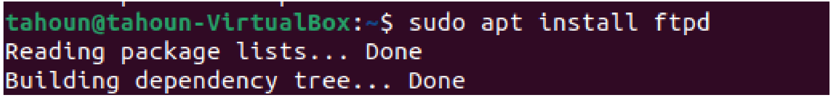
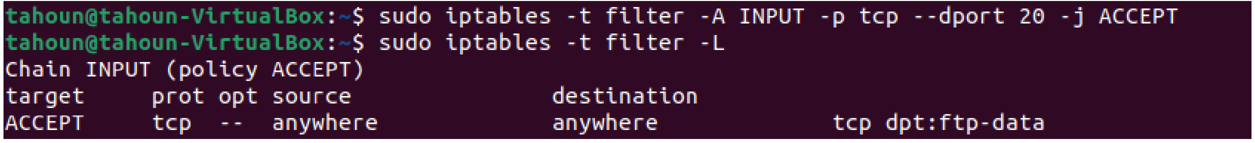
Lab 3

1- Install `ftpd` service on your laptop

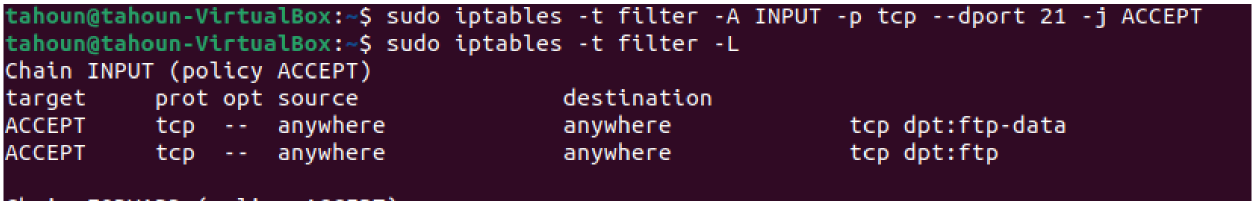


```
tahoun@tahoun-VirtualBox:~$ sudo apt install ftpd
Reading package lists... Done
Building dependency tree... Done
```

