



# Windows Installation Guide for Suricata IDS/IPS/NSM

This is a Suircata Windows Installation Guide -

Compilation from scratch.

Tested on Windows 7, Windows 8, Windows Server 2008R2, Server 2012 64 bit.

Date: 9 Feb 2016

Document Version: 1.4.3

Author: Peter Manev(pevma)









INSTALLATION
CYGWIN - OVERVIEW OF INSTALLATION4
CYGWIN - DOWNLOAD AND INSTALL6
INSTALL SURICATA SPECIFIC DEPENDENCIES15
SYSTEM VARIABLES - ADD PATHS21
GET LIBPCAP - FOR WINDOWS24
START CYGWIN24
JSON log output - eve.json25
COMPILE SURICATA26
Suricata from git - latest version26
Suricata Stable, Beta or RC compilation29
SET UP SURICATA FOR WINDOWS
Set up and copy needed config and dll files32
Download rules
Adjust suricata.yaml configuration33
CHECK ENABLED FEATURES FOR SURICATA
RUN SURICATA
Run Suricata on an un-ip'd interfaces









**3** | Page





This is a guide of how to compile and come up with your own executable/binary of Suricata IDS/IPS on Windows. If you do not want to do that – there is a auto installation (MSI) windows native package here:

#### http://suricata-ids.org/download/

just run it and it will install and set up Suricata for you on your Windows system.

### Installation

### **Cygwin - overview of installation**

**NOTE:** Download - <u>setup-x86.exe</u> (32-bit installation). A compilation under 64 bit Cygwin installation will not work since <u>WinPcap</u> has only 32 bit downloads available and the compilation will fail.

After the installation is done you would need to add the packages below to your Cygwin installation - needed for Suricata to run:

*libmpfr4, libmpfr-devel, mpfr, mingw-pthreads, gcc-core ,make, automake, automake1.9, zlib, zlib-devel, zlib0, autoconf, autoconf2.5, libtool , libglib2.0-devel, libglib2.0\_0 ,pkg-config, libyaml-devel, libyaml0\_2, libpcre1, libpcre-devel, file-devel, gcc-g++, wget* 

Extra and useful libraries/packages for enabling extra features during compile/make time or for compiling from git (latest devel version of Suricata):

*luajit, luaji-devel, libGeoIP-devel, libGeoIP1, libnss-devel, libnss3, libnspr-devel, libnspr4, git* 









The above packages will allow us to enable during compile and build time the following extra features of Suricata –

- Lua (lua scripting)
- ➢ GeolP
- > MD5
- > possibility to git clone the latest code if needed









### Cygwin - download and install

The following installations instructions were executed on Windows Server 2012R2 64 bit.

About 500 -600MB of space needed in total with all the necessary prerequisites installed.

Download <u>http://cygwin.com/setup-x86.exe</u> then double click the setup.exe to install

Go ahead and install it with the default options (basically just click next and ok)

E	Cygwin Setup	-	
	Cygwin Net Release Setup	Program	
	This setup program is used for the initial ins Cygwin environment as well as all subsequ sure to remember where you saved it.	stallation of the lent updates. M	ake
	The pages that follow will guide you throug Please note that Cygwin consists of a large packages spanning a wide variety of purpor install a base set of packages by default. this program at any time in the future to add upgrade packages as necessary.	h the installation e number of oses. We only You can always d, remove, or	ı. run
E Cygwin	Setup - Choose Installation Typ	be 🗕	D X
Choose whether to install or of a local directory.  Install from (download)	lownload from the internet, or install from files n Internet ded files will be kept for future re-use)	s in	
	i without installing		
◯ Install from	n Local Directory		





Select F Selec install	the directory where you ation parameters.	want to install Cy	gwin. Also choose a f	ew	E	
Root Dire	ectory					
C:\cyg	vin				Browse	
Install Fo	r					
<ul> <li>ALLI</li> </ul>	sers (RECOMMENDED)					
Cyg	vin will be available to all u	users of the syste	m.			
⊖ Just	Me					
Cyg	win will still be available to	all users, but Des	sktop Icons, Cygwin I	Menu Entries, and	d important	
Adm	inistrator privileges or if yo	allable to the cul u have specific n	rrent user. Only select leeds.	t this if you lack		





E	Cygwin Setup - Select Local Package Dire	ectory 🗕 🗖 🗙
Select L Selec down	Local Package Directory ct a directory where you want Setup to store the installation files it nloads. The directory will be created if it does not already exist.	E
Local Pa	ackage Directory ers\Administrator\Downloads	Browse
		<u></u>
	< Back	Next > Cancel















Select You Setup ne the appro	<ul> <li>Internet Connection eds to know how you want it to connect to the internet. priate settings below.</li> </ul>	Choose
	Direct Connection	
	Use Internet Explorer Proxy Settings     Ise HTTP/FTP Proxy:	
	Proxy Host	
	Port 80	

Here , select any mirror you want:









Choose a s	ite from this list, or add your own sites to the list		E
	Available Download Sites:		
	http://mirrors.163.com http://cygwin.mirrors.hoobly.com ftp://cygwin.mirrors.pair.com http://cygwin.mirrors.pair.com http://cygwin.parentingamerica.com http://cygwin.skazkaforyou.com http://mirrors.ymnds.com http://mirrors.ymnds.com ftp://mirrors.xmission.com ftp://mirrors.xmission.com ftp://lug.mtu.edu http://lug.mtu.edu ftp://mirror.cs.vt.edu ttp://mirror.cs.vt.edu		
User URL:		Add	ł

