Using the Luddy Hall Security Lab (3115)

Available Machines

There are 24 workstations available, running Red Hat Enterprise Linux and qemu/kvm hypervisor. Each machine is designated by a sticker on the top, labelled H01-H24, corresponding to the name of the host. Hosts are given static IP addresses and DNS entries of the form lab009hxx.soic.indiana.edu, where xx is the number of the host as shown on the top of the machine. These systems are part of the Burrow account domain which allows login by most SICE students. In addition, local accounts for running VMs are set up with usernames seclabu1-seclabu4 as part of a class, per the direction of your instructor. Qemu/kvm was chosen for being open source with no licensing issues, and the ability to have guests continue running when the user logs out of the machine.

Because these systems are intended as a learning environment with few restrictions, the somewhat paradoxical result is that the security lab machines are in many ways the least secure on campus. Users can control other vm guests on the machine they use. Students are expected to be good neighbors to one another.

There are a limited number of static IP addresses available for guests which require them. A static IP is only required if it is necessary to reach the guest directly from outside the lab. DNS entries are of the form lab009gxx[a-g].soic.indiana.edu, where the xx is again the host number, the g stands for guest instead of host, and the letters a through g are assigned in the order in which they are used. No public IP addresses are assigned with dhcp servers, but a private one may be assigned if the guest only requires a NAT'ed network access to the campus network.

Use of VM Guests

Creating a guest

Guests are typically created either by full installation, such as from a .iso file, or by importing an existing image. It may also be that an image has been prepared and distributed to all the machines in the lab, and is ready to go. Virt-manager may be invoked from the command line, or selected from the Applications menu. Below is a screen shot.

![Virtual Machine Manager](image)

To create a new guest, click on the icon of a monitor in the upper left that is lit up. This will result in a pop-up box to create the new guest.

Guests which require a static IP address should use a name for the guest which allows us to determine which static IP addresses are already in use, and who is using them. The recommended nomenclature is something of the form A-I330-username, so that we can see that the static IP for lab009g25a.soic.indiana.edu is in use by a student in I330. The next student would use B-coursename-username, and so on. This name is recognized only within virt-manager, and the only correlation with actual DNS entries is merely our convention. You will not be able to ssh to a guest by using this name. If no static IP address is required, it is helpful to identify the guest in rational fashion, but this is not strictly enforced.

Once the name has been filled in, and the choice of installation methods selected, continue to the next window.
Create a new virtual machine

Step 2 of 5

Locate your install media

- Use CDROM or DVD

- Use ISO image:
  /var/lib/libvirt/images/ubuntu-14.04.1-server-a

Choose an operating system type and version

- OS type: Linux
- Version: Ubuntu 13.10 (Saucy Salamander)

Locate ISO media volume (on lab009h25.soic.indiana.edu)

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Format</th>
<th>Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWASP Broken Web Apps-c11-s005.vmdk</td>
<td>4.00 MB</td>
<td>vmdk</td>
<td>A-1430-rkonig</td>
</tr>
<tr>
<td>OWASP Broken Web Apps-c11.vmdk</td>
<td>0.00 MB</td>
<td>raw</td>
<td></td>
</tr>
<tr>
<td>OWASP Broken Web Apps.nvram</td>
<td>0.01 MB</td>
<td>raw</td>
<td></td>
</tr>
<tr>
<td>OWASP Broken Web Apps.vmsd</td>
<td>0.00 MB</td>
<td>raw</td>
<td></td>
</tr>
<tr>
<td>OWASP Broken Web Apps.vmx</td>
<td>0.00 MB</td>
<td>raw</td>
<td></td>
</tr>
<tr>
<td>OWASP Broken Web Apps.vmxf</td>
<td>0.00 MB</td>
<td>raw</td>
<td></td>
</tr>
<tr>
<td>owaspbwa-release-notes.txt</td>
<td>0.01 MB</td>
<td>raw</td>
<td></td>
</tr>
<tr>
<td>OW-clone.qcow2</td>
<td>8.00 GB</td>
<td>qcow2</td>
<td>A-1430-rkonig</td>
</tr>
<tr>
<td>pool1</td>
<td>0.00 MB</td>
<td>dir</td>
<td></td>
</tr>
<tr>
<td>secwin7.img</td>
<td>16.00 GB</td>
<td>qcow2</td>
<td>secwin7</td>
</tr>
<tr>
<td>SEEDU12.04-clone.qcow2</td>
<td>80.00 GB</td>
<td>qcow2</td>
<td>B-1330-robbik</td>
</tr>
<tr>
<td>SEEDU12.04.qcow2</td>
<td>80.00 GB</td>
<td>qcow2</td>
<td>SEED</td>
</tr>
<tr>
<td>torRC.qcow2</td>
<td>40.00 GB</td>
<td>qcow2</td>
<td></td>
</tr>
<tr>
<td>ubuntu-14.04.1-server-amd64.iso</td>
<td>572.00 MB</td>
<td>iso</td>
<td></td>
</tr>
<tr>
<td>Win7lab.qcow2</td>
<td>40.00 GB</td>
<td>qcow2</td>
<td>Win7lab</td>
</tr>
<tr>
<td>Win7lab.vmdk</td>
<td>40.00 GB</td>
<td>vmdk</td>
<td></td>
</tr>
<tr>
<td>Windows7-64bit.iso</td>
<td>2.96 GB</td>
<td>iso</td>
<td>secwin7</td>
</tr>
</tbody>
</table>
For a typical lab installation, hit the "Browse" button to go to the next screen, select the iso file to be used, then hit the "Choose Volume" button to return to the previous screen. Select an appropriate OS type and Version (if the one being installed is higher than what is available as a choice, pick the closest one available), then go on to the next screen.

