# Suricata IDS/IPS

# Help and Quick Start Guide

# Instructions for Windows

**tested on Windows 10, Windows Server 2012R2/2016 64 bit.**

***Date: 27 August 2018***

***Author: Peter Manev (pevma)***

## Before you start Suricata IDS/IPS

**You MUST have npcap(npcap win installer) installed in order to run Suricata IDS/IPS !**

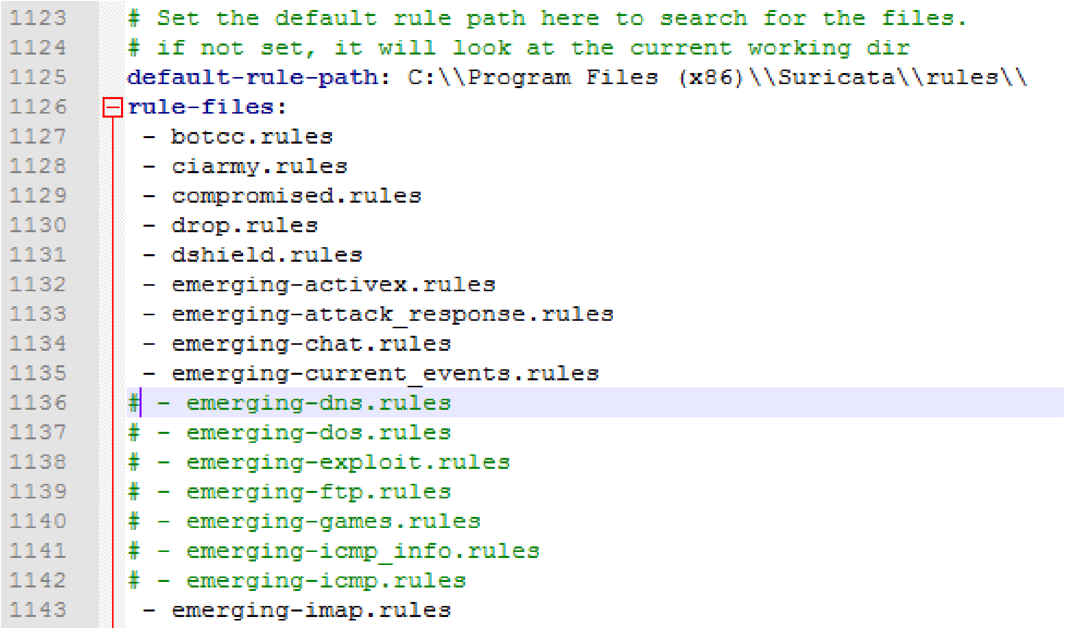
### Rules

You will need rules, because Suricata inspects traffic based on rules. The rules usually reside in the "***INSTALLDIR\rules***" directory. There are non-installed by default. You can install them in any directory you wish, just make sure you change the path in the suricata.yaml configuration file.

You can get them from:

- ProofPoint(Emerging Threads - ETPro ruleset) – the rules there are specially tailored for Suricata, in order to use its advanced and specific features to the maximum. You can also use the free ET Open ruleset.
- Write them yourself – if you have previous experience or you would like just a specific traffic to be inspected, you can write the necessary rules by yourself. You can find some more info on rule writing here:
- Suricata Rule Writing Manual

After you have the rules – specify which rules would you like to activate or deactivate. For example, if you would like to deactivate a rule put a "#" at the beginning of the line:



```
# 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 Files (x86)\\Suricata\\rules\\
rule-files:
 - botcc.rules
 - ciarmy.rules
 - compromised.rules
 - drop.rules
 - dshield.rules
 - emerging-activex.rules
 - emerging-attack_response.rules
 - emerging-chat.rules
 - emerging-current_events.rules
# - emerging-dns.rules
# - emerging-dos.rules
# - emerging-exploit.rules
# - emerging-ftp.rules
# - emerging-games.rules
# - emerging-icmp_info.rules
# - emerging-icmp.rules
 - emerging-imap.rules
```

The ones in green above are deactivated.

## Configuration

It is important that you configure Suricata properly.

Suricata's configuration file is called "suricata.yaml" and holds special syntaxes and all your configurational variables – i.e. networks, interfaces, log files locations/rules directories and many more.