### Click next to continue:

Cygwin S	etup - Select Packages	_ 🗆 X	
Select Packages Select packages to install		E	
Search	◯ Keep	View Category	
Category New	Bin? Src? Size	Package ^	
🗆 All 🕂 Default		≡	
⊡ Admin ♦ Default			
🗄 Archive 🚯 Default			
🗄 Audio 🚯 Default			
🗄 Base 📀 Default			
🕀 Database 🚯 Default			
🕀 Debug 😯 Default			
🕀 Devel 📭 Default		✓	
		>	<b>R</b> K
✓ Hide obsolete packages			
	< Back Nex	t > Cancel	





Next again to proceed with installation of the base packages:

The fo	Ilowing packages are required to satisfy dependencies.		
bzip2	(1.0.6-2) A high-quality block-sorting file compressor (utilities) Required by: tar		^
ca-certif	icates (2.6-1) CA root certificates Required by: libopenssl100		
groff	(1.22.3-1) GNU roff formatter Required by: man-db		~
<	Ш	>	
Select r	required packages (RECOMMENDED)		





Then you are going to see a progress bar:

E	21% - Cygwin Setup 📃 🗖 🗙	
Progress This	s page displays the progress of the download or installation.	
	Downloading	
	cygwin-2.4.0-1.tar.xz from http://cygwin.mirror.constant.com//x Connecting	
	Package:	
	Total:	
	Disk:	
C		
DF		<b>KICAIA</b>
1		
	< Back Next > Cancel	















## Install Suricata specific dependencies

After the installation is finished – we need to install the Suricata specific build dependencies (as described just before this section)

Go back and double-click the very same **setup-x86.exe** – we will need to install the extra packages necessary for Suricata to run.

Click next and ok until you are presented with the following screen:

Search		lear			🔘 Keep 🌘	Prev	Curr	© Exp	View	Category
Category	Current	New	B	S Size	Package					
🗆 Al 🚯 D	efault									
E Acce	ssibility 🚯 Default	t								
🗄 Admir	n 🚯 Default									
🗄 Archin	ve 😯 Default									=
🕀 Audio	Default									
⊞ Base	Default									
🗄 Datab	oase 😯 Default									
⊞ Deve	Default									
E Doc 4	🕑 Default									
Editor	s 🚯 Default									
E Game	s 🚯 Default									
E Gnom	ie 😯 Default									
🗄 Graph	nics 🚯 Default									
⊞ Interp	reters 😯 Default									
	Default									
🗄 Libs 4	Default									
FI Mail A	Pafault									
•										r







Here is where we search select and queue for installation the additional packages needed.

In the picture below , in the search box type in the name of the package- the search will return automatically , results , select the necessary package. Erase the contentment of the search box and type in the name of the next package, select ... and so on.

Do the same for all the needed packages, DO NOT hit next until you have selected all the packages.

E	Cygwin Setup - Select Pa	ckages – 🗆 🗙
Select Packages Select packages to install		E
Search autoconf Clear		◯ Keep
Category Current New	B S Size	Package ^
🗆 All 😌 Default		
🗆 Devel 😯 Default		
O 13-1	🛛 🗆 4k	autoconf: Wrapper scripts for autoconf commands
😯 Skip	n/a n/a 200k	autoconf2.1: Stable version of the automatic configure scrip
0 2.69-2	🛛 🗆 990k	autoconf2.5: An extensible package of m4 macros that proc
Skip	n/a n/a 425k	gcc-tools-epoch1-autoconf: (gcc-special) automatic configu
😯 Skip	n/a n/a 712k	gcc-tools-epoch2-autoconf: (gcc-special) automatic configu
L£J Pert <b>€9</b> Default		~
<		>
✓ Hide obsolete packages		
		< Back Next > Cancel

The necessary packages are:









*libmpfr4, libmpfr-devel, mpfr, mingw-pthreads, gcc-core ,make, automake, automake1.9, zlib, zlib-devel, zlib0, autoconf, autoconf2.5, libtool , libglib2.0-devel, libglib2.0\_0 ,pkg-config, libyaml-devel, libyaml0\_2, libpcre1, libpcre-devel, file-devel, gcc-g++, wget* 

And if you would like to enable extra functionality -

*luajit, luaji-devel, libGeoIP-devel, libGeoIP1, libnss-devel, libnss3, libnspr-devel, libnspr4, git* 

E	Cygwin S	Setup - Select Pack	ages	- 🗆 🗙
Select Packages Select packages to install				E
Search dos2u	ear		◯ Keep	Category
Category Current	New	B S Size	Package	^
□ All  Default □ Debug  Default				
	Skip	n/a n/a 50	lk dos2unix-debuginfo: Debug info for dos2un	ix
El Text 🏘 Default	<b>€</b> 6.0.4-1	⊠ □ 67	k _dos2unix: Converts text files between DOS	and *NIX li
		_		
<				>
✓ Hide obsolete packages				
			< Back Next >	Cancel

After you are done selecting the packages – make sure the "search" box is cleared, click the "view" button until the text on the right of the button displays "pending".