2- enable port 21 and 20 (tcp) using `iptables` command using `INPUT` chain

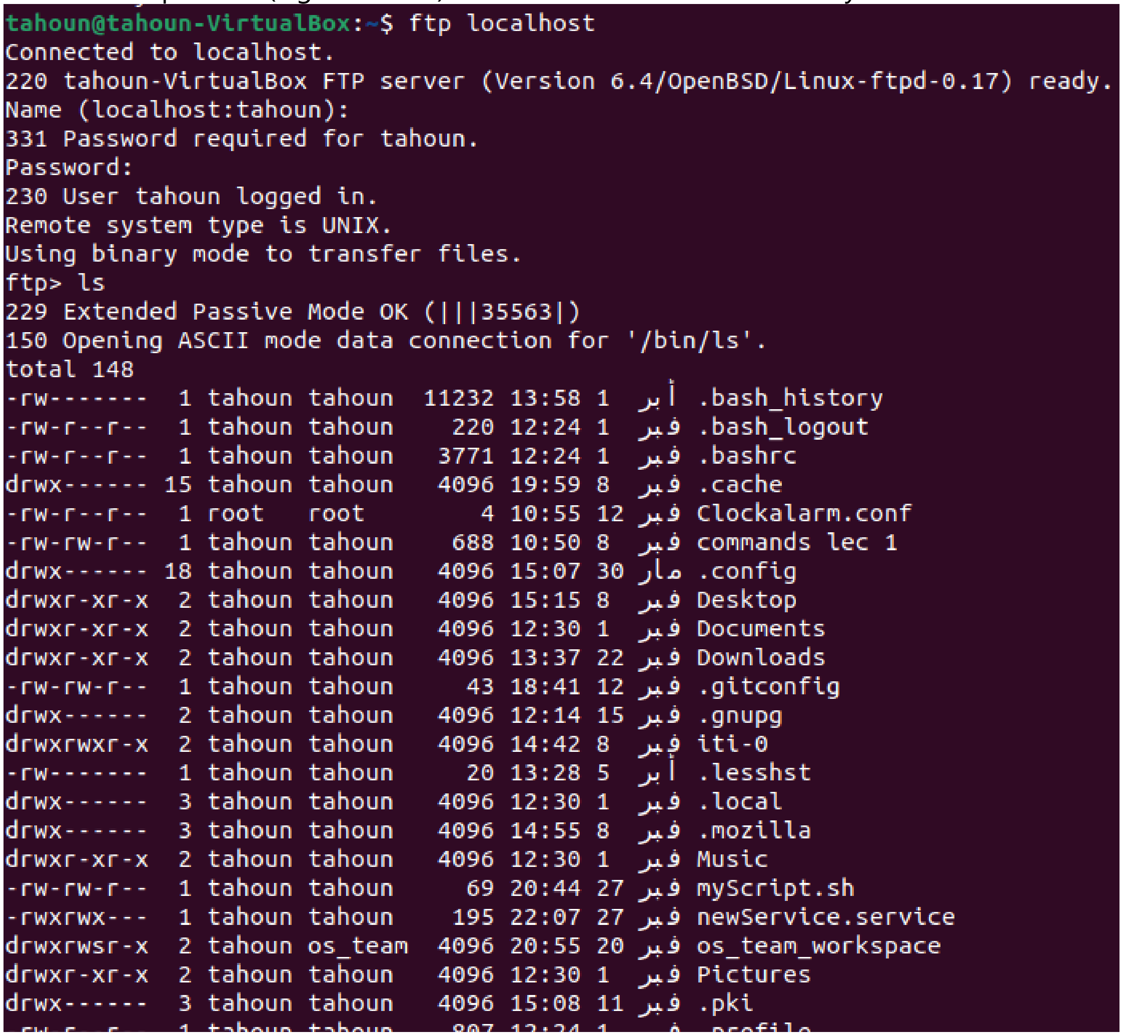


```
tahoun@tahoun-VirtualBox:~$ sudo iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
tahoun@tahoun-VirtualBox:~$ sudo iptables -t filter -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp-data
```



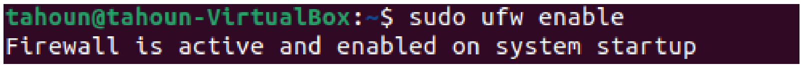
```
tahoun@tahoun-VirtualBox:~$ sudo iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
tahoun@tahoun-VirtualBox:~$ sudo iptables -t filter -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp-data
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp
```

3- connect to ftp server (e.g: localhost) and browse the current directory



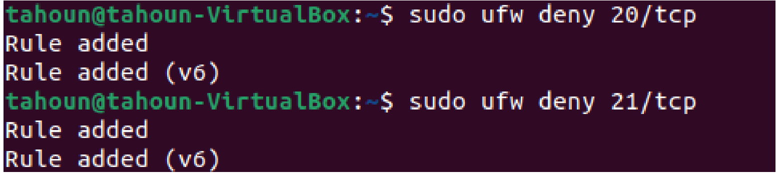
```
tahoun@tahoun-VirtualBox:~$ ftp localhost
Connected to localhost.
220 tahoun-VirtualBox FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
Name (localhost:tahoun):
331 Password required for tahoun.
Password:
230 User tahoun logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Extended Passive Mode OK (|||35563|)
150 Opening ASCII mode data connection for '/bin/ls'.
total 148
-rw-------  1 tahoun tahoun  11232 13:58 1  أبر .bash_history
-rw-r--r--  1 tahoun tahoun    220 12:24 1  فبر .bash_logout
-rw-r--r--  1 tahoun tahoun   3771 12:24 1  فبر .bashrc
drwx------ 15 tahoun tahoun   4096 19:59 8  فبر .cache
-rw-r--r--  1 root   root        4 10:55 12 فبر Clockalarm.conf
-rw-rw-r--  1 tahoun tahoun    688 10:50 8  فبر commands lec 1
drwx------ 18 tahoun tahoun   4096 15:07 30 مار .config
drwxr-xr-x  2 tahoun tahoun   4096 15:15 8  فبر Desktop
drwxr-xr-x  2 tahoun tahoun   4096 12:30 1  فبر Documents
drwxr-xr-x  2 tahoun tahoun   4096 13:37 22 فبر Downloads
-rw-rw-r--  1 tahoun tahoun     43 18:41 12 فبر .gitconfig
drwx------  2 tahoun tahoun   4096 12:14 15 فبر .gnupg
drwxrwxr-x  2 tahoun tahoun   4096 14:42 8  فبر iti-0
-rw-------  1 tahoun tahoun     20 13:28 5  أبر .lesshst
drwx------  3 tahoun tahoun   4096 12:30 1  فبر .local
drwx------  3 tahoun tahoun   4096 14:55 8  فبر .mozilla
drwxr-xr-x  2 tahoun tahoun   4096 12:30 1  فبر Music
-rw-rw-r--  1 tahoun tahoun     69 20:44 27 فبر myScript.sh
-rwxrwx---  1 tahoun tahoun    195 22:07 27 فبر newService.service
drwxrwsr-x  2 tahoun os_team  4096 20:55 20 فبر os_team_workspace
drwxr-xr-x  2 tahoun tahoun   4096 12:30 1  فبر Pictures
drwx------  3 tahoun tahoun   4096 15:08 11 فبر .pki
-rw-r--r--  1 tahoun tahoun    807 12:24 1  فبر .profile
```

