

OSSIM | How to install ossim-agent on **Windows** Box

Document updated: 30 Sept 2005

Created by Matteo Perazzo

I Foreword

OSSIM meaning Open Source Security Information Management and it's principal purpose is to provide a framework for the centralization, management and monitoring of security events. This guideline explains how to install OSSIM Agent + Snort on Windows box.

II Pre-requirements

Have installed OSSIM Server; it can be found at www.ossim.net

III The installation step by step

- 1) Download & Install WinPcap 3.0
<http://www.winpcap.org/install/default.htm>
- 2) Download & Install Snort 2.3.2
<http://www.snort.org/dl/binaries/win32/>
- 3) Download & Install Python
<http://www.activestate.com>
- 4) Download & Install mySQL
<http://prdownloads.sourceforge.net/mysql-python/MySQL-python.exe-1.2.0.win32-my4.0-py2.3.exe?download>
- 5) Download & Install ossim.tar.gz from the official web site:
<http://www.ossim.net/download.php>
- 6) Untar the package. Important note: into /agent/pyossim there are 2 files, "Agent.py" e "agent.py". Extract "Agent.py" before and rename it as "Ajent.py"; so extract "agent.py".
Now edit "Ajent.py to look for "Agent" and replace with "Ajent" wherever it occurs; also edit "agent.py" and replace "Agent" with "Ajent". (This procedure is essential because Windows is not key-sensitive)
- 7) Copy the directory "agent" into the root directory of python (c:\python); now copy the directory "etc/agent/plugin" and the file "etc/agent/config.xml" into the same dir "agent" just copied.

8) Modify the "ossim-agent" file like this:

```
#!C:\Python23\python.exe

import sys
sys.path.append('C:\Python23\agent')
import pyossim.agent

if __name__ == '__main__':
    pyossim.agent.main()
    pyossim.agent.waitforever()
```

9) Modify the "setup.py" file like this:

```
#!C:\Python23\python

from distutils.core import setup

man = [ ('share/man/man8', ['C:\Python23\agent\doc\ossim-agent.8.gz']) ]
doc = [ ('share\doc\ossim-agent', ['C:\Python23\agent\doc\config.dtd',
'C:\Python23\agent\doc\config.xml', 'C:\Python23\agent\INSTALL',
'C:\Python23\agent\COPYING', 'C:\Python23\agent\AUTHORS' ] ) ]
data = man + doc

from pyossim.__init__ import VERSION

setup (
    name            = "ossim-agent",
    version         = VERSION,
    description     = "OSSIM agent",
    author          = "OSSIM Development Team",
    author_email    = "ossim@ossim.net",
    url             = "http://www.ossim.net",
    packages        = [ 'C:\Python23\agent\pyossim' ],
    scripts         = [ 'C:\Python23\agent\ossim-agent' ],
    data_files      = data
)
```

- 10) Install the ossim-agent: rom cmd.exe, execute the command:C:\Python23\python.exe C:\Python23\agent\setup.py install
- 11) Connect snort to ossim-server: open snort.conf & uncomment the line:
 output database: alert, mysql, user=ossim password=ossim dbname=snort
 host=192.168.100.232 sensor_name=192.168.100.81 logfile=fast.log
- 12) From cmd.exe, execute the command:
 snort /SERVICE /INSTALL -c c:\snort\etc\snort.conf -l c:\snort\log -i1
- 13) Modify the file "config.xml": change the IP of OSSIM SERVER, the log dir (ie: c:\agentLog) and comment all the plug-in except snort (note: change all the path of interest)
- 14) Create the directory "c:\agentLog" for the agent logs
- 15) Modify the snort plug-in like this:

```
<?xml version="1.0" encoding='UTF-8' ?>

<!--
  snort & spade detector
  location must point to a fast format log
  enable snort logging adding logfile attribute to output database
  configuration of the snort.conf file:
  output database: alert, mysql, ... *** logfile=alert ***
-->
<plugin id="1001" process="snort" type="detector" start="yes"
enable="yes">
  <startup>c:\snort\bin\snort -l c:\snort\log -c
c:\snort\etc\snort.conf</startup>
  <shutdown>/etc/init.d/snort stop</shutdown>
  <source>fast</source>
  <interface>&interface;</interface>
  <sensor>&sensor;</sensor>
  <location>C:\Snort\log\fast.log</location>
</plugin>
```

16) Connect to ossim-server: try to run this command (without -f option you must kill the "python" task and remove the ossim-agent.pid file from C:\ everytime you want restart the agent)

```
C:\Python23\python.exe C:\Python23\agent\ossim-agent -f -c C:\Python23\agent\config.xml
```

17) Download & untar this file, you should have 2 file, "instsrv.exe" & "srvany.exe"

<http://rapidshare.de/files/4633578/service.rar.html>

18) Copy the files "instsrv.exe" and "srvany.exe" into "c:\windows\system32"

19) From cmd.exe:

```
C:\Windows\System32\INSTSRV.EXE ossim-agent "C:\Windows\System32\SRVANY.EXE"
```

20) Check the registry (regedit) to verify that the ossim-agent value under:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ossim-agent
```

is set to point to SRVANY.EXE

21) From the Edit menu, click Add Key. Type the following and click OK:

Key Name: Parameters

22) Select the Parameters key. From the Edit menu, click Add Value. Type the following and click OK:

Value Name: Application

Data Type : REG_SZ

```
C:\Python23\python.exe C:\Python23\agent\ossim-agent -f -c C:\Python23\agent\config.xml
```

Now, open your Services control panel (located in the Administrative Tools folder) and look for your newly created "ossim-agent" service.

23) Right-click on the service and select 'Start'. Now the ossim-agent should run as a service under Windows.

24) Verify in the "sensor" menu of the ossim web interface that the IP address of the newly created sensor show up. Click on "modify" and enter the agent information.

THAT'S ALL 😊

Quest'opera è stata rilasciata sotto la licenza Creative Commons Attribution-ShareAlike 2.0 Italy. Per leggere una copia della licenza visita il sito web

<http://creativecommons.org/licenses/publicdomain/>

o spedisce una lettera a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.