

# ComputerSecurityStudent (CSS)

HOME | UNIX ▾ | WINDOWS ▾ | SECURITY TOOLS ▾ | LECTURES ▾ | FORENSICS ▾ | SHOPPING ▾ | CONTACT\_US |

| SECURITY TOOLS >> Damn Vulnerable Linux

| Views :  
6180

## (Damn Vulnerable Linux: [DVL])

{ How to Install DVL }

### Section 0. Background Information

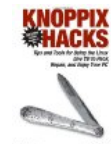
#### 1. What is Damn Vulnerable Linux?

- 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is everything a good Linux distribution isn't. Its developers have spent hours stuffing it with broken, ill-configured, outdated, and exploitable software that makes it vulnerable to attacks.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<sup>2</sup>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



[Knoppix Hacks](#)  
Kyle Rankin  
[Best Price \\$1.75](#)  
or Buy New



[Privacy Information](#)



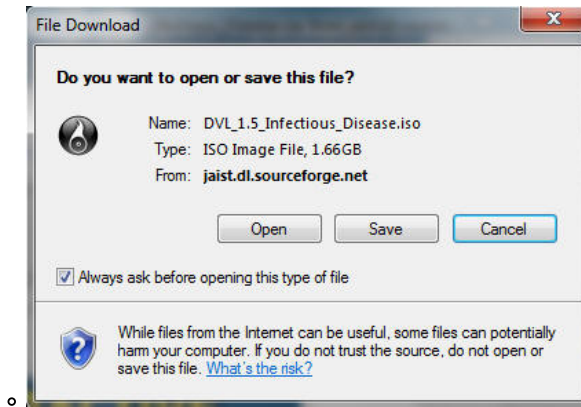
[Knoppix Pocket Reference](#)  
Kyle Rankin  
[Best Price \\$0.57](#)  
or Buy New \$9.95



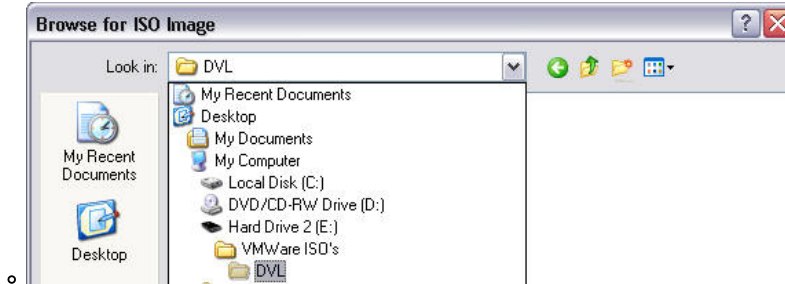
[Privacy Information](#)

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:)

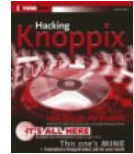


## 2. Start VMware Workstation

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

## 3. Create VMware Image

1. Click on New Virtual Machine.



[Hacking Knoppix](#)  
Scott Granneman  
Best Price \$0.01  
or Buy New



[Privacy Information](#)



[Knoppix](#)  
Alexander Niemann

Buy New



[Privacy Information](#)



[Linux / Knoppix espresso](#)

Christian Immler  
Best Price \$0.01  
or Buy New



[Privacy Information](#)

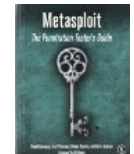


[Metasploit Toolkit for Penetration T...](#)  
David Maynor

Best Price \$12.80  
or Buy New \$42.65



[Privacy Information](#)

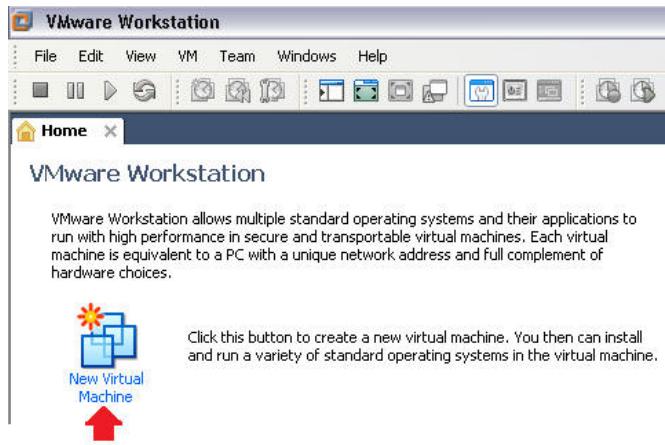


[Metasploit](#)  
David Kennedy, Jim...