Check and make sure all the needed packages are selected! If something is missing, go back and select it!









Click Next:

E						Cygwin Setup - Select Packages	-	o x
Select Packages Select packages to install								E
Search	Clear						◯ Keep	ending
Current	New	Bin?	Src?	Categories	Size	Package		^
	0 13-1			Devel	4k	autoconf: Wrapper scripts for autoconf commands		
	2.69-3			Devel	704k	autoconf2.5: Current version of the automatic configure script builder		
	<b>€</b> 9-1	$\boxtimes$		Devel	3k	automake: Wrapper scripts for automake and aclocal		
	1.9.6-11			Devel	557k	automake 1.9: (1.9) a tool for generating GNU-compliant Makefiles		
	5.25-1			Devel	10k	file-devel: Libraries and header files for file development		
	4.9.3-1			Devel	14,350k	gcc-core: GNU Compiler Collection (C, OpenMP)		
	• 4.9.3-1         •         1         • 1			Devel	7,535k	gcc.g++: GNU Compiler Collection (C++)		
	2.7.0-1			Devel	4,716k	git: Distributed version control system		
	49 1.6.0-1		<u> </u>	Net	9k	libGeoIP-devel: GeoIP C library		
	49 1.6.0-1		<u> </u>	Net	/0k	IbGeoIP1: GeoIP C Ibrary		
	49 2.46.2-2		<u> </u>	Libs	415k	libglib2.0-devel: GNUME core C function library (development)		
	492.46.2-2			Libs	2,/34k	libglib2.0_0: GNOME core C function library (runtime)		
	493.1.3-1		Ц	Libs, Math	196	libmptr-devel: A library for multiple-precision floating-point antimetic with exact rounding (development)		
3.1.3*1	4 3.1.2-2 Cr 4 10 10 1		Η.	Libs, Math	139K	Itomptr4: A library for multiple-precision hoating-point altinitetic with exact rounding (untime)		
			Η.	Libe	1006	Interproever, vetocape Fonable Puntime Ibrary		
	4.10.10-1		Η.	LIDS	10/K	Ilonspr4: Netscape Pontable Runnine Ilonary		
	€ 3.20.1*1		H	Libe	016K	Ibnas 2 Natesana Network Security Services		
	0.8 37.2		H	Libe	3636	librasulaval. Pad Compatible Basyler Evoces library development		
0 27.2	€ 0.372 ⊕ 9.27.1		H	Liba	107k	libpore 1: Ded Compatible Degular Expressions IUTE 9 autime		
0.07 2	A246-2		H	Devel	705k	libbol: Generic library support sont		
	0162		H	Liba	126	libvami devel: YAMI 11 paren library		
	AP016-2		Ē	Libs	42k	litvani0 2 YAMI 11 namer litrary		
	£2.0.4-1		H H	Interpreters	234k	luait: Lua Just-in-Time compiler		
	4 2.0.4-1		Ē	Interpreters	11k	luait-devel: Lua Just-in-Time compiler		
	€4.1-1			Devel	412k	make: The GNU version of the 'make' utility		
	20110507-2		П	Devel	221k	mingw-pthreads: Ubpthread for MinGW.org Win32 toolchain		
	03.1.3-1			Libs, Math	2k	mpfr: A library for multiple-precision floating-point arithmetic with exact rounding		
	0.29-1		Ē	Devel	55k	pkg-config: Package compiling configuration utility		
	O 1.17.1-1			Web	729k	wget: Utility to retrieve files from the WWW via HTTP and FTP		
	1.2.8-2			Libs	35k	zlib: Gzip de/compression library (documentation)		
	1.2.8-3			Libs	114k	zlb-devel: Gzip de/compression library (development)		
1.2.8-3	1.2.8-2			Libs	40k	zlb0: Gzip de/compression library (runtime)		
								~
<						III		>
✓ Hide obsol	lete packages							
							< Back Next >	Cancel

After that click next (make sure the option "select required packages (RECOMMENDED)" is selected!) :









Cygwin Setup - Resolving Dependencies	- 🗆 🗙
<b>Resolving Dependencies</b> The following packages are required to satisfy dependencies.	E
autoconf2.1 (2.13-12) Stable version of the automatic configure script builder Required by: autoconf, automake1.4, automake1.5	^
automake1.10 (1.10.3-2) (1.10) a tool for generating GNU-compliant Makefiles Required by: automake	
automake1.11 (1.11.6-2) (1.11) a tool for generating GNU-compliant Makefiles Required by: automake, libtool	~
<	>
< Back Next >	Cancel

The extra packages that you have selected will start to download and install:









E	0% - Cygwin Setup	- 🗆 🗙
Progress This page displays	the progress of the download or installation.	E
Downloadi autoconf2. Connecting Package: Total: Disk:	ng 1-2.13-12.tar.bz2 from http://mirrors.163.com/cygwi j	
	< Back Next >	Cancel

This could also take 5 min or so. Then click finish:









cygnin octup 1			
Create Icons	uwant it to create a few icons t	for convenient access to the	<b>F</b>
Cygwin enviror	ment.	for convenient access to the	
	Crosta ison on	Dealsten	
	Create Icon on	Desktop	
	Add icon to <u>S</u> t	art Menu	
Installation Stat	18		
Installation Cor	nplete		
		C Back Finie	h Cancel

