# Linux Lab 8 Installing and Removing Software (CentOS)

# Read

Listen to or read CyberAces Module 1 Linux, session 7 Installing Software (<https://tutorials.cyberaces.org/tutorials/view/1-1-7.html>)

*The Linux Command Line*, chapter 14 Package Management and chapter 23 Installing Software, pp 149 - 157 and 297 - 306 in the printed book and pp 172 -18 and 350 - 361 in the pdf.

These are some good references for how the standard “./configure , make , make install” , sequence works.  
<http://tldp.org/LDP/LG/current/smith.html> (see paragraph 6 for an old Linux joke)  
<http://www.opensourceforu.com/2012/06/gnu-make-in-detail-for-beginners/>

# Lab

Install nmap from the CentOS repository using the procedure in slides 11 through 17 in CyberAces\_Module1-Linux\_7\_InstallingSoftware.pdf.

Then update your CentOS VM by following slides 20 and 21 in CyberAces\_Module1-Linux\_7\_InstallingSoftware.pdf.

## Install nmap from the source code. (Optional)

Note: Installing from source code works great sometimes, and other times can be messy. If you like, you can skip removing nmap and reinstalling it from source code. If so, read the paragraph about tar and then skip ahead to review. If you are an intrepid Linux user, go ahead and remove nmap and install from source code.

When you install from source code you can make sure you have the latest version, or the version you want. Remember that if you install from source code, yum upgrade won’t help you; you’ll have to install updates manually.

Since we are compiling from source code, we will need to install a compiler and related development software. This command does that quickly.  
sudo yum install make automake gcc gcc-c++ kernel-devel

Note: if sudo does not work for your user, use su – to switch to root and then add your user to the wheel group with gpasswd -a youruser wheel. Use exit to get back to your user.

Go to <https://nmap.org/download.html> and download the latest tarball of nmap—it’s at the bottom of the section called “Source Code Distribution,” labeled “Latest Stable Nmap release tarball.” The tar, or tape archive program, is used to put multiple files into one file and optionally compress them. (Tar (tape archive) files are often called tarballs. Tar was originally used for backup--the files on the computer were put into a tarball and the tarball was then saved to magnetic tape.) Nmap now compresses its files with bzip2 rather than gzip.

Save the file rather than opening it with the web browser. If you are a hard core terminal person, you can download using [curl](http://www.compciv.org/recipes/cli/downloading-with-curl/) or [wget](https://www.pair.com/support/kb/paircloud-downloading-files-with-wget/). You still must know the download URL, though. You can often get the link using right-click “copy link location” in the browser, and then pasting it. As I write this, the link is <https://nmap.org/dist/nmap-7.80.tar.bz2>.

Extract the nmap files using the tar program. You'll need to use the options to extract (-x) and uncompress (use-j for bzip2 or -z for gzip files, depending on which one you downloaded) the files. It's nice to use the verbose option (-v) so you can see what's going on, and you'll need to use an option (-f) to tell tar that the data is coming from a file (and what its name is.) It doesn't matter much what directory you untar the file to. I chose to move the tarball to my home directory before uncompressing it, although a neater user will create a directory for source files.

tar –xjvf nmap-[version].tar.bz2 (bzip2 compressed) or  
tar -xzvf nmap-[version].tgz (gzip compressed)

Note: [version] will be different, depending on what you download

[john@localhost ~]$ cd Downloads/

[john@localhost Downloads]$ ls

nmap-7.80.tar.bz2

[john@localhost Downloads]$ tar -xjvf nmap-7.80.tar.bz2

nmap-7.80/

nmap-7.80/nse\_nmaplib.cc

nmap-7.80/protocols.cc

nmap-7.80/idle\_scan.cc

<snip>

Change directory (cd) into the directory with the files you just unzipped. For most installations, there is a configure script that does the work of figuring out what distribution you have, where your compilers and libraries are, and it puts that information into something called the Makefile. Look for README and other info files (usually the file names are all Caps.) Sometimes there are special configuration options you can use, and these are often documented in the beginning of the configure file (less configure.) Look to see that there is a file called “configure” in your directory and scan the beginning with less to see if there are interesting options. Also look to see if there is a Makefile. (If configure hasn’t run yet, should will be a Makefile.in but no Makefile.)