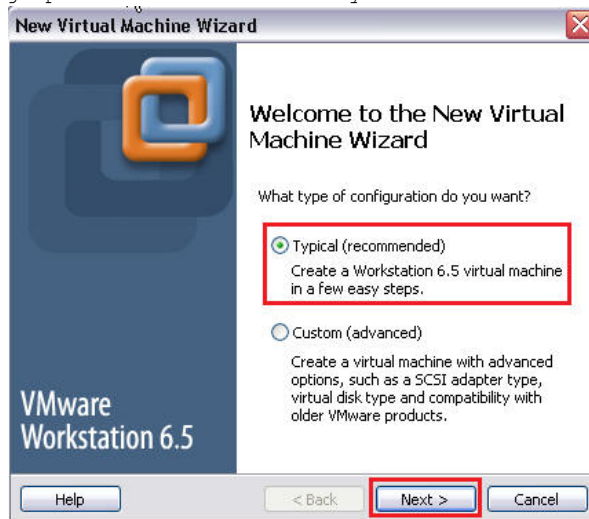
Best Price \$23.95  
or Buy New \$27.87



[Privacy Information](#)

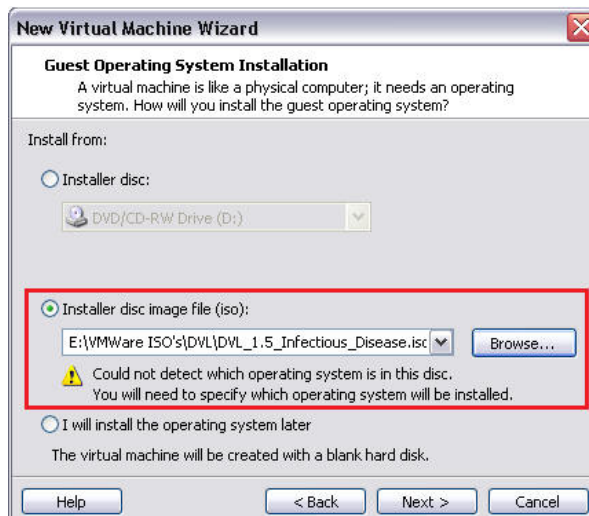


2. Bring up a Firefox Browser on your DVL machine.



3. Select Install disc image file (iso)

- Select the Browse Button



[BackTrack 4](#)  
Shakeel Ali, Tedi ...  
[Best Price \\$47.96](#)  
or Buy New \$47.96  
[Buy from amazon.com](#)

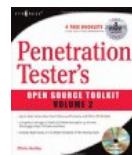
[Privacy Information](#)



[Professional Penetration Testing](#)

Thomas Wilhelm  
[Best Price \\$38.95](#)  
or Buy New \$64.31  
[Buy from amazon.com](#)

[Privacy Information](#)



[Penetration Tester's Open Source Too...](#)

Jeremy Faircloth, ...  
[Best Price \\$6.09](#)  
or Buy New  
[Buy from amazon.com](#)

[Privacy Information](#)



[Writing Security Tools and Exploits](#)

James C. Foster, V...  
[Best Price \\$8.90](#)  
or Buy New \$46.50  
[Buy from amazon.com](#)

[Privacy Information](#)

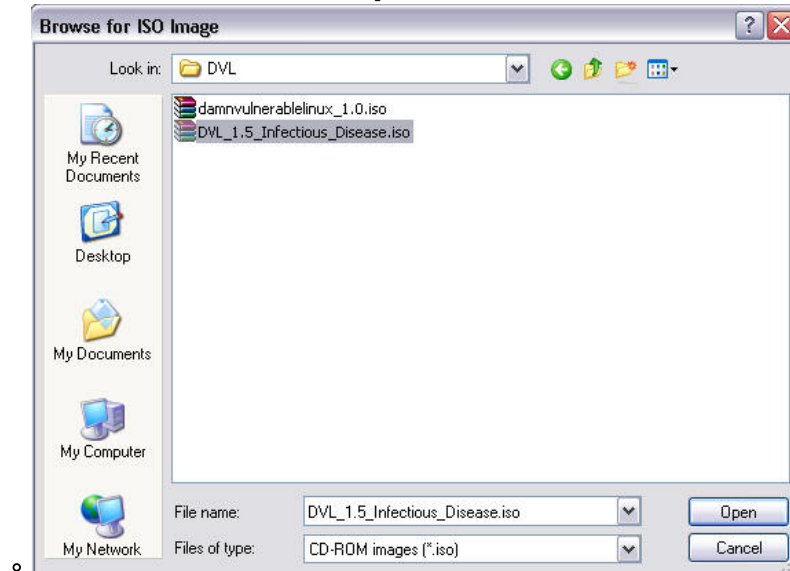


[Dissecting the Hack](#)

