ComputerSecurityStudent (CSS)

(Damn Vulnerable Linux: [DVL])

{ How to Install DVL }

Section 0. Background Information

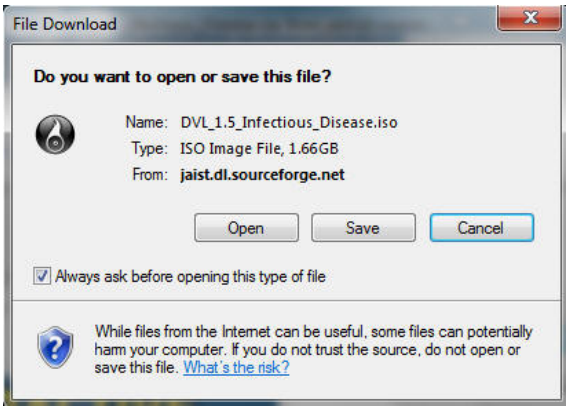
1. What is Damn Vulnerable Linux?
   - Damn Vulnerable Linux (DVL) is everything a good Linux distribution isn't. Its developers have spent hours stuffing it with broken, ill-configured, outdated, and exploitable software that makes it vulnerable to attacks.
   - DVL isn't built to run on your desktop -- it's a learning tool for security students. DVL is a live CD available as a 150MB ISO.
   - It's based on the popular mini-Linux distribution Damn Small Linux (DSL), not only for its minimal size, but also for the fact that DSL uses a 2.4 kernel, which makes it easier to offer vulnerable elements that might not work under the 2.6 kernel.
   - It contains older, easily breakable versions of Apache, MySQL, PHP, and FTP and SSH daemons, as well as several tools available to help you compile, debug, and break applications running on these services, including GCC, GDB, NASM, strace, ELF Shell, DDD, LDasm, LIDa, and more.
   - DVL was initiated by Thorsten Schneider of the International Institute for Training, Assessment, and Certification (IITAC) and Secure Software Engineering (S&#65533;e) in cooperation with Kryshaam from the French Reverse Engineering Team. "The main idea behind DVL," says Schneider, "was to build up a training system that I could use for my university lectures." His goal was to design a Linux system that was as vulnerable as possible, to teach topics such as reverse code engineering, buffer overflows, shellcode development, Web exploitation, and SQL injection.

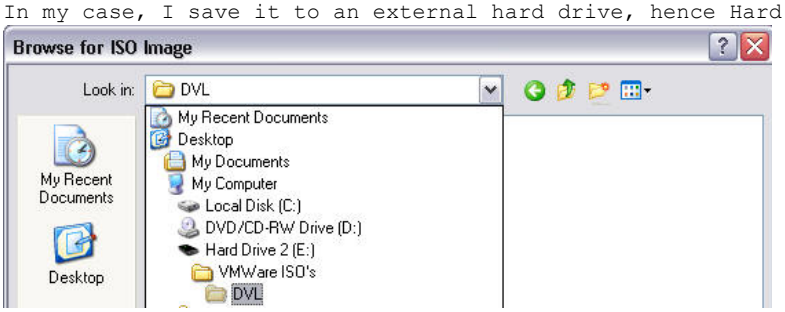
1. Prerequisite

1. You need to have virtualization software that allows you to create operating system images using either an ISO or installation CD. For this "how to", I will be using VMware Workstation. However, you can also use other popular tools, such as, VirtualBox.

2. Download the Damn Vulnerable Linux (DVL) iso

1. Download DVL
   - Click Here

2. Click Save
   - 

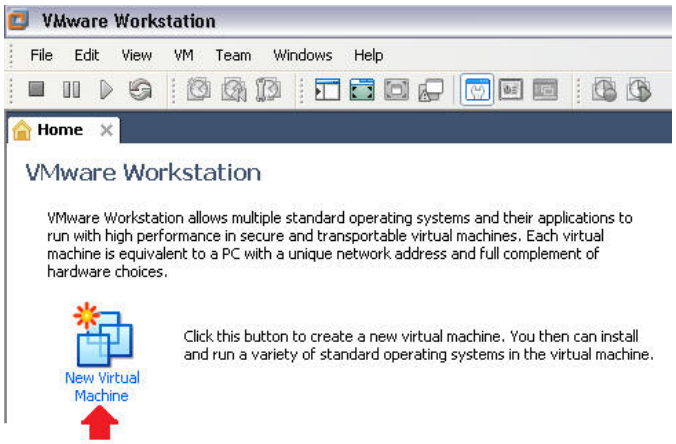
3. Save to C:\VMware ISO's\DVL\
   - In my case, I save it to an external hard drive, hence Hard Drive 2 (E:)
   - 

2. Start VMware Workstation

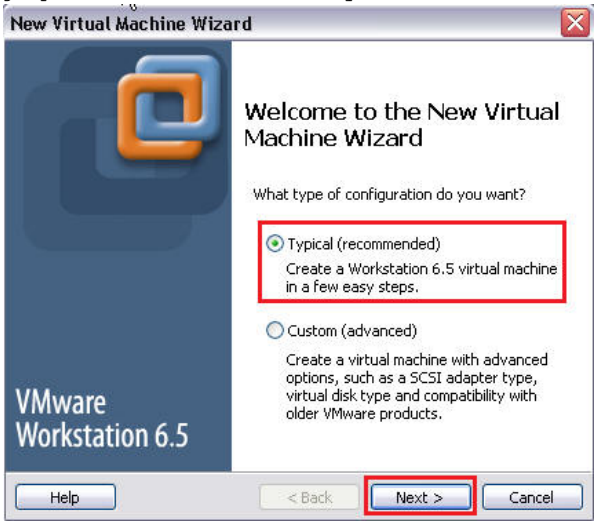
1. Programs --> VMware --> VMware Workstation.

