Linux Penetration Testing Laptop (Ubuntu 8.04 LTS)
This documentation will not go into details on how to install Ubuntu. There are many resources on the Internet that can assist you. You may not even need any help as they do an excellent job making it easy and straight forward. Below I list the commands I run to get my clean installation up and running as a penetration testing laptop.

Updating and upgrading

```
#apt-get update
#apt-get upgrade
```

Adding compilers and kernel source code

```
#sudo apt-get install build-essential
#sudo apt-get install linux-headers-`uname -r`
```

INSTALLING THE TOOLS
Create a source code directory to download all the code into

```
#cd
#mkdir source
#cd source
```

A lot of the source code downloaded will need some package libraries and development files installed before then can configure/compile

```
#apt-get install libssl-dev zlib1g-dev
```

NMAP (Currently we like the beta version as it includes new tools and utilities)
Grab the latest install from www.insecure.org/nmap/

```
#wget http://nmap.org/dist/nmap-4.85BETA7.tar.bz2
#tar jxvf nmap-4.85BETA7.tar.bz2
#cd nmap-4.85BEATA7
#./configure
#make && make install
```

Host file parsing script
Various enumeration scans can leave you with numerous host list files. A simple perl script will be created to allow combining, sorting, and listing of the unique ip addresses from your various lists. Copy and past the following code to the file /usr/bin/unique.pl and make it executable #chmod 777 /usr/bin/unique.pl

```
#!/usr/bin/perl
foreach $argnum (0 .. $#ARGV){
          open (DAT, “$ARGV[$argnum]”) || die(“Could not openfile!”);
          while (<DAT>){
                    chomp;
                    push(@raw_data, $_);
          }
          close(DAT);
}
%seen = ();
@uniq = ();
foreach $item (@raw_data){
          unless($seen{$item}) {
                    $seen{$item} = 1;
                    push(@uniq, $item);
          }
}
@uniq = sort(@uniq);
foreach (@uniq){
          Print “$_\n”;
}
```

Nessus

Dependencies
#apt-get install libssl0.9.8

Nessus is now a closed sources product with pre-compiled binaries available for download. As of Nessus 4 there is a binary available for Ubuntu 8.04 LTS.

Download the latest version from www.nessus.org (currently 4.0.0). Registration will be required to download. This will also give you a key to download all Nessus plugins.

Download Nessus-4.0.0-ubuntu804_i386.deb

Double-click the item (in window manager) to install or from the command line: #dpkg –i Nessus-3.1.4-debian3_i386.deb

Post install configuration

```
#/opt/nessus/sbin/nessus-adduser
        Login : linuxpen
        Authentication (pass/cert) [pass] :  pass
        Login password :
        Login password (again) :
        Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc…)(y/n) [n]: y

        User rules ^D (control-d)
        Is that ok ? (y/n) [y] y

#/opt/nessus/sbin/nessus-mkcert
        CA certificate life time in days [1460]: (accept default)
        Server certificate life time in days [365]: (accept default)
        Your country (two letter code) [FR]: US
        Your state or province name [none]: GA
        Your location (e.g. town) [Paris]: Atlanta
        Your organization [Nessus Users United]: DOAA
        Press [ENTER] to exit
#/opt/nessus/bin/nessus-fetch --register XXXX-XXXX-XXXX-XXXX-XXXX
NOTE: check your email (the one you registered with) for the key code

Download and install the NessusClient 4.0.0 from www.nessus.org.  There is an Ubuntu version of the client
(8.04 LTS Hardy Heron)
#apt-get install libqt4-gui libqt4-core
Accept all dependencies
#dpkg –I NessusClient-4.0.0-ubuntu804.i386.deb

Start nessusd as a background process
#/opt/nessus/sbin/nessusd –D
```

THC-Hydra

```
Various software libraries need to be installed inorder to successfully compile Hydra with all of the
features that we need.
#apt-get install libssl-dev libpq-dev libsvn-dev

Obtain the libssh library from
#wget http:/0xbadc0de.be/libssh/libssh-0.11.tgz
#tar zxvf libssh-0.11.tgz
```

```
#cd libssh-0.11
#./configure
#make && make install
#ln –s /usr/local/lib/libssh.so /usr/lib/libssh.so
```

Obtain the latest Hydra source from http://freeworld.thc.org

```
#wget http://freeworld.thc.org/releases/hydra-5.4-src.tar.gz
#tar zxvf hydra-5.4-src.tar.gz
#cd hydra-5.4-src
#./configure
#make && make install
```

Firewalk

Download the latest package from http://www.packetfactory.net/firewalk/

Download libnet (http://www.packetfactory.net/libnet/dist/libnet.tar.gz) and libdnet (http://libdnet.sourceforge.net)

```
#apt-get install libpcap-dev libpcap0.8 libpcap0.8-dev
```