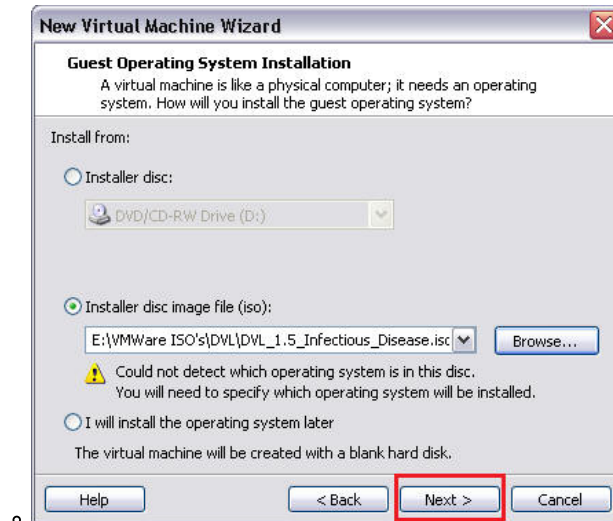
Jayson E. Street, ...  
[Best Price \\$14.08](#)  
or Buy New \$19.03  
[Buy from amazon.com](#)

[Privacy Information](#)

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



[SSH: The Secure Shell](#)

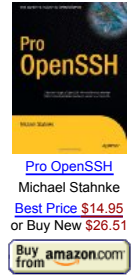
Daniel J. Barrett...

Best Price \$10.99

or Buy New \$27.09

Buy from [amazon.com](#)

[Privacy Information](#)



[Pro OpenSSH](#)

Michael Stahnke

Best Price \$14.95

or Buy New \$26.51

Buy from [amazon.com](#)

[Privacy Information](#)



[Implementing SSH](#)

Himanshu Dwivedi

Best Price \$0.59

or Buy New \$30.63

Buy from [amazon.com](#)

[Privacy Information](#)



[UNIX Shells by Example](#)

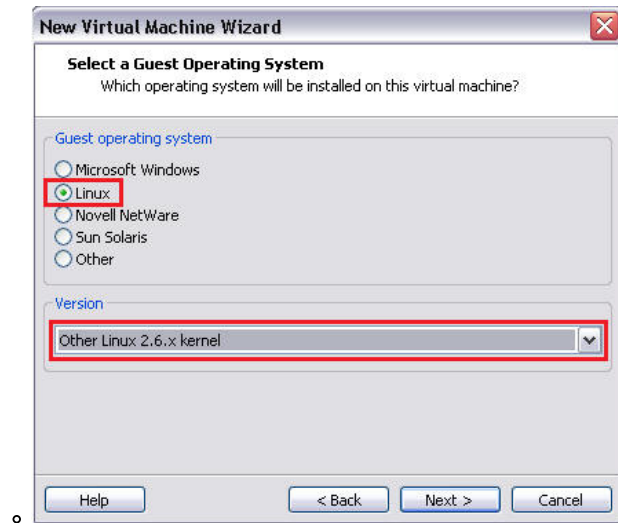
Ellie Quigley

Best Price \$21.09

or Buy New \$36.17

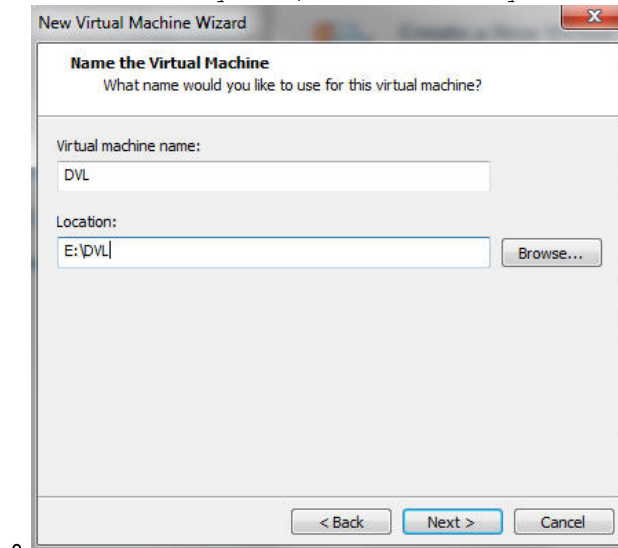
Buy from [amazon.com](#)

[Privacy Information](#)

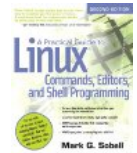


#### 7. Naming and Saving Location

- Virtual machine name: DVL
- Location: In my case, I save it to my external hard drive at [E:\VMware](#)



#### 8. Specify Disk Capacity



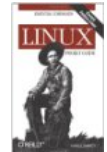
[A Practical Guide to Linux Commands...](#)

Mark G. Sobell

[Best Price \\$29.90](#) or Buy New



[Privacy Information](#)



[Linux Pocket Guide](#)

Daniel J. Barrett

[Best Price \\$0.01](#) or Buy New



[Privacy Information](#)



[Linux Administration](#)

Wale Soyinka

[Best Price \\$4.64](#) or Buy New \$21.12



[Privacy Information](#)



[Beginning Ubuntu Linux](#)

Keir Thomas, Andy ...

