

## **Руководство по установке и использованию Snort на Windows XP**

Перевод и форматирование: Николай Головки

Настоящее руководство предназначено для быстрой установки и запуска Snort на компьютере под управлением Windows XP. Конфигурирование правил, расшифровка информационных сообщений, подстройка под конкретную сеть в этой статье описаны не будут.

Начав с чистого отформатированного жесткого диска, я успешно установил и настроил Snort с помощью изложенных ниже инструкций как на стационарном компьютере, так и на ноутбуке, в том числе для беспроводного соединения и для виртуальной ОС, работающей из-под VMWare. Возможно, есть более легкие или более подходящие методы, чем инструкции в этой статье, но по крайней мере я изложил то, что оказалось полезным в моем случае. Используйте эти инструкции на свой страх и риск.

**Ссылки на программное обеспечение; действительны на момент написания статьи (29 июня 2008)**

1) Microsoft Windows XP Professional с пакетом обновлений SP2

<http://www.microsoft.com/windowsxp/pro/howtobuy/default.mspx>

2) Mozilla Firefox

<http://www.mozilla.com/en-US/firefox/>

3) AVG Anti-Virus Free Edition

<http://free.grisoft.com/ww.download?prd=afe>

4) ZoneAlarm Free Firewall

[http://www.zonealarm.com/store/content/catalog/products/sku\\_list\\_zs.jsp](http://www.zonealarm.com/store/content/catalog/products/sku_list_zs.jsp)

5) Microsoft Baseline Security Analyzer

<http://www.microsoft.com/downloads/details.aspx?FamilyId=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en>

6) ActivePerl

<http://www.activestate.com/store/productdetail.aspx?prdGuid=81fbce82-6bd5-49bc-a915-08d58c2648ca>

7) Notepad++

[http://sourceforge.net/project/showfiles.php?group\\_id=95717&package\\_id=102072](http://sourceforge.net/project/showfiles.php?group_id=95717&package_id=102072)

8) Foxit Reader

[http://www.foxitsoftware.com/pdf/reader\\_2/down\\_reader.htm](http://www.foxitsoftware.com/pdf/reader_2/down_reader.htm)

9) Kiwi Syslog Daemon

<http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/>

10) 7-Zip

<http://www.7-zip.org/>

11) WinPcap

<http://www.winpcap.org/install/default.htm>

12) Snort

<http://www.snort.org/dl/binaries/win32/>

13) Oinkmaster (с графическим интерфейсом)

<http://oinkmaster.sourceforge.net/download.shtml>

По умолчанию все программное обеспечение будет устанавливаться на диск С. Если вы назначите другой диск или другой путь, то все пути, приведенные в этом руководстве, потребуются соответствующим образом изменить.

### **Комментарии к устанавливаемому программному обеспечению**

1) Вам стоит также уделить время установке всех обновлений. Руководства по совершенствованию защиты операционной системы можно найти здесь:

<http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm>

[http://www.nsa.gov/snac/downloads\\_winxp.cfm?MenuID=scg10.3.1.1](http://www.nsa.gov/snac/downloads_winxp.cfm?MenuID=scg10.3.1.1)

Рекомендую прочитать оба руководства.

- 2) Firefox не обязателен; можно использовать Internet Explorer.
- 3) После установки обновите антивирусные базы.
- 4) При установке потребуется настроить брандмауэр.
- 5) Для загрузки MBSA необходима лицензионная операционная система. После установки и запуска инструмента исправьте все обнаруженные им проблемы.
- 6) ActivePerl требуется для запуска Oinkmaster.
- 7) Notepad ++ - бесплатный текстовый редактор, необходимый, в частности, для редактирования файла конфигурации snort.conf.
- 8) Foxit – бесплатная программа для просмотра файлов в формате PDF.
- 9) Kiwi – графический интерфейс, который мы будем использовать для отображения информационных сообщений Snort. Это программное обеспечение вы можете запускать как службу или, по моему примеру, как обычное приложение.
- 10) 7-zip требуется для распаковки дистрибутива Oinkmaster (равно как и многих других установочных пакетов).
- 11) WinPcap необходим для работы Snort.

## 12) Теперь все готово, и можно начинать настройку Snort и Kiwi.

Установите Snort в систему, не изменяя никаких параметров.

Откройте папку **c:\snort** и создайте каталог с именем «temp».

Если вы еще не зарегистрировали вашу версию Snort, это можно сделать здесь:

<https://www.snort.org/pub-bin/register.cgi>

Войдите на сайт Snort с полученными именем и паролем и скопируйте ваш идентификационный код «**Oink Code**».

Кроме того, загрузите набор правил для Snort - **VRT Certified Rules for Snort v2.8**.

Распакуйте загруженный файл (**snortrules-snapshot-2.8.tar**) с помощью 7-ZIP. Ту же операцию произведите с полученным файлом (**snortrules-snapshot-2.8\_s**) и скопируйте его содержимое в папку **c:\snort**; в случае появления запроса на перезапись уже существующих файлов ответьте «Да – для всех».

