

Project 2

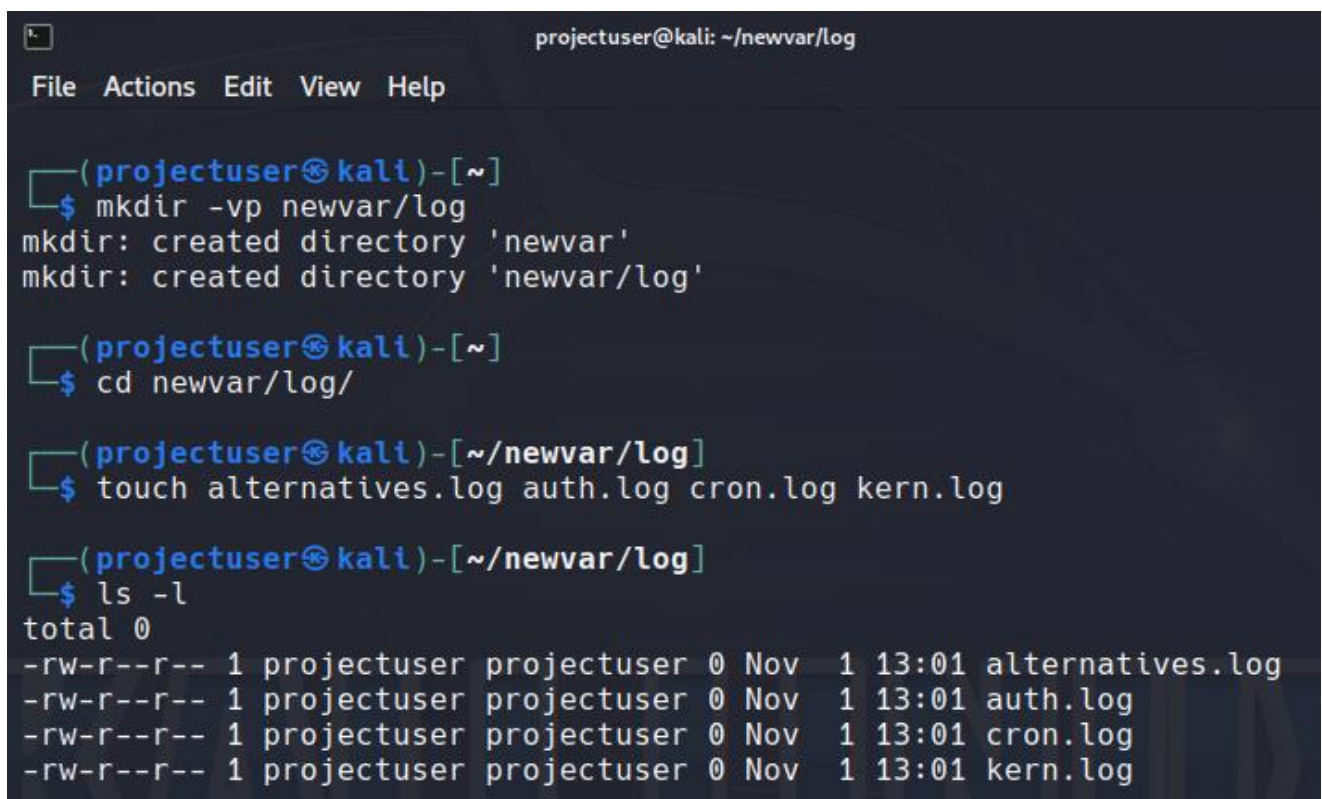
Log file archiving

Project description:

There is suspicious activity in the system, so I need to create and compress a log archive.