[Best Price \\$4.71](#) or Buy New \$25.60



[Privacy Information](#)

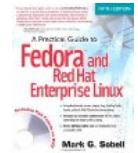


9. Click on the Customize Hardware...



10. Select Memory

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



[Practical Guide to Fedora and Red Ha...](#)

Mark G. Sobell  
Best Price \$1.97  
or Buy New



[Privacy Information](#)



[Beginning the Linux Command Line](#)

Sander van Vugt  
Best Price \$16.88  
or Buy New \$23.19



[Privacy Information](#)



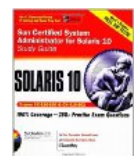
[Unix and Linux System Administration...](#)

Evi Nemeth, Garth ...

Buy New

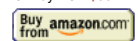


[Privacy Information](#)



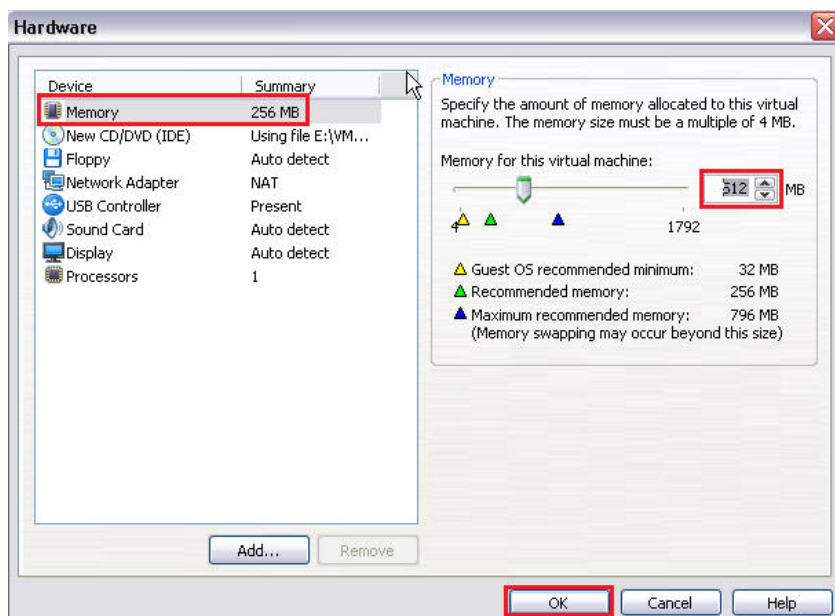
[Sun](#)

Paul Sanghera  
Best Price \$5.01  
or Buy New \$35.27

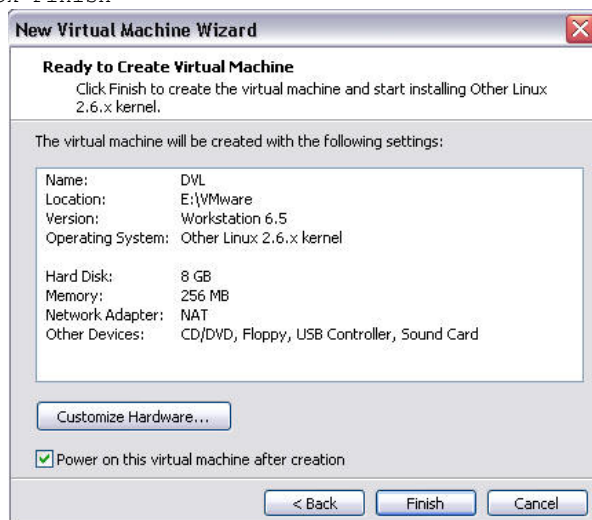


[Privacy Information](#)

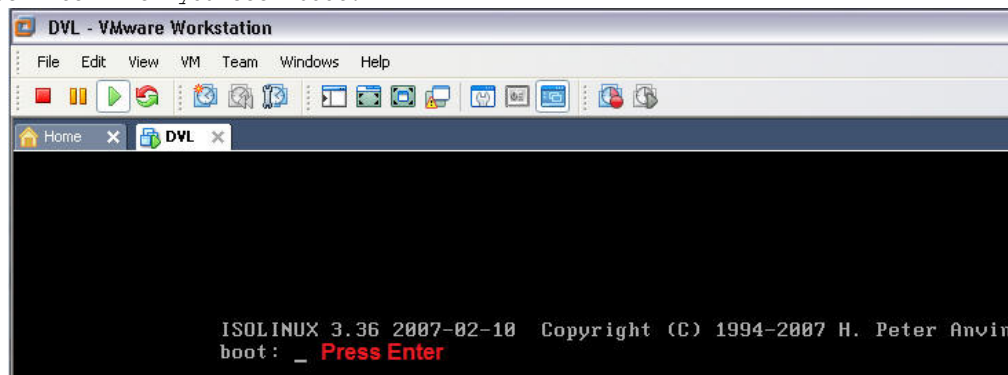




11. Click Finish



12. Press Enter when you see "boot: "



### 3. Login to DVL

#### 1. Credentials (See Below)

- Login: root
- Password: toor

Login as "root", with password "toor", both without quotes, lowercase.

