Linux Penetration Testing Laptop (Ubuntu 11.4 Natty Narwhal)

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 apt-get update
$sudo apt-get upgrade
```

Adding compilers and kernel source code (note: build-essential is included in the Natty Narwhal install)

Installing latest 3.x Kernel (this will fix ad-hoc tethering issues)

Don't remove previous Linux kernel after installing it, new kernel may cause new problems and previous can be used for resume.

1.) Download the debs from http://kernel.ubuntu.com/~kernel-ppa/mainline/v3.0.4-oneiric/

There are three packages need to install in this order: linux-headers-*-all.deb, linux-headers-*-generic-*.deb, and finally linux-image-*.deb.

INSTALLING NECESSARY SOFTWARE (for me)

```
$sudo apt-get install vim abiword gnumeric flash-plugininstaller acroread
```

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 apt-get 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/ nmap
$cd nmap
$./configure
$make
$sudo make install
```

John the Ripper

```
$ wget http://www.openwall.com/john/g/john-1.7.8-jumbo-5.tar.gz
$ tar zxvf john-1.7.8-jumbo-5.tar.gz
$ cd john-1.7.8-jumbo-5/
$ cd src/
$ make linux-x86-64
```

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 11.4 (Ubuntu 10.10 (32 & 64 bits)).
Download the latest version from www.nessus.org (currently 4.4.1). Registration will be required after download and installation. This will also give you a key to download all Nessus plugins.
Download Nessus-4.4.1-ubuntu1010_amd64.deb or Nessus-4.4.1-ubuntu1010_i386.deb depending on your system processor. (Note: this version will work with 11.4)
Below are the LINKS for installing and using Nessus 4.4.1. 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

Thanks to DeckerXL who posted this comment here (http://wiredbytes.com/node/23#comment-61) I was able to get the Oracle password checks compiled into 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

```
$sudo apt-get install libmysqlclient-dev libpcre3-dev libsvn-dev libssh-dev
libncp-dev libidn11-dev postgresql-client libpq-dev libaio-dev
```

For Oracle support you need to download the Oracle Instant Client (Google “oracle instant client download”). The three files you will need to download are the basiclite, sqlplus, and devel rpm packages. We will then need to convert the rpm packages to deb and install.

```
$sudo apt-get install alien
$cd ~/Downloads
$alien -i oracle-instantclient11.2-basiclite-*.rpm
$alien -i oracle-instantclient11.2-devel-*.rpm
$alien -i oracle-instantclient11.2-sqlplus-*.rpm
```

Create the following file (oracle.conf) in ls.so.con.d and add the following (that's where it put my libs for version 11.2 - substitute your version there)
/usr/lib/oracle/11.2/client64/lib

```
$sudo ldconfig
$cd ~/source
$wget http://freeworld.thc.org/releases/hydra-7.0-src.tar.gz
$tar zxvf hydra-7.0-src.tar.gz
$cd hydra-7.0-src
$./configure --with-oracle=/usr/include/oracle/11.2/client64 --with-oracle-
lib=/usr/lib/oracle/11.2/client64/lib
```

Edit the Makefile and manaully add the Oracle include dir to the XIPATHS var on line 6.

```
XIPATHS= -I/usr/include/subversion-1 -I/usr/include/apr-1.0 -I/usr/include/
subversion-1 -I/usr/include/mysql -I/usr/include/oracle/11.2/client64

$make
$sudo make install
```

TRACEROUTE

```
$sudo apt-get install traceroute
```

TCPTRACEROUTE

```
$sudo apt-get install tcptraceroute
```

HPING

```
$sudo apt-get install hping3
```

WIRE SNIFFING

```
$sudo apt-get install wireshark tcpdump
```

ETTERCAP

```
$sudo apt-get 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

```
$wget ftp://ftp.stunnel.org/stunnel/obsolete/3.x/stunnel-3.9.tar.gz
$tar zxvf stunnel-3.9.tar.gz
$cd stunnel-3.9
$./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
```

METASPLOIT 3

Grab the latest version of the 3.x framework

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

Ensure SQLITE3 and Ruby Libraries are installed per instructions in the beginning of the document.

METASPLOIT 4

Download the latest Metasploit from www.metasploit.com

```
$cd ~/Downloads
$chmod 775 framework-4.0.0-linux-x64-mini.run
$sudo ./framework-4.0.0-linux-x64-mini.run
```

Follow the installation GUI

Nikto (current version 2.1.4)

```
$sudo apt-get install libnet-ssleay-perl
$cd ~/tools
$wget http://cirt.net/nikto/nikto-current.tar.gz
$tar zxvf nikto-current.tar.gz
```

SNMP Tools

onesixtyone

```
$cd ~/source
$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
$sudo cp onesixtyone /usr/local/bin
```

snmpenum.pl

```
$sudo apt-get install libnet-snmp-perl
$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

```
$sudo apt-get install libnetpacket-perl libpcap0.8 libpcap0.8-dev libnet-pcap-
perl libnet-dns-perl libnet-rawip-perl libio-socket-ssl-perl
$cd ~/tools/
$wget http://downloads.sourceforge.net/project/sqlninja/sqlninja/0.2.6-rc2/
sqlninja-0.2.6-rc2.tgz
$tar zxvf sqlninja-0.2.5.tgz
$cd sqlninja-0.2.5
```

Change sqlninja.conf line 97 (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
$rm -rf *.bat
$chmod 775 *.sh
$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 ftp://ftp.isc.org/isc/dhcp/dhcp-4.1-ESV-R3.tar.gz
$tar zxvf dhcp-4.1-ESV-R3.tar.gz
$cd dhcp-4.1-ESV-R3
$./configure
$make
$sudo make install
$sudo mkdir /etc/dhcpd
$sudo gedit /etc/dhcpd/dhcpd.conf

            default-lease-time 60;
            max-lease-time 72;

            ddns-update-style none;

            authoritative;

            log-facility local7;

            subnet 192.168.5.0 netmask 255.255.255.0 {
              range 192.168.5.50 192.168.5.100;
              option routers 192.168.5.254;
              option domain-name-servers 192.168.5.254;
            }

$sudo touch /etc/dhcpd/dhcpd.leases
```

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

Aircrack-NG

Note: the aircrack-1.1 source does not compile on Natty Narwhal. An ugly fix is to open comman.mak and remove the -Werror flag on line 70.

```
$cd ~/source
$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
$sudo airodump-ng-oui-update
```

You can also grab aircrack svn.

```
$cd ~/source
$svn co http://trac.aircrack-ng.org/svn/trunk/ aircrack-ng
$make
$sudo make install
$sudo airodump-ng-oui-update
```

Kismet

```
$sudo apt-get 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-2011-03-R2.tar.gz
$tar zxvf kismet-2011-03-R2.tar.gz
$cd kismet-2011-03-R2
$./configure
$make
$sudo make install
$sudo gedit /etc/kismet/kismet.conf
```

Windows and SMB

SMBCLIENT

```
$sudo apt-get 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
```