3. Create VMware Image

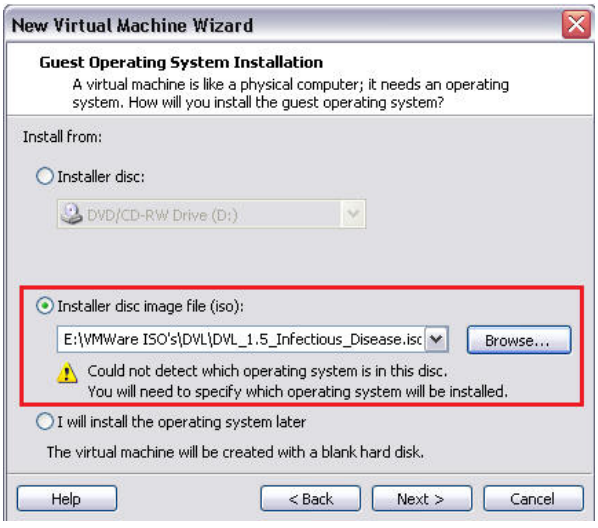
1. Click on New Virtual Machine.

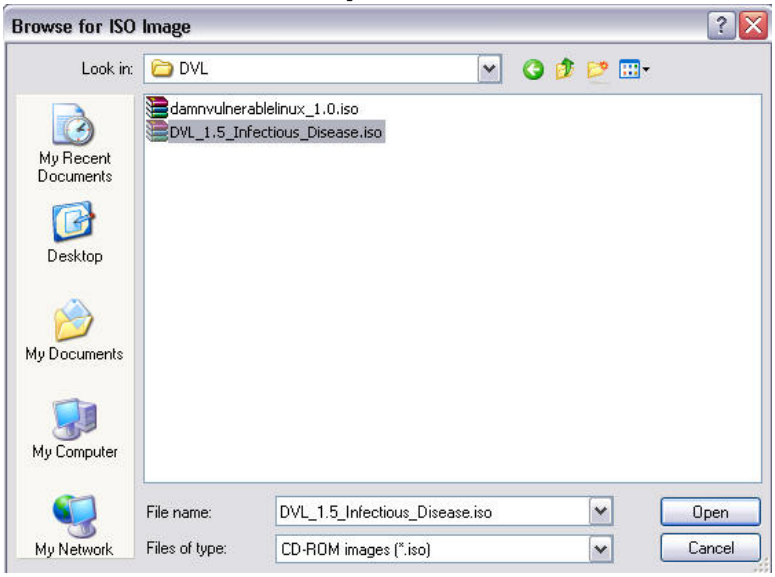


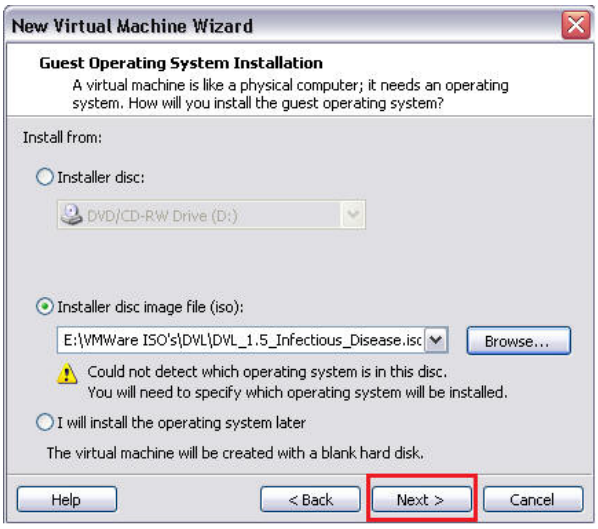
2. Bring up a FireFox Browser on your DVL machine.



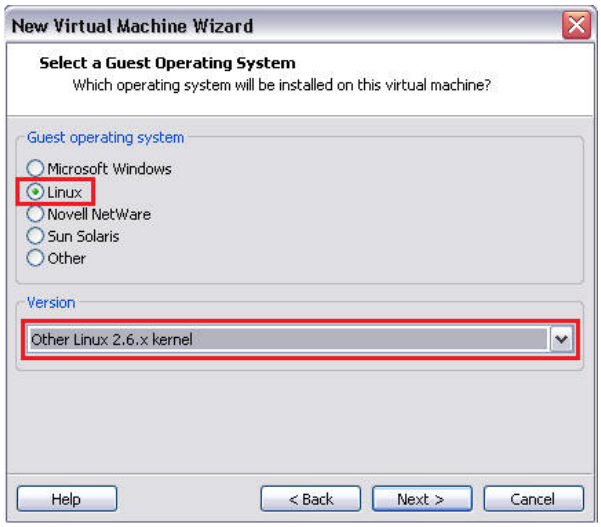
3. Select Install disc image file (iso)
   - Select the Browse Button



