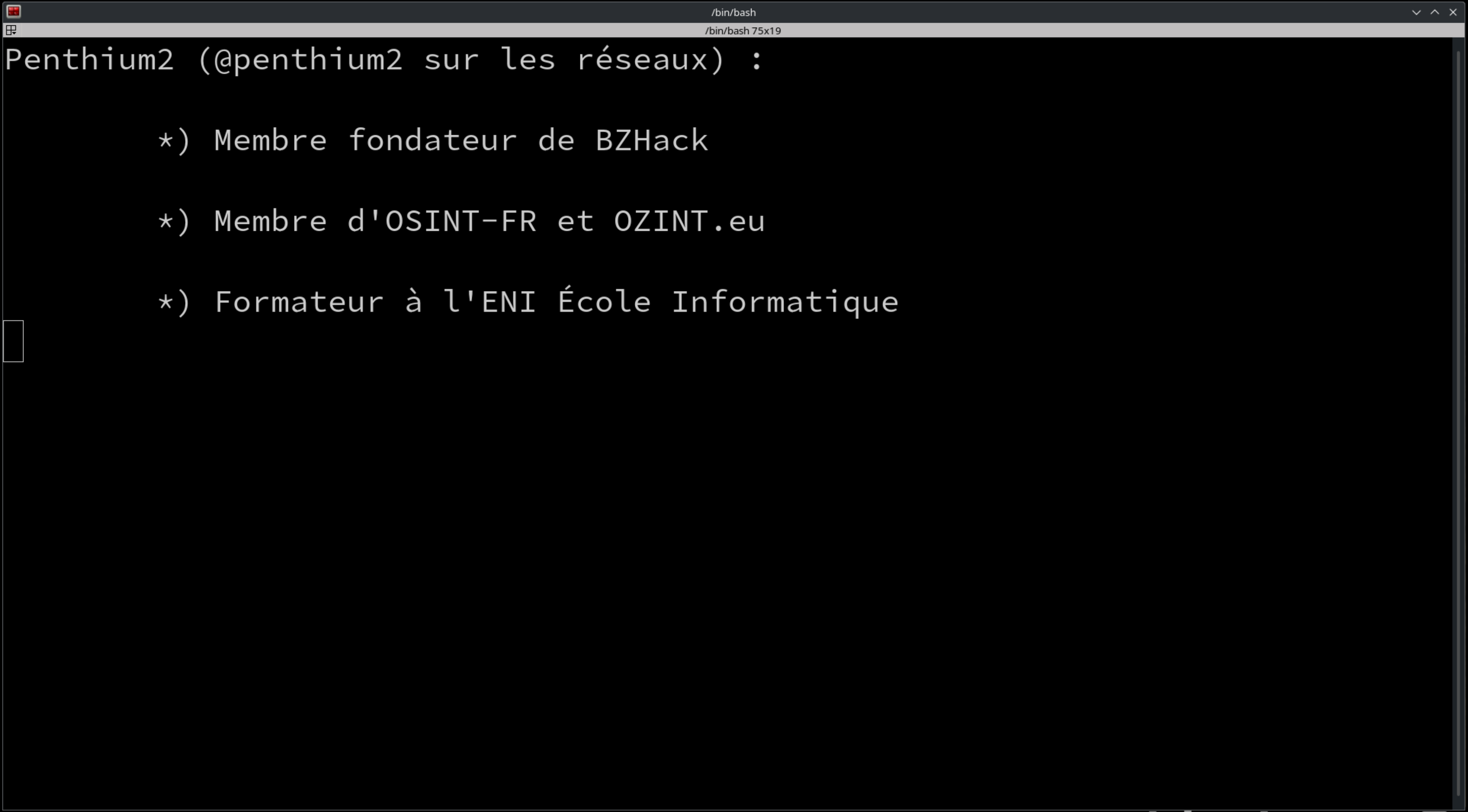
```
SUDO DOWNGRADE PRIVILEGES
```

penthium2

```
SUDO DOWNGRADE PRIVILEGES

Qui suis je ??
```

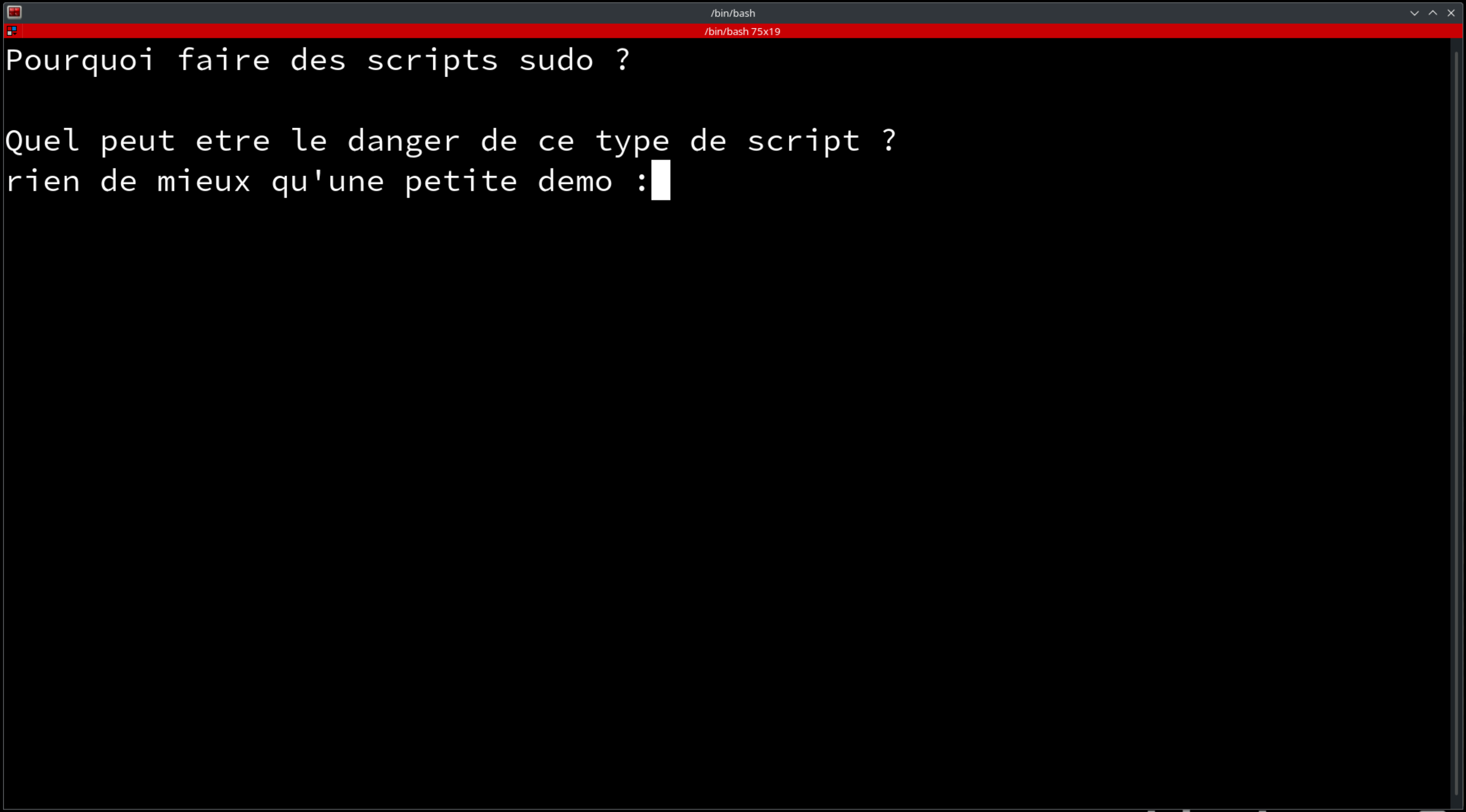
penthium2



```
Penthium2 (@penthium2 sur les réseaux) :

        *) Membre fondateur de BZHack

        *) Membre d'OSINT-FR et OZINT.eu

        *) Formateur à l'ENI École Informatique
```

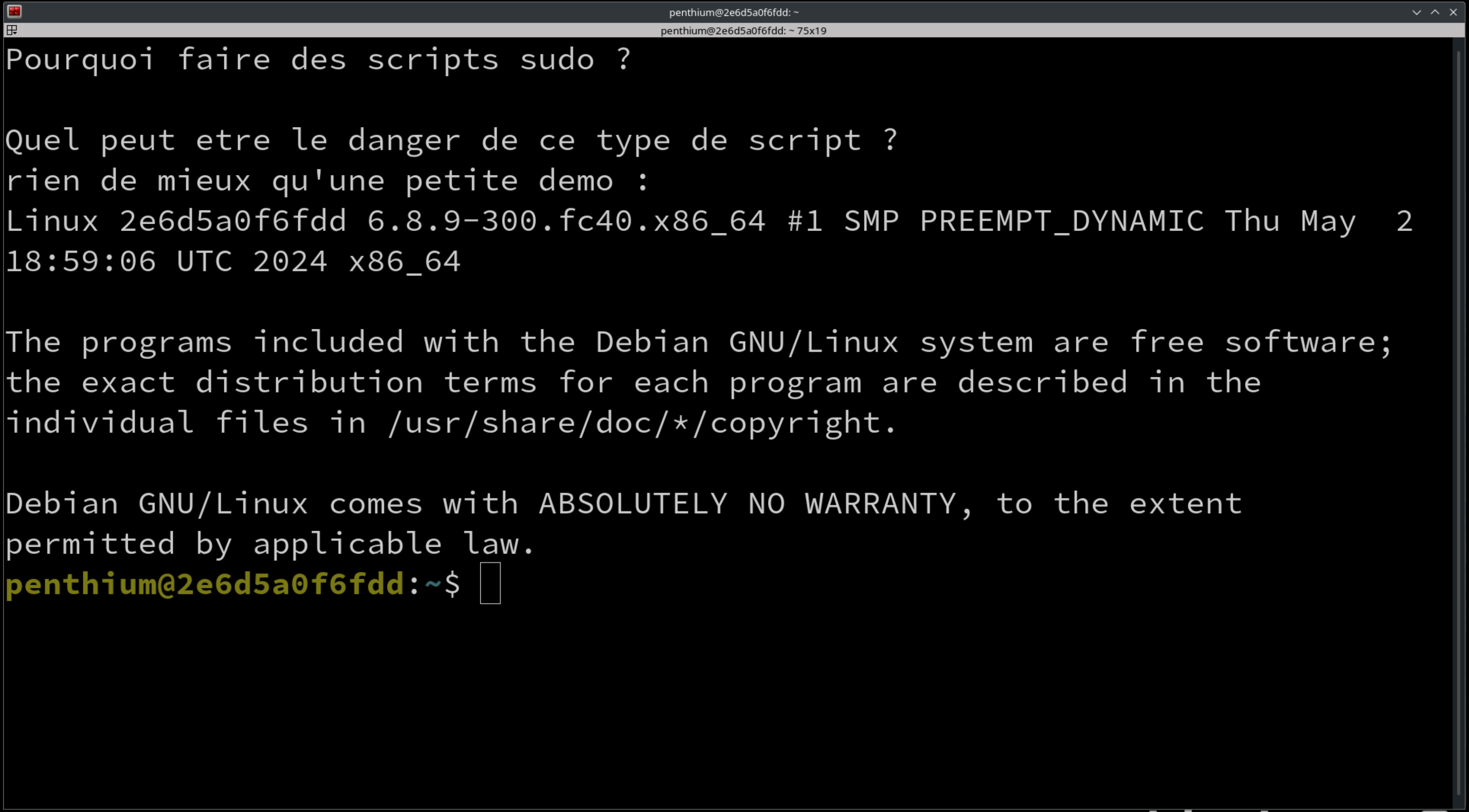
penthium2

```
Pourquoi faire des scripts sudo ?
```