[john@localhost Downloads]$ ls

nmap-7.80 nmap-7.80.tar.bz2

[john@localhost Downloads]$ cd nmap-7.80/

[john@localhost nmap-7.80]$ ls -l

total 15932

-rw-r--r--. 1 john john 11052 Nov 21 2018 acinclude.m4

-rw-r--r--. 1 john john 11453 Sep 19 2017 aclocal.m4

-rw-r--r--. 1 john john 173 Jun 29 2009 BSDmakefile

-rw-r--r--. 1 john john 740693 Jul 31 2019 CHANGELOG

-rw-r--r--. 1 john john 12033 May 28 2019 charpool.cc

-rw-r--r--. 1 john john 10046 May 28 2019 charpool.h

-rw-r--r--. 1 john john 3331 Oct 17 2018 checklibs.sh

-rwxr-xr-x. 1 john john 42938 Feb 14 2015 config.guess

-rwxr-xr-x. 1 john john 35994 Feb 14 2015 config.sub

-rwxr-xr-x. 1 john john 264740 May 24 2019 configure

-rw-r--r--. 1 john john 33201 May 24 2019 configure.ac

<snip>

-rw-r--r--. 1 john john 10792 May 28 2019 MACLookup.h

drwxr-xr-x. 3 john john 174 Aug 2 2019 macosx

-rw-r--r--. 1 john john 13364 May 28 2019 main.cc

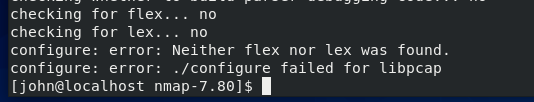
-rw-r--r--. 1 john john 19949 Jun 21 2019 Makefile.in

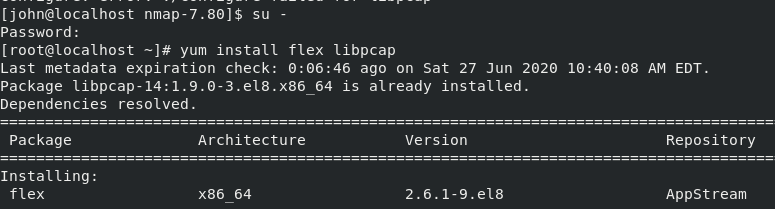
-rwxr-xr-x. 1 john john 10677 Aug 23 2017 missing   
<snip>

### Configure

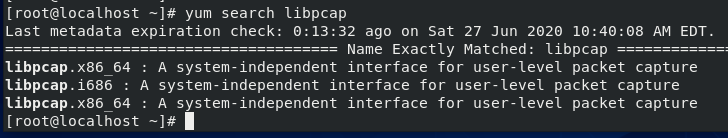
Too bad, no interesting options on this configure file. Run the configure script. If you get a “command not found” error, remember what you need to do to run a script when you are in the same directory as the script. (Hint: the abbreviation for your current directory is ./ )

### Missing Dependencies

The biggest problem installing from source code is that the code often depends on other applications that are not installed on your VM. If there are missing dependencies, ./configure or make will generate errors. Sometimes you have to Google the error messages to find what is missing. In this case, the messages are more helpful. It appears that we need either flex or lex, and libpcap (flex is a program that performs pattern matching on text, and libpcap is the library for packet capture files.)  


So, let’s try installing flex and libpcap.  


Hmm, it can’t find libpcap but yum says it is installed. That often happens when the base version is installed but the development version, which containers headers that nmap needs, are not installed. We can check with  
yum search libpcap



Hmm, no development version listed. This is where source code installations get complicated. Several Google searches tell us that we have to enable additional repositories.  
sudo yum install epel-release  
sudo dnf config-manager --set-enabled PowerTools

Then we can install the development files for libpcap.  
sudo yum install libpcap-devel

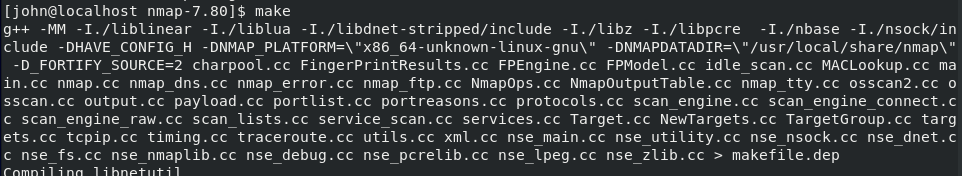
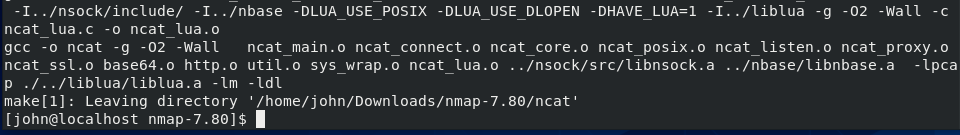
Now we can try ./configure again.  