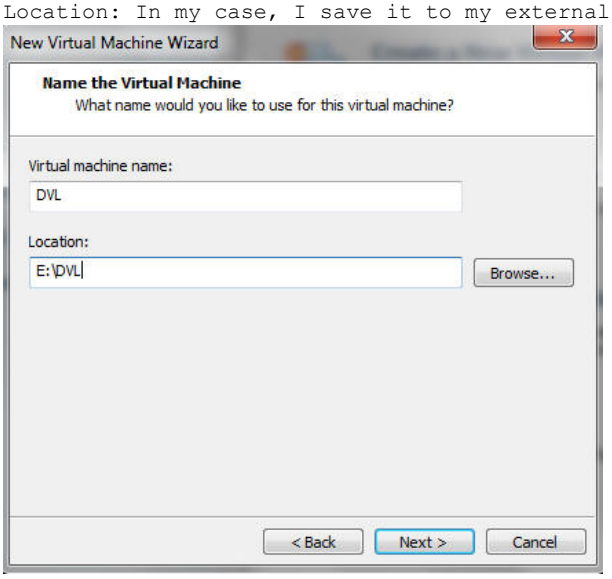
4. Navigate to where you save the DVL iso.
    - In my case, the iso was saved to E:\VMware ISO's\DVL\
    - Select DVL iso and click open
    - 

5. Select Next
    - 

6. Select the Linux OS, and Other Linux 2.6.x kernel

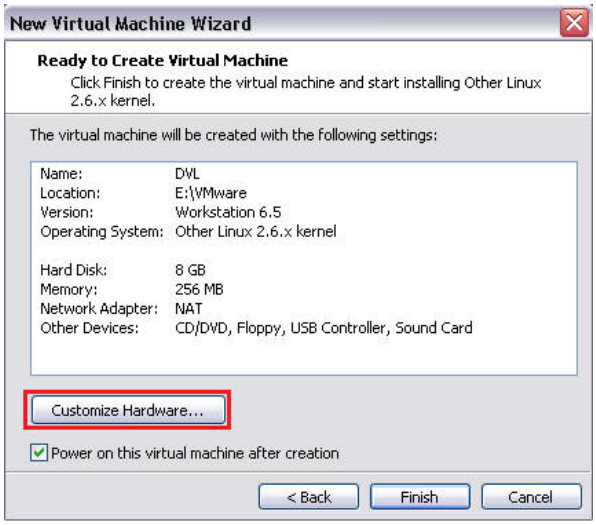


7. Naming and Saving Location
   - Virtual machine name: DVL
   - Location: In my case, I save it to my external hard drive at E:\VMware

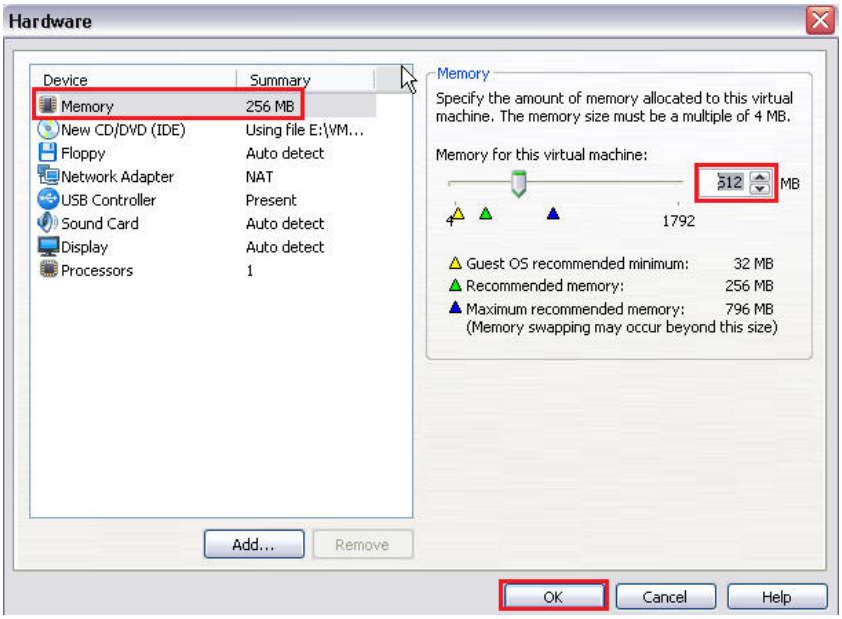


8. Specify Disk Capacity

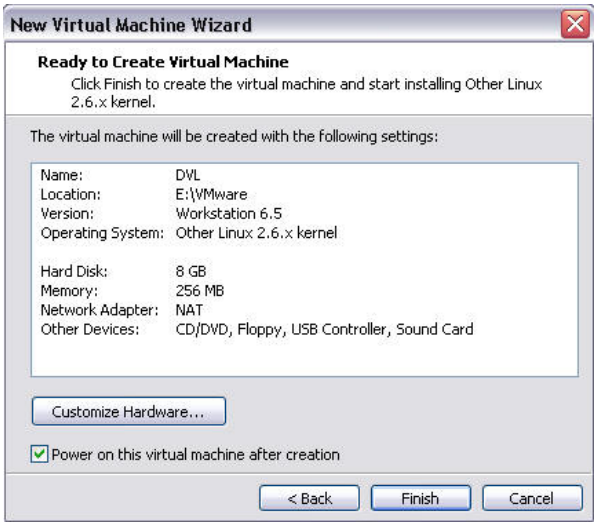
9. Click on the Customize Hardware...



