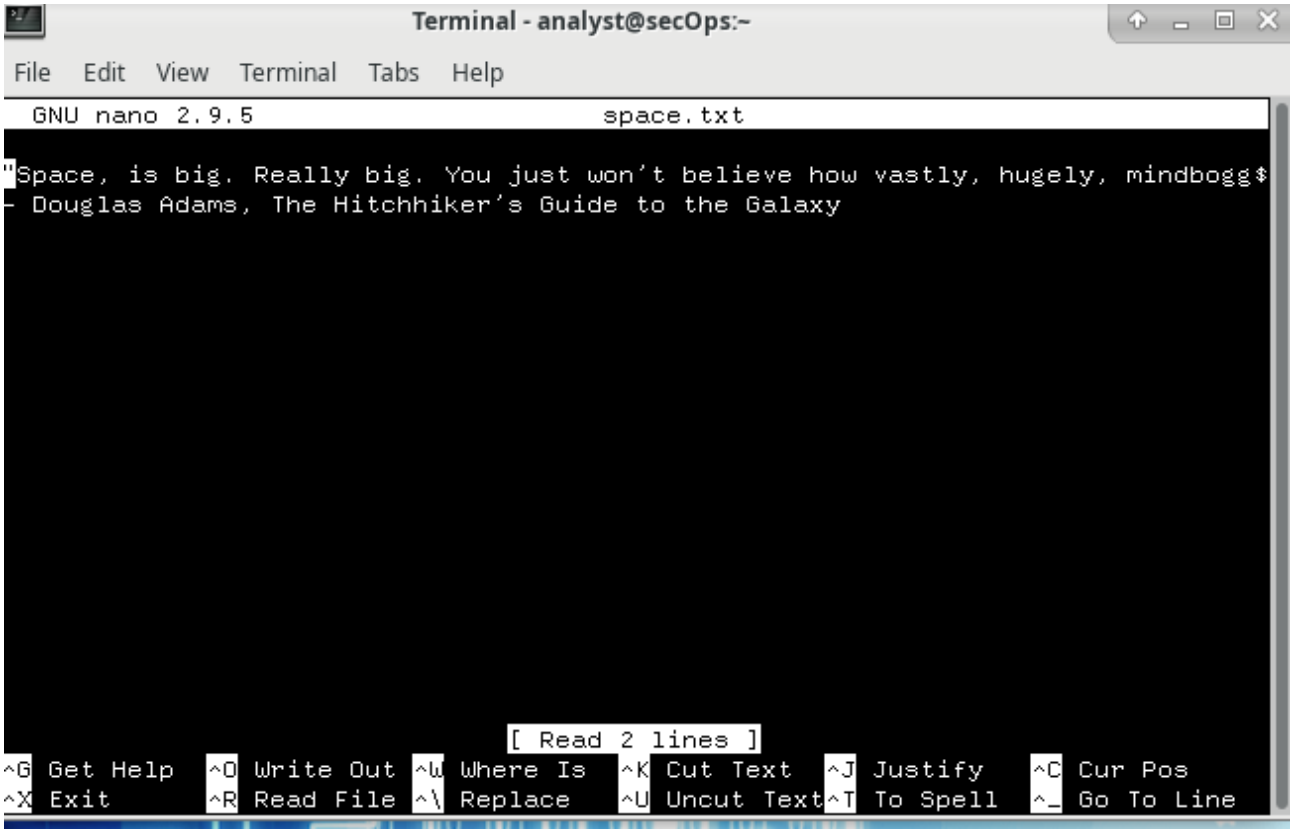
Possiamo aprire i file da terminale.





- ## Part 2: Command Line Text Editors

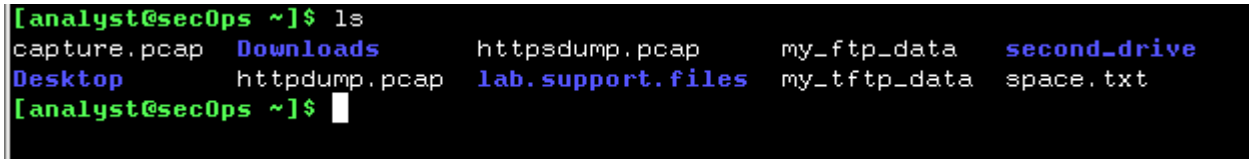
Usiamo “**nano space.txt”** per aprire il file. Dato che non ci sono ritorni a capo la riga viene troncata e ce lo dice attraverso il carattere “$”. Per uscire usiamo **“CTRL+X”.** Per salvare **“CTRL+O”** e ci chiederà se vogliamo salvare o meno le modifiche al file**.** Si usano le frecce per muoversi nel testo, **“Page Up” e “Page Down”** per sfogliare le pagine**,** poi anche **“Ctrl”, “Alt”, “Escape”** o il tasto **“Win”.** Si usa “**Ctrl+G**” per la schermata di aiuto e “**q**” per uscire da essa.



- ## Part 3: Working with Configuration Files

Step 1: Locating Configuration Files

Si usa “**ls**” per elencare la cartella corrente.



“**ls -la”** per vedere i file **nascosti (preceduti dal punto).**

```
[analyst@secOps ~]$ ls -la
total 6348
drwx------ 15 analyst analyst    4096 Sep  5 09:47 .
drwxr-xr-x  3 root    root       4096 Mar 20  2018 ..
-rw-------  1 analyst analyst    1835 Sep  4 13:47 .bash_history
-rw-r--r--  1 analyst analyst      21 Feb  7  2018 .bash_logout
-rw-r--r--  1 analyst analyst      57 Feb  7  2018 .bash_profile
-rw-r--r--  1 analyst analyst      97 Mar 20  2018 .bashrc
-rw-r--r--  1 analyst analyst     141 Feb  7  2018 .bashrc_stock
drwxr-xr-x  8 analyst analyst    4096 Sep  3 07:31 .cache
-rw-r--r--  1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 10 analyst analyst    4096 Sep  3 19:41 .config
drwx------  3 analyst analyst    4096 Sep  3 07:31 .dbus
drwxr-xr-x  2 analyst analyst    4096 Mar 22  2018 Desktop
-rw-r--r--  1 analyst analyst      23 Mar 23  2018 .dmrc
drwxr-xr-x  3 analyst analyst    4096 Mar 22  2018 Downloads
drwx------  3 analyst analyst    4096 Mar 22  2018 .gnupg
-rw-r--r--  1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r--  1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
-rw-------  1 analyst analyst    2520 Sep  5 09:30 .ICEauthority
drwxr-xr-x  2 analyst analyst    4096 Mar 24  2018 .idlerc
drwxr-xr-x  9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-------  1 analyst analyst      67 Sep  3 08:20 .lesshst
drwxr-xr-x  3 analyst analyst    4096 Mar 22  2018 .local
drwx------  5 analyst analyst    4096 Mar 24  2018 .mozilla
-rw-r--r--  1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r--  1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x  2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r--  1 analyst analyst     253 Sep  5 09:32 space.txt
drwx------  2 analyst analyst    4096 Apr  2  2018 .ssh
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-clipboard.pid
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-display.pid
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-draganddrop.pid
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-seamless.pid
drwxr-xr-x  3 analyst analyst    4096 Mar 20  2018 .vim
-rw-------  1 analyst analyst   13912 Jul 19  2018 .viminfo
-rw-------  1 analyst analyst      51 Sep  5 09:30 .Xauthority
-rw-r--r--  1 analyst analyst      16 Mar 22  2018 .xinitrc
-rw-r--r--  1 analyst analyst      16 Mar 22  2018 .Xinitrc
-rw-------  1 analyst analyst     257 Sep  5 09:30 .xsession-errors
-rw-------  1 analyst analyst     380 Sep  4 13:47 .xsession-errors.old
[analyst@secOps ~]$
```

.bashrc è un file nascosto per la configurazione del terminale.

```
[analyst@secOps ~]$ cat .bashrc
export EDITOR=vim

PS1='\[\e[1;32m\][\u@\h \W]\$\[\e[0m\] '
alias ls="ls --color"
alias vi="vim"
[analyst@secOps ~]$
```

In **/etc** si trovano le configurazioni dei servizi di sistema di sistema come la stampa e ftp.

```
[analyst@secOps ~]$ ls /etc
adjtime            initcpio           mtab               security
apparmor.d         inputrc            nanorc             sensors3.conf
arch-release       iproute2           netconfig          sensors.d
avahi              iptables           netctl             services
bash.bash_logout   issue              nginx              shadow
bash.bashrc        kernel             nscd.conf          shadow-
binfmt.d           krb5.conf          nsswitch.conf      shells
ca-certificates    ld.so.cache        ntp.conf           skel
conf.d             ld.so.conf         openldap           snort
crypttab           ld.so.conf.d       openvswitch        ssh
dbus-1             libnl              os-release         ssl
default            lightdm            pacman.conf        sudoers
depmod.d           locale.conf        pacman.d           sudoers.d
dhcpcd.conf        locale.gen         pam.d              sysctl.d
drirc              localtime          passwd             syslog-ng
environment        login.defs         passwd-            systemd
ethertypes         logrotate.conf     pcmcia             tmpfiles.d
fonts              logrotate.d        pkcs11             trusted-key.key
fstab              lvm                polkit-1           ts.conf
gai.conf           machine-id         profile            udev
group              mailcap            profile.d          UPower
group-             mail.rc            protocols          vbox
grub.d             makepkg.conf       pulse              vdpau_wrapper.cfg
gshadow            man_db.conf        rc.d               vimrc
gshadow-           mdadm.conf         rc_keymaps         vsftpd.conf
gtk-2.0            mime.types         rc_maps.cfg        vsftpd.conf_stock
gtk-3.0            mke2fs.conf        request-key.conf   X11
healthd.conf       mkinitcpio.conf    request-key.d      xdg
host.conf          mkinitcpio.d       resolv.conf        xinetd.d
hostname           modprobe.d         resolvconf.conf    yaourtrc
hosts              modules-load.d     rpc
ifplugd            motd               securetty
[analyst@secOps ~]$
```