Untar each of the tarballs

```
#tar zxvf *.tar.gz
#apt-get install flex m4 bison
#cd ../libdnet*
#./configure
#make && make install
#cd ../libnet
#./configure
#make && make install
#cd ../Firewalk
#./configure
```

Trying to compile at this point will give you an error. There is a bug in the code. If you attempt to compile you will note the line number given in firewalk.c where the error occurs (192 or 193).

```
#vim src/firewalk.c
```

Below the line /*empty*/ add **break;**

Make sure to include the semi-colon and save the file. You will be able to compile and install with no errors now.

#make && make install

TRACEROUTE
#apt-get install traceroute

TCPTRACEROUTE
#apt-get install tcptraceroute

SCANRAND and PARATRACE
#apt-get install paketto

HPING
#apt-get install hping2

WIRE SNIFFING
#apt-get install wireshark tcpdump

STUNNEL
When stunnel 4.0 was released, the entire interface changed from where you can type all the details on the command line to one where all the details must be placed within a configuration file. This will not work for the purposes we need. Ubuntu only offers stunnel4. Instructions below will get the latest version of Stunnel 3 up and running.

#apt-get install libssl-dev zlib1g-dev

Download the latest stunnel version 3
http://www.stunnel.org/download/stunnel/src/stunnel-3.26.tar.gz

#wget http://www.stunnel.org/download/stunnel/src/stunnel-3.26.tar.gz
#tar zxvf stunnel-3.26.tar.gz
#cd stunnel-3.26
#./configure --prefix=/usr --bindir=/usr/bin --sbindir=/usr/bin
#make
#make install

When asked enter the following information (or whatever you agency information is)

Country Name (2 letter code) [PL]:US
State or Province Name (full name) [Some-State]:Georgia
Locality Name (eg, city) []:Atlanta
Organization Name (eg, company) [Stunnel Developers Ltd]:DOAA
Organizational Unit Name (eg, section) []:ISAAS
Common Name (FQDN of your server) [localhost]:audits.state.ga.us

UNICORNSCAN

Unicornscan is difficult to configure to make it compile. However, there is an RPM package available. We will convert this package to an native DEB package so we can install it on Ubuntu. Download the binary RPM package from http://www.unicornscan.org

```
#wget http://www.unicornscan.org/releases/unicornscan-0.4.2-0.i386.rpm
#apt-get install alien
#alien –-to-dev unicornscan-0.4.2-0.i386.rpm
#dpkg –i  unicornscan-0.4.2-0.i386.deb
#ln –s /usr/lib/libpcap.so.0.8 /usr/lib/libpcap.so.0.8.3
```

METAPLOIT

Grab the latest version of the framework

```
#apt-get install ruby openssl libopenssl-ruby
```

Accept all dependencies

```
#apt-get install subversion
#svn co http://metasploit.com/svn/framework3/trunk/
```

SQLNinja

Several perl modules are required for this tool to work

```
#perl –MCPAN –e ‘install NetPacket’
#apt-get install libpcap0.8 libpcap0.8-dev
#perl –MCPAN –e ‘install Net::Pcap’
#perl –MCPAN –e ‘install Net::DNS’
#perl –MCPAN –e ‘install Net::RawIP’
```

```
#perl –MCPAN –e ‘install IO::Socket::SSL’

#wget http://downloads.sourceforge.net/sqlninja/sqlninja-0.2.3-r1.tgz
#tar zxvf sqlninja-0.2.3-r1.tgz
#cd sqlninja-0.2.3-r1
```

VMWARE SERVER

Register at www.vmware.com and download the latest version of the VMWare Server software. Installing the latest version of VMWare Server is now easy to do on Ubuntu. As to not reinvent the wheel there is a nice easy tutorial on installing the software on Ubuntu 8.04 (http://www.howtoforge.com/how-to-install-vmware-server-2-on-an-ubuntu-8.04-desktop)

TRUECRYPT Encryption Software
Download the Ubuntu x86 version from http://www.truecrypt.org/downloads.php

```
#tar zxvf truecrypt-6.2-ubuntu-x86.tar.gz
#sh truecrypt-6.2-setup-ubuntu-x86
```

Follow the GUI instructions.

```
Create a volume to use for audit data.
#truecrypt –-size 1000M –-encryption AES –-hash SHA-1 –-filesystem FAT –c workpapers.tc
```

Follow the rest of the prompts for normal volumne, password, and randomness created via mouse movement.
Mount the volume.

```
#mkdir /mnt/workpapers
#truecrypt workpapers.tc /mnt/workpapers
```