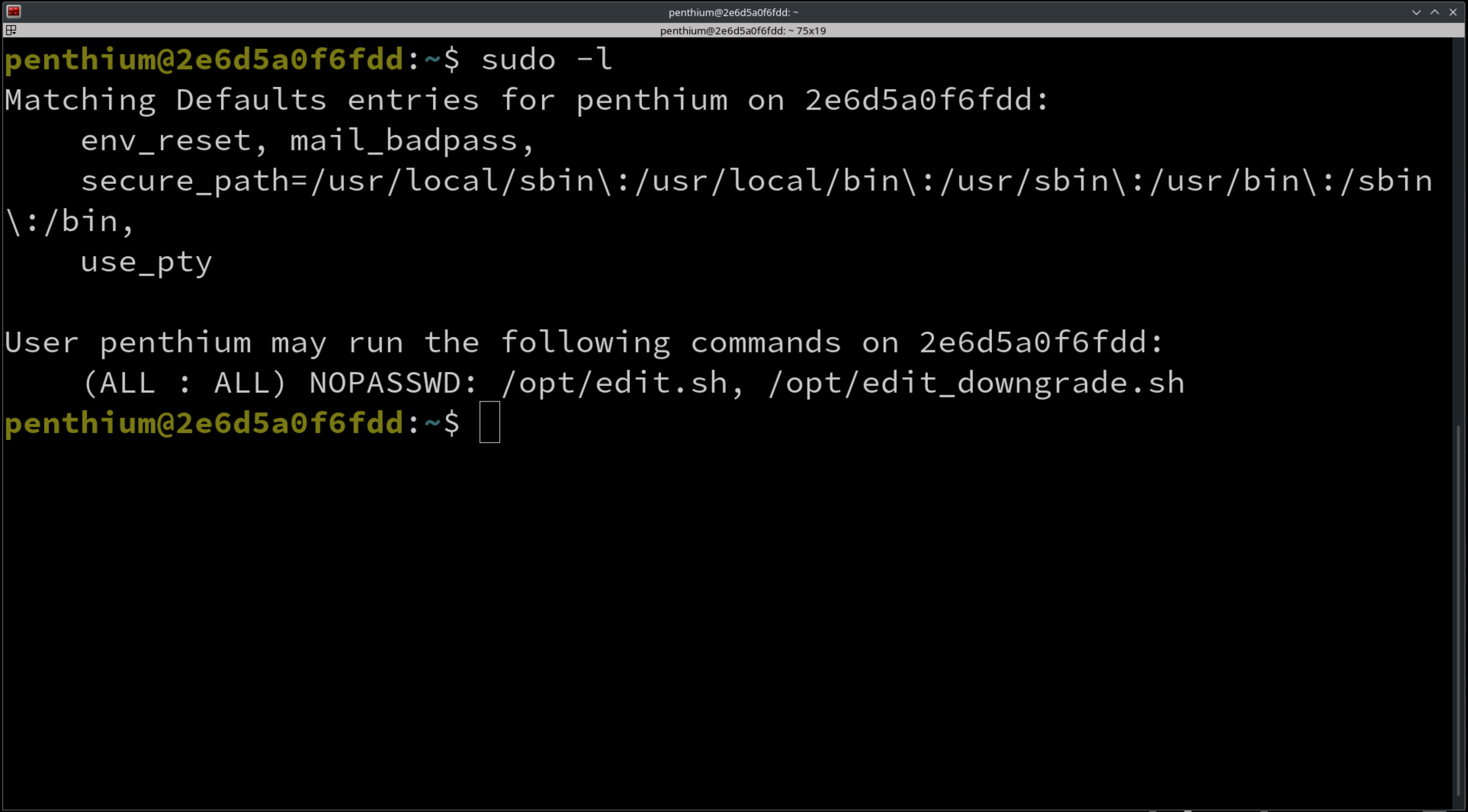


```
Pourquoi faire des scripts sudo ?

Quel peut etre le danger de ce type de script ?
rien de mieux qu'une petite demo :
```

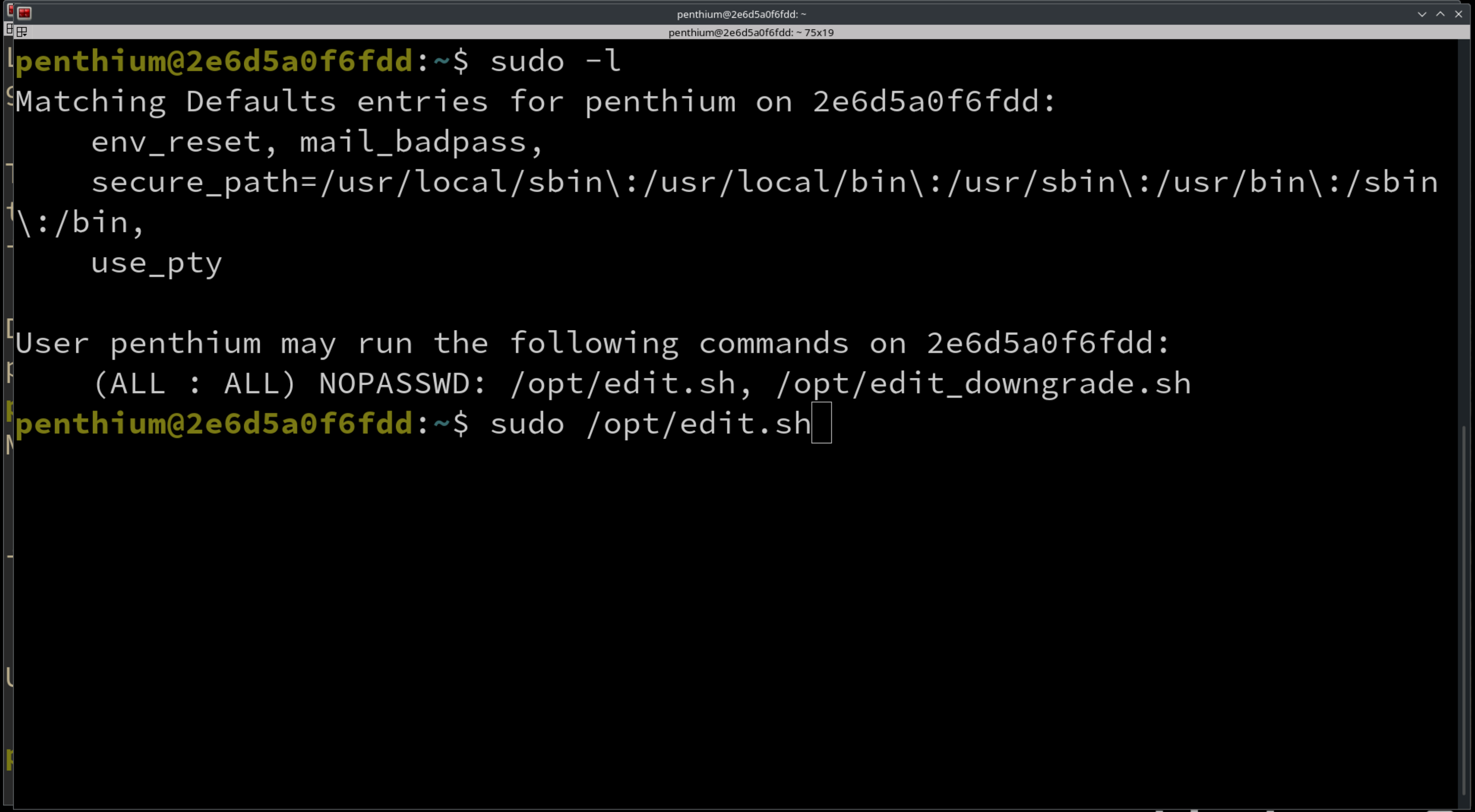
penthium2



```
Pourquoi faire des scripts sudo ?

Quel peut etre le danger de ce type de script ?
rien de mieux qu'une petite demo :
Linux 2e6d5a0f6fdd 6.8.9-300.fc40.x86_64 #1 SMP PREEMPT_DYNAMIC Thu May  2
18:59:06 UTC 2024 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
penthium@2e6d5a0f6fdd:~$ 
```

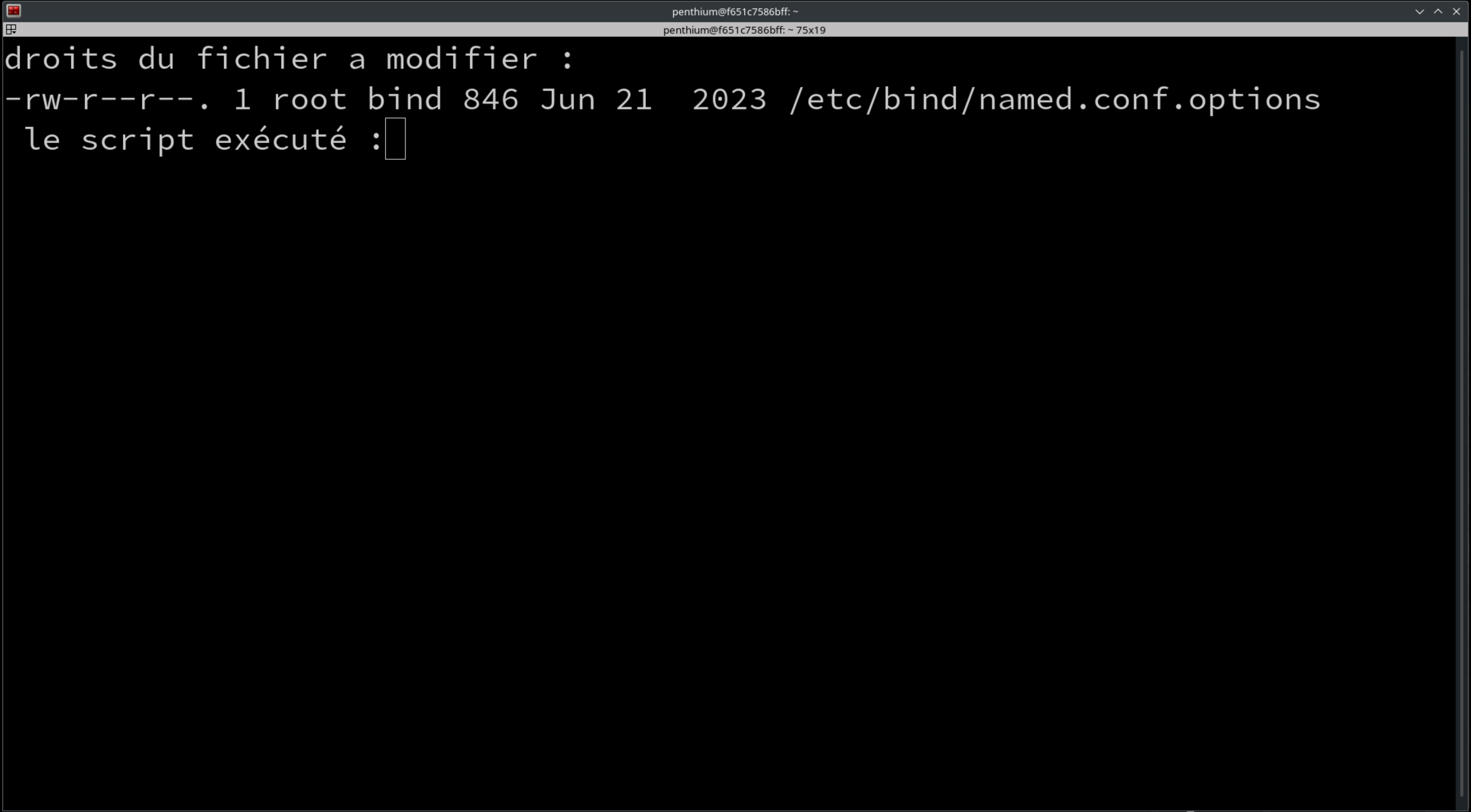


```
penthium@2e6d5a0f6fdd:~$ sudo -l
Matching Defaults entries for penthium on 2e6d5a0f6fdd:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin,
    use_pty

User penthium may run the following commands on 2e6d5a0f6fdd:
    (ALL : ALL) NOPASSWD: /opt/edit.sh, /opt/edit_downgrade.sh
penthium@2e6d5a0f6fdd:~$ 
```