4- enable `ufw` service



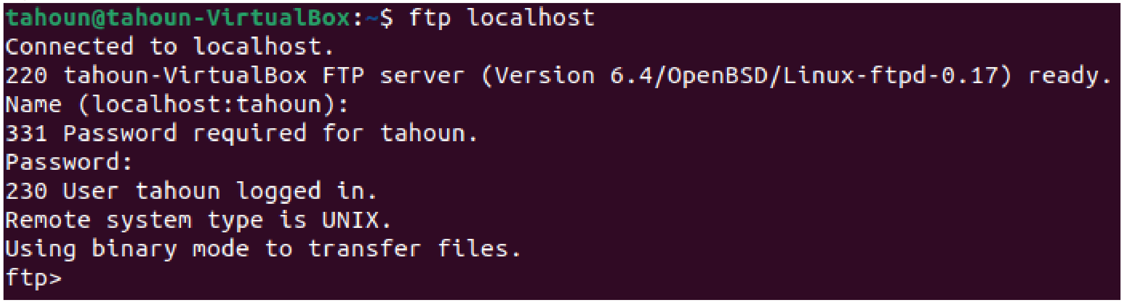
```
tahoun@tahoun-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

5- block port 20 and 21 (tcp) using ufw



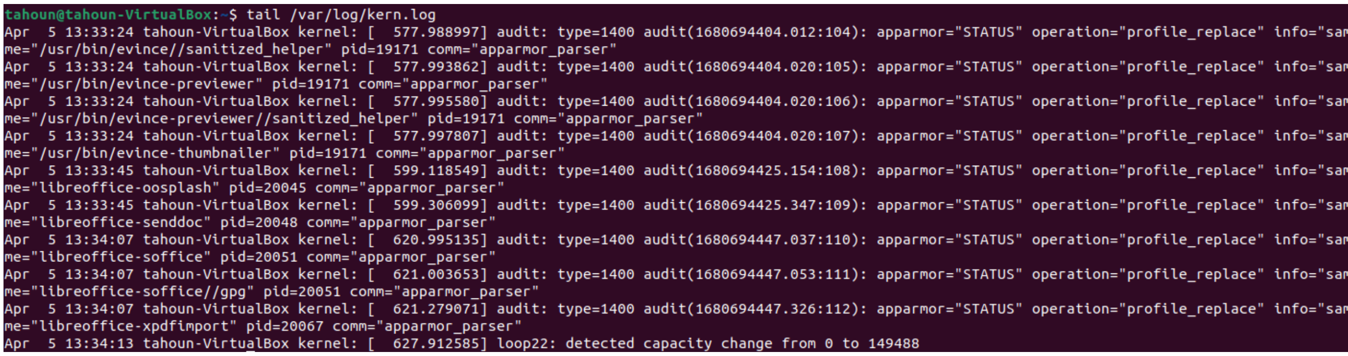
```
tahoun@tahoun-VirtualBox:~$ sudo ufw deny 20/tcp
Rule added
Rule added (v6)
tahoun@tahoun-VirtualBox:~$ sudo ufw deny 21/tcp
Rule added
Rule added (v6)
```

6- try to connect to ftp service.



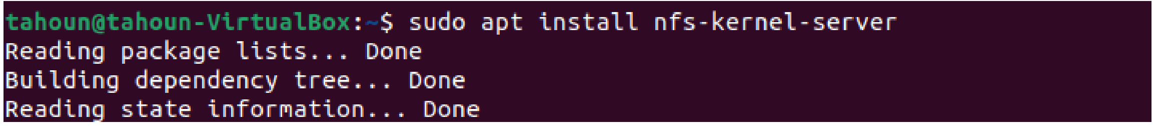
```
tahoun@tahoun-VirtualBox:~$ ftp localhost
Connected to localhost.
220 tahoun-VirtualBox FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
Name (localhost:tahoun):
331 Password required for tahoun.
Password:
230 User tahoun logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