After you login, try the following commands:

startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz (KDE)  
flux .... to run Xwindow system in VESA mode 1024x768 at 75Hz (FluxBox)  
xconf .... to autoconfigure your graphics card for better performance  
ati .... to autoconfigure ati drivers (download ati.lzm required)  
Other commands you may find useful (for experts only!):

configsave/configrestore ... to save and restore all filesystem changes  
fileswap .... to create special file for swapping RAM to your harddisk

When finished, use "poweroff" or "reboot" command and wait until it completes

=====

This distro is based on BackTrack 2.0 Final

=====

- bt login:

### 3. Partition the disk

#### 1. Determine what disk to format

- **Command:** fdisk -l
- **Note:** In my case, the disk is named /dev/sda

```
bt ~ # fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Disk /dev/sda doesn't contain a valid partition table
bt ~ # _
```

#### 2. Select disk to be partitioned

- **Command:** fdisk /dev/sda
- **Input:** m

```
bt ~ # fdisk /dev/sda Press Enter
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.

The number of cylinders for this disk is set to 1044.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
 1) software that runs at boot time (e.g., old versions of LILO)
 2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): m Press Enter
```

#### 3. View the partition table

- Select "p"



```

Command action
a  toggle a bootable flag
b  edit bsd disklabel
c  toggle the dos compatibility flag
d  delete a partition
l  list known partition types
m  print this menu
n  add a new partition
o  create a new empty DOS partition table
p  print the partition table
q  quit without saving changes
s  create a new empty Sun disklabel
t  change a partition's system id
u  change display/entry units
v  verify the partition table
w  write table to disk and exit
x  extra functionality (experts only)

```

Command (m for help): p\_ **Press Enter**

- Note: There is 1044 cylinders

```

Command (m for help): p

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System

```

Command (m for help):

#### 4. Add a new partition

- Select "n"
- Select "p"
- Select "1"
- Select the maximum amount of cylinders 1044.

```

Command (m for help): n
Invalid partition number for type `1'
Command action
  e  extended
  p  primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1044, default 1): 1044

```

#### 5. View newly created partition

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

```

Command (m for help): p

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1          1044          1044       8032+   83   Linux