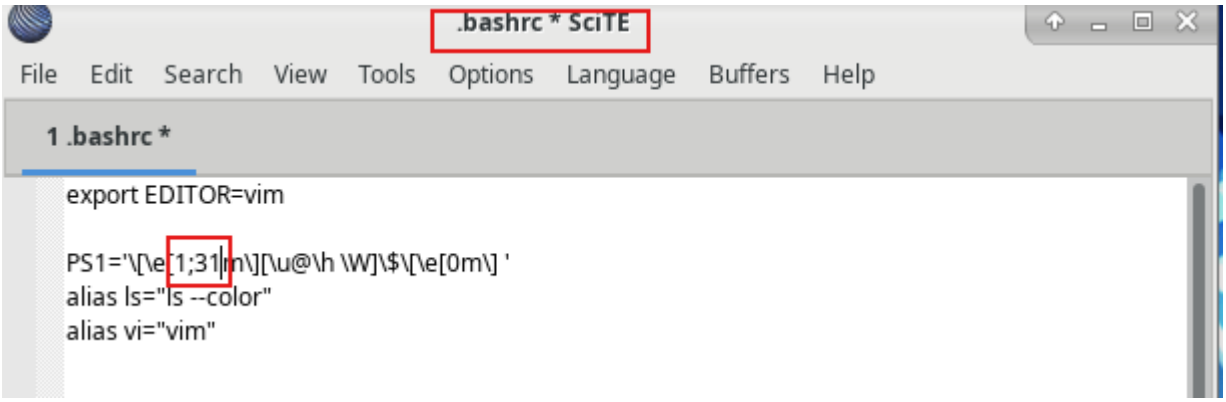
bash.bashrc è il file di configurazione della shell per tutti gli utenti. È possibile modificarlo solo con privilegi **root**.

```
[analyst@secOps ~]$ cat /etc/bash.bashrc
#
# /etc/bash.bashrc
#

# If not running interactively, don't do anything
[[ $- != *i* ]] && return

[[ $DISPLAY ]] && shopt -s checkwinsize

PS1='[\u@\h \W]\$ '

case ${TERM} in
  xterm*|rxvt*|Eterm|aterm|kterm|gnome*)
    PROMPT_COMMAND=${PROMPT_COMMAND:+$PROMPT_COMMAND; }'printf "\033]0;%s@%s:%s\
007" "${USER}" "${HOSTNAME%%.*}" "${PWD/#$HOME/\~}"'

    ;;
  screen*)
    PROMPT_COMMAND=${PROMPT_COMMAND:+$PROMPT_COMMAND; }'printf "\033_%s@%s:%s\033
3\\" "${USER}" "${HOSTNAME%%.*}" "${PWD/#$HOME/\~}"'
    ;;
esac

[ -r /usr/share/bash-completion/bash_completion   ] && . /usr/share/bash-complet
ion/bash_completion
[analyst@secOps ~]$
```

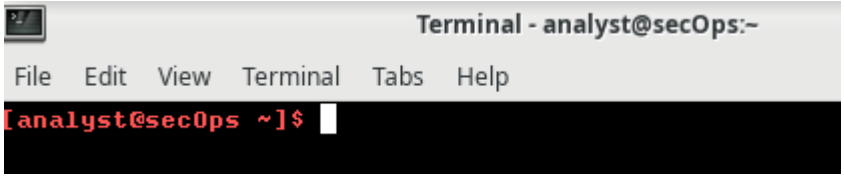
In **/home** invece si trovano i file di configurazione delle applicazioni per permettere agli utenti di modificarli liberamente secondo le loro esigenze.

Step 2: Editing and Saving Configuration files

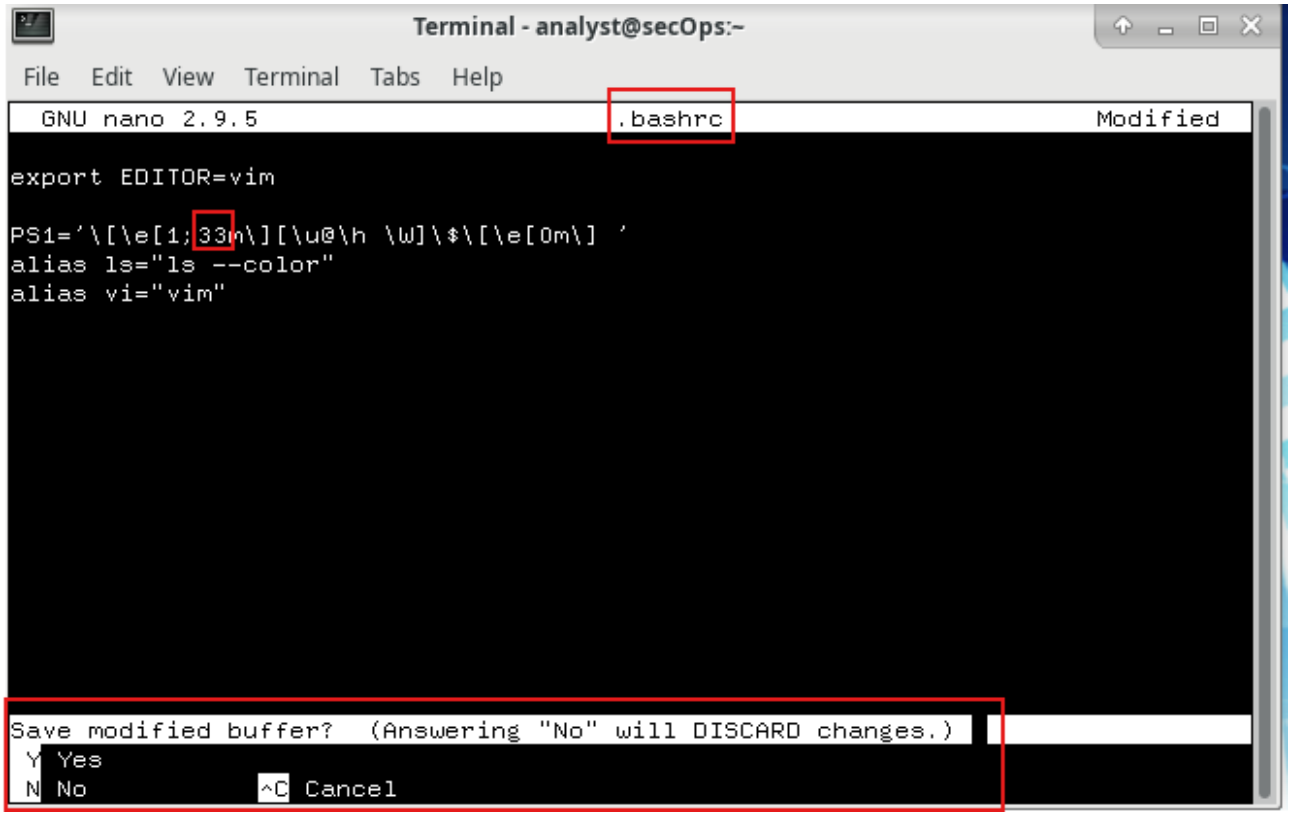
Ora scriviamo **31** al posto del valore **32** in **.bashrc** per cambiare il colore del testo nella shell.



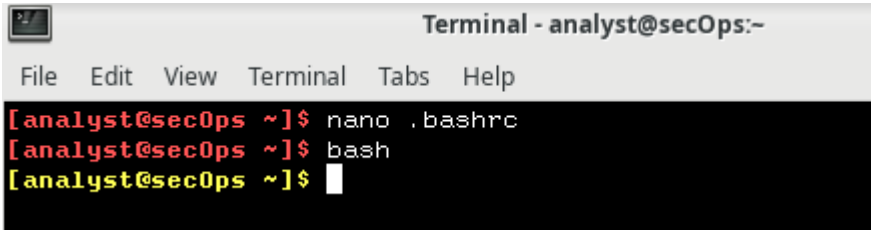
Ora apparirà in rosso anziché in verde, ma solo dopo aver riavviato la shell.



Adesso scriviamo **33** e salviamo le modifiche con l'editor **nano**.



Col comando "**bash**" si fa il refresh della shell e il colore adesso sarà il giallo.



Step 2: Editing Configuration Files for Services

Apro la configurazione di **nginx** con **nano** e lo switch **"-l**" per numerare le righe.

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
  GNU nano 2.9.5              /etc/nginx/custom_server.conf

  1
  2 #user html;
  3 worker_processes  1;
  4
  5 #error_log  logs/error.log;
  6 #error_log  logs/error.log  notice;
  7 #error_log  logs/error.log  info;
  8
  9 #pid        logs/nginx.pid;
 10
 11
 12 events {
 13     worker_connections  1024;
 14 }
 15
 16
 17 http {
 18     include       mime.types;
 19     default_type  application/octet-stream;
                              [ Read 122 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Cambio la porta di ascolto da **81** a **8080**.

