

S11/L4

Parte 1 – Editor di Testo Grafici

1. Ho aperto SciTE dalla GUI

- Effettua il login sulla VM come utente **analyst** password **cyberops**.
- Dal menu superiore: **Applications => CyberOPS => SciTE**.
- Comparirà l'editor SciTE in modalità grafica.

2. Ho creato e salvato space.txt

- “Lo spazio, è grande. Veramente grande. Semplicemente non crederesti quanto vastamente, enormemente, sbalorditivamente grande sia. Voglio dire, potresti pensare che sia lunga la strada fino alla farmacia, ma quella è solo una bazzecola rispetto allo spazio.”
— Douglas Adams, *Guida galattica per gli autostoppisti*
- File => Save, nome file **space.txt** (si salva in /home/analyst).

3. Riaprire SciTE e cercare space.txt

- File => Open
 - **Domanda:** Sei riuscito a trovare subito space.txt?
Risposta: No. SciTE di default mostra solo estensioni “note” => .txt non è tra queste, quindi non appare fino a che non si seleziona “All Files (*)” nel menu filtro dei tipi di file.

4. Aprire SciTE da terminale

- Ho aperto il Terminale
- Ho digitato `ls` → space.txt.
- Ho digitato `scite space.txt`.
 - Il prompt non riappare fino a che SciTE non viene chiuso: ciò avviene perché SciTE è eseguito in foreground, bloccando il terminale finché non termina. Per riavere il prompt, ho chiuso SciTE o premi **Ctrl +C** nel terminale.

Parte 2 – Editor di Testo da Riga di Comando

1. Aprire space.txt con nano

- Nel terminale: `nano space.txt`.

- Il testo appare troncato perché non c'è il wrapping automatico.
- **Domanda:** Quale carattere usa nano per rappresentare che una linea continua oltre i bordi dello schermo?
Risposta: Nano mostra il simbolo \neg (segmento spezzato) alla fine della riga per indicare che la linea continua oltre il margine.

2. Uscire da nano

- **Ctrl + X** → ci chiede se vogliamo salvare (Y o N), poi **Invio** per la conferma.

Parte 3 – Lavorare con i File di Configurazione

3.1 Localizzare i file di configurazione

1. Nella home user

- **ls -l** mostra solo file visibili; molti file di configurazione utente sono nascosti.
- **ls -la** elenca anche i nascosti. es: `.bashrc` - `.bash_profile` - `.bash_history`.

2. Visualizzare `.bashrc`

- **cat .bashrc** → contiene variabili d'ambiente, prompt, alias, ecc.

3. In `/etc`

- **ls /etc** → file di configurazione di sistema (es. `bash.bashrc`, `nginx/`, `ssh/`, ecc.).
- **cat /etc/bash.bashrc** → configurazione di default per tutti gli utenti.
- **Domanda:** Perché i file di configurazione delle applicazioni utente sono salvati nella home e non sotto `/etc`?
Risposta: I file sotto `/etc` richiedono permessi di root per essere modificati e per permettere all'utente normale di personalizzare la propria shell o applicazioni senza privilegi elevati, si usano file nascosti nella home dell'utente.

3.2 Modificare e salvare `.bashrc`

1. Con SciTE

- SciTE non mostra i file nascosti: in **Open** seleziona “All Files (*)” ed ho aperto `.bashrc`.
- Sostituisci **32** (verde) con **31** (rosso) nel codice di escape.
- Salva e chiudi.
- Riapri il terminale: il prompt diventa rosso.

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

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

- **Domanda:** Anche la finestra di terminale già aperta cambia colore?
Risposta: No, quella già aperta carica `.bashrc` al login. Per aggiornare l'attuale, bisogna aprire un nuovo terminale.

2. Con nano

- **nano .bashrc**, ho modificato il 31(rosso) → 33 (giallo).
- Ctrl + X, Y ed invio per la conferma.
- Ho ricaricato il bash ed il prompt diventa giallo.

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

3.3 Modificare configurazione di nginx

1. Ho aperto il file

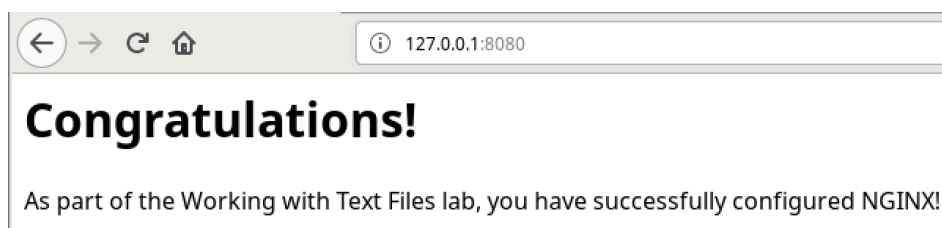
- `sudo nano -l /etc/nginx/custom_server.conf`

2. Modifiche

- Riga 39: `listen 81` → `listen 8080`;
- Riga 47: `root /usr/share/nginx/html/` → `root /usr/share/nginx/html/text_ed_lab/`
- Ctrl + X, Y ed invio per la conferma.