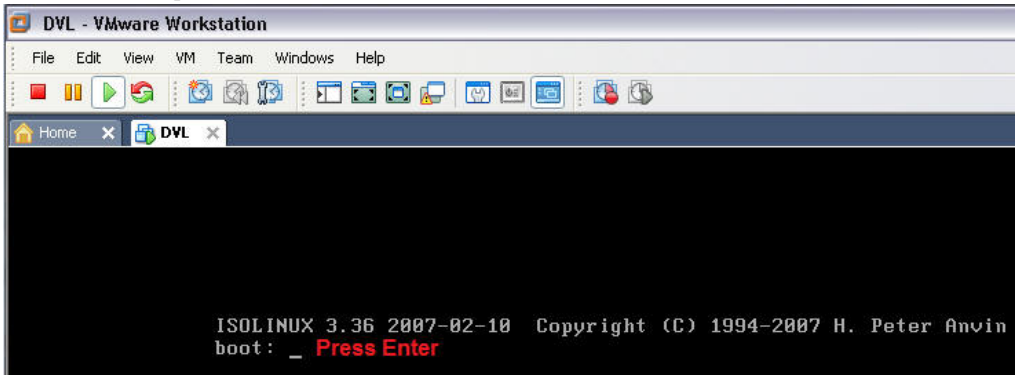
10. Select Memory
    - Increase the memory from 256 MB to 512 MB.
    - Click OK.



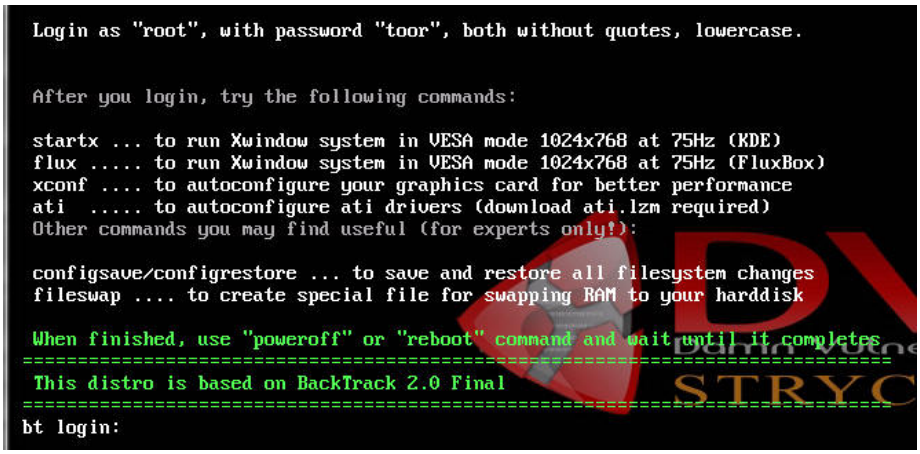
11. Click Finish



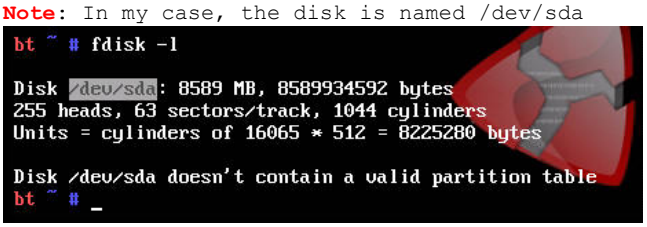
12. Press Enter when you see "boot: "