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
  GNU nano 2.9.5              /etc/nginx/custom_server.conf          Modified

 31     keepalive_timeout  65;
 32
 33     #gzip  on;
 34
 35     types_hash_max_size 4096;
 36     server_names_hash_bucket_size 128;
 37
 38     server {
 39         listen       8080;
 40         server_name  localhost;
 41
 42         #charset koi8-r;
 43
 44         #access_log  logs/host.access.log  main;
 45
 46         location / {
 47             root   /usr/share/nginx/html/;
 48             index  index.html index.htm;
 49         }

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Modifichiamo il percorso alla **riga 47** aggiungendo la cartella **text_ed_lab/** alla fine di esso**.**

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
  GNU nano 2.9.5            /etc/nginx/custom_server.conf            Modified

 31     keepalive_timeout  65;
 32
 33     #gzip  on;
 34
 35     types_hash_max_size 4096;
 36     server_names_hash_bucket_size 128;
 37
 38     server {
 39         listen       8080;
 40         server_name  localhost;
 41
 42         #charset koi8-r;
 43
 44         #access_log  logs/host.access.log  main;
 45
 46         location / {
 47             root   /usr/share/nginx/html/text_ed_lab/;
 48             index  index.html index.htm;
 49         }
Save modified buffer?  (Answering "No" will DISCARD changes.)
 Y Yes
 N No            ^C Cancel
```

Avvio il server con la configurazione modificata.

```
[analyst@secOps ~]$ sudo nginx -c custom_server.conf
[sudo] password for analyst:
[analyst@secOps ~]$
```

A causa di un IP forse errato mi sono connesso usando "**localhost:8080**". La modifica funziona!

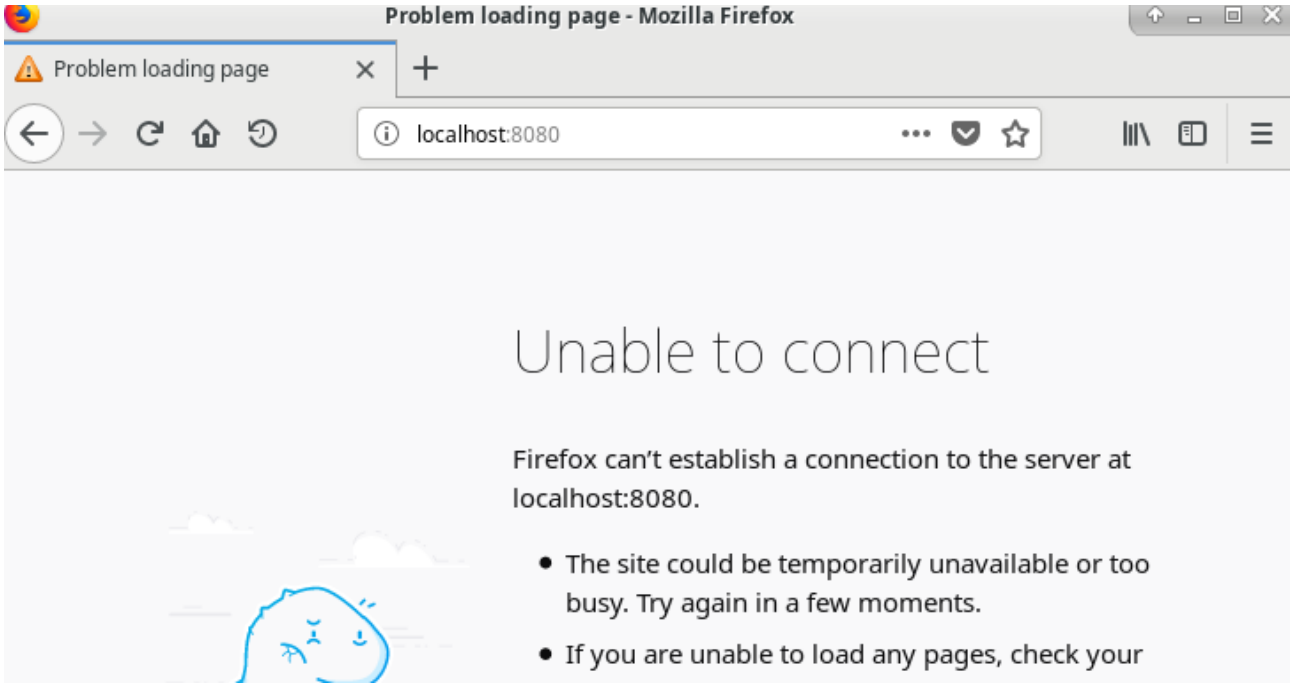
All’avvio del server apparirà un errore a causa del mancato ritrovamento di una risorsa da caricare nella pagina del browser.

```
[analyst@secOps ~]$ 2024/09/05 10:41:31 [error] 857#857: *1 open() "/usr/share/n
ginx/html/text_ed_lab/favicon.ico" failed (2: No such file or directory), client
: 127.0.0.1, server: localhost, request: "GET /favicon.ico HTTP/1.1", host: "loc
alhost:8080"
2024/09/05 10:41:31 [error] 857#857: *1 open() "/usr/share/nginx/html/text_ed_la
b/favicon.ico" failed (2: No such file or directory), client: 127.0.0.1, server:
 localhost, request: "GET /favicon.ico HTTP/1.1", host: "localhost:8080"
```

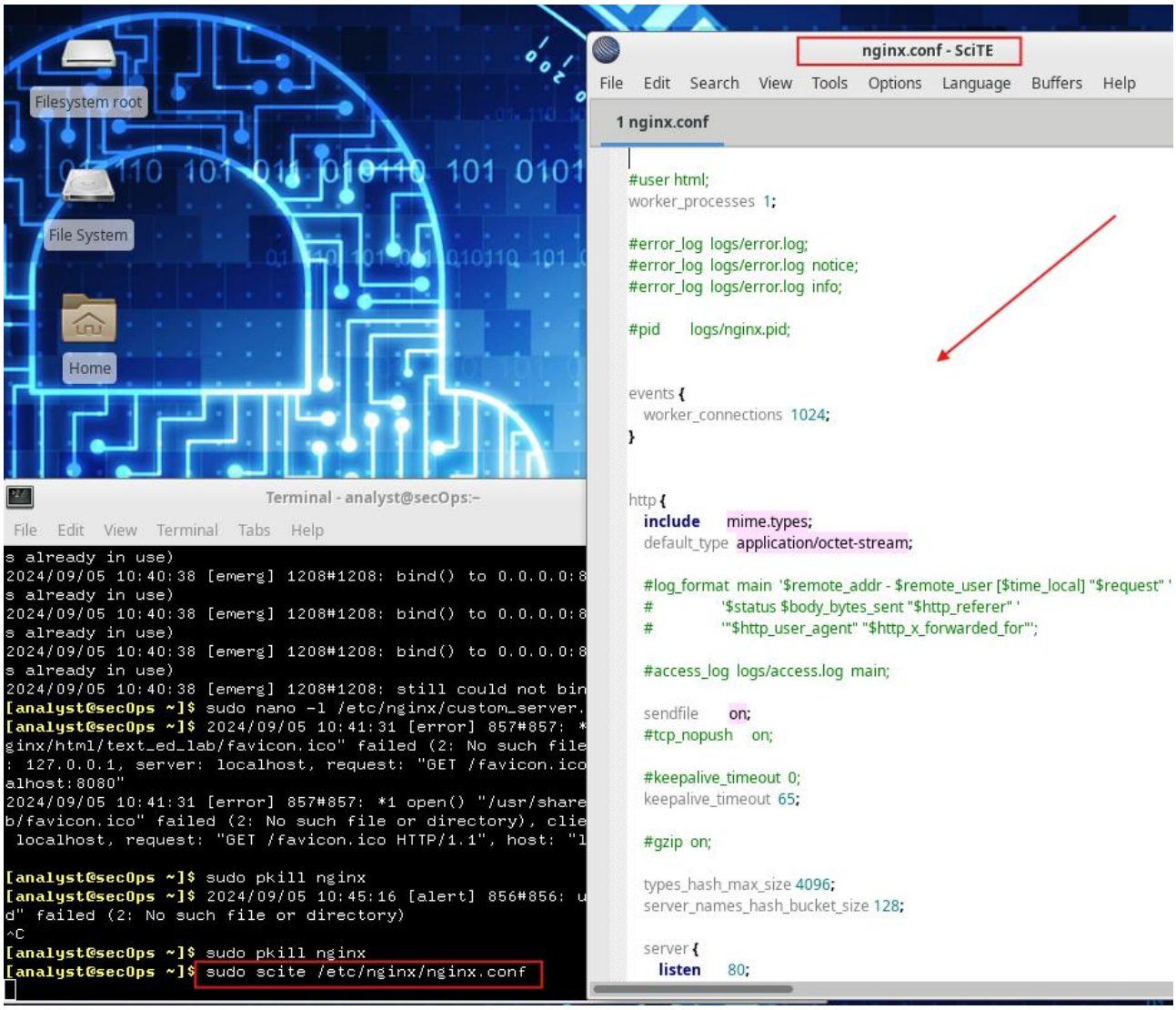
Chiudo il server.