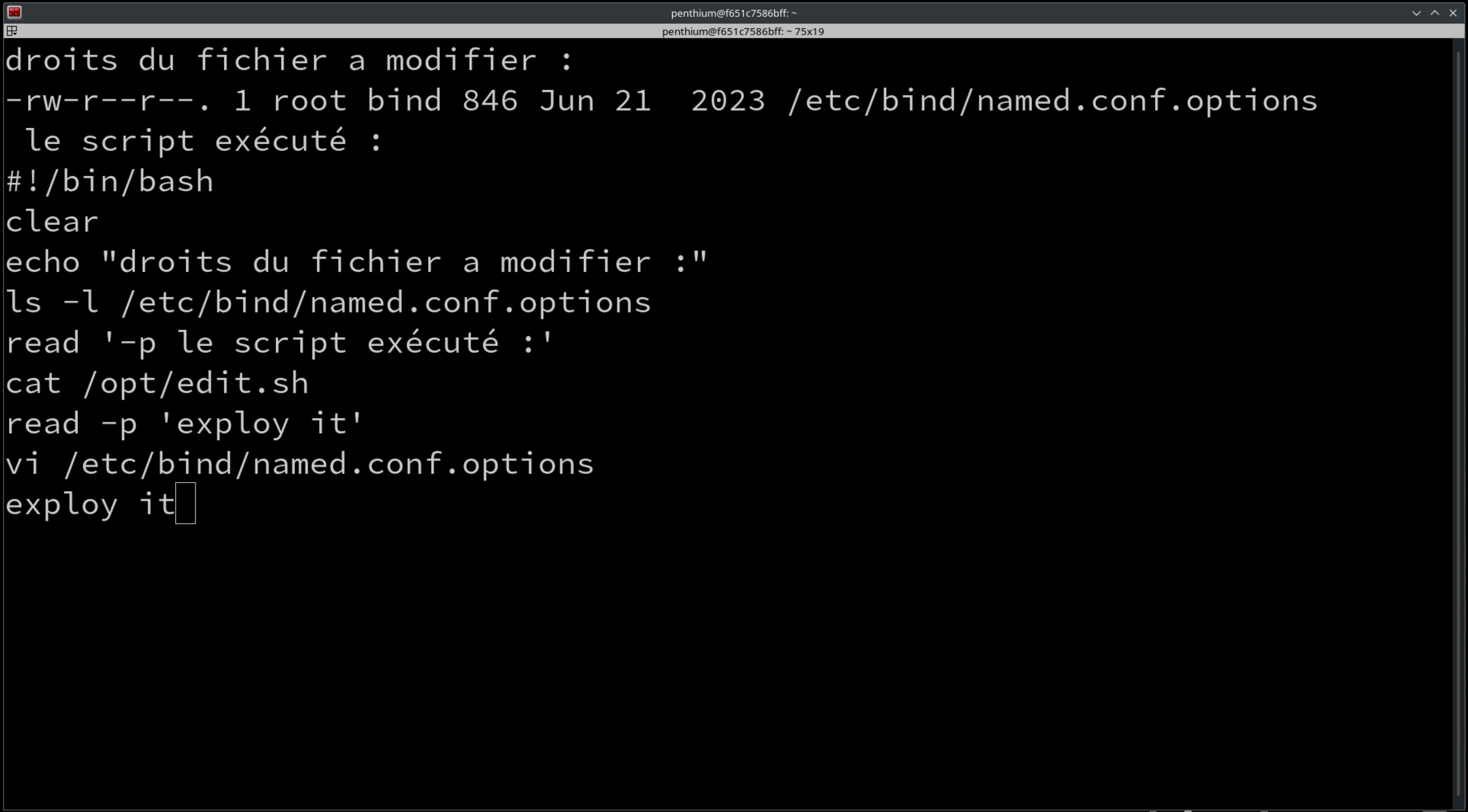


```
penthium@2e6d5a0f6fdd:~$ sudo -l
Matching Defaults entries for penthium on 2e6d5a0f6fdd:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin,
    use_pty

User penthium may run the following commands on 2e6d5a0f6fdd:
    (ALL : ALL) NOPASSWD: /opt/edit.sh, /opt/edit_downgrade.sh
penthium@2e6d5a0f6fdd:~$ sudo /opt/edit.sh
```

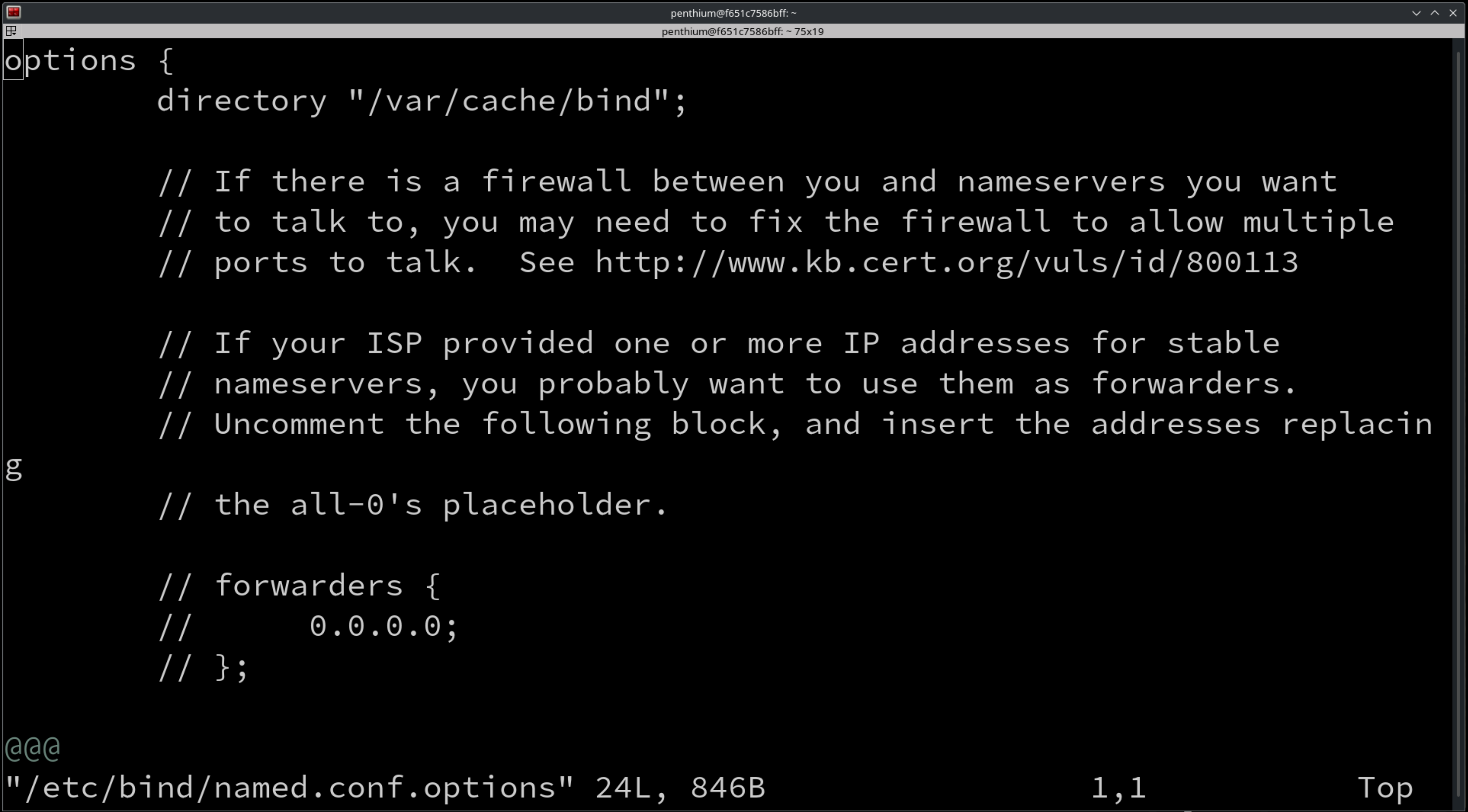
penthium2



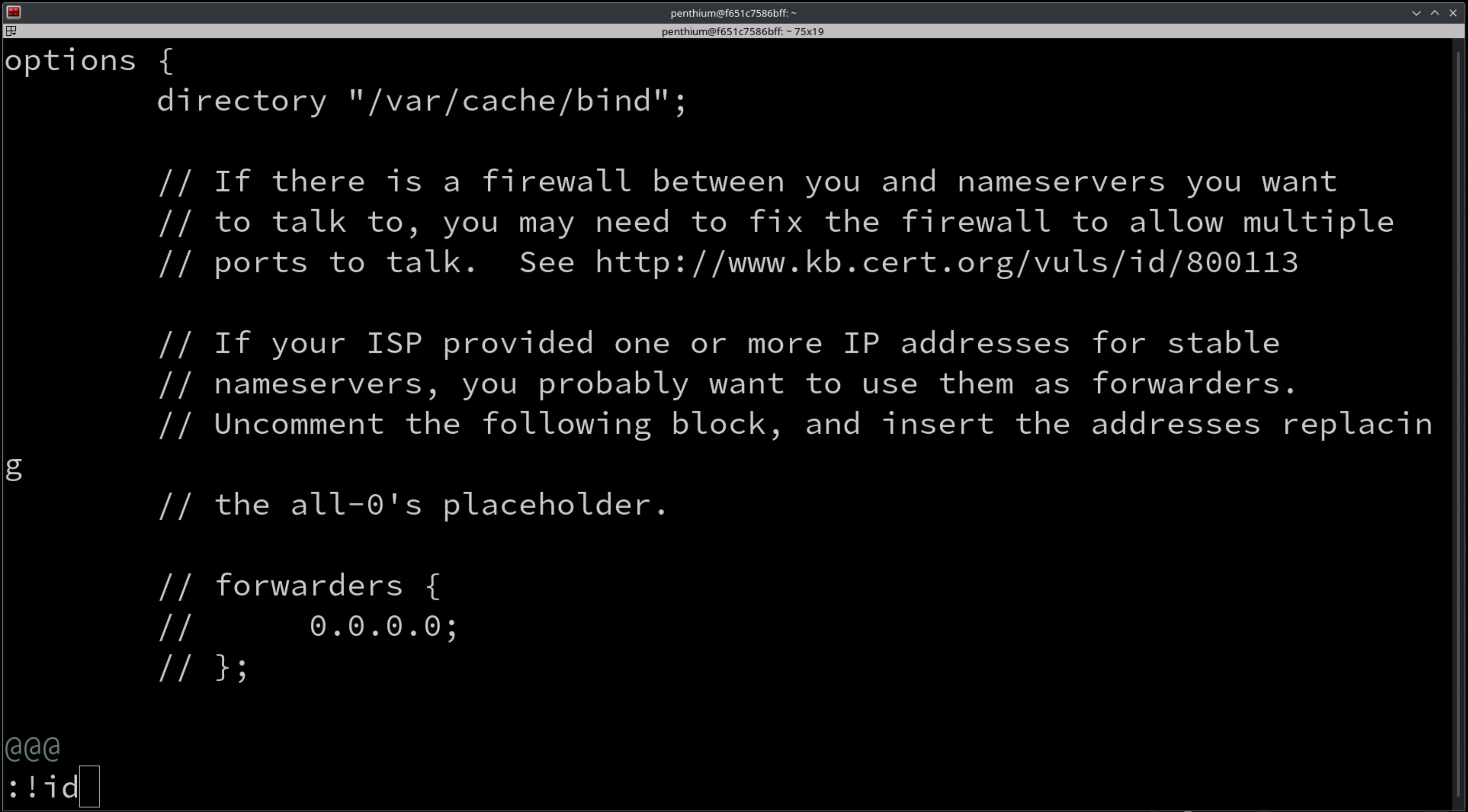
```
droits du fichier a modifier :
-rw-r--r--. 1 root bind 846 Jun 21  2023 /etc/bind/named.conf.options
 le script exécuté :
```