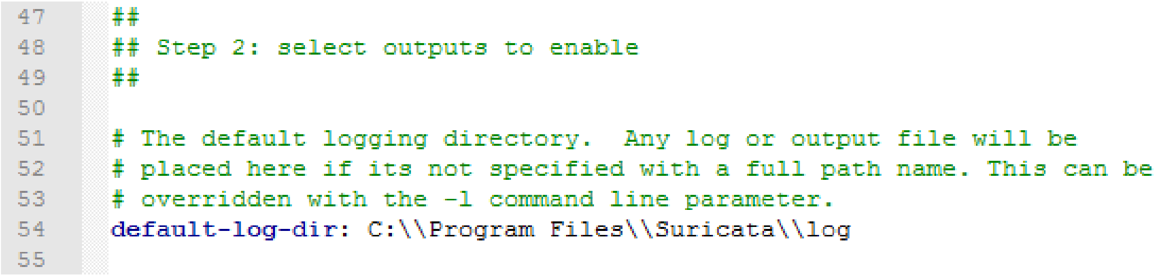
Suricata.yaml already has default values and config options, here we will go over some of them very briefly, so that you can get acquainted better.

For example , if you are not happy with the default options you can change them –

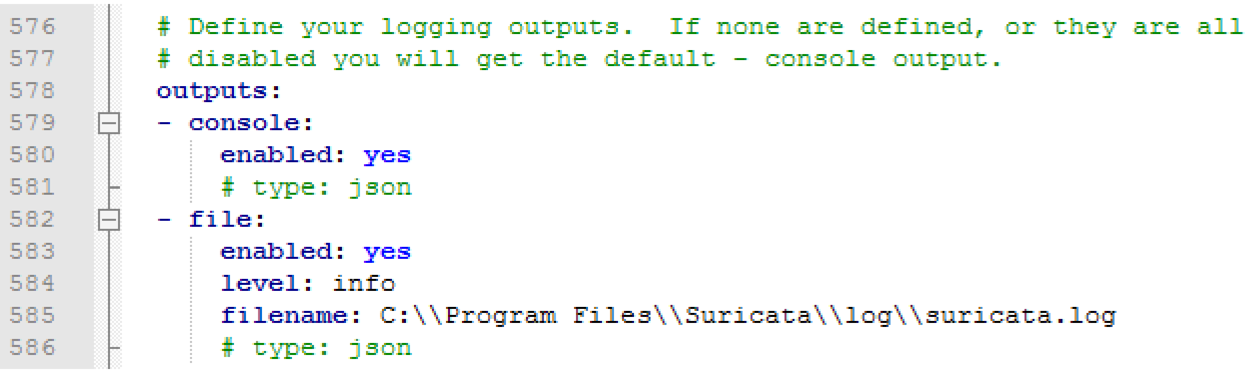
```
”default-log-dir: C:\Suricata\log

………

- file:

     enabled: yes

     filename: C:\\Suricata\\suricata.log

……….

default-rule-path: C:\\Suricata\\rules\\

classification-file: C:\\Suricata\\classification.config

…….
```