```
[analyst@secOps ~]$ sudo pkill nginx
[analyst@secOps ~]$
```

Dopo aver pulito la cronologia recente vedo che il server è davvero stato interrotto quando riprovo a caricarlo.



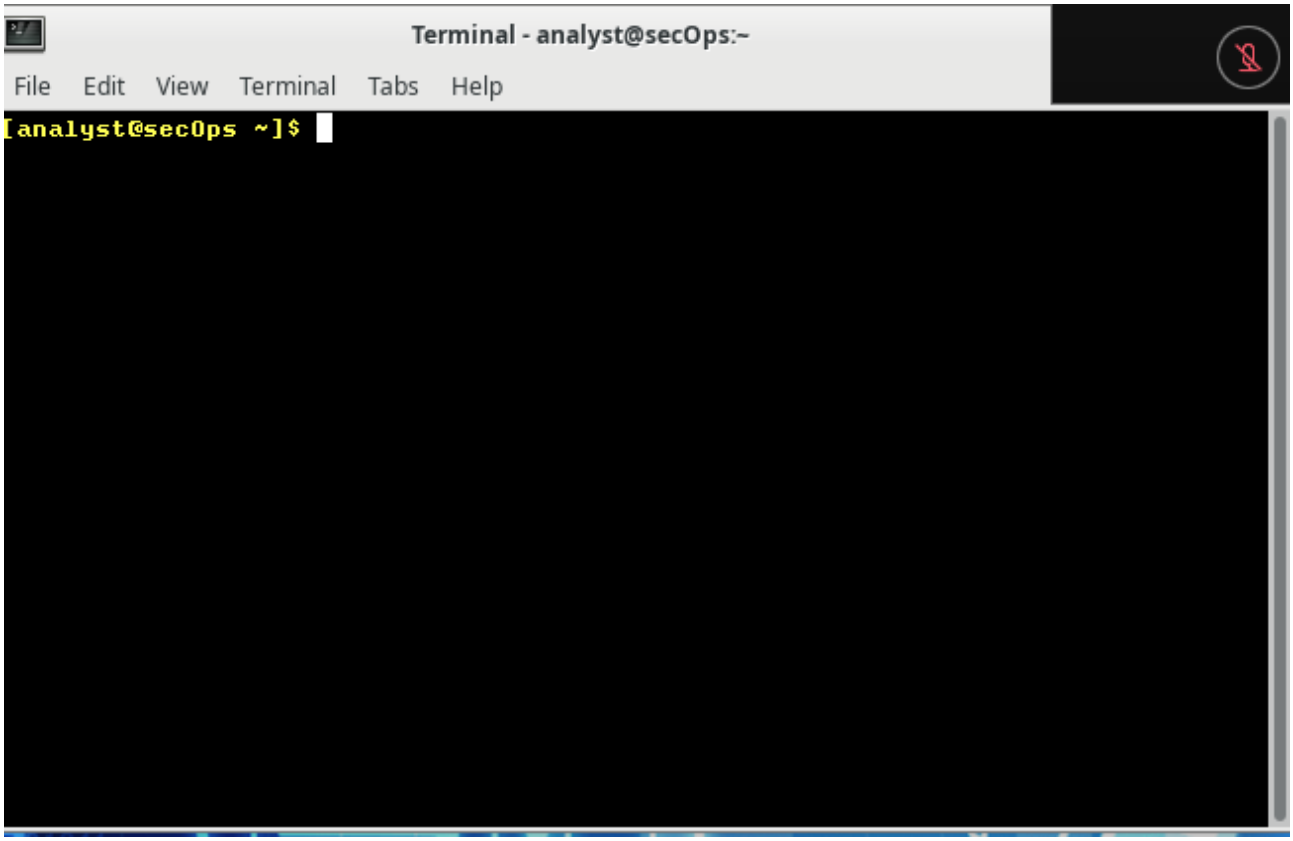
Si può editare il file di configurazione anche con **scite** accedendo tramite sudo ai privilegi di **root**.



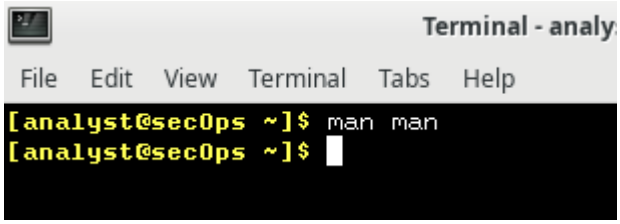
CYBEROPS - Getting Familiar with the Linux Shell

- **Part 1: Shell Basics**

Step 1: Access the Command Line



Step 2: Display Manual Pages from the command line



Sezione di **man** dedicata alla sua stessa comprensione. Tra le sezioni notiamo: sinossi, nome, configurazione, descrizione…

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
MAN(1)                    Manual pager utils                    MAN(1)

NAME
       man - an interface to the on-line reference manuals

SYNOPSIS
       man  [-C  file]  [-d]  [-D]  [--warnings[=warnings]]  [-R encoding] [-L
       locale] [-m system[,...]] [-M path] [-S list]  [-e  extension]  [-i|-I]
       [--regex|--wildcard]   [--names-only]  [-a]  [-u]  [--no-subpages]  [-P
       pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation] [--no-justifi-
       cation]  [-p  string]  [-t]  [-T[device]]  [-H[browser]] [-X[dpi]] [-Z]
       [[section] page[.section] ...] ...
       man -k [apropos options] regexp ...
       man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
       man -f [whatis options] page ...
       man -l [-C file] [-d] [-D] [--warnings[=warnings]]  [-R  encoding]  [-L
       locale]  [-P  pager]  [-r  prompt]  [-7] [-E encoding] [-p string] [-t]
       [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
       man -w|-W [-C file] [-d] [-D] page ...
       man -c [-C file] [-d] [-D] page ...
       man [-?V]
```

Sezione di **man** dedicata al comando **cp.**

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

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
CP(1)                         User Commands                         CP(1)

NAME
       cp - copy files and directories

SYNOPSIS
       cp [OPTION]... [-T] SOURCE DEST
       cp [OPTION]... SOURCE... DIRECTORY
       cp [OPTION]... -t DIRECTORY SOURCE...

DESCRIPTION
       Copy SOURCE to DEST, or multiple SOURCE(s) to DIRECTORY.

       Mandatory  arguments  to  long  options are mandatory for short options
       too.

       -a, --archive
              same as -dR --preserve=all

       --attributes-only
              don't copy the file data, just the attributes

       --backup[=CONTROL]
 Manual page cp(1) line 1 (press h for help or q to quit)
```

Sezione di **man** su **pwd**.

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

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
PWD(1)                    User Commands                    PWD(1)

NAME
       pwd - print name of current/working directory

SYNOPSIS
       pwd [OPTION]...

DESCRIPTION
       Print the full filename of the current working directory.

       -L, --logical
              use PWD from environment, even if it contains symlinks

       -P, --physical
              avoid all symlinks

       --help display this help and exit

       --version
              output version information and exit

       If no option is specified, -P is assumed.
 Manual page pwd(1) line 1 (press h for help or q to quit)
```

Step 3: Create and change directories

Comando per vedere la directory corrente.

```
[analyst@secOps ~]$ pwd
/home/analyst
[analyst@secOps ~]$
```

Creo tre cartelle col comando **mkdir**.

```
[analyst@secOps ~]$ mkdir cyops_folder1
[analyst@secOps ~]$ mkdir cyops_folder2
[analyst@secOps ~]$ mkdir cyops_folder3
[analyst@secOps ~]$ ls -l
total 6232
-rw-r--r-- 1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:06 cyops_folder1
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:06 cyops_folder2
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:07 cyops_folder3
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r-- 1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-r--r-- 1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r-- 1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst     253 Sep  5 09:32 space.txt
[analyst@secOps ~]$
```

Ci spostiamo in una delle cartelle appena create. Dopo aver cambiato posizione cambia pure l'intestazione della shell che ora indica la cartella dove ci siamo spostati (**cyops_folder3**)

```
[analyst@secOps ~]$ cd /home/analyst/cyops_folder3
[analyst@secOps cyops_folder3]$ pwd
/home/analyst/cyops_folder3
[analyst@secOps cyops_folder3]$
```

Da notare anche il simbolo **"$"** che ci indica che abbiamo accesso come utente normale e non come root **"#".**

Con il comando "**cd ~"** ci si sposta alla cartella **home** dell'utente corrente.

```
[analyst@secOps cyops_folder3]$ cd ~
[analyst@secOps ~]$ pwd
/home/analyst
[analyst@secOps ~]$
```

Creo una cartella all'interno di quella precedentemente creata col comando "**mkdir /home/analyst/cyops_folder3/cyops_folder4".**

```
[analyst@secOps ~]$ mkdir /home/analyst/cyops_folder3/cyops_folder4
[analyst@secOps ~]$
```

Controllo la creazione effettiva della directory.

```
[analyst@secOps ~]$ ls -l /home/analyst/cyops_folder3
total 4
drwxr-xr-x 2 analyst analyst 4096 Sep  5 11:15 cyops_folder4
[analyst@secOps ~]$
```

Lo switch "**-a**" ci permette di mostrare tutti i file, anche quelli nascosti.

```
[analyst@secOps ~]$ ls -la /home/analyst/cyops_folder3
total 12
drwxr-xr-x  3 analyst analyst 4096 Sep  5 11:15 .
drwx------ 18 analyst analyst 4096 Sep  5 11:07 ..
drwxr-xr-x  2 analyst analyst 4096 Sep  5 11:15 cyops_folder4
[analyst@secOps ~]$
```

Cambio cartella col comando **cd**.

```
[analyst@secOps ~]$ cd /home/analyst/cyops_folder3
[analyst@secOps cyops_folder3]$ pwd
/home/analyst/cyops_folder3
```

Col comando “cd .” ci si sposta nella directory corrente.

```
[analyst@secOps cyops_folder3]$ cd .
[analyst@secOps cyops_folder3]$ pwd
/home/analyst/cyops_folder3
[analyst@secOps cyops_folder3]$
```

Col comando “**cd ..**” ci si sposta alla directory superiore.

```
[analyst@secOps cyops_folder3]$ cd ..
[analyst@secOps ~]$ pwd
/home/analyst
[analyst@secOps ~]$
```

Si può continuare così fino alla **root** (/).

```
[analyst@secOps ~]$ cd ..
[analyst@secOps home]$ pwd
/home
[analyst@secOps home]$
```

```
[analyst@secOps home]$ cd ..
[analyst@secOps /]$ cd ..
[analyst@secOps /]$
```

Step 4: Redirect Outputs

Il comando **echo** esegue l’eco del messaggio passatogli come argomento, quindi lo mostra sul terminale in output.

```
[analyst@secOps /]$ cd /home/analyst/
[analyst@secOps ~]$ echo This is a message echoed to the terminal by echo.
This is a message echoed to the terminal by echo.
[analyst@secOps ~]$
```