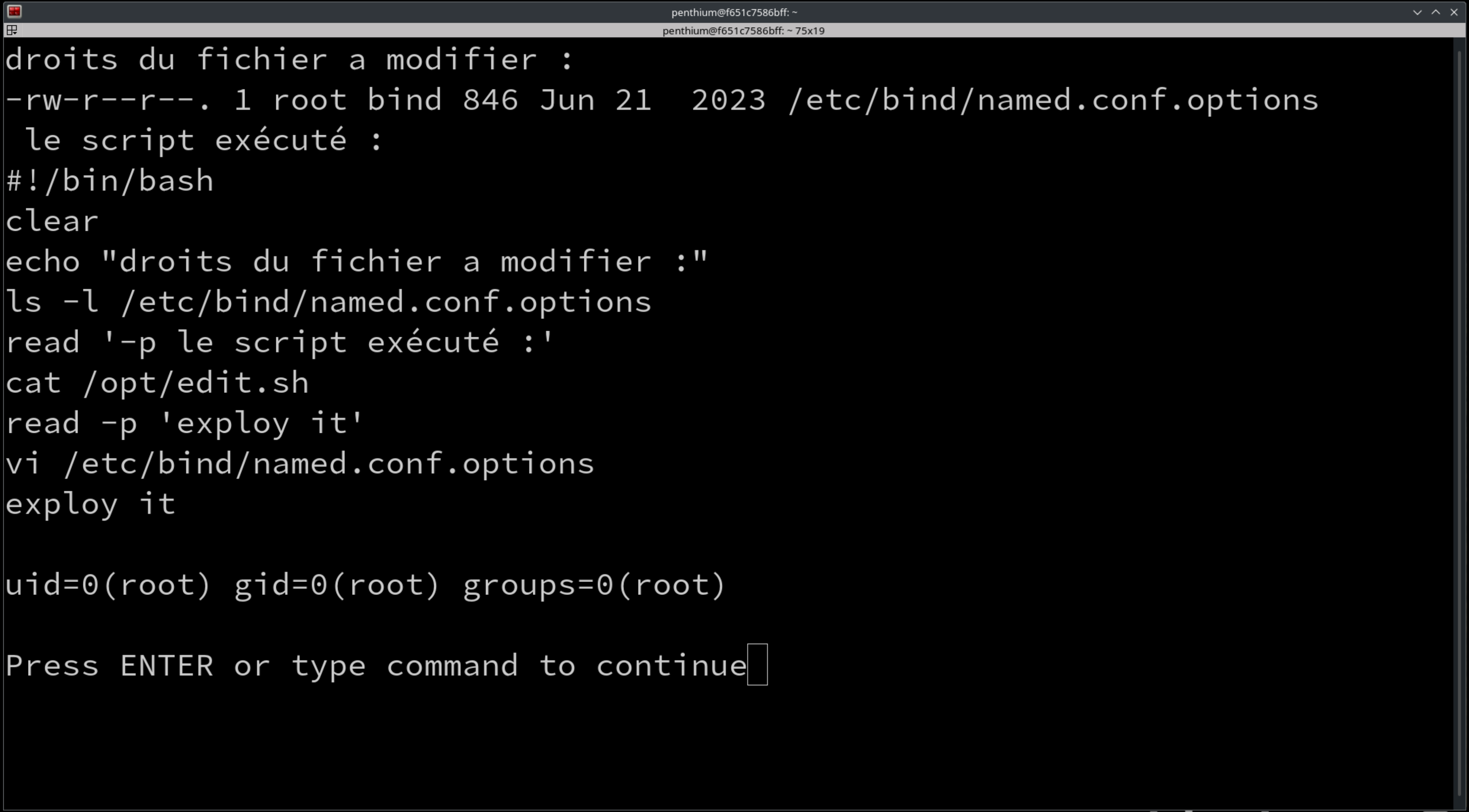
```
droits du fichier a modifier :
-rw-r--r--. 1 root bind 846 Jun 21  2023 /etc/bind/named.conf.options
 le script exécuté :
#!/bin/bash
clear
echo "droits du fichier a modifier :"
ls -l /etc/bind/named.conf.options
read '-p le script exécuté :'
cat /opt/edit.sh
read -p 'exploy it'
vi /etc/bind/named.conf.options
exploy it
```



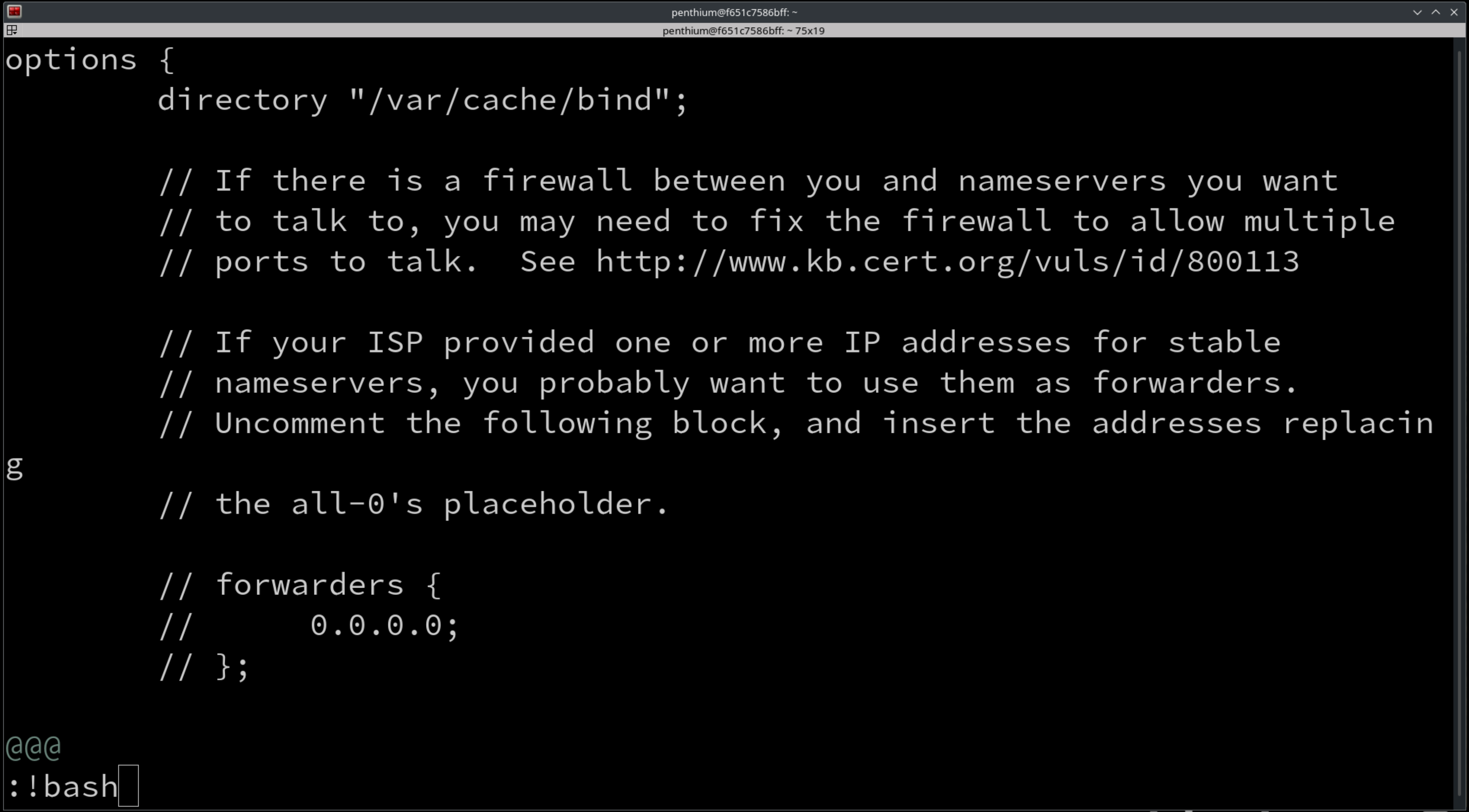
```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacin
g
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

@@@
"/etc/bind/named.conf.options" 24L, 846B                    1,1           Top
```



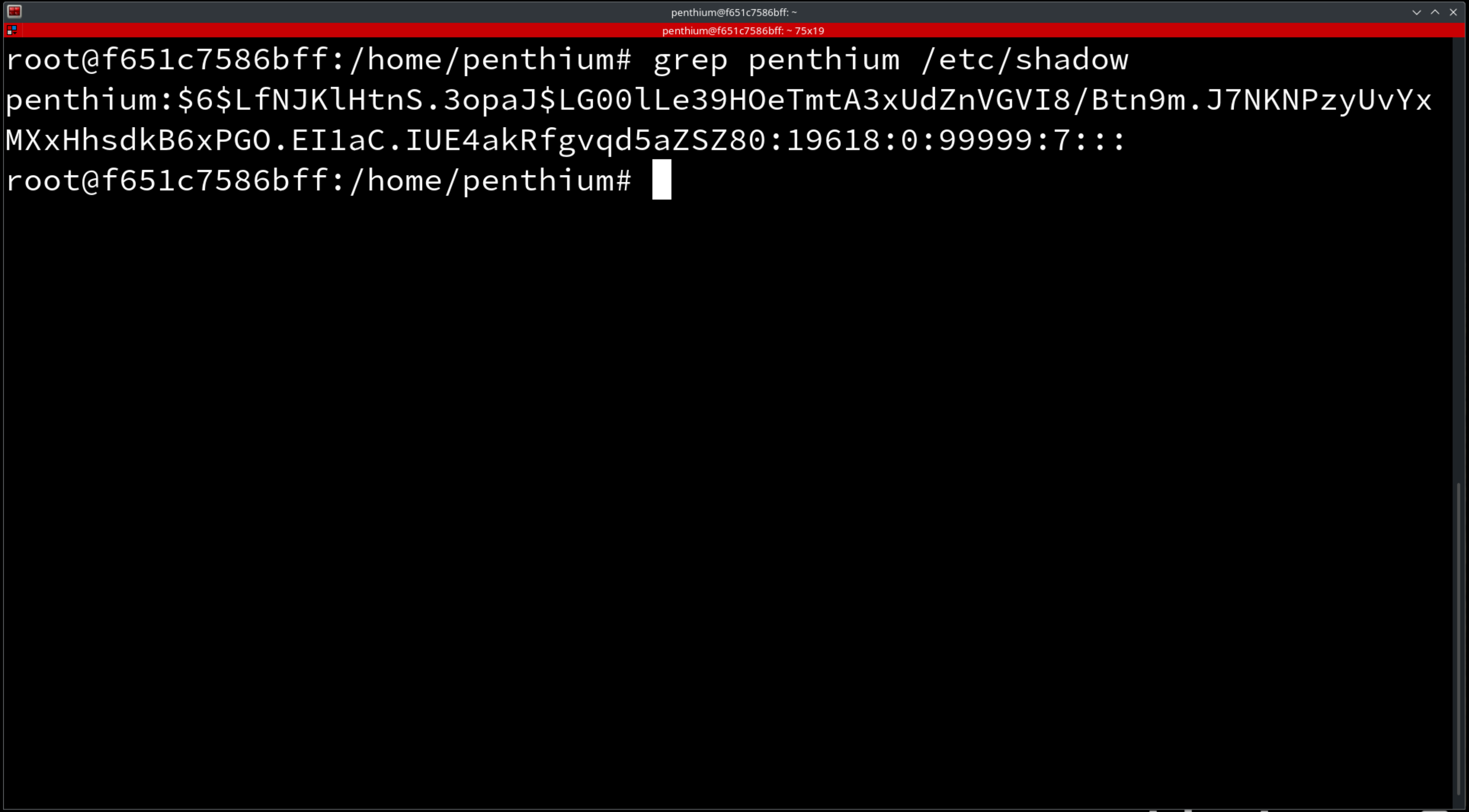
```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacin
g
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

@@@
:!id
```



```
droits du fichier a modifier :
-rw-r--r--. 1 root bind 846 Jun 21  2023 /etc/bind/named.conf.options
 le script exécuté :
#!/bin/bash
clear
echo "droits du fichier a modifier :"
ls -l /etc/bind/named.conf.options
read '-p le script exécuté :'
cat /opt/edit.sh
read -p 'exploy it'
vi /etc/bind/named.conf.options
exploy it

uid=0(root) gid=0(root) groups=0(root)

Press ENTER or type command to continue
```

