Installation for Linux Systems

Many Linux distributions will provide Libpcap, Tcpdump and Ethereal as available packages during installation, or may be available on the installation CD's. If these software packages are available from your Linux distribution vendor, please install these packages according to your system documentation. For example, Fedora Core Linux users can install these packages with the "yum" tool:

```
# yum install libpcap tcpdump ethereal
```

If you are unable to identify the appropriate packages for Libpcap, Tcpdump and Ethereal for your Linux distribution, you can download and compile these tools from source with a C compiler. In order to compile tools from source, you must install the development tools package for your Linux distribution.

Note: The installation instructions assume you are logged in as the root user.

Download Section for Libpcap, Tcpdump, Ethereal and Ngrep

The download location for **Libpcap** is:
http://www.tcpdump.org/release/libpcap-0.8.3.tar.gz

The download location for **Tcpdump** is:
http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz

The download location for **Ngrep** is:
http://unc.dl.sourceforge.net/sourceforge/ngrep/ngrep-1.42-linux-elf-static.bz2

The download location for **Ethereal** is:
http://www.ethereal.com/distribution/ethereal-0.10.9.tar.gz

Installing Libpcap, Tcpdump and Ethereal from source

First make a directory where these files can be built. For example, "**`mkdir ~/SANS`**". Then download the following tar packages for Libpcap, Tcpdump and Ethereal to that directory.

The Libpcap, Tcpdump and Ethereal programs are distributed in a compressed tar archive format. To extract the files run the following commands in this order:

```
# tar -zxf libpcap-0.8.3.tar.gz
# tar -zxf tcpdump-3.8.3.tar.gz
# tar -zxf ethereal-0.10.9.tar.gz
```

After completing the above steps, you will have three subdirectories, libpcap-0.8.3, tcpdump-3.8.3 and ethereal-0.10.9.

The next step is to compile libpcap. To do this, complete the following steps:

```
# libpcap-0.8.3
# ./configure
# make
# cd ..
```

This will not install the libpcap library, only compile it, since we don't need it installed just to compile tcpdump. If you want libpcap installed for future use see the INSTALL file in the libpcap-0.8.3 directory for further instructions.

Now tcpdump can be compiled. To do this, complete the following steps:

```
# cd tcpdump-3.8.3
# ./configure
# make
# make install
# cd ..
```

Running the "`make install`" command will install the tcpdump tool in the /usr/local/sbin directory.

Next we can compile Ethereal. Ethereal is a complex software package; it may require an hour or longer to compile, depending on the speed of your system. To compile and install Ethereal, complete the following steps:

```
# cd ethereal-0.10.9
# ./configure
# make
# make install
# cd ..
```

Running the "`make install`" command will install the Ethereal tools in the /usr/local/bin directory.

Installing Ngrep

The Ngrep tool is conveniently packaged as a static binary for Linux systems. Download Ngrep into the ~/SANS directory you created earlier and extract the archive using the "`bunzip`" command, as shown below:

```
# bunzip2 ngrep-1.42-linux-elf-static.bz2
# chmod 700 ngrep-1.42-linux-elf-static
# mv ngrep-1.42-linux-elf-static /usr/local/sbin/ngrep
```

Validating the Installation

Use the "which" command to ensure that the Tcpdump, Ngrep and Ethereal tools are all in your path.

```
# which ngrep
/usr/local/sbin/ngrep
# which tcpdump
/usr/local/sbin/tcpdump
# which ethereal
/usr/local/bin/ethereal
```

If the "`which`" command does not produce any output for any of the three tools, repeat the installation procedure for the missing tool.