## System variables - add paths

Add path to system variables (Win 7, Win 8, 2008, 2012 Server - Control Panel\System and Security\System\Advanced system settings\Environment Variables) :

C:\cygwin\bin;C:\cygwin\lib\pkgconfig;

Add the above to environment system variables in your windows system!! See the picture below









System Properties				_	x			
Computer Name	Hardware	Advanced	System Protection	Remote				
You must be logged on as an Administrator to make most of these changes.								
Performance	Performance							
Visual effects	, processor s	cheduling, m	emory usage, and vir	tual memor	y			
				Settings				
- User Profiles -								
Desktop settir	ngs related to	o your logon						
	Settings							
Startup and R	ecovery				- II			
System startu	p, system fai	ure, and deb	ugging information					
				Settings				
Environment Variables								
OK Cancel Apply								

Edit the system path variable:









vironment Variables					
User variables for Do	nPedro				
Variable	Value				
PATH	C:\Program Files (x86)\Nmap;C:\win32\ =				
PKG_CONFIG_P	/win32/lib/pkgconfig				
TEMP	%USERPROFILE%\AppData\Local\Temp				
TMP	%USERPROFILE%\AppData\Local\Temp				
New Edit Delete					
Variable	Value				
OS	Windows_NT				
Path	C:\Program Files (x86)\NVIDIA Corpora				
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;				
PROCESSOR_A	AMD64 T				
	New Edit Delete				

Add " C:\cygwin\bin;C:\cygwin\lib\pkgconfig; " without the quotes to the end of the " Variable value path " :

Edit System Variable						
Variable name: Variable value:	Path Ients\IPT;C:\cygwin64\bin;C:\cygwin64\ib\r OK Cancel					









### **Get libpcap - for windows**

Go to <u>http://www.winpcap.org/install/default.htm</u> and download the WinPcap installer for windows (at the time of this writing the current version was 4.1.3 )

Install the WinPcap (double click, and just use the default options, basically click next and ok until finished.)

This is IMPORTANT , this is the development pack, we need that for Suricata to be able to run on Windows.

After that is done go to <u>http://www.winpcap.org/devel.htm</u>. Download the package and unpack it anywhere you like.

Copy libraries (from the unpacked directory) like this:

- ✓ Copy ALL the content of WpdPack\Lib\ to cygwin\lib\
- ✓ Rename "libwpcap" to "libpcap" (in your cygwin\lib\ directory)
- Copy all headers (all the content)from WpdPack\Include\ to C:\cygwin\usr\include\

## **Start Cygwin**

Open CYGWIN. Double click your CYGWIN icon on your desktop. A Linux/bash like command prompt will open:











## JSON log output - eve.json

When compiling Suricata if - libjansson4/dev package is available on the system Suricata will autodetect that and enable it giving JSON log output availability (one can check with **suricata.exe --build-info**)

Since there is no libjansson4 and libjansson-dev package readily available for Cygwin under Windows - it can be manually compiled form source like so:

wget <u>http://www.digip.org/jansson/releases/jansson-2.7.tar.gz</u>

tar xvf jansson-2.7.tar.gz && cd jansson-2.7









./configure --prefix=/usr && make clean && make && make install

That will enable JSON and eve.json availability for log output with Suricata on Windows.

## **Compile Suricata**

### Suricata from git - latest version

(next section describes compilation for stable, beta, RC)

Get and compile Suricata.

As you are still in the CYGWIN environment -

Type in

git clone git://phalanx.openinfosecfoundation.org/oisf.git

Then after it is done

cd oisf

Then we need libhtp:

git clone git://github.com/ironbee/libhtp.git -b 0.5.x









E		/tmp/oisf			_ 🗆 X		
These files are for	the users to personal	ise their cygwin expe	rience.		<u>^</u>		
They will never be o	verwritten nor automa	tically updated.					
'./.bashrc' -> '/home/Administrator//.bashrc' './.bash_profile' -> '/home/Administrator//.bash_profile' './.inputrc' -> '/home/Administrator//.inputrc' './.profile' -> '/home/Administrator//.profile'							
Administrator@WIN-5B	0EU82E444 ~						
₃ cd// bin/ cygdrive/ Cygwin.bat	Cygwin.ico Cygwin-Terminal.ico dev/	etc/ home/ lib/	proc/ sbin/ tmp/	usr/ var/			
Administrator@WIN-5B \$ cd//tmp/	0EU82E444 ~						
Administrator@WIN-58 \$ git clone git://ph Cloning into 'oisf'. remote: Counting obj remote: Compressing remote: Total 42199 Receiving objects: 1 Resolving deltas: 10 Checking connectivit	0EU82E444 /tmp alanx.openinfosecfound ects: 42199, done. objects: 100% (11985/ (delta 34540), reused 00% (42199/42199), 11 0% (34540/34540), don y done.	dation.org/oisf.git 11985), done. 36620 (delta 30167) .52 MiB   316.00 KiB/ e.	s, done.		≡		
Administrator@WIN-5B <b>\$ cd oisf/</b>	0EU82E444 /tmp						
Administrator@WIN-5B0EU82E444 /tmp/oisf \$ git clone git://github.com/ironbee/libhtp.git -b 0.5.x Cloning into 'libhtp' remote: Counting objects: 9963, done. remote: Total 9963 (delta 0), reused 0 (delta 0), pack-reused 9963 Receiving objects: 100% (9963/9963), 9.92 MiB   189.00 KiB/s, done. Resolving deltas: 100% (6031/6031), done. Checking connectivity done. Checking out files: 100% (1850/1850), done.							
Administrator@WIN-5B \$	OEU82E444 /tmp/oisf				~		

