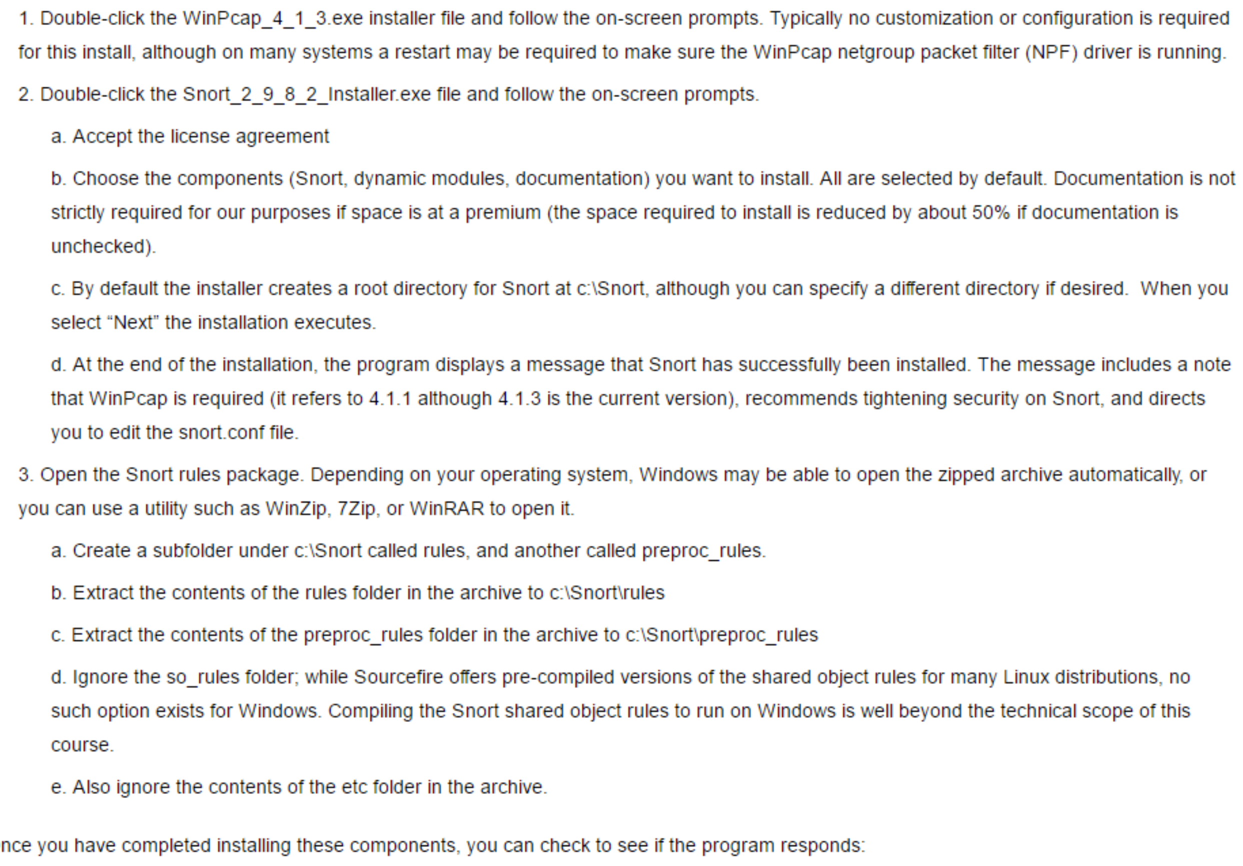
Exercise 12:

To demonstrate intrusion detection system (ids) using any snort.

Installing Snort in Windows:.



1. Double-click the WinPcap_4_1_3.exe installer file and follow the on-screen prompts. Typically no customization or configuration is required for this install, although on many systems a restart may be required to make sure the WinPcap netgroup packet filter (NPF) driver is running.
2. Double-click the Snort_2_9_8_2_Installer.exe file and follow the on-screen prompts.
   a. Accept the license agreement

   b. Choose the components (Snort, dynamic modules, documentation) you want to install. All are selected by default. Documentation is not strictly required for our purposes if space is at a premium (the space required to install is reduced by about 50% if documentation is unchecked).

   c. By default the installer creates a root directory for Snort at c:\Snort, although you can specify a different directory if desired. When you select "Next" the installation executes.

   d. At the end of the installation, the program displays a message that Snort has successfully been installed. The message includes a note that WinPcap is required (it refers to 4.1.1 although 4.1.3 is the current version), recommends tightening security on Snort, and directs you to edit the snort.conf file.
3. Open the Snort rules package. Depending on your operating system, Windows may be able to open the zipped archive automatically, or you can use a utility such as WinZip, 7Zip, or WinRAR to open it.
   a. Create a subfolder under c:\Snort called rules, and another called preproc_rules.