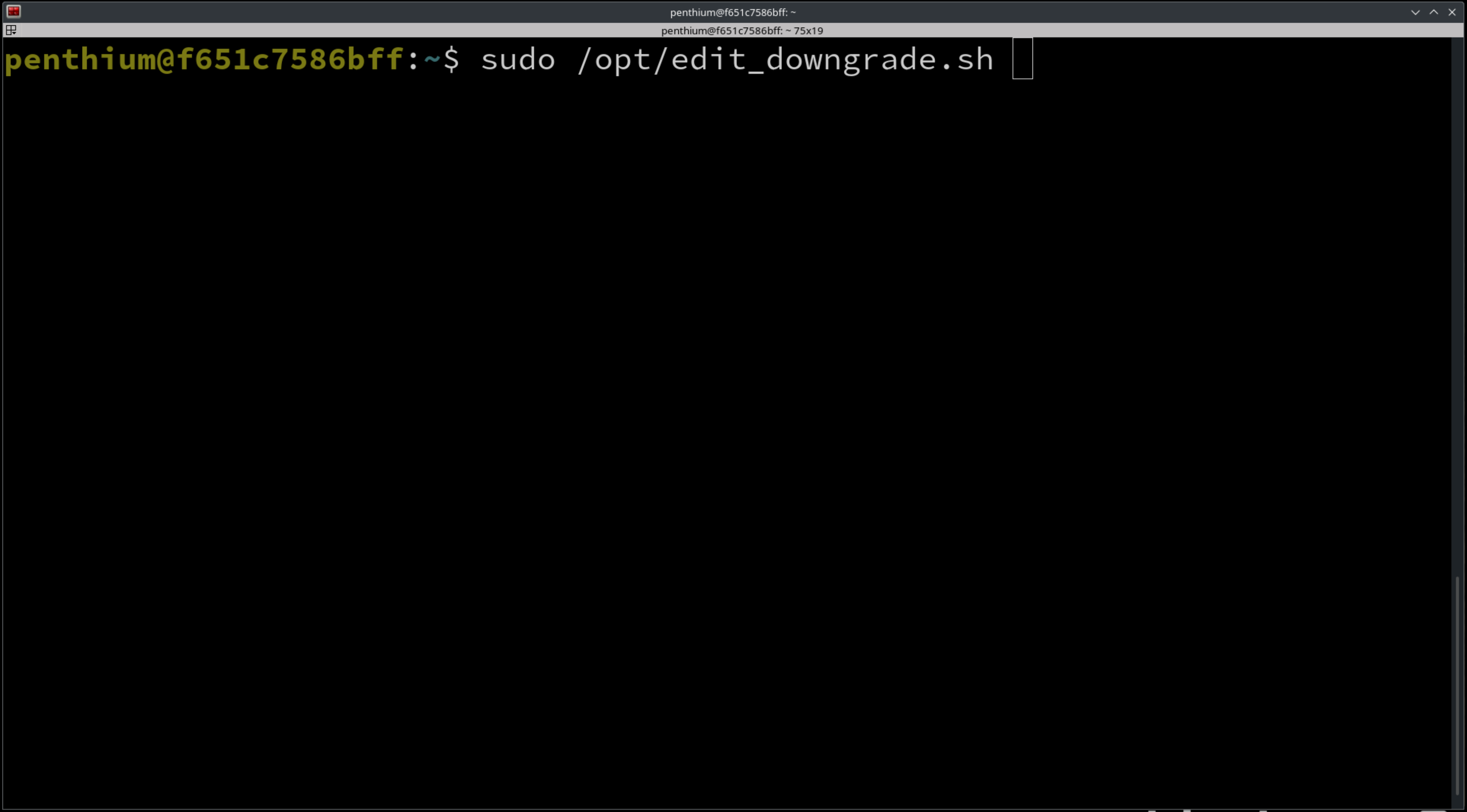


```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacin
g
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

@@@
:!bash
```



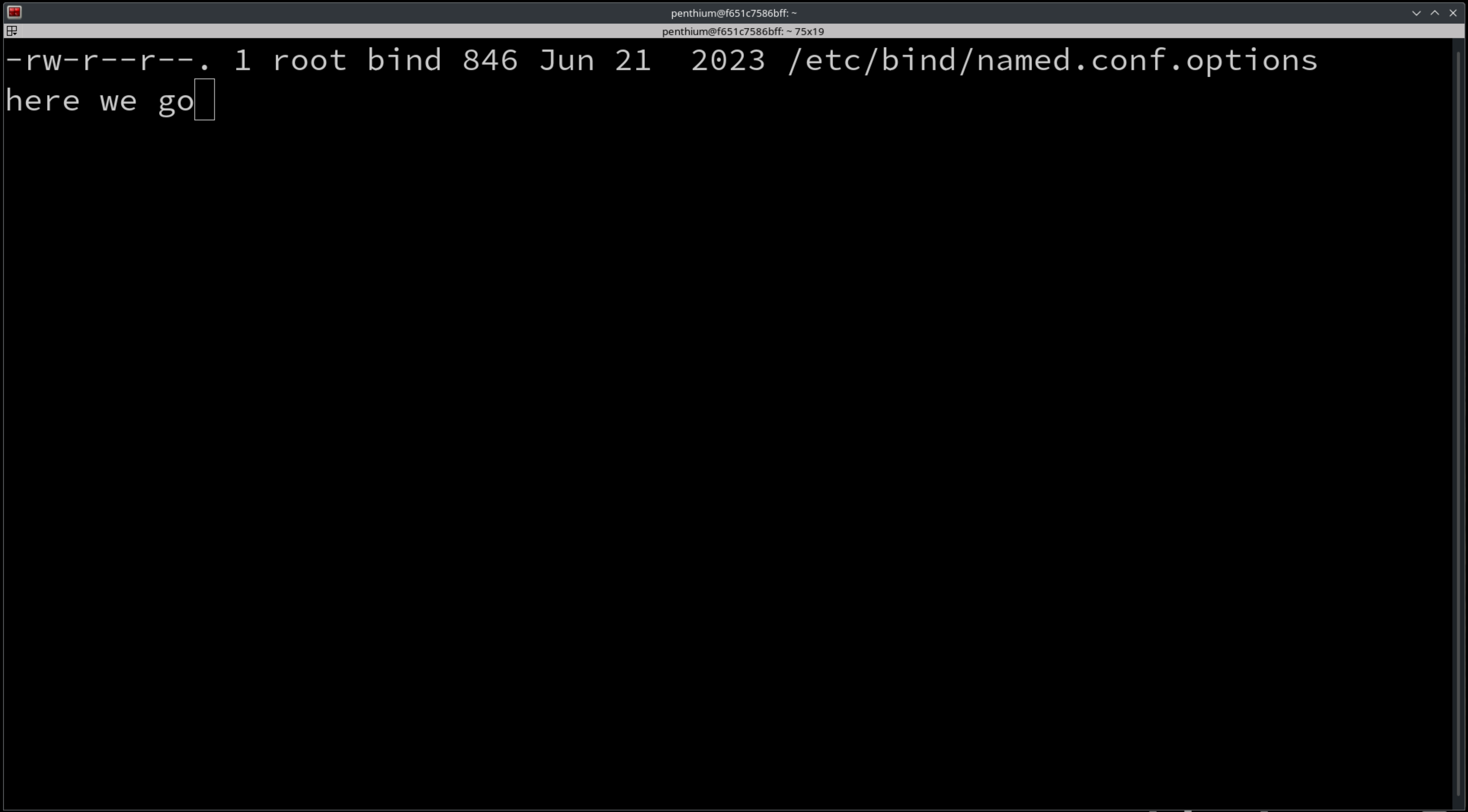
```
root@f651c7586bff:/home/penthium# grep penthium /etc/shadow
penthium:$6$LfNJKlHtnS.3opaJ$LG00lLe39HOeTmtA3xUdZnVGVI8/Btn9m.J7NKNPzyUvYx
MXxHhsdkB6xPGO.EI1aC.IUE4akRfgvqd5aZSZ80:19618:0:99999:7:::
root@f651c7586bff:/home/penthium# 
```