Con l’operatore **“>”** si può scrivere il messaggio dentro un file di testo che viene creato all’esecuzione del comando. Usiamo **cat** per mostrarne il contenuto.

```
[analyst@secOps ~]$ echo This is a message echoed to the terminal by echo. > som
e_text_file.txt
[analyst@secOps ~]$ cat some_text_file.txt
This is a message echoed to the terminal by echo.
[analyst@secOps ~]$
```

Adesso abbiamo sovrascritto il file con un nuovo testo.

```
[analyst@secOps ~]$ echo This is a DIFFERENT message, once again echoed to the t
erminal by echo. > some_text_file.txt
[analyst@secOps ~]$ cat some_text_file.txt
This is a DIFFERENT message, once again echoed to the terminal by echo.
[analyst@secOps ~]$
```

Step 5: Redirect and Append to a Text File

Per non sovrascrivere il file usiamo l'operatore **">>"** che accoda il testo a quello già presente all'interno del file.

```
[analyst@secOps ~]$ echo This is another line of text. It will be APPENDED to th
e output file. >> some_text_file.txt
[analyst@secOps ~]$ cat some_text_file.txt
This is a DIFFERENT message, once again echoed to the terminal by echo.
This is another line of text. It will be APPENDED to the output file.
[analyst@secOps ~]$
```

Step 6: Work with hidden files in Linux

Listiamo i file della home con **"ls -l".**

```
[analyst@secOps ~]$ ls -l
total 6236
-rw-r--r-- 1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:06 cyops_folder1
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:06 cyops_folder2
drwxr-xr-x 3 analyst analyst    4096 Sep  5 11:15 cyops_folder3
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r-- 1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-r--r-- 1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r-- 1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst     142 Sep  5 11:40 some_text_file.txt
-rw-r--r-- 1 analyst analyst     253 Sep  5 09:32 space.txt
```

Con “**ls -la**” vediamo anche i file e le cartelle nascosti. Ovvero quelli il cui nome è preceduto dal punto.

```
[analyst@secOps ~]$ ls -la
total 6364
drwx------ 18 analyst analyst    4096 Sep  5 11:37 .
drwxr-xr-x  3 root    root       4096 Mar 20  2018 ..
-rw-------  1 analyst analyst    2257 Sep  5 10:59 .bash_history
-rw-r--r--  1 analyst analyst      21 Feb  7  2018 .bash_logout
-rw-r--r--  1 analyst analyst      57 Feb  7  2018 .bash_profile
-rw-r--r--  1 analyst analyst      97 Sep  5 10:19 .bashrc
-rw-r--r--  1 analyst analyst     141 Feb  7  2018 .bashrc_stock
drwxr-xr-x  8 analyst analyst    4096 Sep  3 07:31 .cache
-rw-r--r--  1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 10 analyst analyst    4096 Sep  3 19:41 .config
drwxr-xr-x  2 analyst analyst    4096 Sep  5 11:06 cyops_folder1
drwxr-xr-x  2 analyst analyst    4096 Sep  5 11:06 cyops_folder2
drwxr-xr-x  3 analyst analyst    4096 Sep  5 11:15 cyops_folder3
drwx------  3 analyst analyst    4096 Sep  3 07:31 .dbus
drwxr-xr-x  2 analyst analyst    4096 Mar 22  2018 Desktop
-rw-r--r--  1 analyst analyst      23 Mar 23  2018 .dmrc
drwxr-xr-x  3 analyst analyst    4096 Mar 22  2018 Downloads
drwx------  3 analyst analyst    4096 Mar 22  2018 .gnupg
-rw-r--r--  1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r--  1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
-rw-------  1 analyst analyst    2520 Sep  5 09:30 .ICEauthority
drwxr-xr-x  2 analyst analyst    4096 Mar 24  2018 .idlerc
drwxr-xr-x  9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-------  1 analyst analyst      67 Sep  3 08:20 .lesshst
drwxr-xr-x  3 analyst analyst    4096 Mar 22  2018 .local
drwx------  5 analyst analyst    4096 Mar 24  2018 .mozilla
-rw-r--r--  1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r--  1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x  2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r--  1 analyst analyst     142 Sep  5 11:40 some_text_file.txt
-rw-r--r--  1 analyst analyst     253 Sep  5 09:32 space.txt
drwx------  2 analyst analyst    4096 Apr  2  2018 .ssh
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-clipboard.pid
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-display.pid
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-draganddrop.pid
-rw-r-----  1 analyst analyst       4 Sep  5 09:30 .vboxclient-seamless.pid
drwxr-xr-x  3 analyst analyst    4096 Mar 20  2018 .vim
-rw-------  1 analyst analyst   13912 Jul 19  2018 .viminfo
-rw-------  1 analyst analyst      51 Sep  5 09:30 .Xauthority
-rw-r--r--  1 analyst analyst      16 Mar 22  2018 .xinitrc
-rw-r--r--  1 analyst analyst      16 Mar 22  2018 .Xinitrc
-rw-------  1 analyst analyst     543 Sep  5 10:46 .xsession-errors
-rw-------  1 analyst analyst     380 Sep  4 13:47 .xsession-errors.old
[analyst@secOps ~]$
```

Possiamo approfondire con “**man ls**”.

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
LS(1)                          User Commands                          LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information  about  the FILEs (the current directory by default).
       Sort entries alphabetically if none of -cftuvSUX nor --sort  is  speci-
       fied.

       Mandatory  arguments  to  long  options are mandatory for short options
       too.

       -a, --all
              do not ignore entries starting with .
```

- **Part 2: Copying, Deleting, and Moving Files**

Step 1: Copying Files

Con **cp** possiamo copiare i file in altre directory. In questo caso da **/home/analyst/** a **/home/analyst/cyops_folder2**/.

```
[analyst@secOps ~]$ cp some_text_file.txt cyops_folder2/
[analyst@secOps ~]$ ls cyops_folder2/
some_text_file.txt
[analyst@secOps ~]$
```

Ora è in entrambe le cartelle.

```
[analyst@secOps ~]$ ls
capture.pcap   Desktop          lab.support.files  some_text_file.txt
cyops_folder1  Downloads        my_ftp_data        space.txt
cyops_folder2  httpdump.pcap    my_tftp_data
cyops_folder3  httpsdump.pcap   second_drive
[analyst@secOps ~]$
```

Step 2: Deleting Files and Directories

Con **rm** si cancella un file.

```
[analyst@secOps ~]$ rm some_text_file.txt
[analyst@secOps ~]$ ls -l
total 6232
-rw-r--r-- 1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:06 cyops_folder1
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:46 cyops_folder2
drwxr-xr-x 3 analyst analyst    4096 Sep  5 11:15 cyops_folder3
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r-- 1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-r--r-- 1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r-- 1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst     253 Sep  5 09:32 space.txt
[analyst@secOps ~]$
```

Con lo switch "**-r**" (**recursive**) si possono eliminare anche le cartelle e tutto il loro contenuto.

```
[analyst@secOps ~]$ rm -r cyops_folder1/
[analyst@secOps ~]$ ls -l
total 6228
-rw-r--r-- 1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:46 cyops_folder2
drwxr-xr-x 3 analyst analyst    4096 Sep  5 11:15 cyops_folder3
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r-- 1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-r--r-- 1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r-- 1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst     253 Sep  5 09:32 space.txt
[analyst@secOps ~]$
```

Step 3: Moving Files and Directories

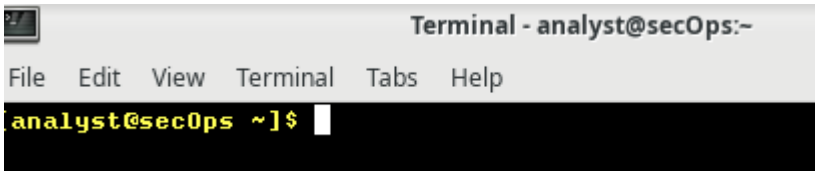
Abbiamo spostato col comando "**mv**" il file **some_text_file.txt** dalla cartella **cyops_folder2** alla directory corrente.

```
[analyst@secOps ~]$ mv cyops_folder2/some_text_file.txt .
[analyst@secOps ~]$ ls -l
total 6232
-rw-r--r-- 1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:54 cyops_folder2
drwxr-xr-x 3 analyst analyst    4096 Sep  5 11:15 cyops_folder3
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r-- 1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-r--r-- 1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r-- 1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst     142 Sep  5 11:46 some_text_file.txt
-rw-r--r-- 1 analyst analyst     253 Sep  5 09:32 space.txt
[analyst@secOps ~]$
```

CYBEROPS - Linux Servers

- **Part 1: Servers**

Step 1: Access the command line



Step 2: Display the services currently running

Il comando "**ps**" si usa per visualizzare i processi attivi.