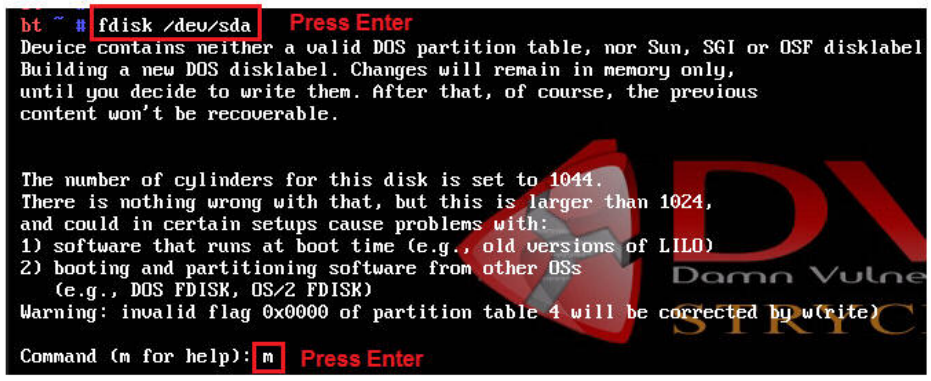


3. Login to DVL

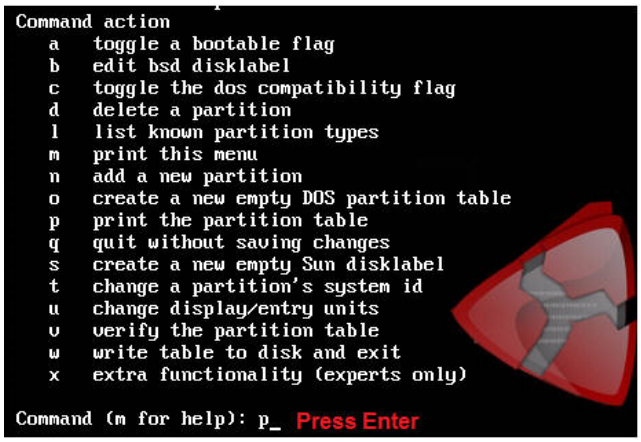
1. Credentials (See Below)
   - Login: root
   - Password: toor
   - 

3. Partition the disk

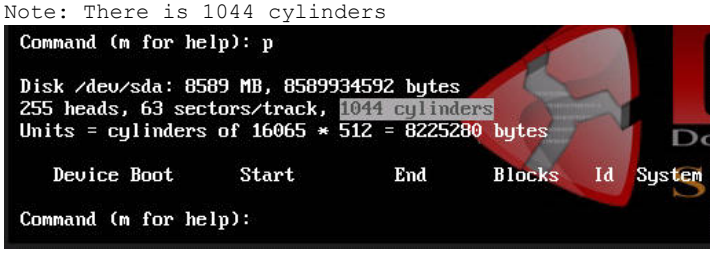
1. Determine what disk to format
   - **Command**: fdisk -l
   - **Note**: In my case, the disk is named /dev/sda
   - 

2. Select disk to be partitioned
   - **Command**: fdisk /dev/sda
   - **Input**: m
   - 

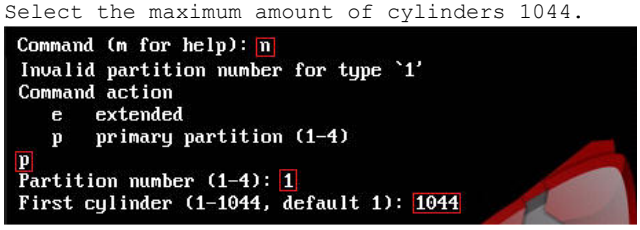
3. View the partition table
   - Select "p"



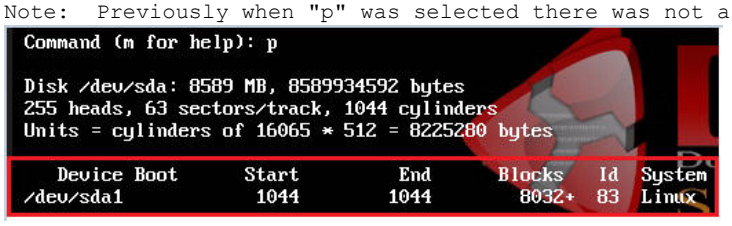
- Note: There is 1044 cylinders



4. Add a new partition
   - Select "n"
   - Select "p"
   - Select "1"
   - Select the maximum amount of cylinders 1044.



5. View newly created partition
   - Select "p"
   - Note: Previously when "p" was selected there was not a partition listed.



6. Save the new partition
   - Select "w"

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

7. Exit out of fdisk
   - Select "q"

```
Command (m for help): q

bt ~ #
```

4. Format the partition

1. Format the partition on /dev/sda
   - **Command**: mkfs.ext3 /dev/sda
   - **Proceed**: y

```
bt ~ # mkfs.ext3 /dev/sda
mke2fs 1.38 (30-Jun-2005)
/dev/sda is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1048576 inodes, 2097152 blocks
104857 blocks (5.00%) reserved for the super user
First data block=0
64 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 25 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
bt ~ #
```

2. Create a folder to mount the partition on.
   - **Command**: mkdir /mnt/dvl

```
bt ~ # mkdir /mnt/dvl
bt ~ # _
```

3. Mount the hard drive to the /mnt/dvl directory
   - **Command**: mount /dev/sda /mnt/dvl

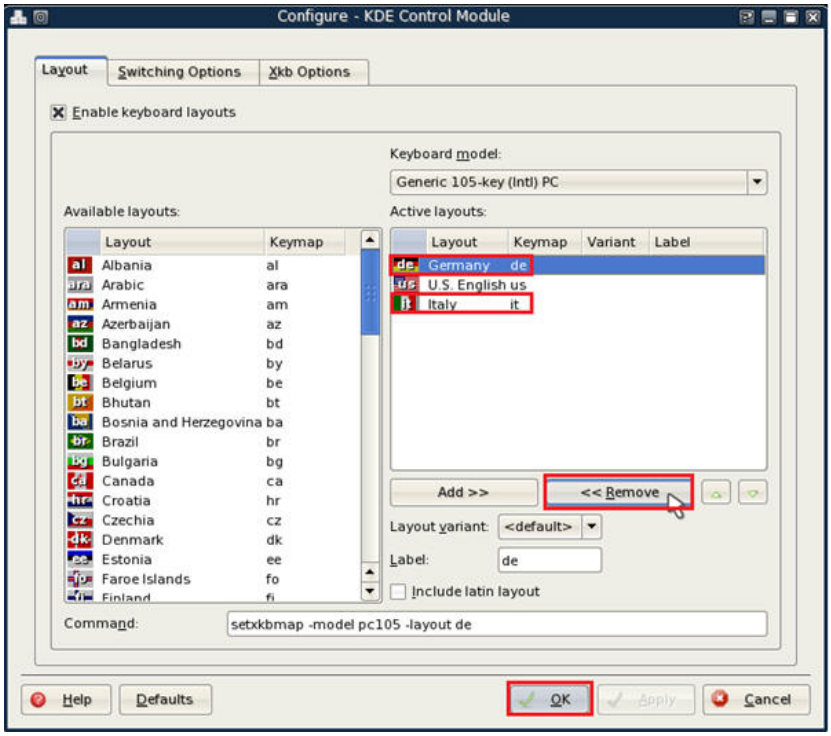
```
bt ~ # mount /dev/sda /mnt/dvl
bt ~ #
```