3. Avviare nginx

- `sudo nginx -c /etc/nginx/custom_server.conf`
- Ho aperto Firefox e visitato **127.0.0.1:8080**.



- **Domanda:** A cosa si riferisce il messaggio di errore?
Risposta: Il messaggio indica che non è stato possibile eseguire il binding sulla porta 8080 perché è già in uso (spesso un altro processo nginx di default è attivo).

4. Arrestare nginx

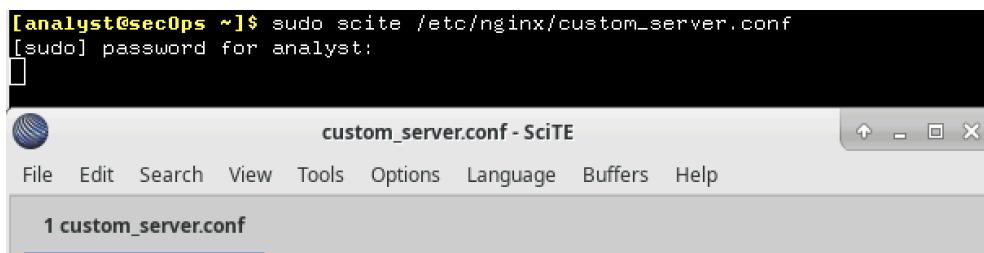
- Ho premuto **Invio** per tornare al prompt, poi `sudo pkill nginx`.
- Ricarica la pagina: la homepage non appare più.

3.4 Domanda Sfida

Puoi modificare `/etc/nginx/custom_server.conf` con SciTE? Descrivi il processo.

Sì, SciTE deve essere eseguito con i permessi di root ad esempio:

`sudo scite /etc/nginx/custom_server.conf`



BONUS – Prendere Familiarità con la Shell Linux

Parte 1 – Basi della Shell

1. Pagine manuale

- **man man** → sezioni: NAME, SYNOPSIS, DESCRIPTION, OPTIONS, SEE ALSO, etc.
- **man cp** → il comando **cp** copia file (source → destination).
- **Domanda:** Qual è la funzione di **pwd** e come trovare info?
Risposta: **pwd** stampa il percorso della directory corrente.

2. Ho creato e cambiato le directory

- **pwd** → `/home/analyst`.
- **ls -l** → elenco dettagliato.
- **mkdir cyops_folder1 - cyops_folder2 - cyops_folder3.**

```
[analyst@sec0ps ~]$ mkdir cyops_folder1
[analyst@sec0ps ~]$ mkdir cyops_folder2
[analyst@sec0ps ~]$ mkdir cyops_folder3
[analyst@sec0ps ~]$ ls -l
total 40
-rw-r--r-- 1 root    root      5043 Jun 10 08:20 capture.pcap
drwxr-xr-x 2 analyst analyst 4096 Jun 12 08:57 cyops_folder1
drwxr-xr-x 2 analyst analyst 4096 Jun 12 08:57 cyops_folder2
drwxr-xr-x 2 analyst analyst 4096 Jun 12 08:57 cyops_folder3
```

- **cd cyops_folder3** → ora si è in /home/analyst/cyops_folder3.
- **Sfida: cd ~** → tilde ~ è l'alias per la home riportando in /home/analyst.

3. Percorsi relativi e speciali

- **ls -la** in **cyops_folder3** mostra (directory corrente) e (genitore).
- **cd .** → resta nella stessa directory.
- **cd ..** → risale di un livello (es. da /home/analyst/cyops_folder3 a /home/analyst).

```
cyops_folder4
```

4. Redirezione output

- **echo "fare echo"** → stampa su schermo.
- **echo "fare echo" > file.txt** → nessun output a schermo (viene creato o sovrascritto file.txt).
 - **Domanda:** È previsto?
 - Sì: => redirige stdout nel file, non c'è più output su terminale.

```
[analyst@secOps ~]$ echo "fare eco"
fare eco
[analyst@secOps ~]$
```

