Linux Penetration Testing Laptop (Ubuntu 9.10 NBR)
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. Currently I use a Dell Vostro A90.

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 (Current Stable is 5.21)

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

```
#wget http://nmap.org/dist/nmap-5.21.tar.bz2
#tar jxvf nmap-5.21.tar.bz2
#cd nmap-5.21
#./configure
#make && 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. Instructions on download and compile are included below.

```
$ wget http://www.openssl.org/source/openssl-0.9.8l.tar.gz
$ tar zxvf openssl-0.9.8l.tar.gz
$ cd openssl-0.9.8l
$ ./config
$ make
$ sudo make install
$ wget http://www.openwall.com/john/g/john-1.7.4.2.tar.gz
$ tar zxvf john-1.7.4.2.tar.gz
$ cd john-1.7.4.2/
$ wget http://www.openwall.com/john/contrib/john-1.7.4.2-jumbo-2.diff.gz
$ gzip -d john-1.7.4.2-jumbo-2.diff.gz
$ patch -p1 < john-1.7.4.2-jumbo-2.diff
$ cd src/
$ make linux-x86-sse2
$cd ../run
$./john
```

John will be found in the run directory

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 9.10.

Download the latest version from www.nessus.org (currently 4.2.0). Registration will be required to download. This will also give you a key to download all Nessus plugins.

Download Nessus-4.2.0-ubuntu910_i386.deb

Below are the LINKS for installing and using Nessus 4.2.0. 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.
#apt-get install libssl-dev libpq-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

TRACEROUTE
#apt-get install traceroute

TCPTRACEROUTE
#apt-get install tcptraceroute

SCANRAND and PARATRACE (no longer supported in Ubuntu. It uses an antiquated version of libnet)
~~#apt-get install paketto~~

HPING
~~#apt-get install hping2~~ (no longer available on 9.10)
#apt-get install hping3

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 died May 15, 2009.

METAPLOIT
Install Ruby with any and all additional packages required.

```
#apt-get install ruby openssl libopenssl-ruby libreadline-ruby rubygems irb1.8 rdoc1.8 ruby-dev libruby
```

Accept all dependencies
Grab the latest version of the framework

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

INSTALL SQLITE3

```
#apt-get install libsqlite3-dev sqlite3 libsqlite3-ruby
```

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'
#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
```

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 easy to do on Ubuntu. 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)

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

```
#tar zxvf truecrypt-6.3a-ubuntu-x86.tar.gz
#sh truecrypt-6.3a-setup-ubuntu-x86

Follow the GUI instructions to install the software.

Create a volume to use for audit data.
#truecrypt --text --encryption=AES --hash=SHA-1 --filesystem=FAT -volumn-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
```