

GETTING AND INSTALLING TOOLS

One advantage to installing Snort on Windows is that the process requires only three primary components: the WinPcap packet capture utility, the Snort installer, and a set of Snort rules. If syslog output is the goal then installing a separate syslog server is a fourth requirement. These requirements are summarized in the table below, followed by retrieval and installation instructions for each component.

Snort requirements (you need these to be able to install Snort on Windows)
Installation packages: <ul style="list-style-type: none">■ Snort: Snort_2_9_12_Installer.exe■ WinPcap: WinPcap_4_1_3.exe■ Snort rules: snortrules-snapshot-29120.tar.gz■ (Optional) Syslog server: SyslogServer-1.2.3-win32.exe

Anytime you are going to be downloading multiple installer files or packages, it's a good idea to settle on a standard place to put them. These instructions assume files will be downloaded directly from the relevant web sites where they are available. Many web browsers use the Downloads folder associated with each Windows user, which is an acceptable approach, although if your system has lots of things in the Downloads folder you might consider setting up a separate sub-folder for the packages associated with Snort.

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_12_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-29120.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 the rules is free and requires no user registration, but if you choose to use the community rules there are changes you must make to the snort.conf configuration file because the rules referenced in the configuration reflects the structure of the registered or subscriber rulesets.

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).

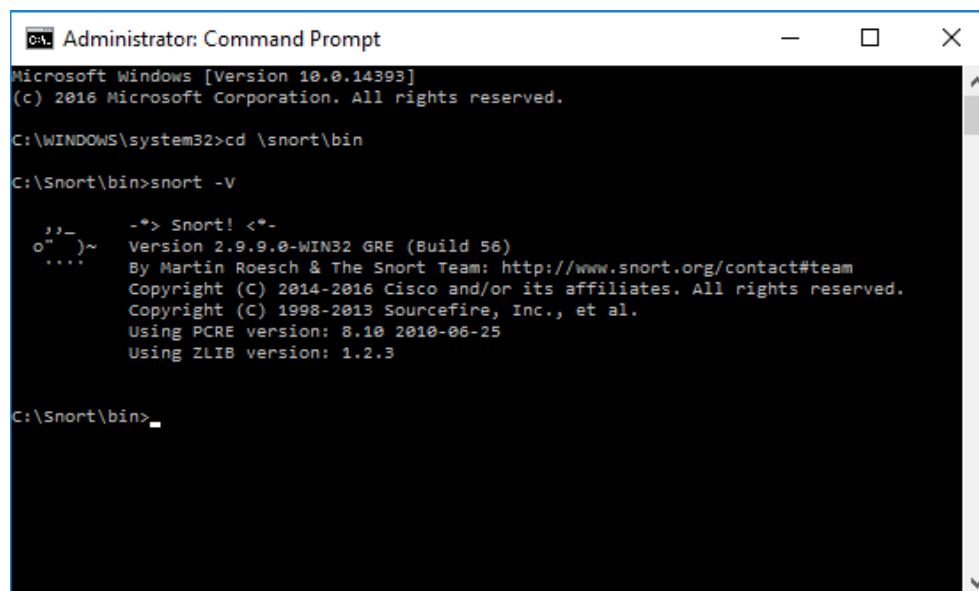
Now install the programs (in the case of WinPcap and Snort) and extract the rules files (in the case of the Snort rules package). It is recommended that WinPcap is installed before Snort, but it is not required; at the end of the Snort installation process the program will prompt that you need to install 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_12_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 2.9.9.0):



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Snort\bin>snort -v

  _ _ _ _ _
o"~)~
....

-*> Snort! <*-
Version 2.9.9.0-WIN32 GRE (Build 56)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2016 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).



Copyright © 2021 SecurityArchitecture.com – All Rights Reserved