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 5.51)

Grab the latest install from www.insecure.org/nmap/

```
$cd ~/source
$wget http://nmap.org/dist/nmap-5.51.tar.bz2
$tar jxvf nmap-5.21.tar.bz2
$cd nmap-5.51
$./configure
$make
$sudo make install
```

NMAP (Current Development)

```
$cd ~/source
$svn co --username guest --password "" svn://svn.insecure.org/nmap/
$cd nmap
$./configure
$make
$sudo make install
```

John the Ripper

```
$ wget http://www.openssl.org/source/openssl-1.0.0c.tar.gz
$ tar zxvf openssl-1.0.0c.tar.gz
$ cd openssl-1.0.0c
$ ./config --openssldir=/usr/local
$ make
$ sudo make install
$ wget http://www.openwall.com/john/g/john-1.7.6.tar.gz
$ tar zxvf john-1.7.6.tar.gz
$ cd john-1.7.6/
$ wget http://www.openwall.com/john/contrib/john-1.7.6-jumbo-3.diff.gz
$ gzip -d john-1.7.6-jumbo-3.diff.gz
$ patch -p1 < john-1.7.6-jumbo-3.diff
$ cd src/
$ make linux-x86-sse2
$ sudo make install
```

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 (Ubuntu 9.10/ Ubuntu 10.04 (32 bits)).

Download the latest version from www.nessus.org (currently 4.4.0). Registration will be required after download and installation. This will also give you a key to download all Nessus plugins.

Download Nessus-4.4.0-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_4.4_installation_guide.pdf
http://www.nessus.org/Nessus_Activation_Code_Installation.pdf
http://www.nessus.org/documentation/nessus_4.4_user_guide.pdf

THC-Hydra
Various software libraries need to be installed in order 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-6.0-src.tar.gz
$tar zxvf hydra-6.0-src.tar.gz
$cd hydra-6.0-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)

HPING
```
$sudo aptitude install hping3
```

WIRE SNIFFING
```
$sudo aptitude install wireshark tcpdump
```

ETTERCAP
```
$sudo aptitude install ettercap-gtk ettercap-common libnet1
```

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
```

METAPLOIT

Grab the latest version of the framework

```
$cd ~/tools
$svn co http://metasploit.com/svn/framework3/trunk/ msf3
$gem install activerecord sqlite3-ruby
```

Ensure SQLITE3 and Ruby Libraries are installed per instructions above.

PATCH AND INSTALL RATPROXY

```
$cd ~/tools
```

```
$wget http://ratproxy.googlecode.com/files/ratproxy-1.58.tar.gz
$tar zxvf ratproxy-1.58.tar.gz
$cd ratproxy
$patch –d . < ~/source/trunk/external/ratproxy/ratproxy_wmap.diff
$make
```

Nikto (current version 2.1.4)

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

SNMP Tools

onesixtyone

```
#wget http://www.phreedom.org/solar/onesixtyone/onesixtyone-0.3.2.tar.gz
#tar zxvf onesixtyone-0.3.2.tar.gz
#cd onesixtyone-0.3.2/
#make
#cp onesixtyone /usr/local/bin
```

snmpenum.pl

```
#apt-get install libnet-snmp-perl
#mkdir ~/tools
#cd ~/tools
#wget http://www.jedge.com/utilities/snmpenum.tar.gz
#tar zxvf snmpenum.tar.gz
```

Database Tools

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/msf3/

OAT (Oracle Audit Tools)
$cd ~/tools
$wget http://www.cqure.net/tools/oat-binary-1.3.1.zip
$unzip oat-binary-1.3.1.zip
$cd oat
$wget http://vulnerabilityassessment.co.uk/classes12.zip

For each script file you need to edit the file and set JDBC=classes12.zip

Wireless Penetration Testing

DHCP Server (Used for Wireless Hacking)

```
$cd ~/source
$wget http://ftp.isc.org/isc/dhcp/dhcp-4.2.0-P2.tar.gz
$tar zxvf dhcp-4.2.0-P2.tar.gz
$cd dhcp-4.2.0-P2
$./configure
$make
$sudo make install

$sudo mkdir /etc/dhcp
$sudo gedit /etc/dhcp/dhcpd.conf
```

```
option domain-name-servers 10.0.0.1;
default-lease-time 60;
max-lease-time 72;
ddns-update-style none;
authoritative;
log-facility local7;
subnet 10.0.0.0 netmask 255.255.255.0 {
       range 10.0.0.100 10.0.0.254;
       option routers 10.0.0.1;
       option domain-name-servers 10.0.0.1;
}
```

```
$sudo touch /etc/dhcp/dhcpd.leases
$sudo chmod 777 /etc/dhcp/dhcpd.leases
```

Aircrack-NG

```
$wget http://download.aircrack-ng.org/aircrack-ng-1.1.tar.gz
$tar zxvf aircrack-ng-1.1.tar.gz
$cd aircrack-ng-1.1
$make
$sudo make install

Ensure libssl-dev is installed as described above
```

Karmasploit

```
$sudo –s
#wlanocnfig ath0 destroy
#wlanconfig ath0 create wlandev wifi0 wlanmode monitor
#airbase-ng –P –C 30 –e “Free WiFi” –v ath1
#ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
#dhcpd –cf /etc/dhcp/dhcpd.conf at0
#cd ~/tools/msf3
#./msfconsole –r karma.rc
```

http://trac.metasploit.com/wiki/Karmetasploit

Kismet

```
$sudo aptitude install flex m4 bison gpsd sox libncurses5-dev libgmp3-dev libexpat1-dev libmagick9-dev
```

Download the latest stable version of libpcap from http://www.tcpdump.org

```
$cd ~/source
$wget http://www.tcpdump.org/release/libpcap-1.1.1.tar.gz
$tar zxvf libpcap-1.1.1.tar.gz
$cd libpcap-1.1.1
$./configure
$make dep
$make
$sudo make install

$cd ~/source
$wget http://www.kismetwireless.net/code/kismet-2011-01-R1.tar.gz
$tar zxvf kismet-2011-01-R1.tar.gz
$cd kismet-2011-01-R1
$./configure
$make
$sudo make install
$sudo gedit /etc/kismet/kismet.conf
```

> [Type a quote from the document or the summary of an interesting point. You can position the text box anywhere in the document. Use the Drawing Tools tab to change the formatting of the pull quote text box.]

Windows and SMB

SMBCLIENT

```
$sudo aptitude install smbclient
```

NBTSCAN

```
$cd ~/tools
$mkdir nbtscan
$cd nbtscan
$wget http://unixwiz.net/tools/nbtscan-source-1.0.35.tgz
$tar zxvf nbtscan-source-1.0.35.tgz
$make
```

Creddump

```
$cd ~/tools
$wget http://creddump.googlecode.com/files/creddump-0.1.tar.bz2
$tar jxvf creddump-0.1.tar.bz2
```