It tells us that we don’t have OpenSSL and LibSSH2 installed, but that will only affect us if we try to decode SSL or SSH traffic. Now for make.

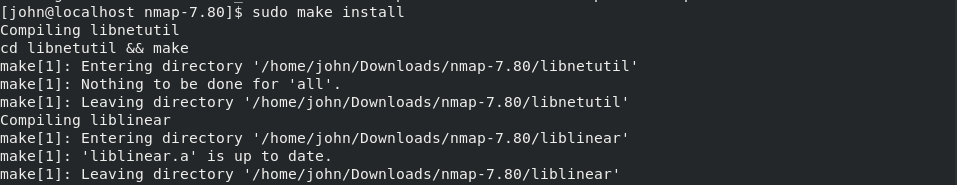
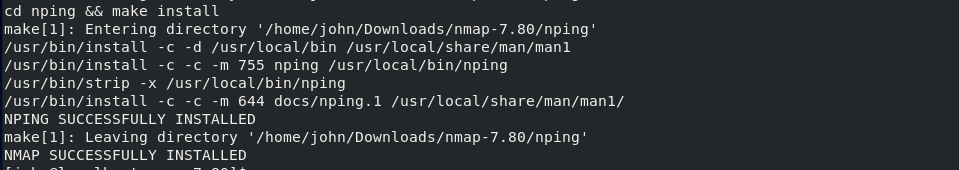
### make

The configure script ran many checks, and if they all passed, generated a Makefile. Use ls to look for it. When you did this before, you should have seen only Makefile.in. Now you should see Makefile.in and Makefile. The command make calls a program that is already installed in your OS. If you run, “which make”, you'll see that it lives in /usr/bin/. If it were missing, you’d have to run, “apt-get install make”. Make saves you the trouble of looking for modules your software depends on (dependencies), compiling each module of the software, compiling them in the proper order, and then linking them all together. For complex software, this is a lot of work. All you need to do is type one word:  
make  
You must type make from the directory that holds your Makefile.  
\*\*Why do you type make instead of ./make ?

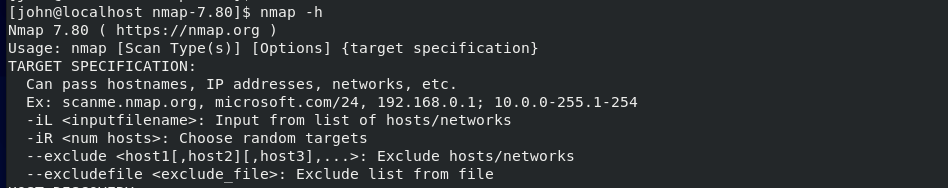
It will compile ~~about a gazillion~~ many files. If you run ls, you'll see ~~a whole bunch of~~ many files that weren't there before. Most of these are \*.o files, or object files. They are compiled binary files that can be linked together to run programs.

  
<lots of output deleted>  
  
No errors. Whew!

### sudo make install

When you run make install, you are telling make that you’ve already compiled the program (see the previous step) and now you want to copy all those object files and binaries into the necessary places on the OS, often to /usr/bin and /usr/local/bin. Those directories require root access, so you’ll have to run as root or use sudo.  
  
<snip>  
  
Whew!

### It runs!



Review

The basic commands we use to install from source code were:

* tar, to decompress the files
* ./configure from the directory tar made, to check for dependencies and create the makefile
* make (same directory as above), to compile all the code
* sudo make install (same directory) to move the compiled files to the proper directories

# Hand in

1. Were you able to install nmap using both methods?
2. What is nmap, anyway?
3. What are possible problems with installing programs from source code?