3. Copy DVL image to hard drive

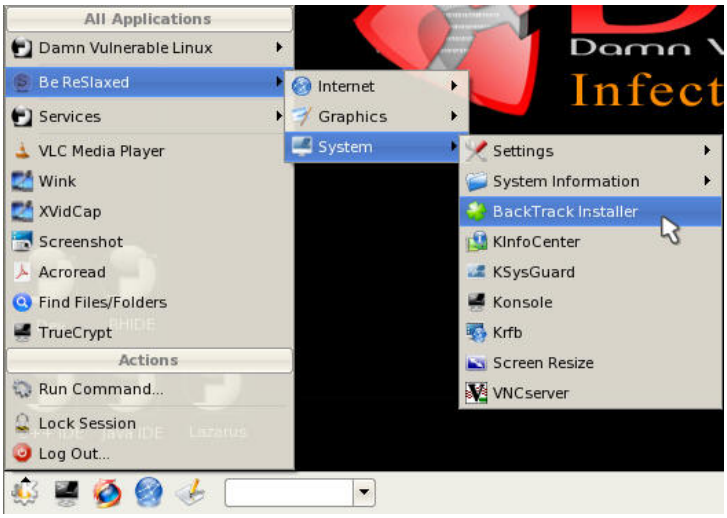
1. startx (See Below)

```
bt ~ # startx_
```

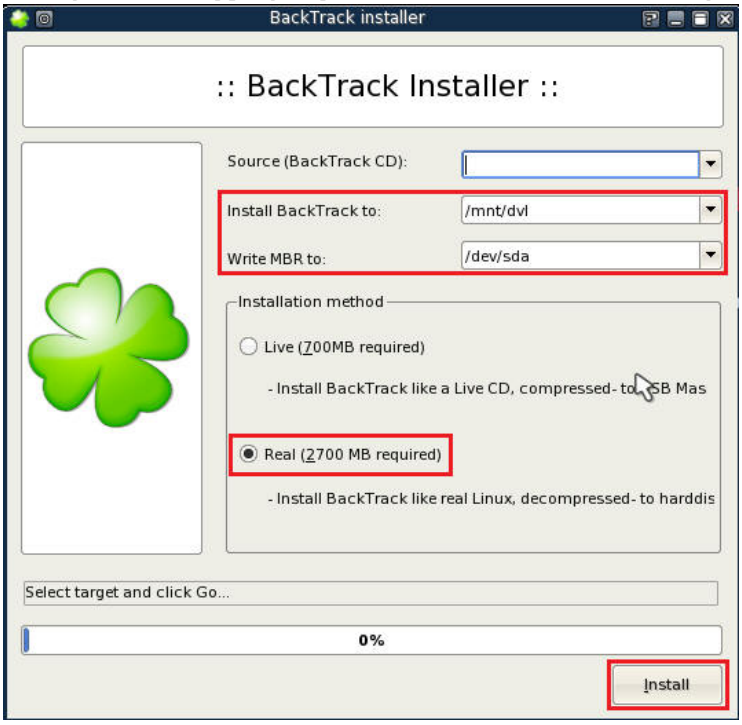
2. Change Language to English (See Below)
    - Right Click on DE and click on Configure
        - 

    - Highlight Germany, Click on Remove.
    - Highlight Italy, Click on Remove.
    - Only U.S. English should be left.
    - Click Apply
    - Click OK
        - 