```
[analyst@secOps ~]$ sudo ps -elf
F S UID          PID  PPID  C PRI  NI ADDR SZ WCHAN  STIME TTY          TIME CMD
4 S root           1     0  0  80   0 - 42151 SyS_ep 09:30 ?        00:00:01 /sbin
1 S root           2     0  0  80   0 -     0 -      09:30 ?        00:00:00 [kthr
1 I root           3     2  0  80   0 -     0 -      09:30 ?        00:00:00 [kwor
1 I root           4     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [kwor
1 I root           6     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [mm_p
1 S root           7     2  0  80   0 -     0 -      09:30 ?        00:00:01 [ksof
1 I root           8     2  0  58   - -     0 -      09:30 ?        00:00:05 [rcu_
1 I root           9     2  0  58   - -     0 -      09:30 ?        00:00:00 [rcu_
1 I root          10     2  0  58   - -     0 -      09:30 ?        00:00:00 [rcu_
1 S root          11     2  0  58   - -     0 -      09:30 ?        00:00:00 [rcuc
1 S root          12     2  0  58   - -     0 -      09:30 ?        00:00:00 [rcub
1 S root          13     2  0 -40   - -     0 -      09:30 ?        00:00:00 [migr
5 S root          14     2  0 -40   - -     0 -      09:30 ?        00:00:00 [watc
1 S root          15     2  0  80   0 -     0 -      09:30 ?        00:00:00 [cpuh
1 S root          16     2  0  80   0 -     0 -      09:30 ?        00:00:00 [cpuh
5 S root          17     2  0 -40   - -     0 -      09:30 ?        00:00:00 [watc
1 S root          18     2  0 -40   - -     0 -      09:30 ?        00:00:00 [migr
1 S root          19     2  0  58   - -     0 -      09:30 ?        00:00:00 [rcuc
1 S root          20     2  0  80   0 -     0 -      09:30 ?        00:00:00 [ksof
1 I root          22     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [kwor
5 S root          23     2  0  80   0 -     0 -      09:30 ?        00:00:00 [kdev
1 I root          24     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [netn
1 S root          25     2  0  80   0 -     0 -      09:30 ?        00:00:00 [rcu_
1 S root          28     2  0  80   0 -     0 -      09:30 ?        00:00:00 [khun
1 S root          29     2  0  80   0 -     0 -      09:30 ?        00:00:00 [oom_
1 I root          30     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [writ
1 S root          31     2  0  80   0 -     0 -      09:30 ?        00:00:00 [kcom
1 S root          32     2  0  85   5 -     0 -      09:30 ?        00:00:00 [ksmd
1 S root          33     2  0  99  19 -     0 -      09:30 ?        00:00:00 [khug
1 I root          34     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [cryp
1 I root          35     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [kint
1 I root          36     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [kblo
1 I root          37     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [edac
1 I root          38     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [devf
1 I root          39     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [watc
1 S root          41     2  0  80   0 -     0 -      09:30 ?        00:00:00 [kswa
1 I root          80     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [kthr
1 I root          81     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [acpi
1 I root          82     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [nvme
1 I root          83     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [ipv6
1 I root          92     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [kstr
1 I root         101     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [char
1 I root         127     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [ata_
1 S root         128     2  0  80   0 -     0 -      09:30 ?        00:00:00 [scsi
1 I root         129     2  0  60 -20 -     0 -      09:30 ?        00:00:00 [scsi
1 S root         130     2  0  80   0 -     0 -      09:30 ?        00:00:00 [scsi
```

Usiamo **sudo** per visualizzare anche i processi che non appartengono all'utente corrente (**analyst**).

Con gli switch “-**ejH**” si vedono i processi in maniera gerarchica, ovvero indentando i processi figli rispetto al processo padre.

```
[analyst@secOps ~]$ sudo /usr/sbin/nginx
[analyst@secOps ~]$
```

```
[analyst@secOps ~]$ sudo ps -ejH
  PID  PGID   SID TTY          TIME CMD
    2     0     0 ?        00:00:00 kthreadd
    3     0     0 ?        00:00:00   kworker/0:0
    4     0     0 ?        00:00:00   kworker/0:0H
    6     0     0 ?        00:00:00   mm_percpu_wq
    7     0     0 ?        00:00:01   ksoftirqd/0
    8     0     0 ?        00:00:05   rcu_preempt
    9     0     0 ?        00:00:00   rcu_sched
   10     0     0 ?        00:00:00   rcu_bh
   11     0     0 ?        00:00:00   rcuc/0
   12     0     0 ?        00:00:00   rcub/0
   13     0     0 ?        00:00:00   migration/0
   14     0     0 ?        00:00:00   watchdog/0
   15     0     0 ?        00:00:00   cpuhp/0
   16     0     0 ?        00:00:00   cpuhp/1
   17     0     0 ?        00:00:00   watchdog/1
   18     0     0 ?        00:00:00   migration/1
   19     0     0 ?        00:00:00   rcuc/1
   20     0     0 ?        00:00:00   ksoftirqd/1
   22     0     0 ?        00:00:00   kworker/1:0H
   23     0     0 ?        00:00:00   kdevtmpfs
   24     0     0 ?        00:00:00   netns
```

```
 550   548   548 ?        00:00:18     VBoxClient
1851  1851  1851 ?        00:00:00   nginx
1852  1851  1851 ?        00:00:00     nginx
```

Netstat è un comando che ci può aiutare a comprendere se ci sono server in esecuzione.

```
[analyst@secOps ~]$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         DGRAM                    10628    /run/systemd/notify
unix  7      [ ]         DGRAM                    10664    /run/systemd/journal/
socket
unix  2      [ ]         DGRAM                    14567    /run/user/1000/system
d/notify
unix  9      [ ]         DGRAM                    10735    /run/systemd/journal/
dev-log
unix  3      [ ]         STREAM     CONNECTED     10993    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     15357
unix  3      [ ]         STREAM     CONNECTED     16099    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     16486    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     13002    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     13362
unix  3      [ ]         STREAM     CONNECTED     13122
unix  3      [ ]         STREAM     CONNECTED     15009
unix  3      [ ]         STREAM     CONNECTED     15941
unix  3      [ ]         STREAM     CONNECTED     11577
unix  3      [ ]         STREAM     CONNECTED     13138
unix  3      [ ]         STREAM     CONNECTED     12675    /run/dbus/system_bus_
socket
unix  3      [ ]         STREAM     CONNECTED     12503    /run/systemd/journal/
```

Lo switch "**-a**" mostra i socket in ascolto e non. "**-n**" usa output numerico ovvero non mostra username o i servizi attivi. "**-p**" mostra i **PID** del processo che avvia la connessione. "**-t**" mostra le connessioni **TCP**. "**-u**" mostra le connessioni **UDP**. Possono essere usati in qualsiasi ordine.

```
[analyst@secOps ~]$ sudo netstat -tunap
[sudo] password for analyst:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:6633            0.0.0.0:*               LISTEN      276/python2.7
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1851/nginx: master
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      306/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      304/sshd
tcp6       0      0 :::22                   :::*                    LISTEN      304/sshd
udp        0      0 10.0.2.15:68            0.0.0.0:*                           224/systemd-network
[analyst@secOps ~]$
```

Sulla porta 80/TCP è attivo il server nginx con PID 1851 che è in stato di ascolto (listen).

In questo modo cerchiamo tramite il comando "**sudo ps -elf | grep 1851**" il processo con **PID 1851**.

Usiamo l'operatore pipe "|" per passare l'output a **grep** che cercherà il valore passatogli **(1851)** e lo mosrerà a schermo.

```
[analyst@secOps ~]$ sudo ps -elf | grep 1851
1 S root      1851     1  0  80   0 -  7192 -      12:02 ?        00:00:00 nginx: master process /usr/
sbin/nginx
5 S http      1852  1851  0  80   0 -  8457 SyS_ep 12:02 ?        00:00:00 nginx: worker process
0 S analyst   1908  1834  0  80   0 -  2720 -      12:22 pts/1    00:00:00 grep 1851
```

Il processo con **PID 1852** è un processo figlio del processo padre di **nginx**.

- ## Part 2: Using Telnet to Test TCP Services

Usiamo **telnet** per collegarci al server **nginx** precedentemente aperto. Digitiamo qualcosa e premiamo INVIO. Appare il messaggio qui sotto.

```
[analyst@secOps ~]$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
ciao
HTTP/1.1 400 Bad Request
Server: nginx/1.12.2
Date: Thu, 05 Sep 2024 16:30:37 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/1.12.2</center>
</body>
</html>
Connection closed by foreign host.
[analyst@secOps ~]$
```

Dato che **nginx** era realmente in ascolto su **IP 127.0.0.1 e porta 80**, abbiamo ricevuto un errore perché le lettere digitate per lui non hanno alcun senso. Inoltre abbiamo appreso, grazie a quel messaggio varie cose: la versione di nginx (**1.12.2**), il fatto che fosse realmente attivo un server.

Usando **telnet** proviamo a collegarci al servizio in ascolto sulla **porta 22**. Si tratta di **OpenSSHv7.7**.

```
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      304/sshd
```

```
[analyst@secOps ~]$ telnet 0.0.0.0 22
Trying 0.0.0.0...
Connected to 0.0.0.0.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.7
aaa
Protocol mismatch.
Connection closed by foreign host.
[analyst@secOps ~]$
```

Usiamo **telnet** per collegarci al servizio su **porta 68.**

```
udp        0      0 10.0.2.15:68            0.0.0.0:*                           224/systemd-network
```

La connessione è rifiutata perché **telnet** usa protocollo **TCP** mentre sulla **68** il servizio attivo usa protocollo **UDP**.

```
[analyst@secOps ~]$ telnet 10.0.2.15 68
Trying 10.0.2.15...
telnet: Unable to connect to remote host: Connection refused
[analyst@secOps ~]$
```

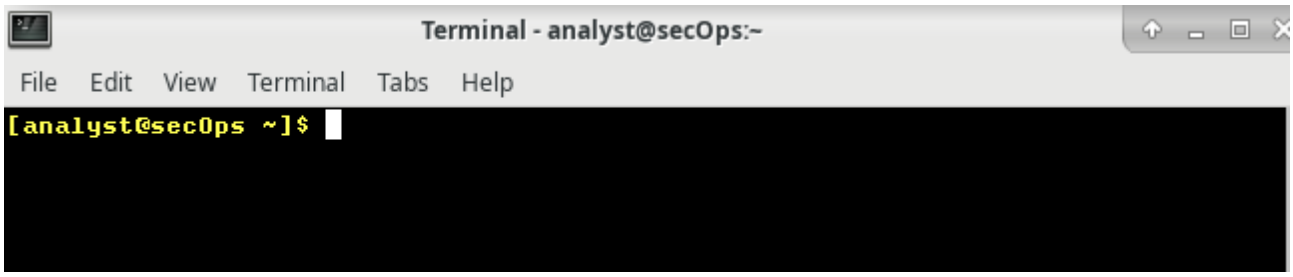
Netstat è uno strumento potente e comodo per avere sotto controllo tutte le connessioni attive sul sistema e le info che ci permettono di identificarle al meglio.

Telnet ci permette di ricavare ulteriori informazioni sui servizi di rete.

CYBEROPS - Navigating the Linux Filesystem and Permission Settings

- **Part 1: Exploring Filesystems in Linux**

Step 1: Access the command line



Step 2: Display the filesystems currently mounted

Il comando **lsblk** mostra tutti i **block devices** sul sistema corrente. **sda**, **sdb** e **sr0** sono dischi, mentre **sda1** e **sdb1** sono le partizioni dei dischi.