***HOME_NET: "[192.168.0.0/16]"     - (here actually you put any network you want Suricata to inspect)***

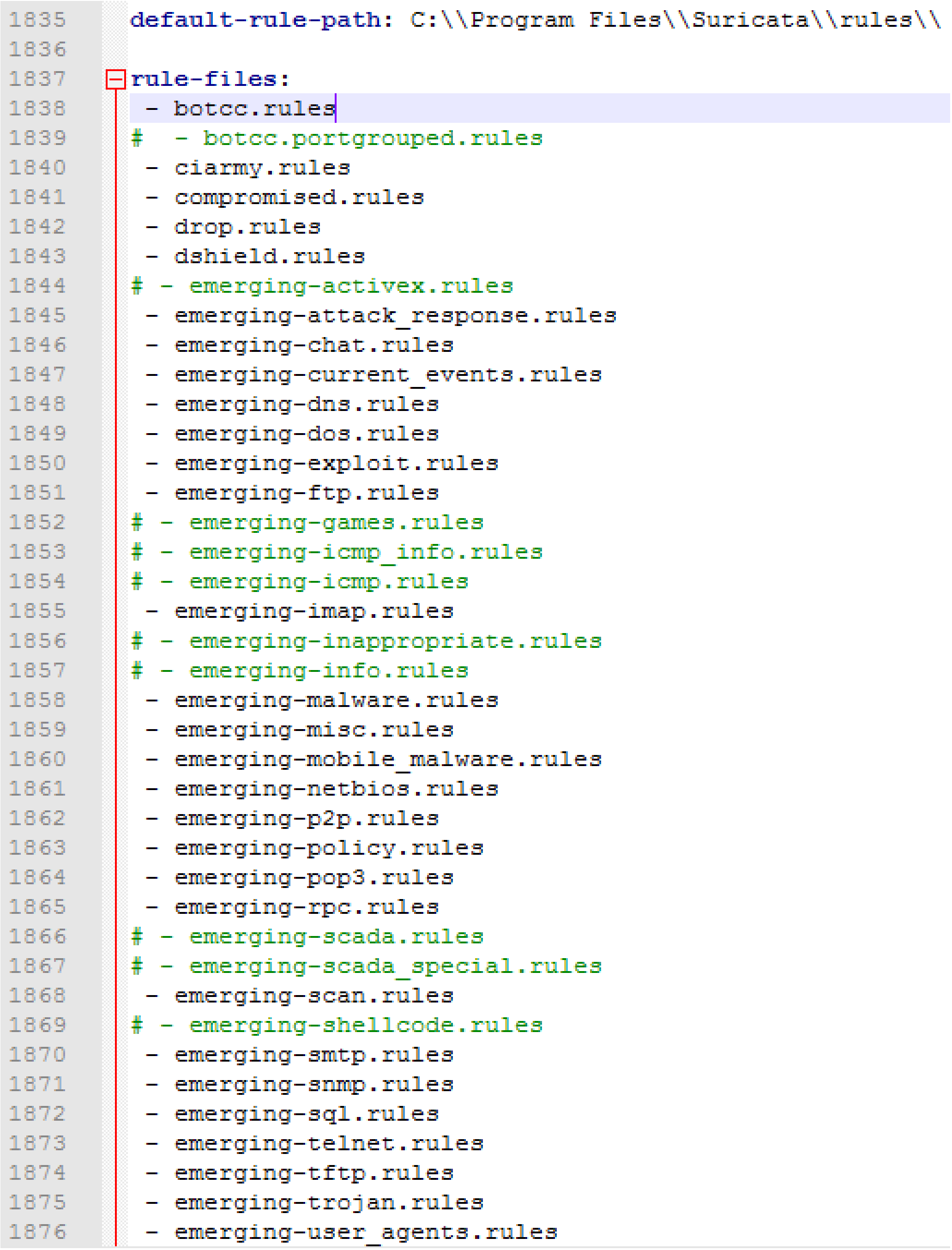
similar to the pic below:



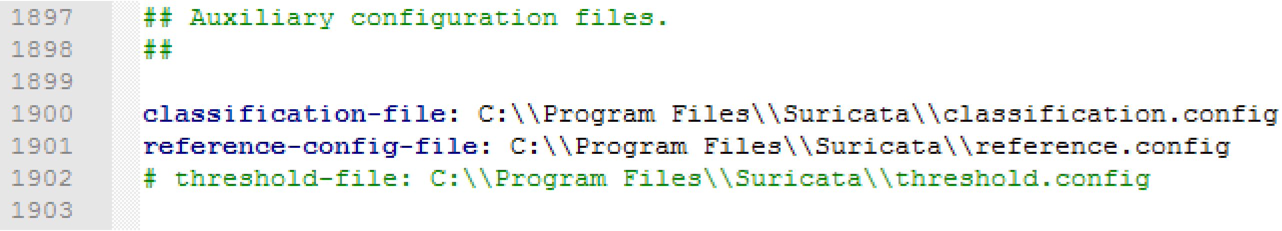
```
##
## Step 2: select outputs to enable
##

# 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 -l command line parameter.
default-log-dir: C:\\Program Files\\Suricata\\log

```



```
# Define your logging outputs.  If none are defined, or they are all
# disabled you will get the default - console output.
outputs:
- console:
    enabled: yes
    # type: json
- file:
    enabled: yes
    level: info
    filename: C:\\Program Files\\Suricata\\log\\suricata.log
    # type: json
```



```
default-rule-path: C:\\Program Files\\Suricata\\rules\\

rule-files:
 - botcc.rules
#   - botcc.portgrouped.rules
 - ciarmy.rules
 - compromised.rules
 - drop.rules
 - dshield.rules
# - emerging-activex.rules
 - emerging-attack_response.rules
 - emerging-chat.rules
 - emerging-current_events.rules
 - emerging-dns.rules
 - emerging-dos.rules
 - emerging-exploit.rules
 - emerging-ftp.rules
# - emerging-games.rules
# - emerging-icmp_info.rules
# - emerging-icmp.rules
 - emerging-imap.rules
# - emerging-inappropriate.rules
# - emerging-info.rules
 - emerging-malware.rules
 - emerging-misc.rules
 - emerging-mobile_malware.rules
 - emerging-netbios.rules
 - emerging-p2p.rules
 - emerging-policy.rules
 - emerging-pop3.rules
 - emerging-rpc.rules
# - emerging-scada.rules
# - emerging-scada_special.rules
 - emerging-scan.rules
# - emerging-shellcode.rules
 - emerging-smtp.rules
 - emerging-snmp.rules
 - emerging-sql.rules
 - emerging-telnet.rules
 - emerging-tftp.rules
 - emerging-trojan.rules
 - emerging-user_agents.rules
```



```
## Auxiliary configuration files.
##

classification-file: C:\\Program Files\\Suricata\\classification.config
reference-config-file: C:\\Program Files\\Suricata\\reference.config
# threshold-file: C:\\Program Files\\Suricata\\threshold.config