7- capture the ufw log to detect the blocked operation



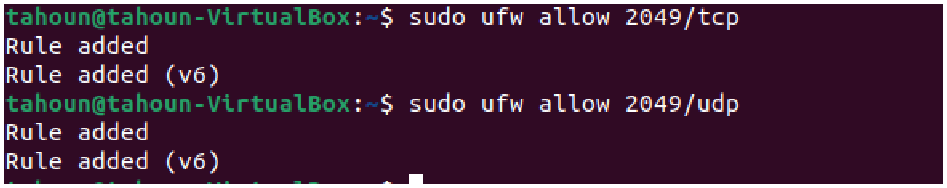
```
tahoun@tahoun-VirtualBox:~$ tail /var/log/kern.log
Apr  5 13:33:24 tahoun-VirtualBox kernel: [  577.988997] audit: type=1400 audit(1680694404.012:104): apparmor="STATUS" operation="profile_replace" info="sam
me="/usr/bin/evince//sanitized_helper" pid=19171 comm="apparmor_parser"
Apr  5 13:33:24 tahoun-VirtualBox kernel: [  577.993862] audit: type=1400 audit(1680694404.020:105): apparmor="STATUS" operation="profile_replace" info="sam
me="/usr/bin/evince-previewer" pid=19171 comm="apparmor_parser"
Apr  5 13:33:24 tahoun-VirtualBox kernel: [  577.995580] audit: type=1400 audit(1680694404.020:106): apparmor="STATUS" operation="profile_replace" info="sam
me="/usr/bin/evince-previewer//sanitized_helper" pid=19171 comm="apparmor_parser"
Apr  5 13:33:24 tahoun-VirtualBox kernel: [  577.997807] audit: type=1400 audit(1680694404.020:107): apparmor="STATUS" operation="profile_replace" info="sam
me="/usr/bin/evince-thumbnailer" pid=19171 comm="apparmor_parser"
Apr  5 13:33:45 tahoun-VirtualBox kernel: [  599.118549] audit: type=1400 audit(1680694425.154:108): apparmor="STATUS" operation="profile_replace" info="sam
me="libreoffice-oosplash" pid=20045 comm="apparmor_parser"
Apr  5 13:33:45 tahoun-VirtualBox kernel: [  599.306099] audit: type=1400 audit(1680694425.347:109): apparmor="STATUS" operation="profile_replace" info="sam
me="libreoffice-senddoc" pid=20048 comm="apparmor_parser"
Apr  5 13:34:07 tahoun-VirtualBox kernel: [  620.995135] audit: type=1400 audit(1680694447.037:110): apparmor="STATUS" operation="profile_replace" info="sam
me="libreoffice-soffice" pid=20051 comm="apparmor_parser"
Apr  5 13:34:07 tahoun-VirtualBox kernel: [  621.003653] audit: type=1400 audit(1680694447.053:111): apparmor="STATUS" operation="profile_replace" info="sam
me="libreoffice-soffice//gpg" pid=20051 comm="apparmor_parser"
Apr  5 13:34:07 tahoun-VirtualBox kernel: [  621.279071] audit: type=1400 audit(1680694447.326:112): apparmor="STATUS" operation="profile_replace" info="sam
me="libreoffice-xpdfimport" pid=20067 comm="apparmor_parser"
Apr  5 13:34:13 tahoun-VirtualBox kernel: [  627.912585] loop22: detected capacity change from 0 to 149488
```