- **echo "fare echo" > file.txt** → sovrascrive completamente il file.
 - **Domanda:** Cosa succede? Il contenuto precedente viene cancellato.
- **echo "ancora una riga" >> file.txt** → accoda alla fine mantenendo il contenuto precedente.

```
[analyst@secOps ~]$ cat file.txt
fare eco
fare eco
```

5. File nascosti

- **ls -l** in home mostra solo file “visibili”.
 - Esempio: 5 elementi.
- **ls -la** mostra anche i nascosti ad esempio:
.bashrc - .cache - .bash_history - .bash_profile - .gnupg - etc.
 - Aggiunge tipicamente dalle 10 voci in più.
- Sì, è possibile nascondere directory antepoendo un punto (es..**mydir**).

Parte 2 – Copiare, Eliminare e Spostare File

1. Ho copiato il file

- **cp some_text_file.txt cyops_folder2/**
 - **Parametri:** sorgente /home/analyst/some_text_file.txt, destinazione /home/analyst/cyops_folder2/.
- Ho verificato con **ls cyops_folder2/** e **ls -l**.

```
[analyst@secOps ~]$ cp file.txt cyops_folder2/
[analyst@secOps ~]$ ls cyops_folder2/
file.txt
[analyst@secOps ~]$ ls -l
total 44
-rw-r--r-- 1 root    root      5043 Jun 10 08:20 capture.pcap
drwxr-xr-x 2 analyst analyst  4096 Jun 12 08:57 cyops_folder1
drwxr-xr-x 2 analyst analyst  4096 Jun 12 09:24 cyops_folder2
drwxr-xr-x 3 analyst analyst  4096 Jun 12 09:02 cyops_folder3
drwxr-xr-x 2 analyst analyst  4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst  4096 Jan 31 05:11 Downloads
-rw-r--r-- 1 analyst analyst    18 Jun 12 09:12 file.txt
drwxr-xr-x 9 analyst analyst  4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst analyst  4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst   256 Jun 12 08:18 space.txt
[analyst@secOps ~]$
```

2. Ho eliminato il file

- **rm file.txt** → rimuove il file.
- **rm -r cyops_folder1** → rimuove ricorsivamente directory e contenuti.

```
[analyst@secOps ~]$ rm file.txt
```

```
[analyst@secOps ~]$ ls -l
total 40
-rw-r--r-- 1 root    root    5043 Jun 10 08:20 capture.pcap
drwxr-xr-x 2 analyst analyst 4096 Jun 12 08:57 cyops_folder1
drwxr-xr-x 2 analyst analyst 4096 Jun 12 09:24 cyops_folder2
drwxr-xr-x 3 analyst analyst 4096 Jun 12 09:02 cyops_folder3
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Jan 31 05:11 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst  256 Jun 12 08:18 space.txt
[analyst@secOps ~]$
```

```
[analyst@secOps ~]$ rm -r cyops_folder1
[analyst@secOps ~]$ ls -l
total 36
-rw-r--r-- 1 root    root    5043 Jun 10 08:20 capture.pcap
drwxr-xr-x 2 analyst analyst 4096 Jun 12 09:24 cyops_folder2
drwxr-xr-x 3 analyst analyst 4096 Jun 12 09:02 cyops_folder3
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Jan 31 05:11 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst  256 Jun 12 08:18 space.txt
[analyst@secOps ~]$
```

3. Ho spostato il file

- `mv cyops_folder2/file.txt .` → sposta il file nella directory corrente.

```
[analyst@secOps ~]$ mv cyops_folder2/file.txt .
[analyst@secOps ~]$ ls -l
total 40
-rw-r--r-- 1 root    root    5043 Jun 10 08:20 capture.pcap
drwxr-xr-x 2 analyst analyst 4096 Jun 12 09:47 cyops_folder2
drwxr-xr-x 3 analyst analyst 4096 Jun 12 09:02 cyops_folder3
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Jan 31 05:11 Downloads
-rw-r--r-- 1 analyst analyst  18 Jun 12 09:24 file.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst  256 Jun 12 08:18 space.txt
[analyst@secOps ~]$
```

- **Domanda:** Quale comando hai usato?

Risposta: `mv cyops_folder2/file.txt .`

Riflessione

- **Vantaggi della CLI Linux:**
 - **Remoto:** si lavora via SSH su server headless.
 - **Velocità:** operazioni rapide con pochi comandi.
 - **Scriptabilità:** automazione di attività ripetitive con script.
 - **Controllo preciso:** opzioni granulari per ogni comando.
 - **Ridotte risorse:** richiede meno overhead rispetto a GUI.