I CAN GO EVERYWHERE NOW
HACKERMAN
FROM 1975
imgflip.com

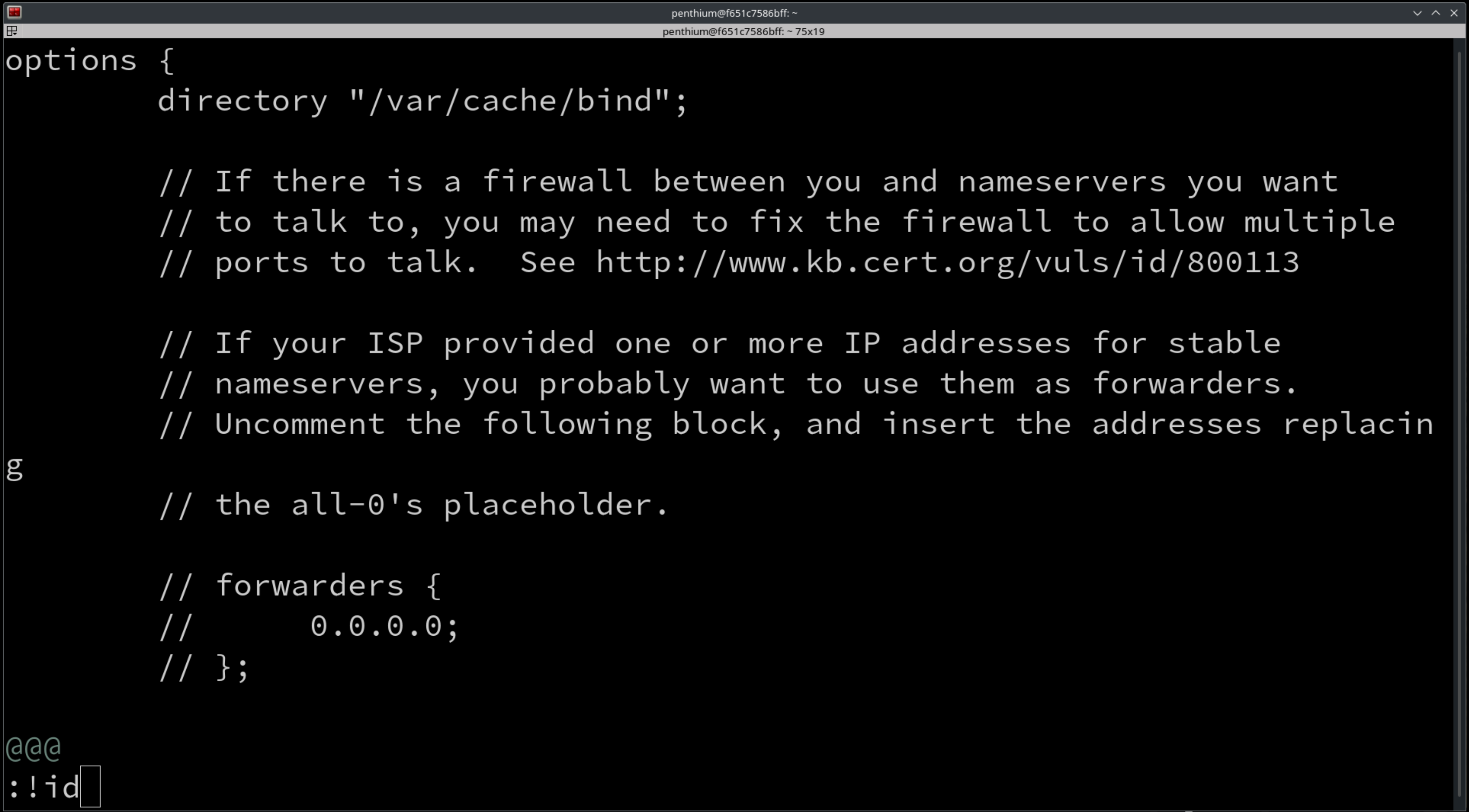


```
penthium@f651c7586bff:~$ sudo /opt/edit_downgrade.sh
```

penthium2

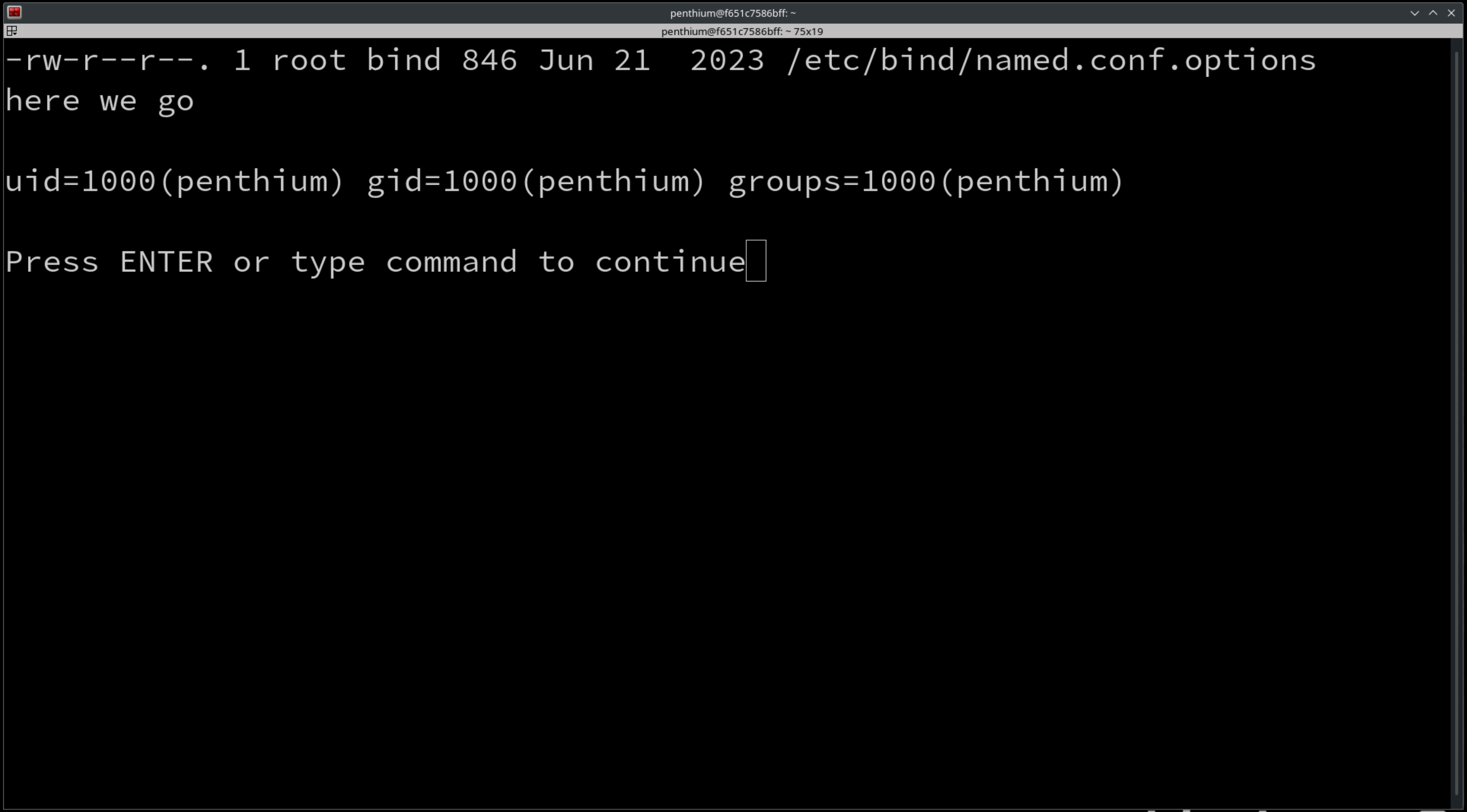


```
-rw-r--r--. 1 root bind 846 Jun 21  2023 /etc/bind/named.conf.options
here we go
```

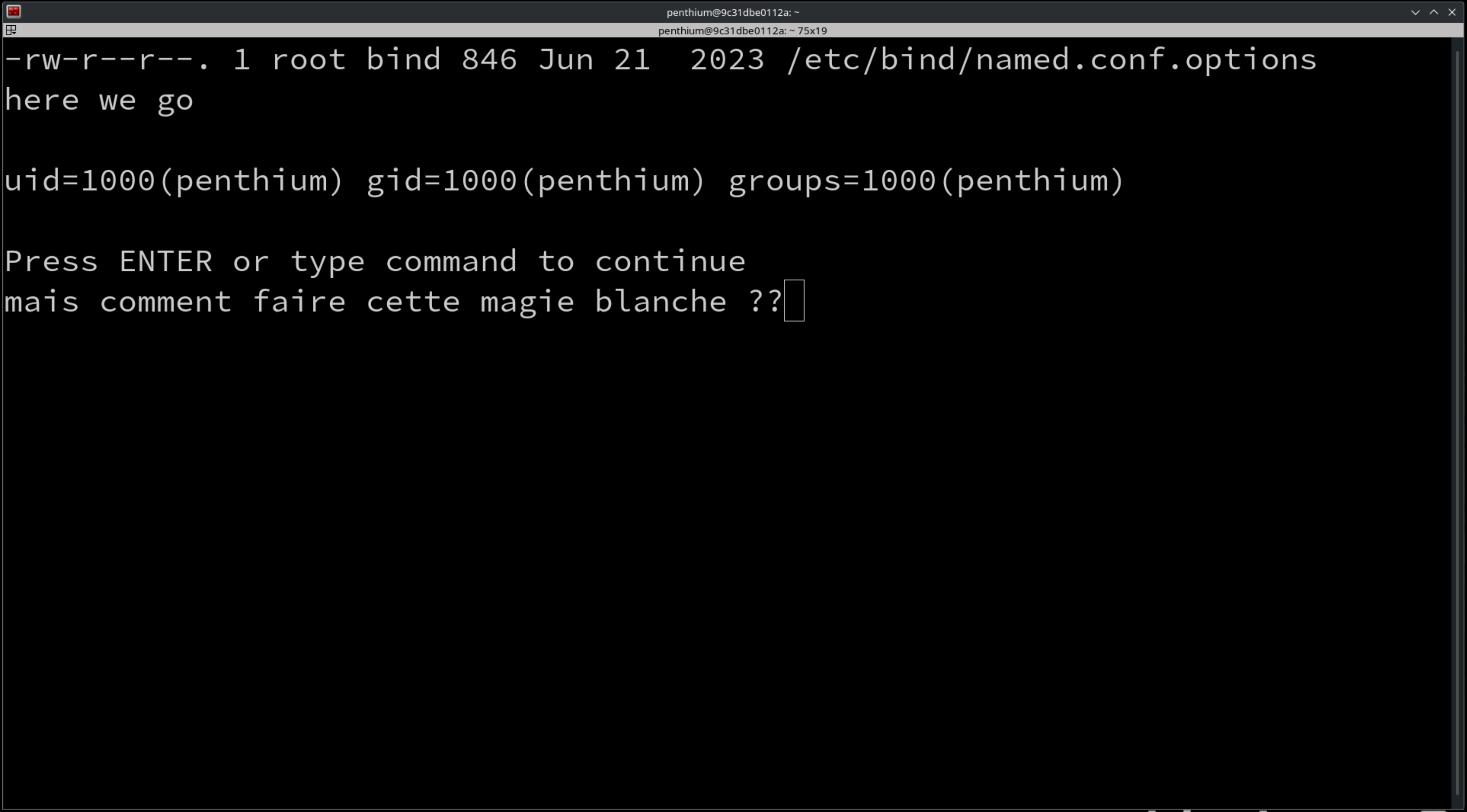


```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacin
g
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

@@@
:!id
```