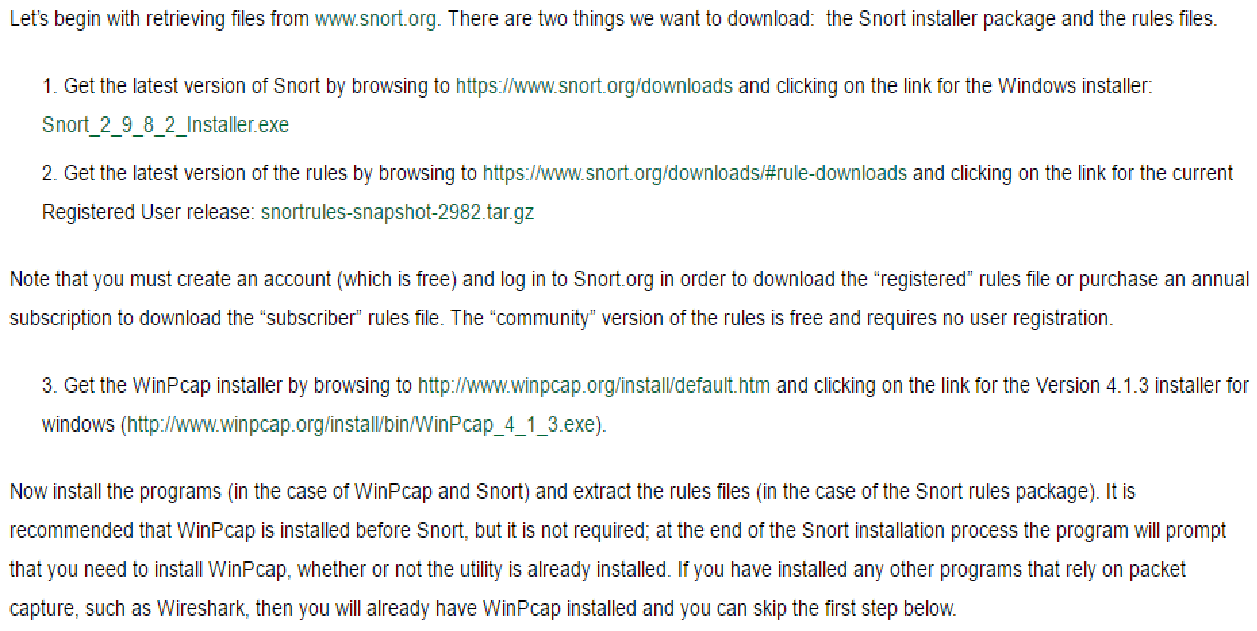
   b. Extract the contents of the rules folder in the archive to c:\Snort\rules

   c. Extract the contents of the preproc_rules folder in the archive to c:\Snort\preproc_rules

   d. Ignore the so_rules folder; while Sourcefire offers pre-compiled versions of the shared object rules for many Linux distributions, no such option exists for Windows. Compiling the Snort shared object rules to run on Windows is well beyond the technical scope of this course.

   e. Also ignore the contents of the etc folder in the archive.

Once you have completed installing these components, you can check to see if the program responds:



Let's begin with retrieving files from www.snort.org. There are two things we want to download: the Snort installer package and the rules files.

1. Get the latest version of Snort by browsing to https://www.snort.org/downloads and clicking on the link for the Windows installer: Snort_2_9_8_2_Installer.exe
2. Get the latest version of the rules by browsing to https://www.snort.org/downloads/#rule-downloads and clicking on the link for the current Registered User release: snortrules-snapshot-2982.tar.gz

Note that you must create an account (which is free) and log in to Snort.org in order to download the "registered" rules file or purchase an annual subscription to download the "subscriber" rules file. The "community" version of the rules is free and requires no user registration.