Then we execute the following command(type and hit enter):

./autogen.sh && ./configure --enable-luajit --enable-pie --enable-geoip --disablegccmarch-native --with-libnss-libraries=/usr/lib --with-libnssincludes=/usr/include/nss/ --with-libnspr-libraries=/usr/lib --with-libnsprincludes=/usr/include/nspr && make clean && make

That will start configuration and compilation of Suricata.

The part -

-with-libnss-libraries=/usr/lib --with-libnss-includes=/usr/include/nss/ --withlibnspr-libraries=/usr/lib -with-libnspr-includes=/usr/include/nspr









Like so:











Let it run.....this could take a few minutes or so

## After it is done your **suricata.exe** binary will be located under **src/.libs/suricata.exe**:

E /tmp/oisf – 🗆 🗙	
<pre>/tmp/oisf make[3]: Entering directory '/tmp/oisf/contrib' make[3]: Nothing to be done for 'all-am'. make[3]: Leaving directory '/tmp/oisf/contrib' make[2]: Leaving directory '/tmp/oisf/contrib' Making all in scripts make[2]: Entering directory '/tmp/oisf/scripts' Making all in suricatasc make[3]: Entering directory '/tmp/oisf/scripts/suricatasc' make[3]: Entering directory '/tmp/oisf/scripts/suricatasc' make[3]: Entering directory '/tmp/oisf/scripts/suricatasc' make[3]: Entering directory '/tmp/oisf/scripts/suricatasc' make[3]: Entering directory '/tmp/oisf/scripts/suricatasc' copying build_ creating build_ creating build_ creating build/lib/suricatasc copying src/_initpy -&gt; build/lib/suricatasc running build_scripts</pre>	
<pre>creating build/scripts-2.7 copying and adjusting suricatasc -&gt; build/scripts-2.7 changing mode of build/scripts-2.7/suricatasc from 644 to 755 make[3]: Leaving directory '/tmp/oisf/scripts/suricatasc' make[3]: Entering directory '/tmp/oisf/scripts' make[3]: Leaving directory '/tmp/oisf/scripts' make[2]: Leaving directory '/tmp/oisf/scripts' make[2]: Entering directory '/tmp/oisf/scripts' make[2]: Leaving directory '/tmp/oisf/scripts' make[2]: Leaving directory '/tmp/oisf' make[2]: Leaving directory '/tmp/oisf' make[2]: Leaving directory '/tmp/oisf' make[1]: Leaving directory '/tmp/oisf'</pre>	
Administrator@WIN-5B0EU82E444 /tmp/oisf \$ ls -lh src/.libs/ lt-suricata.c suricata.exe suricata_ltshwrapper Administrator@WIN-5B0EU82E444 /tmp/oisf \$ ls -lh src/.libs/ total 22M -rw-rr- 1 Administrator None 29K Jan 17 17:15 lt-suricata.c -rwxr-xr-x 1 Administrator None 22M Jan 17 17:15 suricata.exe -rw-rr 1 Administrator None 6.2K Jan 17 17:15 suricata.exe	
Administrator@WIN-5B0EU82E444 /tmp/oisf \$	-

## Suricata Stable, Beta or RC compilation

As you are still in the CYGWIN environment -









### This section uses Suricata 3.0RC3 as an example.

If you want to install Suricata stable you can find it here - <u>http://suricata-ids.org/download/</u>

go to a tmp dir. Type in and hit enter to complete each step:

- 1) wget http://www.openinfosecfoundation.org/download/suricata-3.0RC3.tar.gz
- 2) tar -zxf suricata-3.0RC3.tar.gz
- 3) cd suricata-3.0RC3
- 4) libtoolize -c && autoreconf -fv --install && ./configure --enable-luajit --enablepie --enable-geoip --disable-gccmarch-native --with-libnss-libraries=/usr/lib --with-libnss-includes=/usr/include/nss/ --with-libnspr-libraries=/usr/lib --withlibnspr-includes=/usr/include/nspr && make clean && make

The part -

-with-libnss-libraries=/usr/lib --with-libnss-includes=/usr/include/nss/ --withlibnspr-libraries=/usr/lib -with-libnspr-includes=/usr/include/nspr

will enable DM5s functionality for Suricata.