Steps:

- Create abstract log files:



```
projectuser@kali: ~/newvar/log
File Actions Edit View Help

(projectuser@kali)-[~]
$ mkdir -vp newvar/log
mkdir: created directory 'newvar'
mkdir: created directory 'newvar/log'

(projectuser@kali)-[~]
$ cd newvar/log/

(projectuser@kali)-[~/newvar/log]
$ touch alternatives.log auth.log cron.log kern.log

(projectuser@kali)-[~/newvar/log]
$ ls -l
total 0
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 alternatives.log
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 auth.log
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 cron.log
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 kern.log
```

- Create an archive for logs, and then view the result:

```
projectuser@kali: ~/newvar/log
File Actions Edit View Help

(projectuser@kali)-[~]
$ cd newvar/log

(projectuser@kali)-[~/newvar/log]
$ ls -l
total 0
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 alternatives.log
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 auth.log
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 cron.log
-rw-r--r-- 1 projectuser projectuser 0 Nov  1 13:01 kern.log

(projectuser@kali)-[~/newvar/log]
$ tar -cvf archive.tar *.log
alternatives.log
auth.log
cron.log
kern.log

(projectuser@kali)-[~/newvar/log]
$ tar -tf archive.tar
alternatives.log
auth.log
cron.log
kern.log

(projectuser@kali)-[~/newvar/log]
$ ls -l archive.tar
-rw-r--r-- 1 projectuser projectuser 10240 Nov  1 13:56 archive.tar
```

- Creating archive compression and deleting files (as well as an independent archive). View the result:

```
projectuser@kali: ~/newvar/log
File Actions Edit View Help

(projectuser@kali)-[~/newvar/log]
$ ls -l
total 16
-rw-r--r-- 1 projectuser projectuser 0 Nov 1 13:01 alternatives.log
-rw----- 1 projectuser projectuser 10240 Nov 1 13:56 archive.tar
-rw-r--r-- 1 projectuser projectuser 45 Nov 1 14:21 archive.tar.gz
-rw-r--r-- 1 projectuser projectuser 0 Nov 1 13:01 auth.log
-rw-r--r-- 1 projectuser projectuser 0 Nov 1 13:01 cron.log
-rw-r--r-- 1 projectuser projectuser 0 Nov 1 13:01 kern.log

(projectuser@kali)-[~/newvar/log]
$ tar -czf archive.tar.gz archive*

(projectuser@kali)-[~/newvar/log]
$ rm alternatives.log auth.log cron.log kern.log archive.tar

(projectuser@kali)-[~/newvar/log]
$ ls -l
total 4
-rw-r--r-- 1 projectuser projectuser 297 Nov 1 14:21 archive.tar.gz

(projectuser@kali)-[~/newvar/log]
$ gzip -l archive.tar.gz
              compressed      uncompressed   ratio uncompressed_name
                297             20480    98.6% archive.tar
```

- Change permissions for the compressed archive and the directory of the archive itself:

```
projectuser@kali: ~  
File Actions Edit View Help  
  
(projectuser@kali)-[~]  
$ ls -l  
total 16  
drwxrwx--T 2 eng-admin Engineering 4096 Oct 29 19:42 Engineering  
drwxrwx--T 2 is-admin IS 4096 Oct 29 19:42 IS  
drwxr-xr-x 3 projectuser projectuser 4096 Nov 1 13:01 newvar  
drwxrwx--T 2 sales-admin Sales 4096 Oct 29 19:42 Sales  
  
(projectuser@kali)-[~]  
$ chmod g-rwx,o-rwx newvar/log/  
  
(projectuser@kali)-[~]  
$ chmod g-rwx,o-rwx newvar  
  
(projectuser@kali)-[~]  
$ ls -l  
total 16  
drwxrwx--T 2 eng-admin Engineering 4096 Oct 29 19:42 Engineering  
drwxrwx--T 2 is-admin IS 4096 Oct 29 19:42 IS  
drwx----- 3 projectuser projectuser 4096 Nov 1 13:01 newvar  
drwxrwx--T 2 sales-admin Sales 4096 Oct 29 19:42 Sales  
  
(projectuser@kali)-[~]  
$ chmod u-x newvar/log/archive.tar.gz  
  
(projectuser@kali)-[~]  
$ ls -l newvar/log/archive.tar.gz  
-rw----- 1 projectuser projectuser 297 Nov 1 14:21 newvar/log/archive.tar.gz  
  
(projectuser@kali)-[~]  
$
```

Summary:

Abstract log files have been created. The files were placed in an archive that was compressed. The archive and directory permissions have been changed.