penthium2

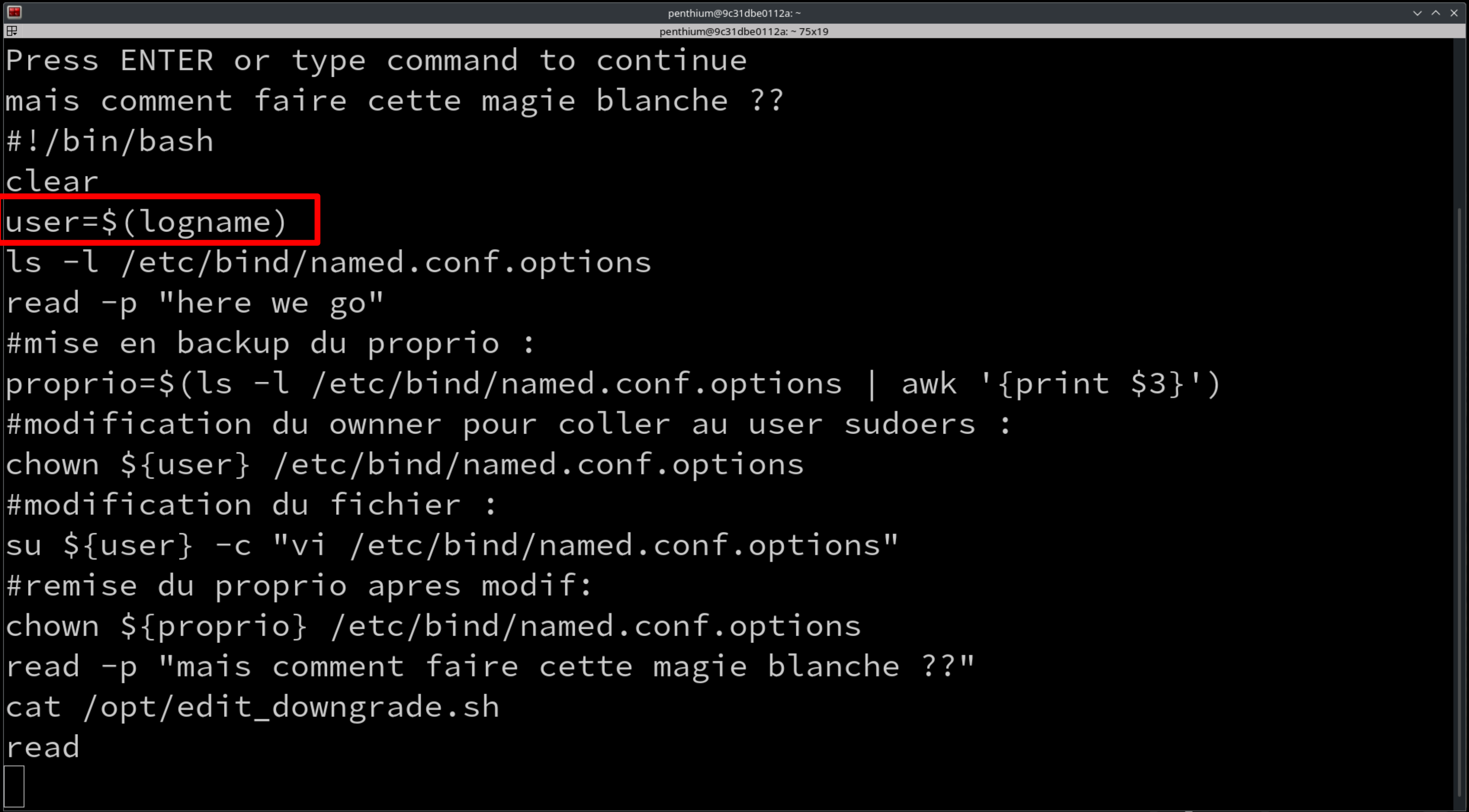


```
-rw-r--r--. 1 root bind 846 Jun 21  2023 /etc/bind/named.conf.options
here we go

uid=1000(penthium) gid=1000(penthium) groups=1000(penthium)

Press ENTER or type command to continue
```

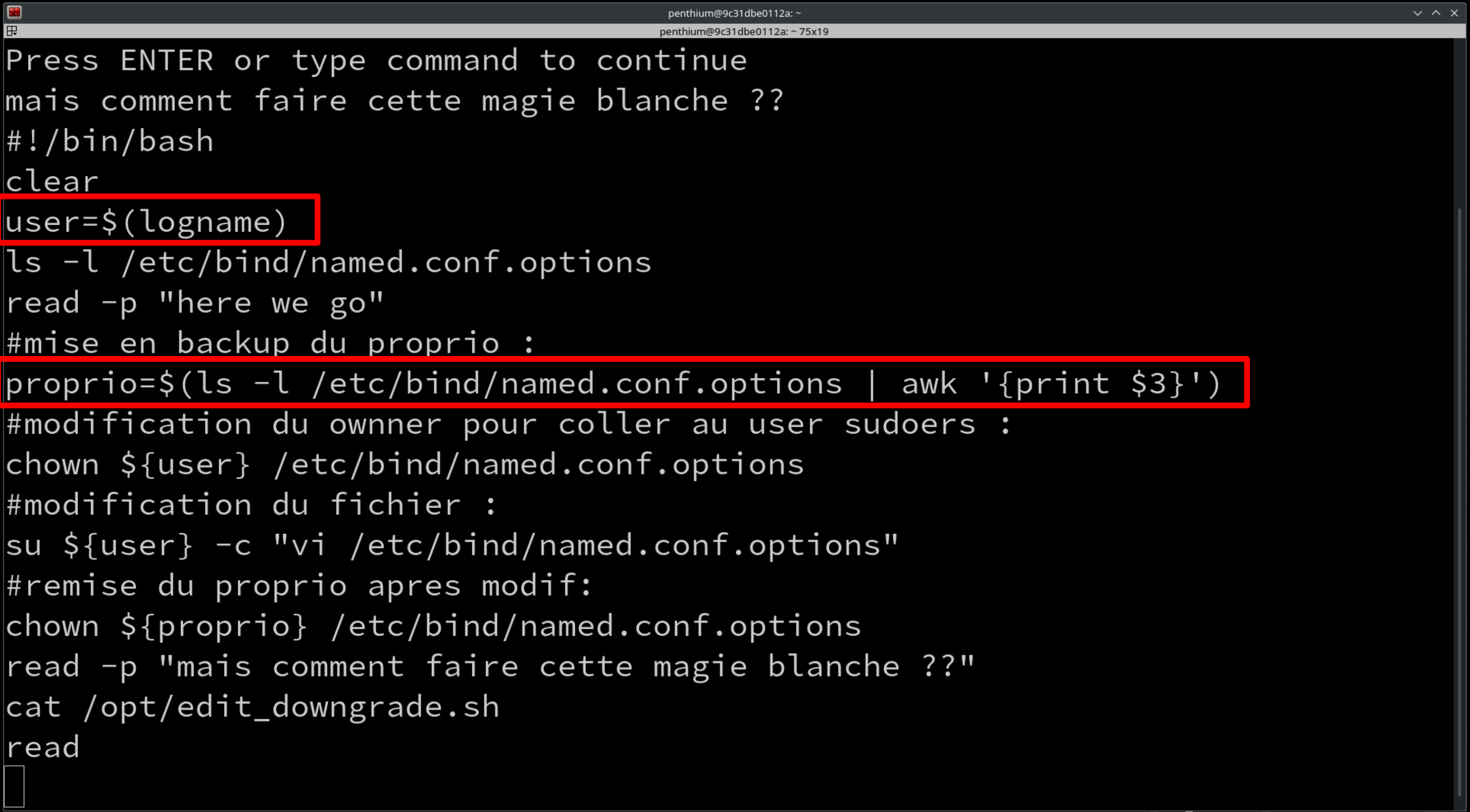


```
-rw-r--r--. 1 root bind 846 Jun 21  2023 /etc/bind/named.conf.options
here we go

uid=1000(penthium) gid=1000(penthium) groups=1000(penthium)

Press ENTER or type command to continue
mais comment faire cette magie blanche ??
```

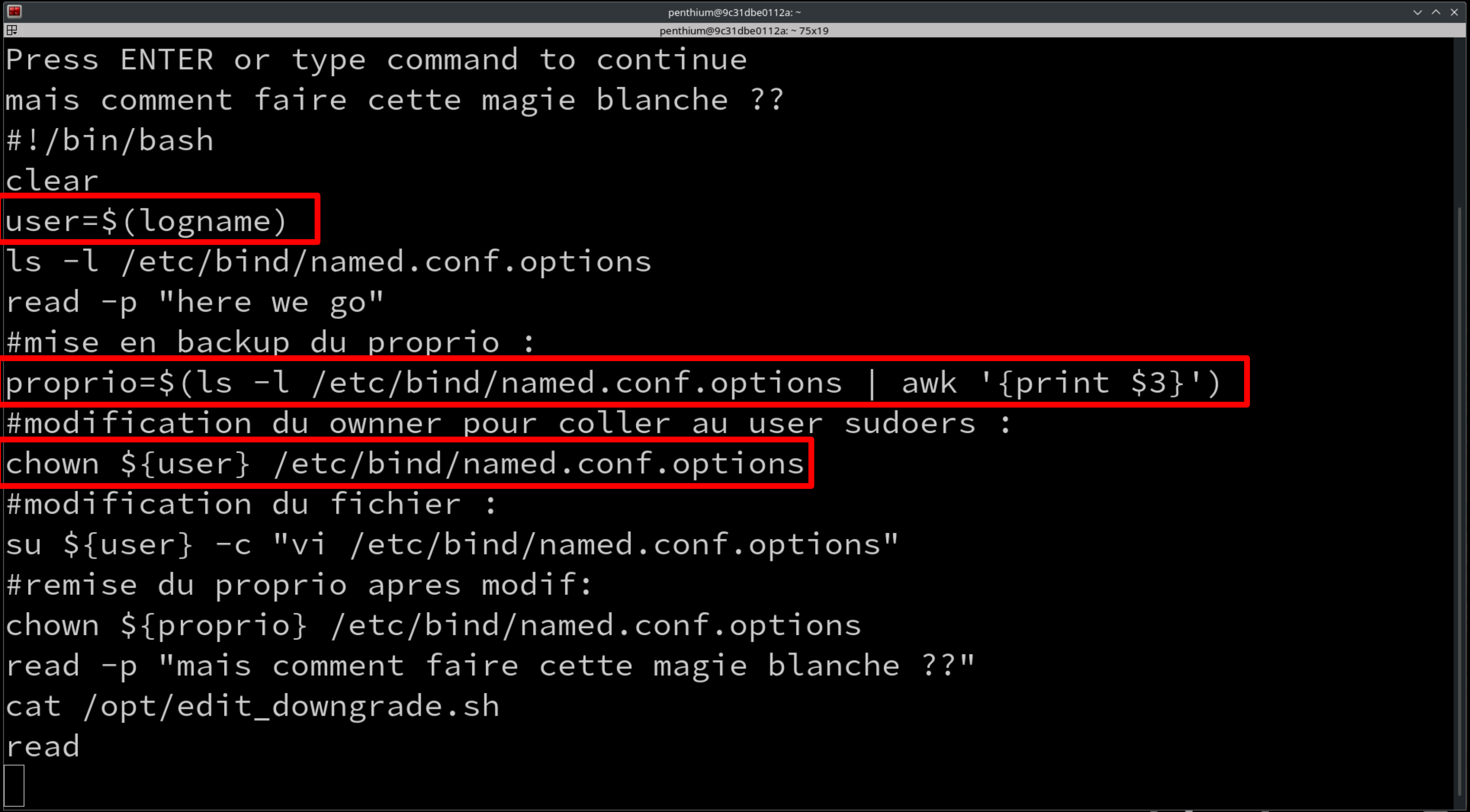
penthium2



```
Press ENTER or type command to continue
mais comment faire cette magie blanche ??
#!/bin/bash
clear
user=$(logname)
ls -l /etc/bind/named.conf.options
read -p "here we go"
#mise en backup du proprio :
proprio=$(ls -l /etc/bind/named.conf.options | awk '{print $3}')
#modification du ownner pour coller au user sudoers :
chown ${user} /etc/bind/named.conf.options
#modification du fichier :
su ${user} -c "vi /etc/bind/named.conf.options"
#remise du proprio apres modif:
chown ${proprio} /etc/bind/named.conf.options
read -p "mais comment faire cette magie blanche ??"
cat /opt/edit_downgrade.sh
read
```