**NOTE:** Please not the difference in the compilation line (4 above) for stable/beta/RC and for git.

After done the *suricata.exe* binary will be located in the folder /*src/.libs/suricata.exe* 









E /tmp/suricata-3.0RC3	_		
running build_scripts creating build/scripts-2.7 copying and adjusting suricatasc -> build/scripts-2.7 changing mode of build/scripts-2.7/suricatasc from 644 to 755 make[3]: Leaving directory '/tmp/suricata-3.0RC3/scripts/suricatasc' make[3]: Entering directory '/tmp/suricata-3.0RC3/scripts' make[3]: Nothing to be done for 'all-am'. make[3]: Leaving directory '/tmp/suricata-3.0RC3/scripts' make[2]: Leaving directory '/tmp/suricata-3.0RC3/scripts' make[2]: Leaving directory '/tmp/suricata-3.0RC3/scripts' make[2]: Entering directory '/tmp/suricata-3.0RC3/scripts' make[2]: Leaving directory '/tmp/suricata-3.0RC3' make[2]: Leaving directory '/tmp/suricata-3.0RC3' make[2]: Leaving directory '/tmp/suricata-3.0RC3'		^	
Administrator@WIN-5B0EU82E444 /tmp/suricata-3.ORC3 \$			
Administrator@WIN-5BOEU82E444 /tmp/suricata-3.0RC3 \$ ls -lh src/.libs/ total 22M -rw-rr- 1 Administrator None 29K Jan 17 17:34 lt-suricata.c -rwxr-xr-x 1 Administrator None 22M Jan 17 17:34 suricata.exe -rw-rr- 1 Administrator None 6.2K Jan 17 17:34 suricata_ltshwrapper			
Administrator@WIN-5B0EU82E444 / <mark>tmp/suricata-3.ORC3</mark> \$			
		~	

Next steps.

For the instructions below if you want to use stable or RC3 (as opposed to latest git Suricata) – just substitute the **oisf** directory with the appropriate name – **suricata-3.0RC3** for example.

## Set up Suricata for Windows









### Set up and copy needed config and dll files

Create the following directories:

- C:\Program Files (x86)\Suricata\log
- C:\Program Files (x86)\Suricata\log\files
- C:\Program Files (x86)\Suricata\log\certs
- C:\Program Files (x86)\Suricata\rules

Then copy the suricata.exe file from C:\cygwin\tmp\oisf\src\.libs to C:\Program Files (x86)\Suricata

NOTE: It is not a must to place Suricata in C:\Program Files (x86)\Suricata you can place it anywhere you would like.

Copy (from C:\cygwin\bin)

- 1. cyggcc\_s-1.dll
- 2. cygGeolP-1.dll
- 3. cygluajit-5.1-2.dll
- 4. cygmagic-1.dll
- 5. cygnspr4.dll
- 6. cygnss3.dll
- 7. cygnssutil3.dll
- 8. cygpcre-1.dll
- 9. cygplc4.dll
- 10.cygplds4.dll
- 11.cygwin1.dll

12.cygz.dll









to your C:\Program Files (x86)\Suricata directory

Also copy C:\cygwin\usr\share\misc\magic.mgc to your C:\Program Files (x86)\Suricata directory

### **Download rules**

Go to <u>http://rules.emergingthreats.net/open/suricata/</u>

Download a rule set.

http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz

Unzip/untar the rule set in the C:\Suricata\rules directory.

Then go to C:\cygwin\tmp\oisf

Сору

classification.config , reference.config and suricata.yaml to

C:\Program Files (x86)\Suricata

### Adjust suricata.yaml configuration

Open suricata.yaml with an editor – Notepad, Notepad++, whichever you like and change the following lines:





**33** | Page





# The default logging directory. Any log or output file will be # placed here if its not specified with a full path name. This can be *# overridden with the -I command line parameter.* default-log-dir: C:\\Program Files (x86)<u>\\Suricata\\log\\</u> .... .... *# Magic file. The extension .mgc is added to the value here.* #magic-file: /usr/share/file/magic *magic-file: C:\Program Files (x86)\Suricata\magic.mgc* ... . . . outputs: - console: enabled: yes # type: json - file: enabled: yes filename: C:\\Program Files (x86)\\Suricata\\log\\suricata.log # type: json . . . . . .

# Set the default rule path here to search for the files.# if not set, it will look at the current working dir









default-rule-path: C:\\Program File	s (x86)\\Suricata\\rules\\
-------------------------------------	----------------------------

...

•••

classification-file: C:\Program Files (x86)\Suricata\classification.config

reference-config-file: C:\Program Files (x86)\Suricata\reference.config

•••

•••

vars:

# Holds the address group vars that would be passed in a Signature.

# These would be retrieved during the Signature address parsing stage.

address-groups:

HOME\_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]" (adjust network ranges here to the ones that you want Suricata to inspect)

EXTERNAL\_NET: "!\$HOME\_NET"

HTTP\_SERVERS: "\$HOME\_NET"

SMTP\_SERVERS: "\$HOME\_NET"

