1 Overview

This section is meant to give you a general overview of how we expect you to use KVM. It is possible to ssh into your honeypot with X11 forwarding enabled (the \texttt{-X} flag for ssh) and thus have KVM spawn a separate window for the VM within the ssh session. This is useful for quick sessions in which you want to see if something is working, etc. The disadvantage of this approach is that if you want to keep your VM running for some extended period of time, you would need to keep your ssh session alive. This will clearly become a problem.

In order to address this, we will use vncviewer to connect to KVM and provide us with a display, the problem with this is that the vnc protocol is insecure (i.e., runs unencrypted) over the network. To address this problem we will tell KVM to only accept connections from \texttt{localhost} and build a ssh tunnel for the vnc traffic.

2 Creating a Disk Image

Before you are able to start KVM, you will need to create a virtual disk. For this you will need to use the \texttt{qemu-img} utility. We recommend that you create a disk 50 GB in size and in raw format. We recommend the raw format as this will allow you to mount the image from the host if necessary. If you choose to create a disk smaller that 50 GB, make sure that you will not need more as resizing a disk is not a straightforward task. If you choose to create a disk larger than 50 GB, make sure that enough space remains on the host. It may also make sense to back up this image within your network home directory (i.e., on \texttt{praksrv}), once it is in a setup state. For information on using the \texttt{qemu-img} utility, please see the appropriate man pages.

2.1 Example

Here is a simple example of creating a 50 GB raw disk called \texttt{disk.img}:

\begin{verbatim}
qemu-img create -f raw disk.img 50G
\end{verbatim}
3 Creating a ssh Tunnel

This portion is fairly straightforward, you must ssh into your honeypot, thereby providing a few extra ssh arguments. Assuming that you want to use display 1, here is proper command:

```
ssh -L localhost:5901:localhost:5901 <user>@<hostname>
```

This command starts a ssh session in which all traffic sent on port 5901 of the local host is forwarded to port 5901 of the remote host and vice versa and this only for traffic originating from the local host. For more information refer the ssh man pages.

4 Starting KVM

Due to the fact that the networking is setup in a specific way and for some of the setup tools root access is required, we have embedded some important steps in a KVM start-up script. It is important that you use this script to start KVM, otherwise your virtual machine will start behind a virtual NAT box bound to the eth0 interface (i.e., within the Control Network). The following is required to start KVM with the correct network setup:

```
kvm_start.sh -net nic,macaddr=<mac_address>
```

In addition there are further options that will be helpful:

- **-vnc localhost:1** This has KVM listen for incoming vnc connections for display 1 on which to display output. In addition, KVM will only accept connections from localhost. This is used in conjunction with a ssh tunnel.
- **-k de** This sets the keyboard layout to German. This must be used when using the -vnc option.
- **-usbdevice tablet** This will sync the mouse cursor when using vnc to display output.
- **-hda <disk_image>** This will set disk_image as the primary hard drive.
- **-m <ram_size>** This will set the RAM size to ram_size in MB.
- **-cdrom <cd_image>** This will start KVM with cd_image in a virtual cdrom drive. cd_image may either be an ISO image or a cdrom device node (e.g., /dev/cdrom).
- **-boot d** This will boot the machine from the cdrom drive. Booting from the hard disk is the default.
- **-daemonize** This will start KVM as a daemon. This is useful for leaving a VM running after you logout. Though, be sure to use the -vnc option in conjunction with this, so that you have a way to access a display.

There are many more available options. For further details, see the KVM man pages.
4.1 Example

Here a simple example of starting a VM from a disk image called disk.img with 512 MB of RAM:

```
```

4.2 Choosing a MAC Address

When choosing a MAC address please choose one with the following first 3 bytes: 00:60:67. That is, please choose a MAC address of the form:

```
00:60:67:XX:XX:XX
```

where you may freely choose the last three bytes (XX:XX:XX). Though, make sure with other groups that we have no duplicate MAC addresses within our network. This would lead to interesting network problems.

5 Using vncviewer

If you have created a ssh tunnel and started KVM with the -vnc option, you may now use vncviewer from your workstation. This is a client that will connect to KVM on the honeypot and show you the display. Assuming that you want to use display 1, here is the command you will use:

```
vncviewer localhost:1
```