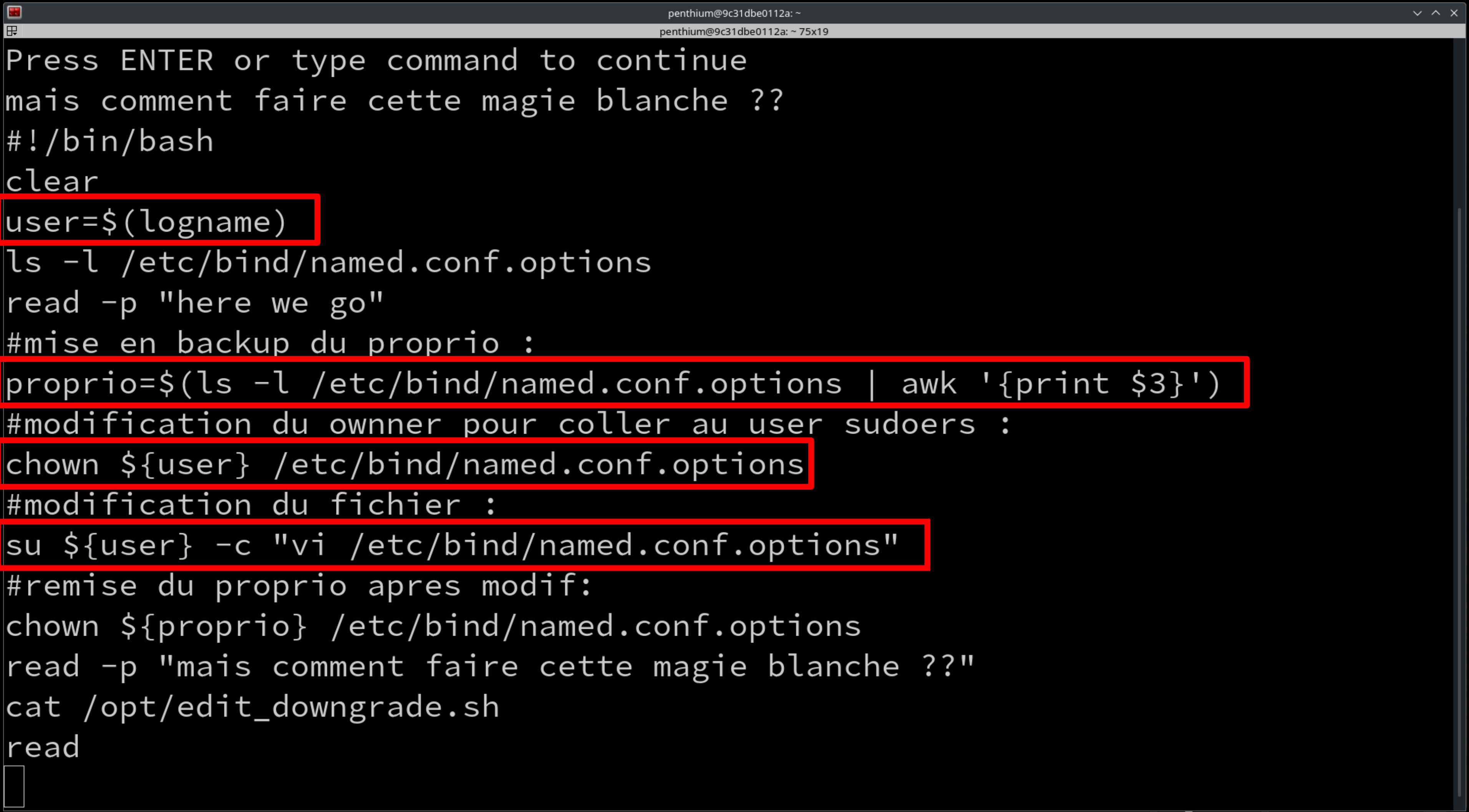


```
Press ENTER or type command to continue
mais comment faire cette magie blanche ??
#!/bin/bash
clear
user=$(logname)
ls -l /etc/bind/named.conf.options
read -p "here we go"
#mise en backup du proprio :
proprio=$(ls -l /etc/bind/named.conf.options | awk '{print $3}')
#modification du ownner pour coller au user sudoers :
chown ${user} /etc/bind/named.conf.options
#modification du fichier :
su ${user} -c "vi /etc/bind/named.conf.options"
#remise du proprio apres modif:
chown ${proprio} /etc/bind/named.conf.options
read -p "mais comment faire cette magie blanche ??"
cat /opt/edit_downgrade.sh
read
```

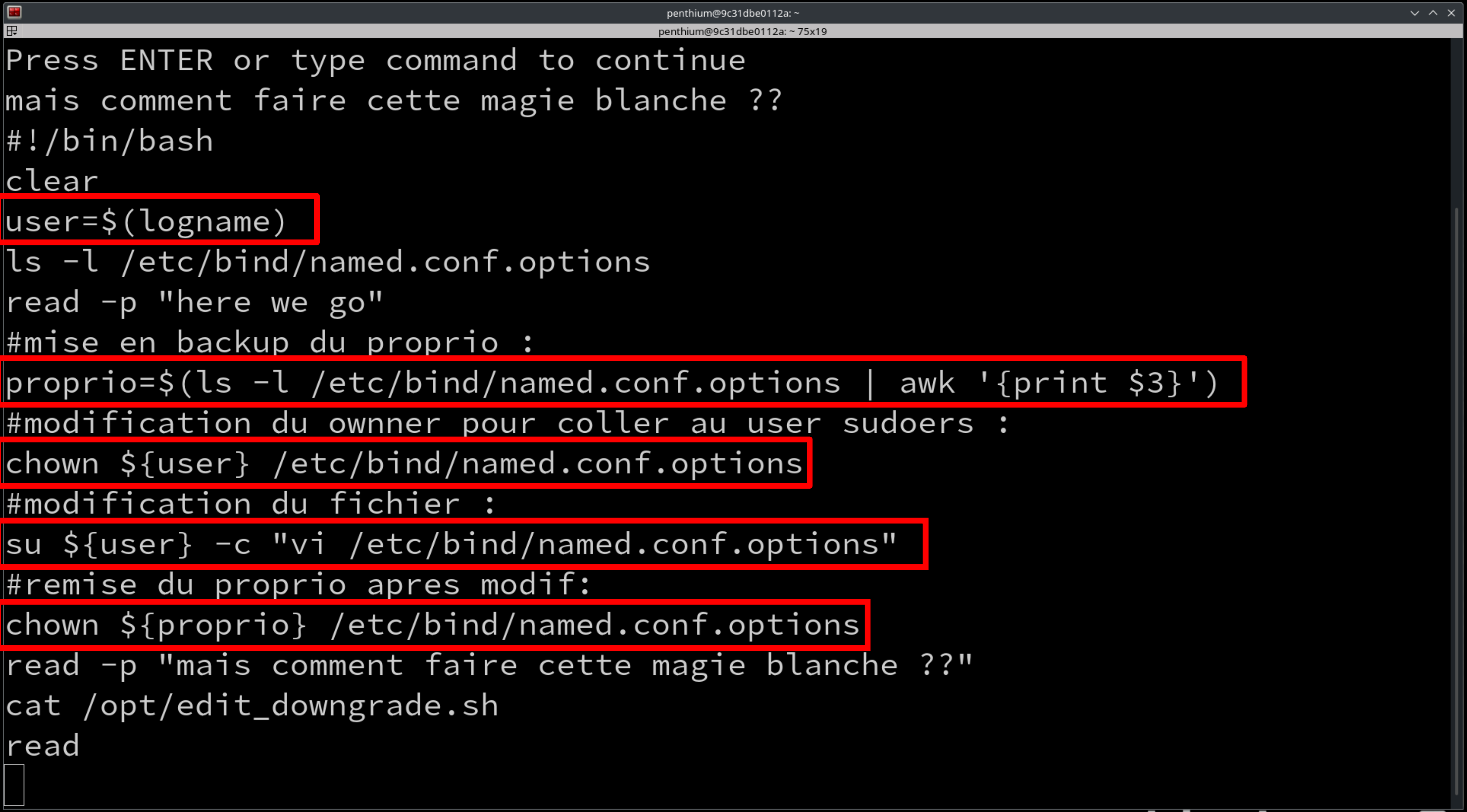


```
Press ENTER or type command to continue
mais comment faire cette magie blanche ??
#!/bin/bash
clear
user=$(logname)
ls -l /etc/bind/named.conf.options
read -p "here we go"
#mise en backup du proprio :
proprio=$(ls -l /etc/bind/named.conf.options | awk '{print $3}')
#modification du ownner pour coller au user sudoers :
chown ${user} /etc/bind/named.conf.options
#modification du fichier :
su ${user} -c "vi /etc/bind/named.conf.options"
#remise du proprio apres modif:
chown ${proprio} /etc/bind/named.conf.options
read -p "mais comment faire cette magie blanche ??"
cat /opt/edit_downgrade.sh
read
```

penthium2



```
Press ENTER or type command to continue
mais comment faire cette magie blanche ??
#!/bin/bash
clear
user=$(logname)
ls -l /etc/bind/named.conf.options
read -p "here we go"
#mise en backup du proprio :
proprio=$(ls -l /etc/bind/named.conf.options | awk '{print $3}')
#modification du ownner pour coller au user sudoers :
chown ${user} /etc/bind/named.conf.options
#modification du fichier :
su ${user} -c "vi /etc/bind/named.conf.options"
#remise du proprio apres modif:
chown ${proprio} /etc/bind/named.conf.options
read -p "mais comment faire cette magie blanche ??"
cat /opt/edit_downgrade.sh
read
```



```
Press ENTER or type command to continue
mais comment faire cette magie blanche ??
#!/bin/bash
clear
user=$(logname)
ls -l /etc/bind/named.conf.options
read -p "here we go"
#mise en backup du proprio :
proprio=$(ls -l /etc/bind/named.conf.options | awk '{print $3}')
#modification du ownner pour coller au user sudoers :
chown ${user} /etc/bind/named.conf.options
#modification du fichier :
su ${user} -c "vi /etc/bind/named.conf.options"
#remise du proprio apres modif:
chown ${proprio} /etc/bind/named.conf.options
read -p "mais comment faire cette magie blanche ??"
cat /opt/edit_downgrade.sh
read
```

ReactionGIFS.me

```
resumons tout cela !
```

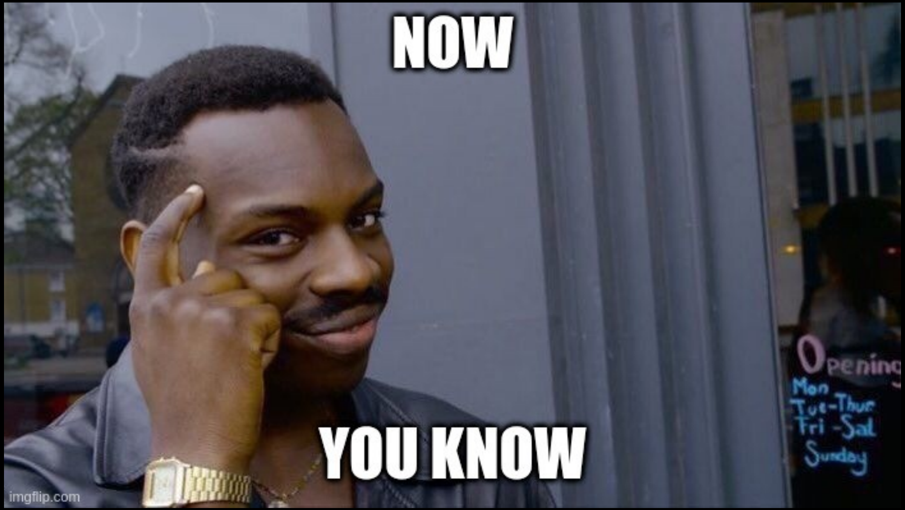
penthium@9c31dbe0112a: ~

penthium@9c31dbe0112a: ~ 75x19

resumons tout cela !

Dans un script avec élévation de privilège,
les commandes sensibles peuvent être exécutées avec des droits plus faibles
 via :

```
su <user à faible privilège> -c '<commande à éxécuter>'
```



```
penthium@9c31dbe0112a: ~
penthium@9c31dbe0112a: ~ 75x19
 penthium2@fedora
```

penthium2