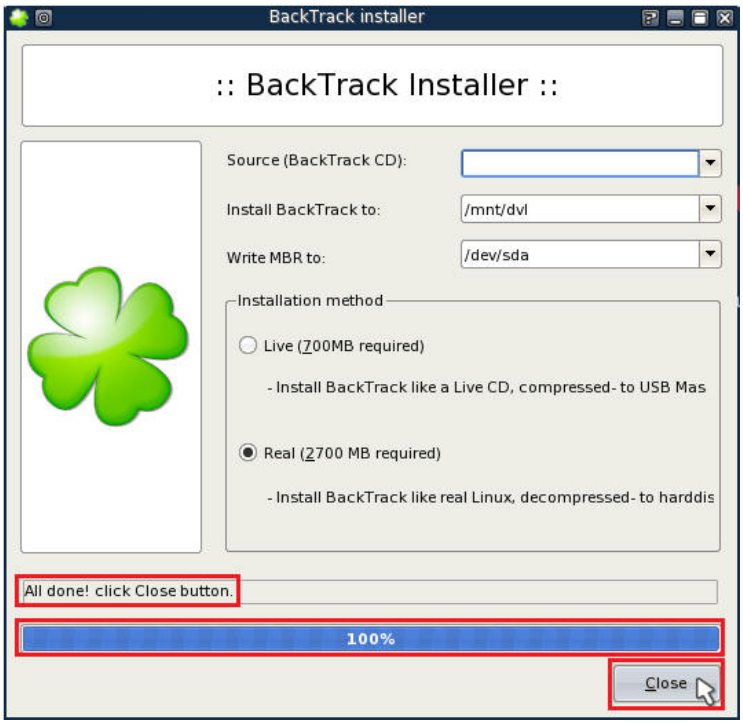
3. Start the backlash installer



4. Configure installer as seen below
   - Note: If the installer completes in a few seconds, then the installer actually failed. The installer should take 5 to 10 minutes to complete. You should see messages like copying /opt with the status bar inching slowly forward.

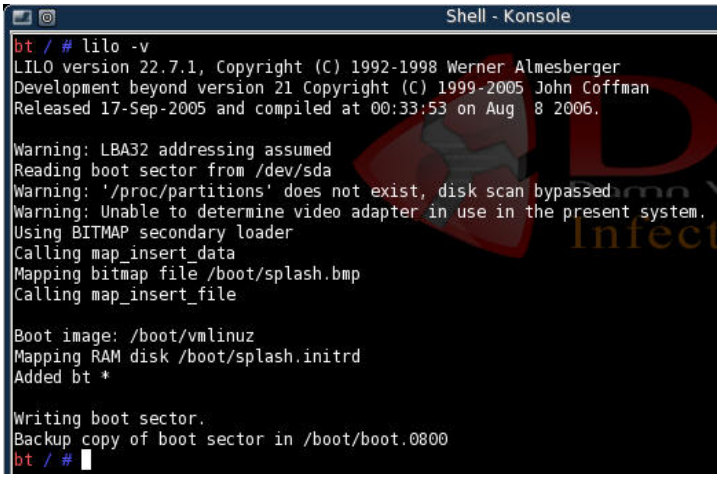


5. Click the close button, when you see a status message of "All done! click Close button" and a status bar of 100% complete



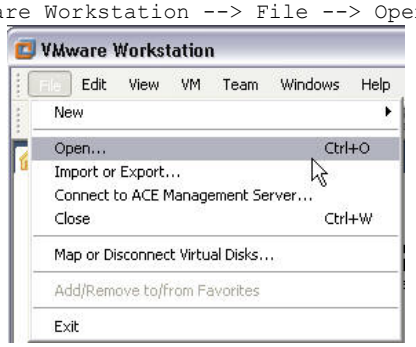
6. Start up a terminal

7. Install the boot loader
   - **Command**: lilo -v

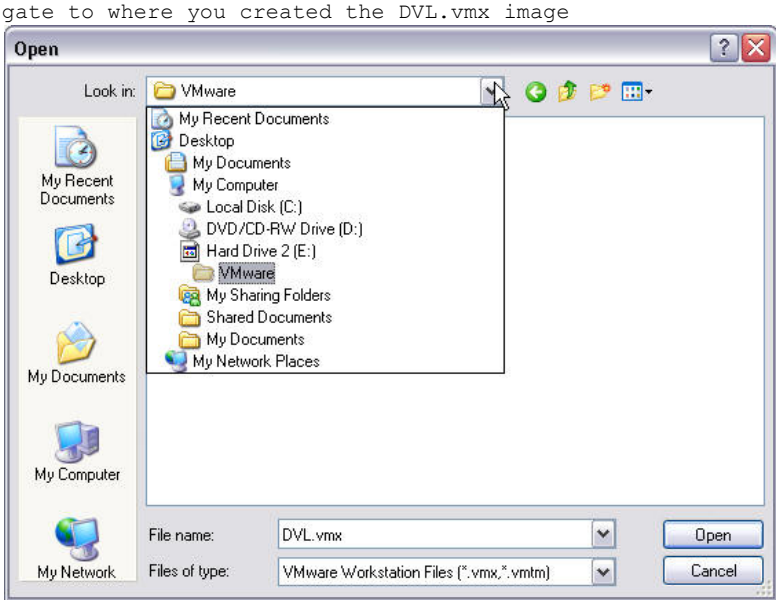


8. **Command**: poweroff

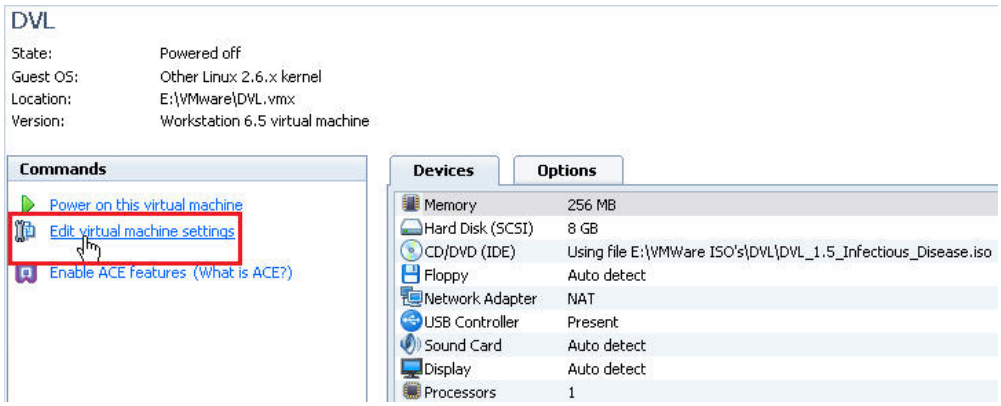
9. Edit virtual machine settings
    - VMware Workstation --> File --> Open