```

#### 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)

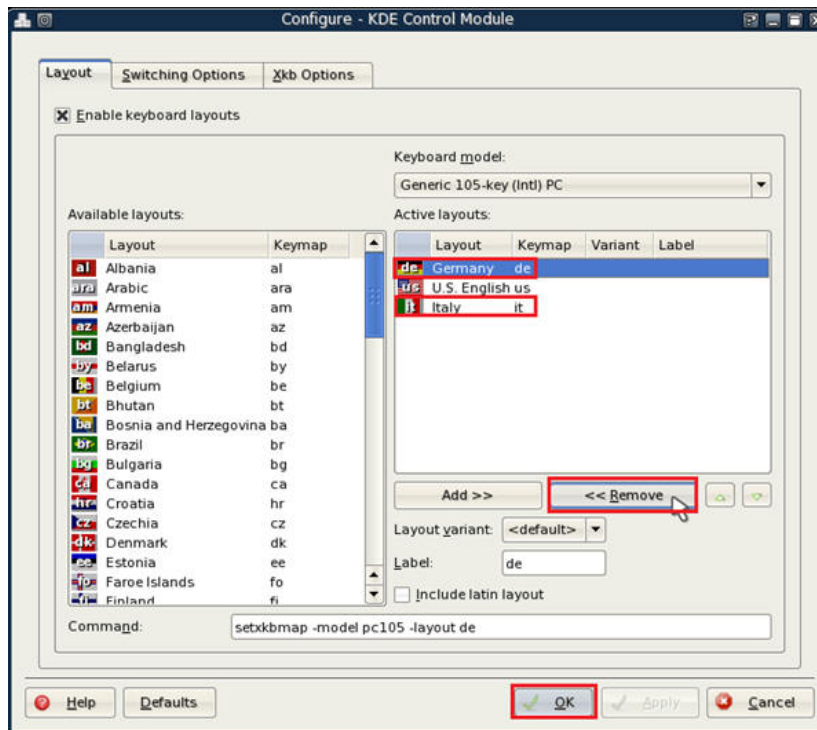
- `bt ~ # startx_`

## 2. Change Language to English (See Below)

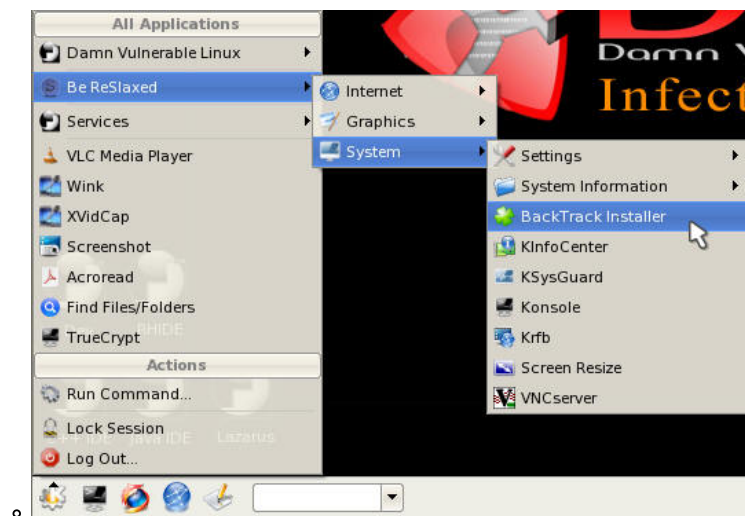
- Right Click on DE and click on Configure