3. Get the WinPcap installer by browsing to http://www.winpcap.org/install/default.htm and clicking on the link for the Version 4.1.3 installer for windows (http://www.winpcap.org/install/bin/WinPcap_4_1_3.exe).

Now install the programs (in the case of WinPcap and Snort) and extract the rules files (in the case of the Snort rules package). It is recommended that WinPcap is installed before Snort, but it is not required; at the end of the Snort installation process the program will prompt that you need to install WinPcap, whether or not the utility is already installed. If you have installed any other programs that rely on packet capture, such as Wireshark, then you will already have WinPcap installed and you can skip the first step below.

1. Double-click the WinPcap_4_1_3.exe installer file and follow the on-screen prompts. Typically no customization or configuration is required for this install, although on many systems a restart may be required to make sure the WinPcap netgroup packet filter (NPF) driver is running.

2. Double-click the Snort_2_9_8_2_Installer.exe file and follow the on-screen prompts.

    a. Accept the license agreement

    b. Choose the components (Snort, dynamic modules, documentation) you want to install. All are selected by default. Documentation is not strictly required for our purposes if space is at a premium (the space required to install is reduced by about 50% if documentation is unchecked).

    c. By default the installer creates a root directory for Snort at c:\Snort, although you can specify a different directory if desired. When you select "Next" the installation executes.

    d. At the end of the installation, the program displays a message that Snort has successfully been installed. The message includes a note that WinPcap is required (it refers to 4.1.1 although 4.1.3 is the current version), recommends tightening security on Snort, and directs you to edit the snort.conf file.

3. Open the Snort rules package. Depending on your operating system, Windows may be able to open the zipped archive automatically, or you can use a utility such as WinZip, 7Zip, or WinRAR to open it.

    a. Create a subfolder under c:\Snort called rules, and another called preproc_rules.

    b. Extract the contents of the rules folder in the archive to c:\Snort\rules

    c. Extract the contents of the preproc_rules folder in the archive to c:\Snort\preproc_rules

    d. Ignore the so_rules folder; while Sourcefire offers pre-compiled versions of the shared object rules for many Linux distributions, no such option exists for Windows. Compiling the Snort shared object rules to run on Windows is well beyond the technical scope of this course.

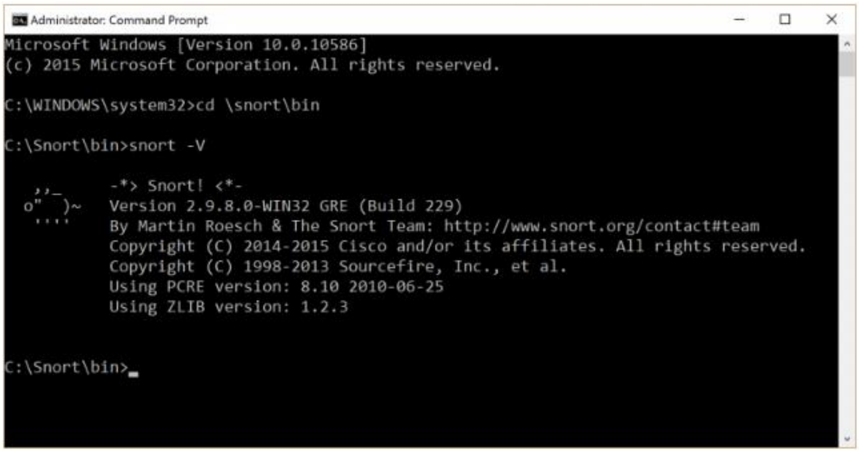
    e. Also ignore the contents of the etc folder in the archive.

Once you have completed installing these components, you can check to see if the program responds:

1. Change to the Snort program directory: `c:\>cd \Snort\bin`

2. Check the installed version for Snort: `c:\Snort\bin>snort -V`

3. The -V option (it must be a capital V) simply returns the current installed version of the program. If Snort is installed on the system, you should see something similar to the screenshot below (which shows an installed version 2.9.8.0):



```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd \snort\bin

C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.8.0-WIN32 GRE (Build 229)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3


C:\Snort\bin>_
```

4. You should also check to see what network adapters are on your system, so you can tell Snort to listen on the appropriate interface when it runs. To see a list of interfaces, run the command: `C:\Snort\bin>snort -W`

On current Windows systems there will be at least two (Ethernet and wireless), three if there is a modem in the computer, and four or more depending on what additional software is installed on the computer. If both wired and wireless network interfaces are active, you should disable one before you try to run Snort, since Windows offers no way to direct a program to use a specific interface when multiple connections are available. Record the number of the interface you will use (the instructions below assume the interface number is 2; substitute the appropriate number for your computer when using the **-i** option in Snort start-up commands.