## **Check enabled features for Suricata**

### Open a cmd as ADMINISTRATOR!!!.

Got to C:\Program Files (x86)\Suricata and execute





35 | Page









**36 |** Page





Administrator: Cor	mmand Prompt 📃 🗖 🗙	
C:\Program Files (x86)\Suricata> C:\Program Files (x86)\Suricata>suricata.exebuild-info This is Suricata version 3.0dev (rev 44a444b) Features: PCAP_SET_BUFF LIBPCAP_VERSION_MAJOR=1 HAVE_PACKET_FANOUT HAVE_HTP_URI_ NORMALIZE_HOOK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT TLS SIMD support: none Atomic intrisics: 1 2 4 8 byte(s) 32-bits, Little-endian architecture GCC version 4.9.3, C version 199901 L1 cache line size (CLS)=64 thread local storage method:thread		
compiled with LibHIP v0.5.18, linked again Suricata Configuration: AF_PACKET support: PF_RING support: NFQueue support: NFLOG support: IPFW support: Netmap support:	st LibHIP v0.5.18 no no no no no no	
DAG enabled: Napatech enabled: Unix socket enabled: Detection enabled:	no no yes	
libnss support: libnspr support: libjansson support: hiredis support: Prelude support: PCRE jit: LUA support: libluajit: libgeoip: Non-bundled htp: Old barnyard2 support: CUDA enabled:	yes yes no no yes yes, through luajit yes yes no no no no	
Suricatasc install: Unit tests enabled: Debug output enabled: Debug validation enabled: Profiling enabled:	yes no no no	
Generic build parameters: Installation prefix: Configuration directory: Log directory:	no No /usr/local C:\Program Files (x86)\Suricata\ C:\Program Files (x86)\Suricata\log	
——prefix ——sysconfdir ——localstatedir	NONE /usr/local/etc /usr/local/var	
Host: Compiler: GCC Protect enabled: GCC march native enabled: GCC Profile enabled: Position Independent Executable enabled: CFLAGS PCAP_CFLAGS SECCFLAGS	i686-pc-cygwin gcc (exec name) / gcc (real) no no no yes -g -02	
C:\Program Files (x86)\Suricata>		







### Open a cmd as ADMINISTRATOR!!!.

Got to C:\Program Files (x86)\Suricata and execute

### C:\Program Files (x86)\Suricata>suricata.exe -c suricata.yaml -i 10.0.2.15 -v

like shown on the picture below (in this case – 10.0.2.15 is the IP/interface I want Suricata to listen to, i.e. the IP that my network card has been configured with):

Administrator: Command Prompt - suricata.exe -c suricata.yaml -i 10.0.2.15 -v 💶 💌
C:\Program Files (x86)\Suricata>suricata.exe -c suricata.yaml -i 10.0.2.15 -v
nslated 10.0.2.15 to pcap device \Device\NPF_{156DACD3-585B-400A-AC12-AAACFE8398
[136] 17/1/2016 20:08:34 - (suricata.c:1073) (Notice) (SCPrintUersion) Thi s is Suricata version 3.0dev (rev 44a444b)
[136] 17/1/2016 20:08:34 - (util-cpu.c:170) (Info) (UtilCpuPrintSummary) C PUs/cores online: 1
[136] 17/1/2016 20:08:34 - (app-layer-htp.c:2251) <info> (HTPConfigSetDefault sPhase2) 'default' server has 'request-body-minimal-inspect-size' set to 3388</info>
2 and 'request-body-inspect-window' set to 4053 after randomization. [136] 17/1/2016 20:08:34 - (app-layer-htp.c:2266) (HTPConfigSetDefault Description: default (application) and (application) after randomization (ATPConfigSetDefault)
19 and 'response-body-inspect-window' set to 16872 after randomization.
DNS per flow memcap (state-memcap): 524288 [136] 17/1/2016 20:08:34 - (app-layer-dns-udp.c:361) (Info) (DNSUDPConfigure)
DNS global memcap: 16777216

And you have yourself Suricata running (the start time could depend the PC/Server CPU/MEM availability and of course how many rules and what options you have enabled in suricata.yaml ):