```
[analyst@secOps ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda       8:0    0   10G  0 disk
└─sda1    8:1    0   10G  0 part /
sdb       8:16   0    1G  0 disk
└─sdb1    8:17   0 1023M  0 part
sr0      11:0    1 1024M  0 rom
```

Il comando **mount** ci mostra tutti i filesystem del sistema.

```
[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=2015992k,nr_inodes=503998,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
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)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
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/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=32,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,p
ipe_ino=10658)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
configfs on /sys/kernel/config type configfs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=404332k,mode=700,uid=1000,gid=1000)
[analyst@secOps ~]$
```

Sulla partizione **sda1** si trova **il root filesystem (/).**

```
[analyst@secOps ~]$ mount | grep sda1
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
```

I file nella **root** del sistema sono salvati nella partizione **sda1**.

```
[analyst@secOps ~]$ cd /
[analyst@secOps /]$ ls -l
total 52
lrwxrwxrwx   1 root root     7 Jan  5  2018 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Apr 16  2018 boot
drwxr-xr-x  19 root root  3120 Sep  5 09:30 dev
drwxr-xr-x  58 root root  4096 Apr 17  2018 etc
drwxr-xr-x   3 root root  4096 Mar 20  2018 home
lrwxrwxrwx   1 root root     7 Jan  5  2018 lib -> usr/lib
lrwxrwxrwx   1 root root     7 Jan  5  2018 lib64 -> usr/lib
drwx------   2 root root 16384 Mar 20  2018 lost+found
drwxr-xr-x   2 root root  4096 Jan  5  2018 mnt
drwxr-xr-x   2 root root  4096 Jan  5  2018 opt
dr-xr-xr-x 131 root root     0 Sep  5 09:30 proc
drwxr-x---   8 root root  4096 Sep  3 10:43 root
drwxr-xr-x  17 root root   500 Sep  5 12:02 run
lrwxrwxrwx   1 root root     7 Jan  5  2018 sbin -> usr/bin
drwxr-xr-x   6 root root  4096 Mar 24  2018 srv
dr-xr-xr-x  13 root root     0 Sep  5 09:30 sys
drwxrwxrwt   8 root root   220 Sep  5 10:48 tmp
drwxr-xr-x   9 root root  4096 Apr 17  2018 usr
drwxr-xr-x  12 root root  4096 Apr 17  2018 var
```

Step 3: Manually mounting and unmounting filesystems

Controlliamo se la cartella **second_drive** sia vuota.

```
[analyst@secOps /]$ cd ~
[analyst@secOps ~]$ ls -l
total 6232
-rw-r--r-- 1 root    root       6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Sep  5 11:54 cyops_folder2
drwxr-xr-x 3 analyst analyst    4096 Sep  5 11:15 cyops_folder3
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 root    root     255772 Sep  3 11:22 httpdump.pcap
-rw-r--r-- 1 root    root    6079944 Sep  3 19:41 httpsdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
-rw-r--r-- 1 root    root          0 Sep  3 10:47 my_ftp_data
-rw-r--r-- 1 root    root          0 Sep  3 10:59 my_tftp_data
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst     142 Sep  5 11:46 some_text_file.txt
-rw-r--r-- 1 analyst analyst     253 Sep  5 09:32 space.txt
[analyst@secOps ~]$ mkdir second_drive
mkdir: cannot create directory 'second_drive': File exists
[analyst@secOps ~]$ ls -l second_drive/
total 0
[analyst@secOps ~]$
```

Abbiamo montato la partizione **/dev/sdb1** in **second_drive**. Adesso nella cartella compare tutto il contenuto della partizione appena montata.

```
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@secOps ~]$ ls -l second_drive/
total 20
drwx------ 2 root     root     16384 Mar 26  2018 lost+found
-rw-r--r-- 1 analyst analyst    183 Mar 26  2018 myFile.txt
[analyst@secOps ~]$
```

Visualizziamo i dettagli solo delle partizioni **/dev/sd*** con "**mount | grep /dev/sd**".

```
[analyst@secOps ~]$ mount | grep /dev/sd
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
/dev/sdb1 on /home/analyst/second_drive type ext4 (rw,relatime,data=ordered)
```

Dopo aver smontato la partizione **sdb1** la cartella **second_drive** sarà nuovamente vuota.

```
[analyst@secOps ~]$ sudo umount /dev/sdb1
[analyst@secOps ~]$ ls -l second_drive/
total 0
[analyst@secOps ~]$
```

- ## Part 2: File Permissions

Step 1: Visualize and Change the File Permissions

Visualizziamo i permessi dei files nella cartella **lab.support.files/scripts/.**

```
[analyst@secOps ~]$ cd lab.support.files/scripts/
[analyst@secOps scripts]$ ls -l
total 60
-rwxr-xr-x 1 analyst analyst  952 Mar 21  2018 configure_as_dhcp.sh
-rwxr-xr-x 1 analyst analyst 1153 Mar 21  2018 configure_as_static.sh
-rwxr-xr-x 1 analyst analyst 3459 Mar 21  2018 cyberops_extended_topo_no_fw.py
-rwxr-xr-x 1 analyst analyst 4062 Mar 21  2018 cyberops_extended_topo.py
-rwxr-xr-x 1 analyst analyst 3669 Mar 21  2018 cyberops_topo.py
-rw-r--r-- 1 analyst analyst 2871 Mar 21  2018 cyops.mn
-rwxr-xr-x 1 analyst analyst  458 Mar 21  2018 fw_rules
-rwxr-xr-x 1 analyst analyst   70 Mar 21  2018 mal_server_start.sh
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 net_configuration_files
-rwxr-xr-x 1 analyst analyst   65 Mar 21  2018 reg_server_start.sh
-rwxr-xr-x 1 analyst analyst  189 Mar 21  2018 start_ELK.sh
-rwxr-xr-x 1 analyst analyst   85 Mar 21  2018 start_miniedit.sh
-rwxr-xr-x 1 analyst analyst   76 Mar 21  2018 start_pox.sh
-rwxr-xr-x 1 analyst analyst  106 Mar 21  2018 start_snort.sh
-rwxr-xr-x 1 analyst analyst   61 Mar 21  2018 start_tftpd.sh
```

Ad esempio, il proprietario (**owner**) di **cyops.mn** è l'utente **analyst** e il suo gruppo **analyst**.

Nella prima colonna abbiamo i permessi sul file:

"-" Indica che è un file

"rw-" indica che utente **analyst** ha accesso in scrittura e lettura

“r- -" indica che il gruppo **analyst** ha l’accesso in lettura

“r- -“ indica che chiunque altro ha solo accesso in lettura

Nessuno ha permesso di esecuzione sul file.

Con **touch** creiamo da zero un nuovo file. Ma nella cartella **/mnt** serve il permesso di **root** per farlo.

```
[analyst@secOps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
[analyst@secOps scripts]$
```

Qui si vede con il comando “**ls -ld /mnt**”. Lo switch “**-d**” mostra i permessi della directory padre, ovvero **/mnt**. Qui si vede che **/mnt** è una cartella su cui solo l’**utente root** può avere permesso di **lettura, scrittura e esecuzione**. Gli utenti del **gruppo root** solo **lettura** ed **esecuzione**. Tutti gli altri hanno solo permessi di **esecuzione**. Quindi per usare **touch** dovremmo usare **sudo**.

```
[analyst@secOps scripts]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan  5  2018 /mnt
[analyst@secOps scripts]$
```

Montiamo **sdb1** in **second_drive** come in precedenza. E mostriamo il suo contenuto. Vediamo i permessi del file **myFile.txt**: **-rw-rw-r-x**.

```
[analyst@secOps scripts]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@secOps scripts]$ cd ~/second_drive/
[analyst@secOps second_drive]$ ls -l
total 20
drwx------ 2 root     root     16384 Mar 26  2018 lost+found
-rw-r--r-- 1 analyst analyst    183 Mar 26  2018 myFile.txt
[analyst@secOps second_drive]$
```

Con il comando “**sudo chmod 665 myFile.txt**” modifichiamo i permessi del file. I permessi sono cambiati: **-rw-rw-r-x**.

```
[analyst@secOps second_drive]$ sudo chmod 665 myFile.txt
[analyst@secOps second_drive]$ ls -l
total 20
drwx------ 2 root     root     16384 Mar 26  2018 lost+found
-rw-rw-r-x 1 analyst analyst    183 Mar 26  2018 myFile.txt
[analyst@secOps second_drive]$
```

Il comando **chmod** cambia i permessi usando il formato **ottale**. 6 in binario è 110 e 5 è 101.

Quindi sarebbe:

utente → 110 → rw-

gruppo → 110 → rw-

altri → 101 → r-x

Col comando **“sudo chmod 777 myFile.tx”** si darebbero tutti i permessi a chiunque abbia accesso al file.

Con “**sudo chown analyst myFile.txt**” si cambia il proprietario del file. Per modificare sia l’utente che il gruppo si può usare il comando **sudo chown analyst:analyst myFile.txt.**

```
[analyst@secOps second_drive]$ sudo chown analyst myFile.txt
[sudo] password for analyst:
[analyst@secOps second_drive]$ ls -l
total 20
drwx------ 2 root     root     16384 Mar 26  2018 lost+found
-rw-rw-r-x 1 analyst analyst    183 Mar 26  2018 myFile.txt
```

Possiamo quindi scrivere tranquillamente dentro il file dato che siamo l’utente analyst.

