Linux Penetration Testing Laptop (Ubuntu 10.4 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

```
$sudo aptitude update
$sudo aptitude upgrade
```

Adding compilers and kernel source code

```
$sudo aptitude install build-essential
$sudo aptitude install linux-headers-`uname -r`
```

```
INSTALLING THE TOOLS
Create a source code and tools directory to download all the code into
$mkdir ~/source
$mkdir ~/tools

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

$sudo aptitude install libssl-dev zlib1g-dev libpq-dev libssh-dev ruby openssl libopenssl-ruby libreadline-
ruby rubygems irb1.8 rdoc1.8 ruby-dev libruby subversion libsqlite3-dev sqlite3 libsqlite3-ruby libpcap0.8
libpcap0.8-dev xtightvncviewer

Accept all dependencies
```

NMAP (Current Stable is 5.21)

```
Grab the latest install from www.insecure.org/nmap/
$cd ~/source
$wget http://nmap.org/dist/nmap-5.21.tar.bz2
$tar jxvf nmap-5.21.tar.bz2
$cd nmap-5.21
$./configure
$make
$sudo make install
```

John the Ripper

Password cracking Windows hashes on Linux using John the Ripper (JtR). If you prefer the Linux operating system JtR is the password cracking utility to use. By default JtR does not support the hashes that we are interested in cracking. See below for installation and patching instructions for JtR. Applying the patch to JtR adds the functionality to crack NTLM and MS-Cache passwords.

```
$./john --format=mscash --rules --wordlist=<PASSWORD_LIST> <CACHE_HASH_FILE>
$./john --format=nt --rules --wordlist==<PASSWORD_LIST> <NTLM_HASHE_FILE>
```

For additional information you can read the JtR documentation and wiki from Openwall.

OpenSSL is needed. This can be installed through your package manager or may already be installed. Remember to install the development package libssl-dev. Instructions on download and compile are included below.

```
$ wget http://www.openssl.org/source/openssl-1.0.0a.tar.gz
$ tar zxvf openssl-1.0.0a.tar.gz
$ cd openssl-1.0.0a
$ ./config --openssldir=/usr/local
$ make
$ sudo make install
$ wget http://www.openwall.com/john/g/john-1.7.5.tar.gz
$ tar zxvf john-1.7.5tar.gz
$ cd john-1.7.5/
$ wget http://www.openwall.com/john/contrib/john-1.7.5-jumbo-3.diff.gz
$ gzip -d john-1.7.3-jumbo-3.diff.gz
$ patch -p1 < john-1.7.5-jumbo-3.diff
$ cd src/
$ make linux-x86-sse2
```

John will be found in the run directory.

Nessus

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 10.4.

Download the latest version from www.nessus.org (currently 4.2.2). Registration will be required to download. This will also give you a key to download all Nessus plugins.

Download Nessus-4.2.2-ubuntu910_i386.deb (Note: this version will work with 10.4)

Below are the LINKS for installing and using Nessus 4.2.2. These documents can explain everything far better than I can.
http://www.nessus.org/documentation/nessus_4.2_installation_guide.pdf
http://www.nessus.org/Nessus_Activation_Code_Installation.pdf
http://www.nessus.org/documentation/nessus_4.2_user_guide.pdf

THC-Hydra
Various software libraries need to be installed inorder to successfully compile Hydra with all of the features that we need.

Obtain the latest Hydra source from http://freeworld.thc.org
```
$cd ~/source
$wget http://freeworld.thc.org/releases/hydra-5.7-src.tar.gz
$tar zxvf hydra-5.7-src.tar.gz
$cd hydra-5.4-src
$./configure
$make
$sudo make install
```

TRACEROUTE
```
$sudo aptitude install traceroute
```

TCPTRACEROUTE
```
$sudo aptitude install tcptraceroute
```

SCANRAND and PARATRACE (no longer supported in Ubuntu. It uses an antiquated version of libnet)
~~$sudo aptitude install paketto~~

HPING

~~$sudo aptitude install hping2~~ (no longer available on 10.4)
$sudo aptitude install hping3

WIRE SNIFFING
$sudo aptitude 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.

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
$sudo 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 died May 15, 2009.

METAPLOIT
Grab the latest version of the framework
$cd ~/tools

```
$svn co http://metasploit.com/svn/framework3/trunk/
```

Ensure SQLITE3 per instructions above.

PATCH AND INSTALL RATPROXY

```
$cd ~/source
$wget http://ratproxy.googlecode.comfiles/ratproxy-1.51.tar.gz
$tar zxvf ratproxy-1.51.tar.gz
$cd ratproxy
$patch –d . < ~/tools/trunk/external/ratproxy/ratproxy_wmap.diff
$make
```

SQLNinja

```
Several perl modules are required for this tool to work
$perl –MCPAN -e ‘install NetPacket’
$sudo aptitude 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/project/sqlninja/sqlninja/0.2.5/sqlninja-0.2.5.tgz
$tar zxvf sqlninja-0.2.5.tgz
$cd sqlninja-0.2.5

Change sqlninja.conf line 71 (value msfpath) to the following:
msfpath = ~/tools/trunk/
```

Nikto

```
$mkdir ~/tools
$cd ~/tools
$wget http://cirt.net/nikto/nikto-current.tar.gz
$tar zxvf nikto-current.tar.gz
```

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 broken on Ubuntu 10.4. As to not reinvent the wheel there is a nice easy tutorial on installing the software on Ubuntu 9.10 (http://www.ubuntugeek.com/how-to-install-vmware-server-2-0-x-in-ubuntu-9-10-karmic.html)

I had issues installing vmware and had to do the following steps.

```
$ aptitude -y install build-essential linux-headers-$(uname -r) psmisc
$cd ~/source
$ tar zxvf VMware-server-2.0.2-203138.i386.tar.gz
$ cd vmware-server-distrib/
$ wget -O - http://www.ubuntugeek.com/images/vmware-server.2.0.1_x64-modules-2.6.30.4-fix.tgz | tar xvfz -
$sudo ./vmware-server.2.0.1_x64-modules-2.6.30.4-fix.sh
$sudo perl vmware-install.pl
```

TRUECRYPT Encryption Software

Download the Linux x86 version from http://www.truecrypt.org/downloads.php

```
$ tar zxvf truecrypt-7.0-linux-x86.tar.gz
$sudo sh truecrypt-7.0-setup-x86
```

Follow the instructions to install the software.

Create a volume to use for audit data.

```
$truecrypt --text --encryption=AES --hash=SHA-1 --filesystem=FAT --volume-type=normal -c workpapers.tc
Enter volume size (sizeK/size[M]/sizeG): 1G

Enter password: <password>
Re-enter password: <password>

Enter keyfile path [none]: <ENTER>

Please type at least 320 randomly chosen characters and then press Enter:
```

```
Done: 100%  Speed:  1.5MB/s Left: 0 s

The TrueCrypt volume has been successfully created.

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