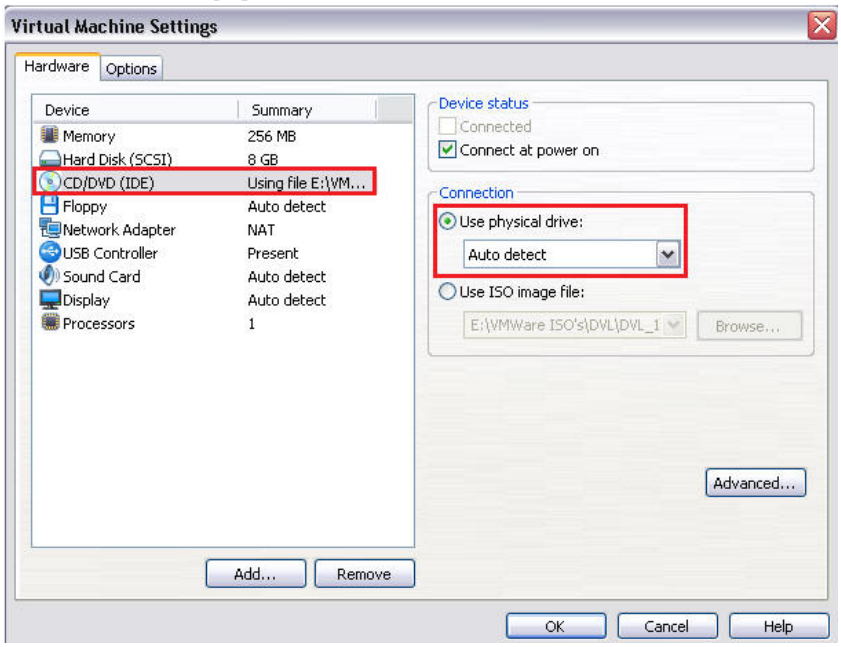
    - Navigate to where you created the DVL.vmx image



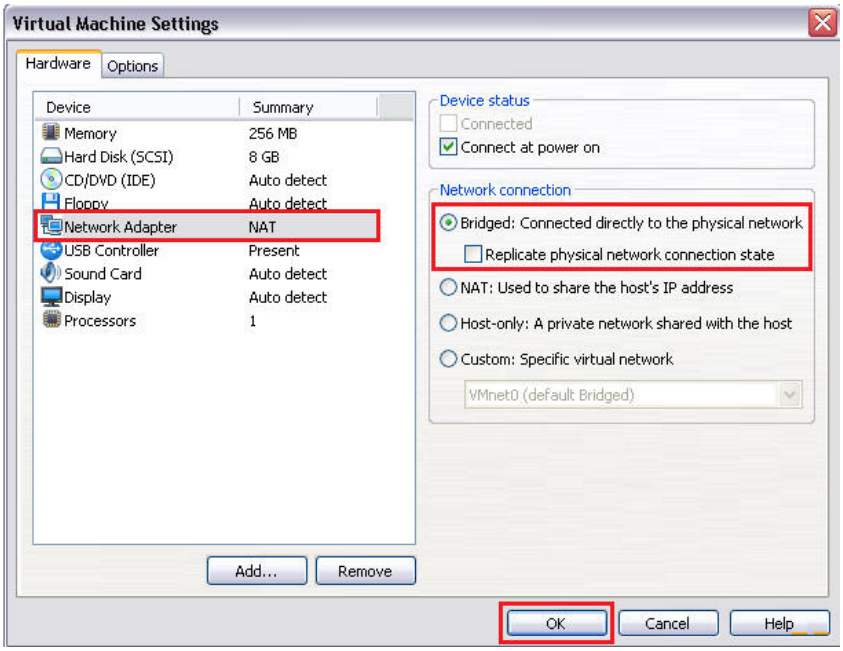
    - Edit Virtual machine settings



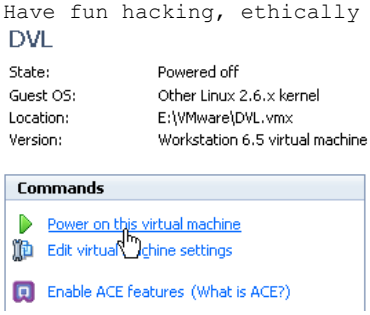
- Highlight CD/DVD
  - Select the "Use physical drive:" radio button



- Highlight CD/DVD
  - Select the "Bridged: Connected..." radio button
  - Select OK



10. Power on this virtual machine
    - Have fun hacking, ethically of course.



Section: Proof of Lab

1. Have fun hacking, ethically of course.