The next thing to do is to edit the snort.conf file to make it reflect the environment where your computer is running (see Configuring Snort with snort.conf). You should make sure that when you edit the file, you are working on the one in **c:\Snort\etc** (and not any other versions that may exist in temporary or download directories).

CONFIGURING SNORT

Getting Snort installed successfully can be a challenge, but it is also only the first step in setting the tool up so you can launch it to start monitoring traffic and generating alerts. To get Snort ready to run, you need to change the default configuration settings file (which is created as part of the Snort installation) to match your local environment and operational preferences. If you accepted the default locations proposed during the Windows installer execution, then the snort.conf file will be located in the directory **C:\Snort\etc**. The configuration file is plain text, so you can use any text editor to edit it, but Wordpad (or even better, the free Notepad++) is recommended at least for the first time to ensure the proper formatting is maintained (when opening the baseline snort.conf file in Notepad all the text runs together).

When you open the file for viewing or editing, you will see it is organized into nine parts or steps:

1. Set the network variables
2. Configure the decoder
3. Configure the base detection engine
4. Configure dynamic loaded libraries
5. Configure preprocessors
6. Configure output plugins
7. Customize your rule set
8. Customize preprocessor and decoder rule set
9. Customize shared object rule set

As you can see, there are a lot of ways to customize Snort, and making sense of the entire snort.conf file can be a little daunting. To get running for the first time, many of the defaults can be left alone. The following edits are recommended:

1. Step 1

    a. Change the declaration for **HOME_NET** to your actual home network IP address range, rather than leaving the default "**any**". The simplest way to do this is to use a CIDR format expression, to cover the entire range of relevant addresses (particularly when using Network Address Translation such as in environments protected by gateways or routers.

    i. For a typical home network, the expression will be `192.168.0.1/24` or `192.168.1.1/24` (if you're not sure whether your third number is a 0 or 1, check your gateway/router documentation or just ping it. If you want to cover all IP addresses beginning with 192.168, then use the expression `192.168.0.0/16`

    ii. In a typical large office network using network address translation, the expression will be `10.0.0.0/8`

    iii. In some environments (including home environments connecting to the Internet via cable modem without the use of a gateway or router) the appropriate IP address range to use may be dictated by the ISP from which you get your Internet service.

    iv. If you are unsure which IP address range to specify for your home network, you can quickly check to see the IP address assigned to your computer by opening a command shell window and typing `ipconfig` at the prompt.

    v. Finally, you can leave the **HOME_NET** declaration as "**any**" if you are unable to accurately determine a specific IP range to use.

    b. Change the declaration for **EXTERNAL_NET** to **!$HOME_NET** – this expression means the external network will be defined as any IP address that is not part of the home network. **Important!** If you leave **HOME_NET** declared as "any" you ***cannot*** use **!$HOME_NET**, as the expression will translate to "not any" and throw an error when you try to start Snort.

    c. Generally speaking, you can leave unchanged all the other server declarations, although if you want you can reduce the list of web server ports declared for **HTTP_PORTS**.

    d. Change the var **RULE_PATH** declaration to match the actual location of your rules files. Typically the rules will be stored in **c:\Snort\rules**, so you can use that full path name or whatever the right location is on your system.

    e. Similarly, change the **PREPROC_RULE_PATH** to match the appropriate directory location on your system, such as **c:\Snort\preproc_rules**.

    f. Comment out (meaning put a # character in the first position in the line) the **SO_RULE_PATH** declaration, as the Windows implementation of Snort doesn't use shared object rules.

g. The reputation preprocessor is a relatively recent addition to Snort that allows you to configure trusted or untrusted IP addresses using separately referenced files that list the addresses (whitelist for trusted, blacklist for untrusted). If you intend to enable the reputation preprocessor then the path to the whitelist and blacklist files needs to be provided at the end of step 1. **Please note:** if you leave the reputation preprocessor enabled, you *must* create the whitelist and blacklist rules files referenced in the preprocessor configuration, or Snort will generate an error and fail to start. If you want to work with the reputation preprocessor later, be sure to comment it out in step 5.