For Redhat/Centos up to 7, and Ubuntu up to the LTS 12.04, the default is usually sufficient. For more recent Ubuntu releases, 2GB of ram is better. For Windows, typically 2-4GB of ram is needed. 1 CPU core is generally sufficient unless instructed otherwise. Then proceed.
The default of 8.0GB is sometimes small, if there is going to be database work. Something like 12-16GB gives us a little breathing room. By default, the "Allocate entire disk now" box is checked. **It is advisable to uncheck this box,** as the performance gain is minimal, and this allows for smaller disk images. Letting the disk image grow only as needed will be particularly helpful in making any back-up of the image. Then proceed as usual.
In the last screen here, Advanced options has been selected. The typical choices for a primary network interface would be either a Bridged device, as would be required for a static IP, or a NAT device, if no incoming connections are required. Other characteristics, such as specific emulated devices for a NIC or a graphics card, can be selected by choosing to customize the configuration before installation. When everything is ready, hit "Finish" and go through the normal installation steps for the OS to be installed.

Managing guests

In the first screenshot above, there are several buttons which can be used to manage an existing guest. Next to the "create" button, there are buttons to open, run, pause, shutdown, or pick types of shutdown.

Open will open up a console for the guest. If the guest is running, the console will display a message informing the user of this. Otherwise, it will open whatever type of console (terminal or graphical) has been installed. More on this below.

Run will attempt to start a guest that has been shutdown.

Pause will pause a guest without shutting it down. It does not free up ram resources, but does allow snapshots to be taken without turning the guest off.

Shutdown will send a shutdown signal to the guest. Not all guests will acknowledge this.

There is also a dropdown menu for other types of shutdown. In order of "emergency", they are reboot, shutdown, force reset and force off. Force off is similar to a power failure. Once can also save the state of the system without powering it down, which might be useful for testing items such as kernel modifications.

If the console has been opened, a couple of new selections become available, as shown.
The diamond-shaped icon on the right allows the user to go into full-screen mode, thus appearing for the most part as though the guest console is the only OS running.

The little light-bulb-like icon is for displaying and modifying the machine details. Clicking on it brings up a new screen that looks something like this:
From this screen, additional hardware can be added, such as a second virtual NIC, or existing virtual hardware can be modified. Common choices might be to change the emulated hardware, such as the graphics card or NIC, or to add a virtual cdrom and attach it to a .iso file. No changes will be made active until the “Apply” button has been selected and the virtual guest has been restarted. It is also possible to allocate additional or modify CPU parameters, if the guest will recognize it.

Networking in the Lab

There are three types of physical network choices available in the lab.

Campus Network

Any virtual guest which is to be accessible from outside the lab must use a static IP address from the pool available for our use. There is no publicly routable dhcp server. In order to use a static IP, determine the next available address and DNS entry for a guest on the host machine being used. As noted previously, the DNS entry would be similar to this: lab009g25b.soic.indiana.edu. Using nslookup, dig, or ping on the host, the numeric form of the IP address can be found, and entered appropriately for the guest OS configuration. When completed, this will appear exactly as though it were running on physical hardware. Access to the rest of the internet is allowed, and incoming access from campus/vpn works.
Set-up:
Device type: Bridged (br0)
IP Address: Look up from corresponding DNS entry, e.g. lab009g25b.soic.indiana.edu is 156.56.103.131
Gateway: 156.56.103.1
Netmask: 255.255.255.0
DNS: 129.79.1.1

Lab Network

All machines in the lab have a second NIC installed. This network is available only within the lab, and only statically assigned non-routable addresses. Addresses should be chosen of the form 192.168.xx.[1-255], where xx is the number of the host, and 1-255 would be chosen as assigned for the lab. The netmask excludes the IP addresses in the range for the internal virtual network (192.168.122.[1-255]). Communication between guests on different host machines within the lab is possible.

Set-up:
Device type: Bridged (lab)
IP Address: 192.168.xx.[1-255], where xx is the host number and the last octet is arbitrarily assigned. Addresses are static unless lab instructors request a dhcp server.
Gateway: None
Netmask: 255.255.192.0
DNS: None, unless set up by request

Internal Virtual Network

If incoming access from outside the lab (e.g., ssh, web server) is not required, and only outgoing requests are needed (e.g., apt-get), the internal network on the host is sufficient. There is an internal dhcp server for this network, and IP addresses will be arbitrarily assigned within the range 192.168.122.[1-255]. To communicate between guests on the same host, log in to each guest and find the IP address. The virtual devices here are treated in much the same manner as actual devices connected to a wireless router. Network address translation (NAT) is used for communication on the campus network. It is possible to reach outside web sites, for example, but not possible to ssh in and log in to a guest using only this type of network connection.

Set-up:
Device Type: Virtual network 'default': NAT
All other parameters set automatically by internal dhcp server. Guest should specify dynamic IP address type.