8- install `nfs` service on your system



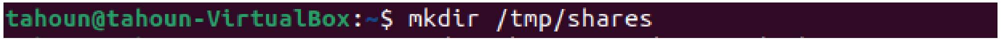
```
tahoun@tahoun-VirtualBox:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

9- enable nfs service on the firewall

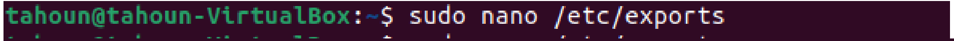


```
tahoun@tahoun-VirtualBox:~$ sudo ufw allow 2049/tcp
Rule added
Rule added (v6)
tahoun@tahoun-VirtualBox:~$ sudo ufw allow 2049/udp
Rule added
Rule added (v6)
```

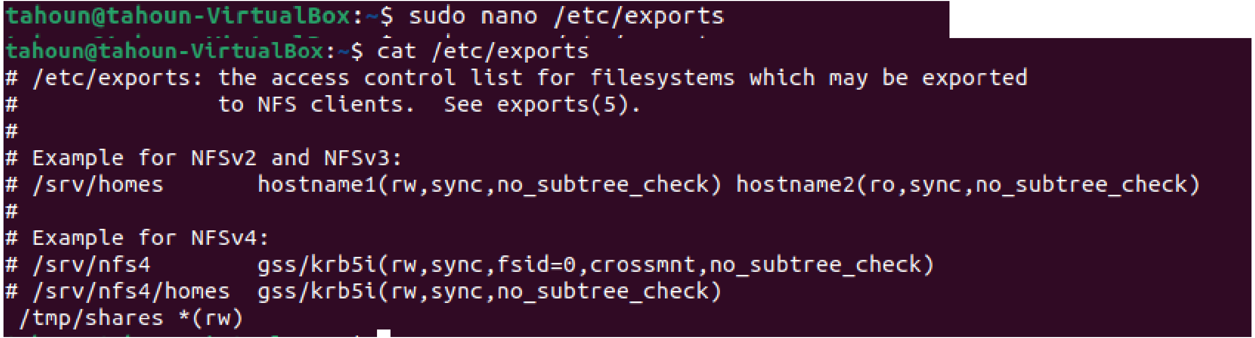
10- create and share /tmp/shares folder using `exportfs` command and `/etc/exports` file



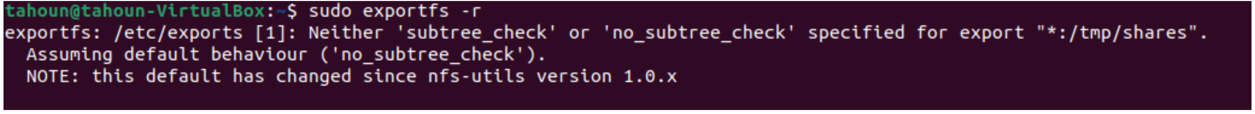
```
tahoun@tahoun-VirtualBox:~$ mkdir /tmp/shares
```



```
tahoun@tahoun-VirtualBox:~$ sudo nano /etc/exports
```

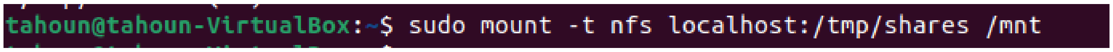