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

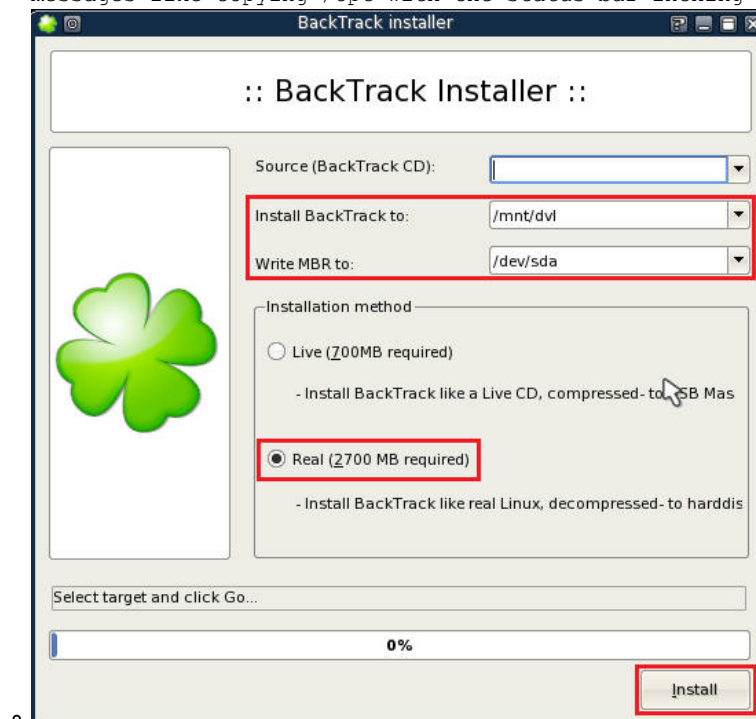


## 3. Start the backlash installer

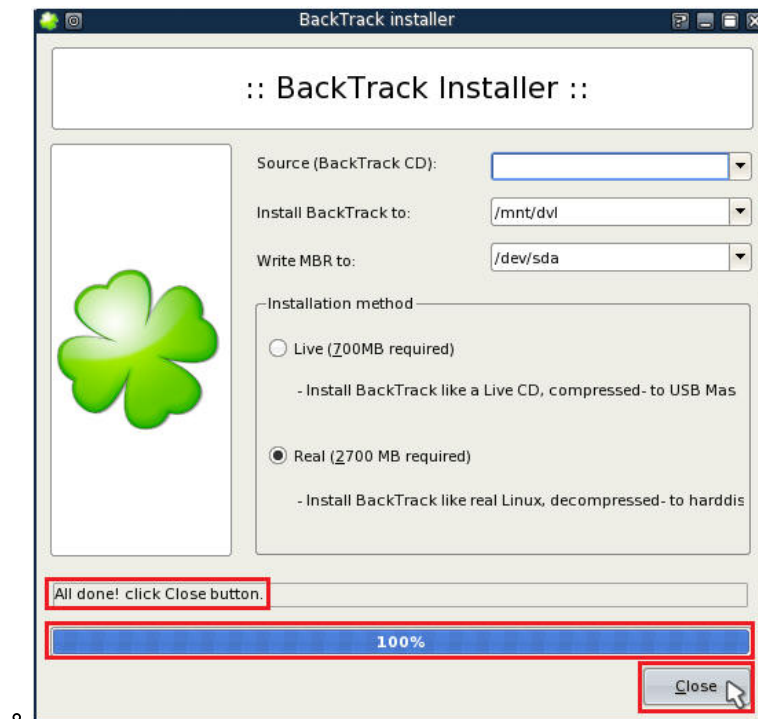


4. Configure installer as seen below

- 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

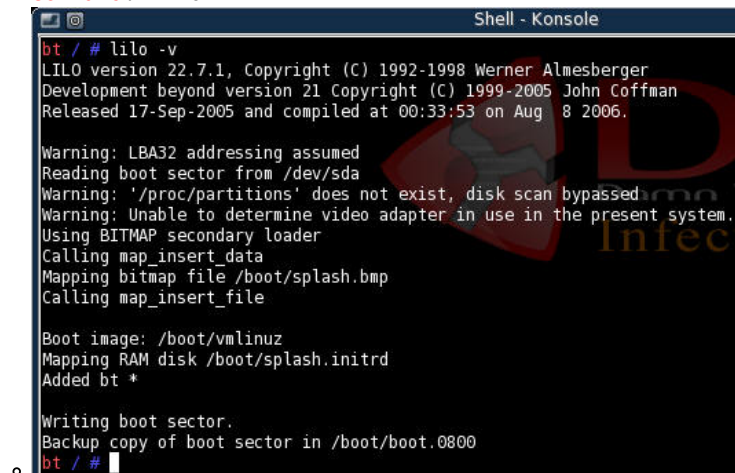


6. Start up a terminal



7. Install the boot loader

◦ **Command:** lilo -v

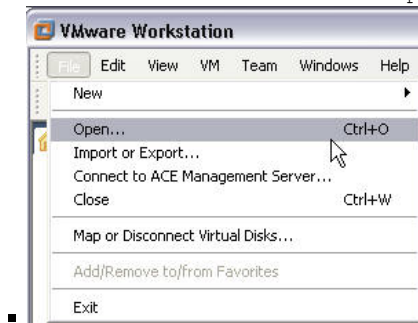


8. **Command:** poweroff

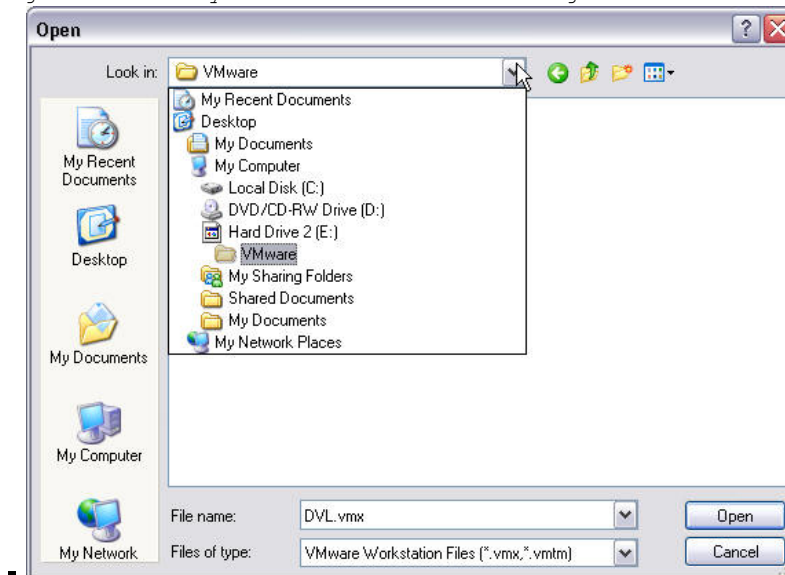


9. Edit virtual machine settings

- VMware Workstation --> File --> Open

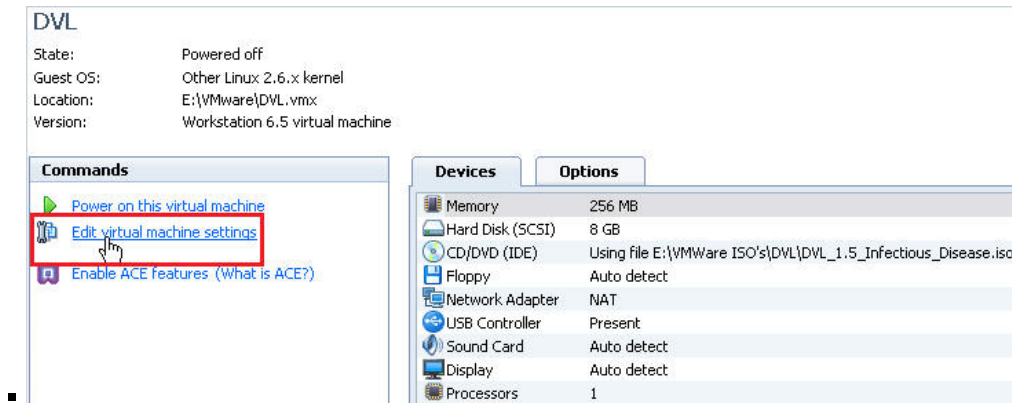


- Navigate to where you created the DVL.vmx image