🔤 Administrator: Command Prompt - suricata.exe -c suricata.yaml -i 10.0.2.15 -v 💶 🗖	
[136] 17/1/2016 20:08:34 - (stream-top.c:475) (Info) (StreamTcpInitConfig stream.reassembly "memcap": 134217728	a, v
[136] 17/1/2016 - 20:08:34 - (stream-top.c:493) (Info) (StreamTopInitConfig stream.reassembly "depth": 1048576	a>
[136] 17/1/2016 - 20:08:34 - (stream-top.c:576) (Info) (StreamTopInitConfig stream.reassembly "toserver-chunk-size": 2537	g>
[136] 17/1/2016 - 20:08:34 - (stream-tcp.c:578) (Info) (StreamTcpInitConfig stream.reassembly "toclient-chunk-size": 2600	<mark>g&gt;</mark>
[136] 17/1/2016 - 20:08:34 - (stream-tcp.c:591) (Info) (StreamTcpInitConfig stream.reassembly.raw: enabled	<mark>a&gt;</mark>
[136] 17/1/2016 - 20:08:34 - (stream-tcp-reassemble.c:451) (Info) (StreamTo	cpRea
[136] 17/1/2016 20:08:34 - (stream-tcp-reassemble.c:451) (Info) (StreamTo ssemblyConfig) segment nool: nktsize 16, nrealloc 512	cpRea
[136] 17/1/2016 20:08:34 - (stream-tcp-peasemble.c:451) (Info) (StreamTe seemble.config) segment nool: nktsize 112, nrealloc 512	cpRea
[136] 17/1/2016 20:08:34 - (stream-tcp-reassemble.c:451) (Info) (StreamTe ssemble.config) segment nool: nktsize 248 nrealloc 512	cpRea
[136] $17/1/2016 - 20:08:34 - (stream-tcp-reassemble.c:451) (Info) (StreamTcp-reassemble.c)$	cpRea
<b>[136]</b> $17/1/2016 - 20:08:34 - (stream-top-reassemble.c:451) (Info) (StreamTop-reassemble.c:451) (Info) $	cpRea
[136] $17/1/2016 - 20:08:34 - (stream-top-reassemble.c:451) (Info) (StreamTop-reassemble.c:451) (Info) (StreamTop-reassemble.c:451) (Info)$	cpRea
[136] 17/1/2016 20:08:34 - (stream-top-reassemble.c:451) (Info) (StreamTop-reassemble.c:451) (Info)	cpRea
[136] 17/1/2016 20:08:34 - (stream-top-reassemble.c:487) (Info) (StreamTop-reassemble.c:487) (Info)	cpRea
[136] 17/1/2016 20:08:34 - (stream-top-reasemble.c:500) (Info) (Stream)	cpRea
$[136] 17/1/2016 - 20:08:34 - (ippair.c:21) \langle Info \rangle \langle IPPairInitConfig \rangle - a$	lloca
[136] 17/1/2016 20:08:34 - (ippair.c:234) (Info) (IPPairInitConfig) pr	reall
Clated 1000 ippairs of size $72$ [136] $17/1/2016 - 20:08:34 - \langle ippair.c: 236 \rangle \langle Info \rangle \langle IPPairInitConfig \rangle - ij$	ppair
<pre>memory usage: 334144 bytes, maximum: 16777216 [136] 17/1/2016 20:08:34 - <util=magic.c:62> <info> <magicinit> using </magicinit></info></util=magic.c:62></pre>	magi
C-file C:\Program Files (X86)\Suricata\magic.mgc [136] 17/1/2016 20:08:34 - (suricata.c:1950) {Info> (SetupDelayedDetect)	D
elayed detect disabled [ <mark>136] 17/1/2016 20:08:34 - (reputation.c:620) (Info</mark> ) (SRepInit) IP rep	putat
ion_disabled [ <mark>136]</mark> 17/1/2016 20:08:34 - (detect.c:416) (Info) (ProcessSigFiles) Lo	ading
rule file: C:\Program Files (x86)\Suricata\rules\botcc.rules [136] 17/1/2016 20:08:34 - (detect.c:416) (Info) (ProcessSigFiles) Lo:	ading
rule file: C:\Program Files (x86)\Suricata\rules\ciarmy.rules [136] 17/1/2016 20:08:34 - (detect.c:416) {Info> (ProcessSigFiles) Lo:	ading
rule file: C:\Program Files (x86)\Suricata\rules\compromised.rules [136] 17/1/2016 20:08:34 - (detect.c:416) {Info> (ProcessSigFiles) Loa	ading
rule file: C:\Program Files (x86)\Suricata\rules\drop.rules [136] 17/1/2016 20:08:34 - (detect.c:416) <info> (ProcessSigFiles) Lo:</info>	ading
rule file: C:\Program Files (x86)\Suricata\rules\dshield.rules [136] 17/1/2016 20:08:34 - (detect.c:416) {Info> (ProcessSigFiles) Log	ading
rule file: C:\Program Files (x86)\Suricata\rules\emerging-activex.rules [136] 17/1/2016 20:08:35 - (detect.c:416) {Info> (ProcessSigFiles) Loa	ading
rule file: C:\Program Files (x86)\Suricata\rules\emerging-attack_response.;	rules
[136] 17/1/2016 20:08:35 - (detect.c:416) (Info) (ProcessSigFiles) Lo. rule file: C:\Program Files (x86)\Suricata\rules\emerging-chat.rules	ading
[136] 17/1/2016 20:08:35 - (detect.c:416) (Info) (ProcessSigFiles) Lov rule file: C:\Program Files (x86)\Suricata\rules\emerging-current_events.ru	ading ules
[136] 17/1/2016 20:08:35 - (detect.c:416) (Info) (ProcessSigFiles) Lo. rule file: C:\Program Files (x86)\Suricata\rules\emerging-dns.rules	ading
[136] 17/1/2016 - 20:08:35 - (detect.c:416) (Info) (ProcessSigFiles) Log rule file: C:\Program Files (x86)\Suricata\rules\emerging-dos.rules	ading
[136] 17/1/2016 20:08:35 - (detect.c:416) (Info) (ProcessSigFiles) Los rule file: C:\Program Files (x86)\Suricata\rules\emerging-exploit rules	ading
[136] 17/1/2016 20:08:35 - (detect.c:416) (Info) (ProcessSigFiles) Lo	ading 🗠

Run Suricata on an un-ip'd interfaces









If you need to run Suricata on an un-ip'd interfaces(thanks to Rich Rumble for pointing that out):

You can get the NIC UUID in a variety of ways, the simplest is using a single command for WMIC:(from cmd prompt paste in the following)

wmic nicconfig get ipaddress,SettingID

If you know your NIC's IP you can filter the results with findstr:

wmic nicconfig get ipaddress,SettingID | findstr 1.2.3.4

(replace 1.2.3.4 with your NIC's IP)

Then use that as your interface argument:

suricata.exe -c suricata.yaml -i \\DEVICE\\NPF\_\{EE7B2A76-9343-449F-B3D8-3CB0F37DCA49\}

Make sure the double slashes are used, and a backslash is placed before the curly braces!

That's it.

From here on it is up to you to configure Suricata the way it suits you best!

Thanks for trying Suricata!

### Info and documentation

You can find much more info about setting up and tuning Suricata here:





40 | Page





**41 |** Page

