

Virtual Lab with VMware

digg this story

Discuss in Forums {mos_smf_discuss:/root}

By EH-Net Member Negrita

Some of you reading this may be studying for Certified Ethical Hacker (CEH) or perhaps some other certification at the moment. While reading the study material and installing some of the tools on a box may suffice for some, others would prefer to have an actual lab to do their penetration testing. Buying separate boxes for all your Operating Systems (OSs) can be quite expensive, and may deter some people from wanting to do certs in the first place (unless someone else is paying for it). Thankfully there is a cheap solution to all this and you can get to learn some new things on the way.

The Exam Prep CEH book by Michael Gregg (which I'm using) recommends using at least 3 boxes; a Microsoft Windows Server, a Microsoft Windows Client and a Linux Client. After getting into things, Michael Gregg recommends installing a Linux Server too, as these are the systems you'll most probably be working with afterwards.

Virtualization is a method of using "logical" computers as opposed to using physical ones. To simplify my last statement, this means that you can install a virtual computer to run on your physical box as if it were an application. While there are a few virtualization software vendors in the market, the 2 main players are VMware and Microsoft. Some of the others include Bochs, PearPC, Parallels, SVISTA and XenSource, which are all open source. Check out this comparative table with a much fuller list. In this tutorial, I'll discuss how I've used 2 VMware products to set up my lab. The first is VMware Player and the second is VMware Workstation. I'm certainly no expert on virtualization or these tools, but I'm gladly sharing with you all how I set things up for myself, in the hope that it will help some of you too or at least give you an interesting read.

Before getting started, there are a few facts and some terminology you should know about virtual machines;

1. The main Operating System on the box is known the "host", while the virtual computers running on them are known as "guests".
2. A guest with a disk drive of say 4Gb will create a file of 4Gb on the host OS. Make sure you have enough disk space.
3. The guest OS uses RAM taken from the host. Before running a guest OS on the host, you must make sure you have

enough RAM to support both/all OSs running concurrently.

4. A 64-bit guest OS cannot run on a 32-bit host OS. Make sure the guest OS matches the host's CPU.

5. Most importantly, YOU MUST HAVE A VALID LICENSE FOR ALL OS'S RUNNING ON YOUR SYSTEM. For example, if you have a Windows XP guest running on a Linux host, you must have a valid license for both OSs (Yes I know Linux comes with a GPL copyleft). Just because the XP machine is virtual doesn't exempt it from needing a license.

One of the tools I use is called VMware Player, a FREE application that allows you to run predefined virtual guests, which can also be downloaded for FREE. All the FREE virtual machines offered are obviously open source. VMware Player can be played on Windows 2000 Pro and Server, Windows XP Home and Pro, and also Windows Server 2003. It can also be played on various flavours of Red Hat Enterprise Linux, SUSE Linux, Mandrake Linux and Ubuntu Linux.

After downloading and installing VMware Player, you'll want something to play on it. Go to the VMTN Virtual Appliance web page and look through the list of virtual appliances available. You can choose from a wide variety of regular distros like Kubuntu, Gentoo, Debian, Fedora Core, FreeBSD, etc. A very large variety of tools and applications can be found like VPN servers, proxies, firewalls and scanners, and Nagios and other network monitors. Of particular interest to the hacking community are the specialised security appliances such as BackTrack. When downloading a virtual appliance take note of the primary accounts (root) username and password which should be on the download page.

One particularly useful appliance is the LiveCD Virtual Appliance which as the name suggests, allows you to play a live CD. You don't actually have to have a CD in the tray for this to work, but rather the live CD's iso image which must be placed in the same directory as the LiveCD Virtual Appliance. The iso image must be renamed "livecd.iso" for it to work.

Now that you've got your favourite linux distro running, you may start to wonder about the Windows part of the test lab. Surprisingly there is a FREE and legal solution to all this too. VMware Player will only play preinstalled virtual machines, but to create those virtual machines you need a program like VMware Workstation (which I use) or VMware Server. VMware Workstation comes fully functional with a FREE 30 day evaluation license. Once installed, you can use it to create as many virtual machines as you like. The list of supported host OSs is similar to that mentioned above for VMware Player, but the list of guest OSs includes practically all versions of Windows from Windows 95 to Vista including both 32 and 64-bit options, and also a variety of 32 and 64-bit open source OS versions and flavours such as Red Hat Enterprise Linux, SUSE Linux, Mandrake Linux, Turbolinux, Ubuntu Linux, Sun JDS, Novell, FreeBSD, Sun Solaris and other custom Linux installs with a 2.4.x or 2.6.x kernel.

Microsoft will let you download and install a 64-bit version of Windows XP Professional together with a 120 day evaluation license, and a 32 or 64-bit version of Windows Server 2003 together with a 180 day evaluation license. This should be more than enough time to study for CEH and probably a few other certs too.

Adding a new virtual machine is as simple as clicking File>New>Virtual Machine, and then following the instructions of the wizard. First choose if you want a typical or custom install. You will be prompted for the type of OS, the virtual machine's name (i.e. Win2K3 No.1), the machine's location on the host OS, the type of network connection (more on that later), and the capacity of the guest OS hard disk. You can change the amount of RAM the guest uses amongst other things, by clicking on "Edit virtual machine settings" afterwards. This can also be set, by choosing a custom install from the wizard. The custom install will also allow you to use a guest with 2 CPUs. When choosing the guest's disk size, leave enough space for the OS install and for the tools you'll want to install on it afterwards. I find that 4Gb is more than adequate. Next put your install CD in the tray and click "Start this virtual machine". The install is just like that of a regular OS. You can install and download as many virtual machines as your host HDD can hold, but remember that if you don't have enough RAM, you won't be able to run them all concurrently.

After downloading and installing all the guests you want, you'll want to connect them together in a network. When you install VMware Player or Workstation, the application will install 2 default NIC's on the host. The first is called VMnet1

and the second VMnet8. The NICs can be enabled in 3 different modes; Bridged, NAT and Host-only. When installing a new guest, if you chose a typical install, the install will default to Bridged mode. Host-only mode will not allow the guest network access. Most of the virtual appliances I downloaded had been configured to use VMnet8 in NAT mode, which gives the guest OS access to the internet via the host's network connection, so you can surf the internet, and download tools and updates. On each guest I configured a default gateway of 192.168.42.1 and an IP in the 192.168.42.0/24 range. I then pinged the default gateway and some of the other guests to test the network connectivity. This can also be configured using teams. I'm no expert on teams, but more info about them can be found [here](#).

Finally a few words must be said about VMware Tools. VMware Tools is an all-important add on application which allows many things, such as support for faster graphics performance, synchronizing the clocks between the host and guest OSs and also supports file sharing and drag-and-drop features between the host and guests. More info about VMware tools can be found [here](#).

As I've said earlier, I'm not an expert on these topics and they are provided as-is for your use and knowledge. I will gladly receive criticism and comments in the corresponding post in the forum.