```
tahoun@tahoun-VirtualBox:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
 /tmp/shares *(rw)
```



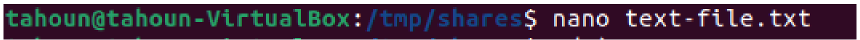
```
tahoun@tahoun-VirtualBox:~$ sudo exportfs -r
exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specified for export "*:/tmp/shares".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x
```

11- mount the remote share on `/mnt` folder (you can using localhost as well)

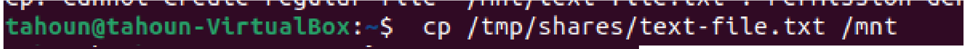


```
tahoun@tahoun-VirtualBox:~$ sudo mount -t nfs localhost:/tmp/shares /mnt
```

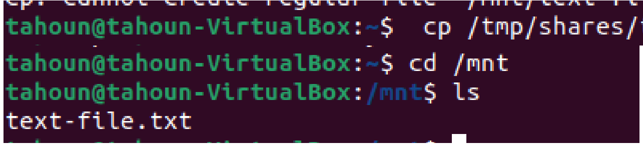
12- copy some files to the remote share



```
tahoun@tahoun-VirtualBox:/tmp/shares$ nano text-file.txt
```

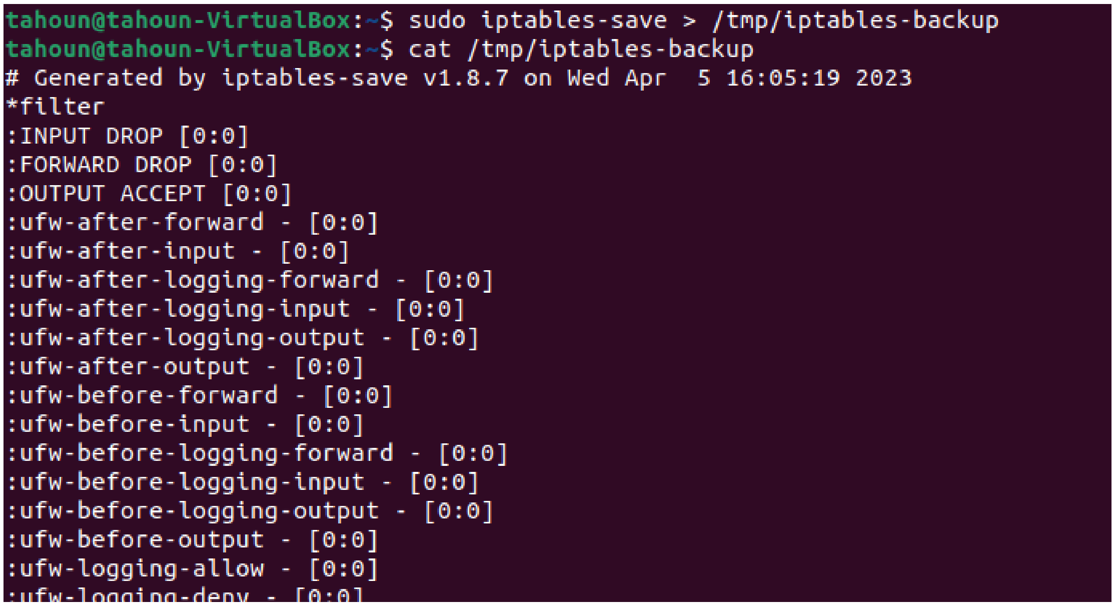


```
tahoun@tahoun-VirtualBox:~$  cp /tmp/shares/text-file.txt /mnt
```



```
tahoun@tahoun-VirtualBox:~$ cd /mnt
tahoun@tahoun-VirtualBox:/mnt$ ls
text-file.txt
```

13- save `iptables` rules to `/tmp/iptables-backup` file



```
tahoun@tahoun-VirtualBox:~$ sudo iptables-save > /tmp/iptables-backup
tahoun@tahoun-VirtualBox:~$ cat /tmp/iptables-backup
# Generated by iptables-save v1.8.7 on Wed Apr  5 16:05:19 2023
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-before-input - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-logging-allow - [0:0]
:ufw-logging-deny - [0:0]
```