2. Step 2

a. For most users, there are no changes needed to the decoder configurations.

b. At the end of this section, there is a configuration setting to indicate the default directory where Snort logs should be written. Uncomment this line by deleting the # character in the first position and edit the line to include the **c:\Snort\log** default directory path.

3. Step 3

a. For most users, there are no changes needed to the base detection engine settings, so move on to step 4. These settings are used for performance tuning and reflect memory and processing capabilities.

4. Step 4

a. Change the dynamic loaded library path references to reflect their location in Windows, and in the case of the dynamic engine to replace the default Linux filename with the Windows equivalent. Snort references these locations and loads the libraries at start-up.

i. **dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor**

ii. **dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll**

iii. Comment out (put a # in the first position in the line) the **dynamicdetection directory** declaration.

b. Note that the dynamic engine is actually pointing to a file, while the other two declarations point to directories. It's always a good idea to double-check the accuracy of these locations by browsing to them with the file browser or performing directory listings from the command line. Be sure there is no trailing character on the dynamic preprocessor directory.

c. One point to be aware of when configuration is done and you move one to running Snort: loading the dynamic libraries requires Snort to write to the Windows registry, an action typically requiring administrator privileges. For this reason the command shell should be launched with the "Run as administrator" option from the Windows start menu when preparing to start Snort.

5. Step 5

a. Be aware that there are many, many preprocessors for use with Snort, and you very likely will not want or need to have all of them running. Each preprocessor has a separate readme file with configuration options and settings documented in it, so if you want to use a particular preprocessor, you should consult those files or the Snort manual to make sure you set them up properly.

b. Comment out (put a # in the first position on the line) all the rows in the Inline packet normalization preprocessor. This preprocessor is only used when Snort is implemented in in-line IPS mode, and Snort should ignore it otherwise, but on Windows it will cause an error if left uncommented.

c. For general-purpose Snort usage, it usually makes sense to disable (comment out) some of the preprocessors, particularly ones like those for normalization listed first in Step 5 that only apply to Snort in in-line mode. Of the others, it is fine to leave default preprocessors active, but at a minimum it is a good idea to keep at least the following preprocessors active (using default configuration settings):

i. **frag3**

ii. **stream5**

iii. **http_inspect**

iv. **ftp_telnet**

v. **smtp**

vi. **dns**

vii. **ssl**

viii. **sensitive_data**

d. The most recent releases of Snort include some very interesting new preprocessors, some of which are not included in snort.conf by default. You can learn more about these preprocessors and the configuration syntax used to add them to the file in Step 5 by consulting the Snort documentation or the "readme" file for each preprocessor.

e. As noted in Step #1 above, if you choose to keep the **reputation preprocessor** enabled you must create whitelist and blacklist files corresponding to the references in the configuration settings for the reputation preprocessor, which is at the very end of Step #5. You can opt to comment it out for initial setup and come back to it later. Snort by default includes a set of rules in a file called "blacklist.rules" that *is not* used by the reputation preprocessor. For this reason it is strongly recommended to avoid later confusion that you choose names for the whitelist and blacklist files that do not include "rules" in the names (for example, "white.list" and "black.list").

6. Step 6

   a. Typically, only one of the output plugins is used with Snort at any one time. The default in recent releases of Snort is unified2, but as noted above this is not well supported on Windows platforms. If you intend to use syslog, then uncomment that line to activate the syslog output plugin. If you intend to use screen output only, leave all the output plugins commented out.

      i. Uncomment and edit the syslog output line in snort.conf, so it reads like this:

      `output alert_syslog: host=127.0.0.1:514, LOG_AUTH LOG_ALERT`

      ii. **Note**: If you choose to use syslog output, then you also need to install and run a syslog server; see Installing a Syslog Server.

   b. If you have used previous versions of Snort, you may notice that there are no database output configuration options in the snort.conf file. As of the 2.9.3 version of Snort direct logging to database is no longer supported.

   c. Leave the metadata reference lines at the end of step 6 ***uncommented***: `include classification.config` and `include reference.config`

7. Step 7

   a. If you have installed the Snort VRT ruleset, then you can tailor the series of include statements in step 7 to match whatever environment characteristics and types of rules you want. For initial testing, sometimes it can be helpful to reduce the number of rules loaded at start-up, but make sure that the line for "**local.rules**" remains uncommented, as that is where you will place the rules that you write yourself.

   b. For first-time users, you may want to comment out most of the include statements listed in step 7 until you verify your configuration.

   c. If you create your own rules in separate rules files (instead of adding them to local.rules), add an include statement for your custom files following the same syntax you see for all the other statements in step 7.