```
[analyst@secOps second_drive]$ echo test >> myFile.txt
[analyst@secOps second_drive]$ cat second_drive/myFile.txt
cat: second_drive/myFile.txt: No such file or directory
[analyst@secOps second_drive]$ cat myFile.txt
This is a file stored in the /dev/sdb1 disk.
Notice that even though this file has been sitting in this disk for a while, it
couldn't be accessed until the disk was properly mounted.
test
[analyst@secOps second_drive]$
```

Step 2: Directory and Permissions

La lettera “**d**” all’inizio dei permessi indica che quella risorsa è una cartella. **chown** e **chmod** funzionano anche sulle cartelle.

```
-rw-r--r-- 1 analyst analyst    255 Mar 21  2018 letter_to_grandma.txt
-rw-r--r-- 1 analyst analyst  24464 Mar 21  2018 logstash_tutorial.log
drwxr-xr-x 2 analyst analyst   4096 Mar 21  2018 malware
-rwxr-xr-x 1 analyst analyst    172 Mar 21  2018 mininet_services
drwxr-xr-x 2 analyst analyst   4096 Mar 21  2018 openssl_lab
```

- **Part 3: Symbolic Links and other Special File Types**

b → block files

c → character device

l → symbolic link

```
[analyst@secOps lab.support.files]$ ls -l /dev
total 0
crw-r--r--  1 root root      10, 235 Sep  6 10:19 autofs
drwxr-xr-x  2 root root          140 Sep  6 10:19 block
drwxr-xr-x  2 root root          100 Sep  6 10:19 bsg
crw-------  1 root root      10, 234 Sep  6 10:19 btrfs-control
drwxr-xr-x  3 root root           60 Sep  6 10:19 bus
lrwxrwxrwx  1 root root            3 Sep  6 10:19 cdrom -> sr0
drwxr-xr-x  2 root root         2820 Sep  6 10:19 char
crw-------  1 root root       5,   1 Sep  6 10:19 console
lrwxrwxrwx  1 root root           11 Sep  6 10:19 core -> /proc/kcore
crw-------  1 root root      10,  61 Sep  6 10:19 cpu_dma_latency
crw-------  1 root root      10, 203 Sep  6 10:19 cuse
drwxr-xr-x  6 root root          120 Sep  6 10:19 disk
drwxr-xr-x  3 root root          100 Sep  6 10:19 dri
crw-rw----  1 root video     29,   0 Sep  6 10:19 fb0
lrwxrwxrwx  1 root root           13 Sep  6 10:19 fd -> /proc/self/fd
crw-rw-rw-  1 root root       1,   7 Sep  6 10:19 full
crw-rw-rw-  1 root root      10, 229 Sep  6 10:19 fuse
crw-------  1 root root     245,   0 Sep  6 10:19 hidraw0
crw-rw----  1 root audio     10, 228 Sep  6 10:19 hpet
drwxr-xr-x  2 root root            0 Sep  6 10:19 hugepages
lrwxrwxrwx  1 root root           25 Sep  6 10:19 initctl -> /run/systemd/initc
tl/fifo
drwxr-xr-x  4 root root          360 Sep  6 10:19 input
crw-r--r--  1 root root       1,  11 Sep  6 10:19 kmsg
drwxr-xr-x  2 root root           60 Sep  6 10:19 lightnvm
lrwxrwxrwx  1 root root           28 Sep  6 10:19 log -> /run/systemd/journal/d
ev-log
crw-rw----  1 root disk      10, 237 Sep  6 10:19 loop-control
drwxr-xr-x  2 root root           60 Sep  6 10:19 mapper
crw-r-----  1 root kmem       1,   1 Sep  6 10:19 mem
crw-------  1 root root      10,  58 Sep  6 10:19 memory_bandwidth
drwxrwxrwt  2 root root           40 Sep  6 10:19 mqueue
drwxr-xr-x  2 root root           60 Sep  6 10:19 net
crw-------  1 root root      10,  60 Sep  6 10:19 network_latency
crw-------  1 root root      10,  59 Sep  6 10:19 network_throughput
crw-rw-rw-  1 root root       1,   3 Sep  6 10:19 null
crw-r-----  1 root kmem       1,   4 Sep  6 10:19 port
crw-------  1 root root     108,   0 Sep  6 10:19 ppp
crw-------  1 root root      10,   1 Sep  6 10:19 psaux
crw-rw-rw-  1 root tty        5,   2 Sep  6 10:32 ptmx
drwxr-xr-x  2 root root            0 Sep  6 10:19 pts
crw-rw-rw-  1 root root       1,   8 Sep  6 10:19 random
lrwxrwxrwx  1 root root            4 Sep  6 10:19 rtc -> rtc0
crw-rw----  1 root audio     250,   0 Sep  6 10:19 rtc0
brw-rw----  1 root disk       8,   0 Sep  6 10:19 sda
brw-rw----  1 root disk       8,   1 Sep  6 10:19 sda1
brw-rw----  1 root disk       8,  16 Sep  6 10:19 sdb
brw-rw----  1 root disk       8,  17 Sep  6 10:19 sdb1
drwxrwxrwt  2 root root           40 Sep  6 10:19 shm
crw-------  1 root root      10, 231 Sep  6 10:19 snapshot
drwxr-xr-x  3 root root          180 Sep  6 10:19 snd
```

Vediamo qui le differenze tra **hard link** e **soft link**. Il primo viene indicato come fosse un **file** mentre il secondo è palesemente un **collegamento** al file reale. Un **hard link** è di fatto un **puntatore** alla zona di memoria del **file** e quindi se il file venisse eliminato lo si potrebbe comunque aprire tramite l'**hard link**.

```
[analyst@secOps ~]$ echo "symbolic" > file1.txt
[analyst@secOps ~]$ ls
capture.pcap   Desktop    httpdump.pcap      myFile.txt    second_drive
cyops_folder2  Downloads  httpsdump.pcap     my_ftp_data   some_text_file.txt
cyops_folder3  file1.txt  lab.support.files  my_tftp_data  space.txt
[analyst@secOps ~]$ cat file1.txt
symbolic
[analyst@secOps ~]$ echo "hard" > file2.txt
[analyst@secOps ~]$ cat file2.txt
hard
[analyst@secOps ~]$ ln -s file1.txt file1symbolic
ln: target 'file1symbolic' is not a directory
[analyst@secOps ~]$ ln -s file1.txt file1symbolic
[analyst@secOps ~]$ ln file2.txt file2hard
[analyst@secOps ~]$ ls -l
total 6248
-rw-r--r-- 1 root     root        6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst     4096 Sep  5 11:54 cyops_folder2
drwxr-xr-x 3 analyst analyst     4096 Sep  5 11:15 cyops_folder3
drwxr-xr-x 2 analyst analyst     4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst     4096 Mar 22  2018 Downloads
lrwxrwxrwx 1 analyst analyst        9 Sep  6 10:38 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst analyst        9 Sep  6 10:37 file1.txt
-rw-r--r-- 2 analyst analyst        5 Sep  6 10:38 file2hard
-rw-r--r-- 2 analyst analyst        5 Sep  6 10:38 file2.txt
-rw-r--r-- 1 root     root      255772 Sep  3 11:22 httpdump.pcap
```

Modificando i nomi infatti il **symlink** non funziona mentre l'**hard link** si**.**

```
[analyst@secOps ~]$ mv file1.txt file1new.txt
[analyst@secOps ~]$ mv file2.txt file2new.txt
[analyst@secOps ~]$ ls -l
total 6248
-rw-r--r-- 1 root     root        6679 Sep  3 07:36 capture.pcap
drwxr-xr-x 2 analyst analyst     4096 Sep  5 11:54 cyops_folder2
drwxr-xr-x 3 analyst analyst     4096 Sep  5 11:15 cyops_folder3
drwxr-xr-x 2 analyst analyst     4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst     4096 Mar 22  2018 Downloads
-rw-r--r-- 1 analyst analyst        9 Sep  6 10:37 file1new.txt
lrwxrwxrwx 1 analyst analyst        9 Sep  6 10:38 file1symbolic -> file1.txt
-rw-r--r-- 2 analyst analyst        5 Sep  6 10:38 file2hard
-rw-r--r-- 2 analyst analyst        5 Sep  6 10:38 file2new.txt
-rw-r--r-- 1 root     root      255772 Sep  3 11:22 httpdump.pcap
-rw-r--r-- 1 root     root     6079944 Sep  3 19:41 httpsdump.pcap
drwxr-xr-x 9 analyst analyst     4096 Jul 19  2018 lab.support.files
-rw-r--r-- 1 analyst analyst        5 Sep  6 10:23 myFile.txt
-rw-r--r-- 1 root     root           0 Sep  3 10:47 my_ftp_data
-rw-r--r-- 1 root     root           0 Sep  3 10:59 my_tftp_data
drwxr-xr-x 3 root     root        4096 Mar 26  2018 second_drive
-rw-r--r-- 1 analyst analyst      142 Sep  5 11:46 some_text_file.txt
-rw-r--r-- 1 analyst analyst      253 Sep  5 09:32 space.txt
[analyst@secOps ~]$ cat file1symbolic
cat: file1symbolic: No such file or directory
[analyst@secOps ~]$ cat file2hard
hard
[analyst@secOps ~]$
```