Откройте файл **c:\snort\etc\snort.conf** с помощью Notepad++ и выполните следующие операции:

- измените строку 194 на

```
var RULE_PATH c:\snort\rules
```

- измените строки 289-293 на

```
dynamicpreprocessor file c:\snort\lib\snort_dynamicpreprocessor\sfdcerpc.dll
```

```
dynamicpreprocessor file c:\snort\lib\snort_dynamicpreprocessor\sfdns.dll
```

```
dynamicpreprocessor file c:\snort\lib\snort_dynamicpreprocessor\sfftptelnet.dll
```

```
dynamicpreprocessor file c:\snort\lib\snort_dynamicpreprocessor\sف_smtр.dll
dynamicpreprocessor file c:\snort\lib\snort_dynamicpreprocessor\sف_ssh.dll
```

- измените строку 312 на

```
dynamicengine c:\snort\lib\snort_dynamicengine\sف_engine.dll
```

- измените строку 816 на

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

Сам я предпочитаю включать все наборы правил и уже затем вносить коррективы; вы можете поступить так же. Для этого перейдите к строкам 925 - 979 и удалите знак комментария #, стоящий перед каждой из них.

**Теперь сохраните файл и закройте его.** Помните, что для более тонкой подстройки программного обеспечения под вашу сетевую конфигурацию этот файл, как и многие другие файлы конфигурации, может потребовать дополнительного редактирования.

При желании вы можете скопировать файл **c:\snort\etc\snort.conf** в **c:\snort** или любое другое размещение, чтобы иметь под рукой резервную копию.

Откройте командную строку Windows и выполните следующую команду:

```
c:\snort\bin\snort -W
```

В результате выполнения команды будет отображен номер вашего адаптера.

После этого выполните другую команду:

```
c:\snort\bin\snort -v -iX
```

(замените букву X на номер адаптера, полученный при помощи предыдущей команды)

Откройте новое окно командной строки и выполните команду:

```
ping snort.org
```

Если все настроено верно, вы увидите, что в окне командной строки отображается некоторый текст. Это информационные сообщения Snort.

Завершите процесс Snort с помощью сочетания клавиш Ctrl+C и закройте окна командной строки.

Теперь запустите Kiwi, нажмите кнопку ОК, затем сочетание клавиш Ctrl+T. Если Kiwi работает нормально, программа отобразит тестовое сообщение.

С помощью Notepad ++ создайте файл со следующим содержимым:

```
c:\snort\bin\snort -iX -s -l c:\snort\log\ -c c:\snort\etc\snort.conf
```

(замените букву X на номер адаптера, полученный ранее)

Сохраните файл на Рабочий стол под именем **SnortStart.bat**.

Запустите **SnortStart.bat** и подождите (около 30 секунд), пока Snort не отобразит свой логотип.

Откройте командную строку Windows и выполните команду:

```
ping google.com
```

Теперь информационные сообщения Snort будут выводиться через графический интерфейс Kiwi.

13) С помощью 7-ZIP распакуйте файл **oinkmaster.tar**. Ту же операцию произведите с полученным файлом (**oinkmaster-2.0**), после чего скопируйте папку **oinkmaster-2.0** в каталог **c:\snort**.

Откройте командную строку Windows и выполните команду:

```
ppm install Tk
```

Когда установка будет завершена, выполните другую команду:

```
ppm install Win32::FileOp
```

После завершения операции закройте окно командной строки.

Откройте папку **c:\snort\oinkmaster-2.0\contrib** и скопируйте файл **oinkgui** на Рабочий стол; переименуйте файл в **Update Snort Rules**. Запустите файл, чтобы приступить к настройке Oinkmaster.

Измените первую строку на **C:/Snort/oinkmaster-2.0/oinkmaster.pl**

Измените вторую строку на **C:/Snort/oinkmaster-2.0/oinkmaster.conf**

Откройте с помощью Notepad ++ файл **C:/Snort/oinkmaster-2.0/oinkmaster.conf** и выполните следующую операцию:

- измените строку 52 на

```
url = http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-2.4.tar.gz
```

Вместо **<oinkcode>** вставьте код Oink Code, полученный вами ранее.

Сохраните файл и закройте Notepad ++.



Измените третью строку на `C:/Snort/rules`

Перейдите на вкладку «Optional files and directories».

Измените третью строку на `C:/Snort/temp`

Измените четвертую строку на `C:/Program Files/Notepad++/notepad++.exe`

Вернитесь на предыдущую вкладку и нажмите на кнопку «Save current settings», затем на кнопку «Update rules».

Дождитесь завершения обновления правил и нажмите кнопку «Exit», чтобы закрыть приложение.

Помните, что после каждого обновления правил Snort необходимо перезапустить, чтобы изменения вступили в силу.

Я буду благодарен за комментарии или сообщения об ошибках, возникших в процессе выполнения этой инструкции.

Kasey

snortguide@gmail.com