8. Step 8

   a. There are not very many settings in step 8, so in general you just want to make sure that you uncomment any rules here that correspond to preprocessors you configured to load in step 5. By default, if you kept the standard settings in step 2 and enabled at least some preprocessors, the uncomment the first two lines in step 8

      i. `include $PREPROC_RULE_PATH\preprocessor.rules`

      ii. `include $PREPROC_RULE_PATH\decoder.rules`

   b. If you enabled the sensitive_data preprocessor (in step 5), then uncomment the third line in step 8: `include $PREPROC_RULE_PATH\sensitive-data.rules`

   c. Make sure the rules you declare in these statements are actually present in the appropriate directory (such as **c:\Snort\preproc_rules**)

9. Step 9

   a. The rules referenced in Step #9 are shared object rules, which are different from (although similarly named) the rules listed in Step #7. Because shared object rules are not well supported on Windows, leave all the shared object rules commented out in step 9.

   b. Leave the event thresholding line at the end of step 9 ***un-commented***: `include threshold.conf`

GENERATING ALERTS

To see if Snort is working, beyond just getting it to load without errors (not a trivial feat in itself), it is helpful to generate some alerts. The easiest way to do this to validate setup and configuration is to create a couple of testing rules, load them in Snort, and trigger them so you can check to see if they generate alerts as expected. Put your testing rules in the **local.rules** file that is located in the **c:\Snort\rules** directory.

1. Open **local.rules** with a text editor such as Notepad++ or Wordpad.
2. Move down beyond the commented header information to the first blank line. Start with some generic rules to test network traffic detection. Enter the following, all on one line: `alert icmp any any -> any any (msg:”ICMP Testing Rule”; sid:1000001; rev:1;)`
3. Press Enter to move to a new line, and create another rule to check TCP traffic detection: `alert tcp any any -> any 80 (msg:”TCP Testing Rule”; sid:1000002; rev:1;)`
4. Press Enter to move to a new line, and create another rule to check UDP traffic detection: `alert udp any any -> any any (msg:”UDP Testing Rule”; sid:1000003; rev:1;)`
5. You can create any number of additional rules you like; just be sure to start each one on a new line.
6. Save the file and exit the editor. **Note:** If you use Notepad, it is important to save the file as type “All Files” rather than the text documents default. The default will add “.txt” to the rule file name (so it will become local.rules.txt) and Snort will generate an error when it tries to load the file.

If you load these rules by starting Snort with the **-A console** option, when you test the rules by performing the steps listed below, you can see the output on the screen as it happens. Note that the startup command shown below uses interface #2, which is often the correct choice, but many systems have multiple network interfaces so it is a good idea to determine which one you want Snort to monitor by running the command `snort -W` to see the available interfaces.

1. Open a command shell by locating Command Prompt in the Accessories of the Windows start menu.
2. Right-click on Command Prompt and select “Run as administrator”
3. Navigate to the directory where Snort is installed: `c:\Windows\system32> cd \Snort\bin`
4. Start Snort: `c:\Snort\bin> snort -i 2 -c c:\Snort\etc\snort.conf -A console`
5. Open *another* Command Prompt window, leaving Snort running in the first (you do not need to run the second one as administrator).
6. Send a ping command to your local gateway (or any other host): `c:\> ping 192.168.1.1`
7. Open a web browser and browse to any web page.
8. You should see the alerts Snort produces in the first terminal shell where Snort is running.

Ordinarily, you won’t need to do anything special to generate UDP alerts, because the operating system already generates plenty of UDP activity (such as ARP requests and responses or SSDP traffic) when it is connected to a network. If you are running standalone and don’t see any UDP alerts, you can open a browser and enter a URL in the address bar; DNS lookups typically use UDP by default.