

Esplorazione dei Filesystem in Linux

Questa parte dell'attività ha approfondito la gestione e il montaggio dei filesystem nel sistema operativo Linux, in particolare utilizzando il filesystem ext4. L'obiettivo principale è stato esplorare come Linux riconosce e gestisce le unità di memoria.

1. **Avvio del Terminale e Visualizzazione dei Filesystem Montati:** Dopo aver avviato il terminale sulla VM CyberOps Workstation, è stato utilizzato il comando `lsblk` per elencare i dispositivi di blocco presenti. Il risultato ha mostrato tre dispositivi: `sda`, `sdb` e `sr0`, dove `sda` e `sdb` sono dischi rigidi, ognuno con una singola partizione (`sda1` e `sdb1` rispettivamente). Si è quindi usato il comando `mount` per visualizzare i dettagli sui filesystem montati, con particolare attenzione al filesystem radice (`/`), montato su `/dev/sda1` e formattato in ext4.
2. **Montaggio Manuale e Smontaggio di Filesystem:** È stato montato manualmente il filesystem `/dev/sdb1` sulla directory `second_drive` nella home dell'utente. Utilizzando `mount`, è stato confermato che `/dev/sdb1` fosse correttamente montato. Successivamente, è stato utilizzato il comando `umount` per smontare il filesystem, riportando la directory `second_drive` al suo stato iniziale.

Part 2: Permessi sui File

Nella seconda parte dell'attività, è stata esplorata la gestione dei permessi sui file, che in Linux vengono rappresentati da un set di definizioni che specificano cosa possono fare gli utenti e i gruppi con un determinato file.

1. **Visualizzazione dei Permessi sui File:** Dopo essersi spostati nella directory `/home/analyst/lab.support.files/scripts/`, è stato utilizzato `ls -l` per elencare i file presenti e i relativi permessi. Ad esempio, per il file `cyops.mn`, i permessi erano `-rw-r--r--`, indicando che l'utente proprietario `analyst` può leggere e scrivere sul file, mentre altri utenti possono solo leggerlo.
2. **Creazione di File e Permessi delle Directory:** È stato tentato di creare un file vuoto nella directory `/mnt` utilizzando `touch`, ma l'operazione è fallita a causa dei permessi della directory, posseduta dall'utente `root`. Per eseguire correttamente l'operazione, è stato necessario specificare i permessi di scrittura tramite `sudo` o modificare i permessi della directory `/mnt`.

In sintesi, questa attività ha fornito un'esperienza pratica su come Linux gestisce i filesystem e implementa i permessi, consentendo di comprendere meglio la sicurezza e la gestione dei file e delle directory nel sistema operativo Linux.

Linux Filesystem e Settaggio Permessi

Part 1: Exploring Filesystems in Linux

1. Visualizza dispositivi a blocchi

Comando: **lsblk** mostra i dispositivi: **sr0**, **sda** (10GB) e **sdb** (1GB).

2. Visualizza filesystem montati

Comando: **mount** per elencare i filesystem montati.

```
[analyst@sec0ps ~]$ 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

[analyst@sec0ps ~]$ 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=4080288K,nr_inodes=1020072,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,nodelegate)
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/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
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/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
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/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=35,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=10124)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
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)
configfs on /sys/kernel/config type configfs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=817192K,mode=700,uid=1000,gid=1000)
[analyst@sec0ps ~]$ mount | grep sda1
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
```

3. Montaggio manuale di /dev/sdb1

Creazione della directory `second_drive` in `home/analyst`, montaggio di `/dev/sdb1`.

```
[analyst@sec0ps ~]$ cd /
[analyst@sec0ps /]$ 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 Oct 28 05:21 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 143 root root 0 Oct 28 05:21 proc
drwxr-x--- 7 root root 4096 Apr 17 2018 root
drwxr-xr-x 17 root root 480 Oct 28 05:21 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 Oct 28 05:21 sys
drwxrwxrwt 8 root root 200 Oct 28 05:21 tmp
drwxr-xr-x 9 root root 4096 Apr 17 2018 usr
drwxr-xr-x 12 root root 4096 Apr 17 2018 var
[analyst@sec0ps /]$ cd ~
[analyst@sec0ps ~]$ ls -l
total 16
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22 2018 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
[analyst@sec0ps ~]$ ls -l second_drive/
total 0
[analyst@sec0ps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@sec0ps ~]$ 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
```

4. Smontaggio del filesystem

Usa `umount` per smontare `/dev/sdb1`.

```
[analyst@secOps ~]$ sudo umount /dev/sdb1
```

Part 2: File Permissions

1. Verifica e modifica permessi file

Comando: `ls -l` su `cyops.mn` per verificare i permessi (proprietario: `analyst`, gruppo: `analyst`, permessi `-rw-r--r--`).

```
[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 mail_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
```

2. Modifica dei permessi della directory /mnt

Il comando `touch` fallisce su `/mnt` perché possiede permessi limitati (`drwxr-xr-x`).

3. Modifica permessi di myFile.txt

Comando: `chmod 665 myFile.txt` per settare i permessi a `-rw-rw-r-x`.

4. Cambio del proprietario del file

Comando `chown` per cambiare il proprietario del file `myFile.txt` a `root`.

```
[analyst@secOps scripts]$ sudo mount /dev/sdb1 ~/second_drive/
[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]$ sudo chmod 665 myFile.txt
[analyst@secOps second_drive]$ sudo chown analyst myFile.txt
[analyst@secOps second_drive]$ echo test >> myFile.txt
[analyst@secOps second_drive]$ cat myFile.txt
This is a file stored in the /dev/sdb1 disk.
```

Part 3: Symbolic Links and other Special File Types

1. Esame dei tipi di file

Comando: `ls -l` in `/home/analyst` per visualizzare file (indicati da `-`) e directory (indicate da `d`).

2. Creazione di symbolic e hard link

Comando `ln -s` per creare link simbolico a `file1.txt`, `ln` per link hard a `file2.txt`.

3. Effetti sui link dopo rinomina dei file originali

Comando: rinomina `file1.txt` e `file2.txt` per osservare i cambiamenti. Il link simbolico `file1symbolic` si rompe, mentre il link hard `file2hard` rimane funzionante.

```
[analyst@sec0ps ~]$ echo "symbolic" > file1.txt
[analyst@sec0ps ~]$ cat file1.txt
symbolic
[analyst@sec0ps ~]$ echo "hard" > file2.txt
[analyst@sec0ps ~]$ cat file2.txt
hard
[analyst@sec0ps ~]$ ln -s file1.txt file1symbolic
ln: target 'file1symbolic' is not a directory
[analyst@sec0ps ~]$ ln file2.txt file2hard
[analyst@sec0ps ~]$ ls -l
total 28
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 Oct 28 05:50 file1.txt
-rw-r--r-- 2 analyst analyst   5 Oct 28 05:51 file2hard
-rw-r--r-- 2 analyst analyst   5 Oct 28 05:51 file2.txt
drwxr-xr-x 9 analyst analyst 4096 Oct 28 05:48 lab.support.files
drwxr-xr-x 3 root      root    4096 Mar 26  2018 second_drive
[analyst@sec0ps ~]$ mv file1.txt file1new.txt
[analyst@sec0ps ~]$ mv file2.txt file2new.txt
[analyst@sec0ps ~]$ cat file1symbolic
cat: file1symbolic: No such file or directory
[analyst@sec0ps ~]$ cat file2hard
hard
```