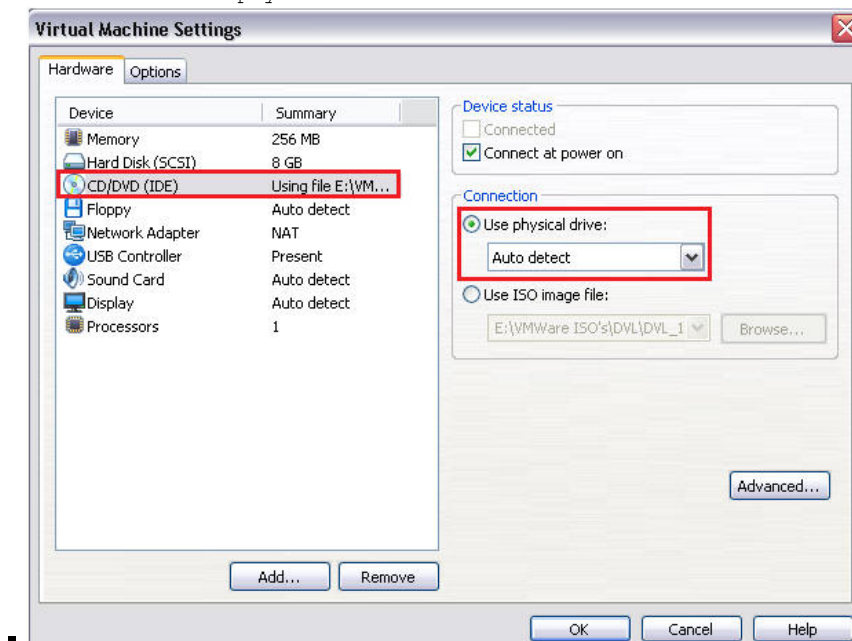


- Edit Virtual machine settings

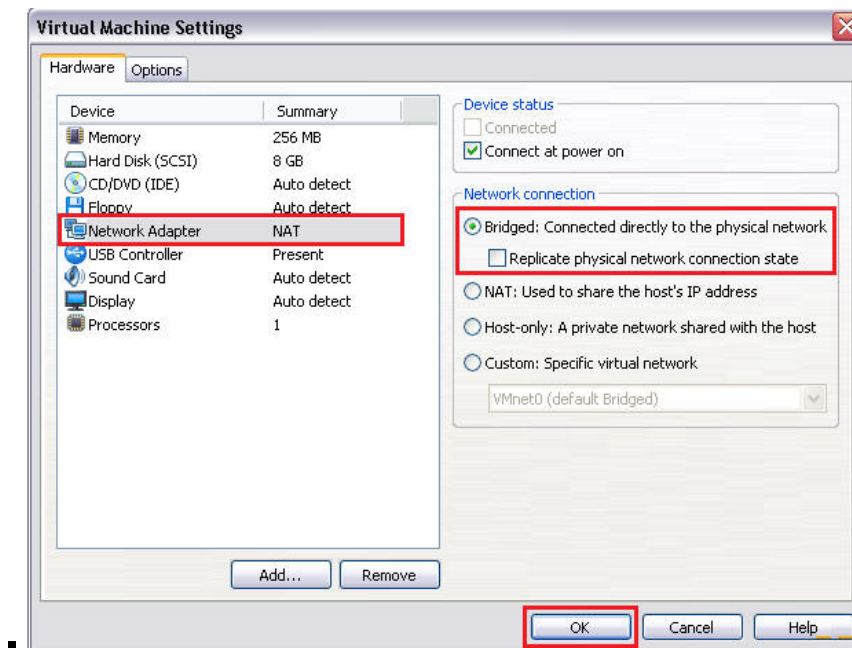




- Highlight CD/DVD
  - Select the "Use physical drive:" radio button



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



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

#### DVL

State: Powered off  
 Guest OS: Other Linux 2.6.x kernel  
 Location: E:\VMware\DVL.vmx  
 Version: Workstation 6.5 virtual machine

**Commands**

- [Power on this virtual machine](#)
- [Edit virtual machine settings](#)
- [Enable ACE features \(What is ACE?\)](#)

## Section: Proof of Lab

1. Have fun hacking, ethically of course.