How to recover KVM Virtual Machine root password

Written by Friends
Saturday, 19 April 2014 09:47 -

This procedure shows how to recover root password on a KVM Virtual Machine running Linux OS and which uses LVM partitioning schema.

1) Login as root on your KVM HOST System

2) run virsh to shutdown your Virtual Machine for which you want to recover root password

virsh

3) Get your VM ID using virsh command list:

list

Id Name State
_____
2 my-vm-linux running

4) Shut it down using:

shutdown 2

Domain 2 is being shutdown

exit

5) now let's mount your VM IMG file on your host system so that we can change root password (To proceed you'll need two extra tools: kpartx and lvm2 so please install as appropriate for your linux distro on your HOST system)

6) Use "kpartx" to read partition tables & create device maps of your image:

kpartx -av .img

(Please note: usually on Red Hat based compliant systems, so CentOS, Fedora, RHEL and PacketLinux your Virtual Machine Image file should be in /var/libvirt/images)

7) Use "pvscan" to see your LVM block devices for physical volume:

pvscan

PV /dev/mapper/loop1p5 VG vg_kvm_vm lvm2 [97.41 GiB / 0 free]
 PV /dev/md127p2 VG vg_kvmserver lvm2 [1.82 TiB / 0 free]
 Total: 2 [1.91 TiB] / in use: 2 [1.91 TiB] / in no VG: 0 [0]

8) Use "vgscan" to see your LVM physical volumes & volume groups.

vgscan

Reading all physical volumes. This may take a while…
 Found volume group "vg_kvm_vm" using metadata type lvm2

9) Use "lvscan" to see your LVM block devices for logical volumes.
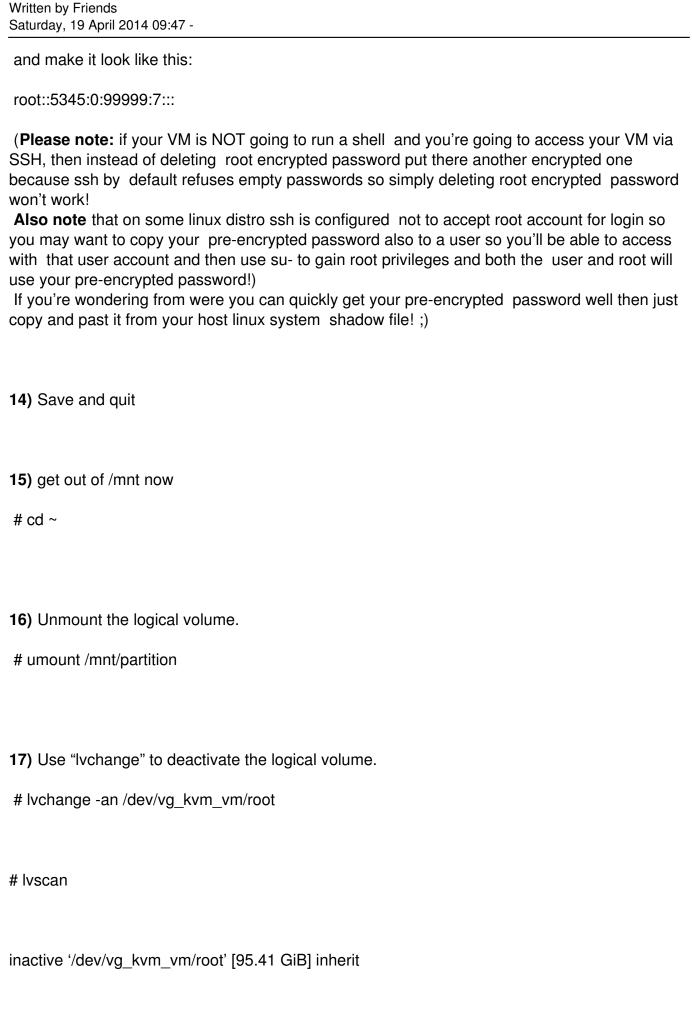
```
# lvscan
```

```
inactive '/dev/vg_kvm_vm/root' [95.41 GiB] inherit
 inactive '/dev/vg_kvm_vm/swap_1′ [2.00 GiB] inherit
 ACTIVE '/dev/vg_kvmserver/lv_root' [50.00 GiB] inherit
 ACTIVE '/dev/vg_kvmserver/lv_home' [1.76 TiB] inherit
 ACTIVE '/dev/vg_kvmserver/lv_swap' [7.69 GiB] inherit
```

10) Use "lvchange" to activate the logical volume, to make it useable.

```
# lvchange -ay /dev/vg_kvm_vm/root
```

```
# lvscan
 ACTIVE '/dev/vg_kvm_vm/root' [95.41 GiB] inherit
 inactive '/dev/vg_kvm_vm/swap_1′ [2.00 GiB] inherit
 ACTIVE '/dev/vg_kvmserver/lv_root' [50.00 GiB] inherit
 ACTIVE '/dev/vg_kvmserver/lv_home' [1.76 TiB] inherit
 ACTIVE '/dev/vg_kvmserver/lv_swap' [7.69 GiB] inherit
```

11) Mount your volume using:

```
# mount /dev/vg_kvm_vm/root /mnt
```

12) Get into /etc/ and edit your shadow password as described:

```
# cd /mnt/etc
# vi shadow
```

13) Locate the root user in shadow password file and change the password with an empty one:

```
root:$8$gbwrd7.g/:5345:0:99999:7:::
```

and make it look like this:

root::5345:0:99999:7:::

 (**Please note:** if your VM is NOT going to run a shell and you're going to access your VM via SSH, then instead of deleting root encrypted password put there another encrypted one because ssh by default refuses empty passwords so simply deleting root encrypted password won't work!
 Also note that on some linux distro ssh is configured not to accept root account for login so you may want to copy your pre-encrypted password also to a user so you'll be able to access with that user account and then use su- to gain root privileges and both the user and root will use your pre-encrypted password!)
 If you're wondering from were you can quickly get your pre-encrypted password well then just copy and past it from your host linux system shadow file! ;)

14) Save and quit

15) get out of /mnt now

 # cd ~

16) Unmount the logical volume.

 # umount /mnt/partition

17) Use "lvchange" to deactivate the logical volume.

 # lvchange -an /dev/vg_kvm_vm/root

lvscan

inactive '/dev/vg_kvm_vm/root' [95.41 GiB] inherit

```
inactive '/dev/vg_kvm_vm/swap_1' [2.00 GiB] inherit
ACTIVE '/dev/vg_kvmserver/lv_root' [50.00 GiB] inherit
ACTIVE '/dev/vg_kvmserver/lv_home' [1.76 TiB] inherit
ACTIVE '/dev/vg_kvmserver/lv_swap' [7.69 GiB] inherit
```

18) Use "vgchange" to deactivate the volume group.

```
# vgchange -an vg_kvm_vm
0 logical volume(s) in volume group "vg_test1" now active
```

19) Use "kpartx" to delete device maps of your image.

```
kpartx -dv .img
```

```
del devmap : loop10p2
del devmap : loop10p1
loop deleted : /dev/loop1
```

20) Ok at this point you can boot up your Virtual Machine and try to login!