```

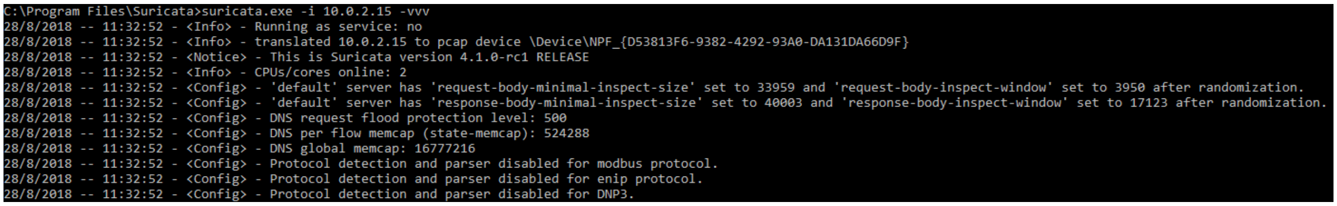
***NOTE: Please make sure that the directories are created or exist if you change from the default ones***

## Running Suricata

Open a cmd and go to your Suricata Directory OR just double click the icon on your desktop and execute:

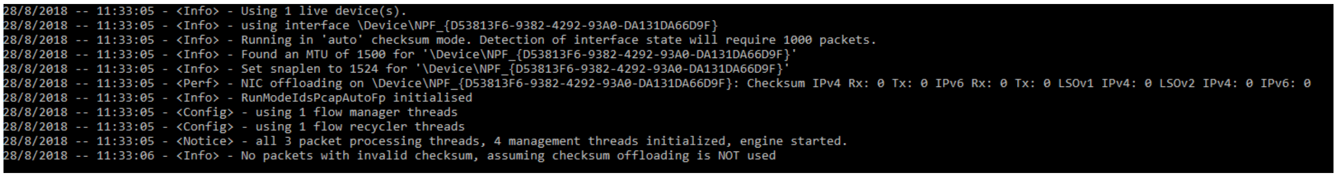
*suricata.exe -c suricata.yaml -i 10.0.2.15*

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):



```
C:\Program Files\Suricata>suricata.exe -i 10.0.2.15 -vvv
28/8/2018 -- 11:32:52 - <Info> - Running as service: no
28/8/2018 -- 11:32:52 - <Info> - translated 10.0.2.15 to pcap device \Device\NPF_{D53813F6-9382-4292-93A0-DA131DA66D9F}
28/8/2018 -- 11:32:52 - <Notice> - This is Suricata version 4.1.0-rc1 RELEASE
28/8/2018 -- 11:32:52 - <Info> - CPUs/cores online: 2
28/8/2018 -- 11:32:52 - <Config> - 'default' server has 'request-body-minimal-inspect-size' set to 33959 and 'request-body-inspect-window' set to 3950 after randomization.
28/8/2018 -- 11:32:52 - <Config> - 'default' server has 'response-body-minimal-inspect-size' set to 40003 and 'response-body-inspect-window' set to 17123 after randomization.
28/8/2018 -- 11:32:52 - <Config> - DNS request flood protection level: 500
28/8/2018 -- 11:32:52 - <Config> - DNS per flow memcap (state-memcap): 524288
28/8/2018 -- 11:32:52 - <Config> - DNS global memcap: 16777216
28/8/2018 -- 11:32:52 - <Config> - Protocol detection and parser disabled for modbus protocol.
28/8/2018 -- 11:32:52 - <Config> - Protocol detection and parser disabled for enip protocol.
28/8/2018 -- 11:32:52 - <Config> - Protocol detection and parser disabled for DNP3.
```

And you have yourself Suricata running:



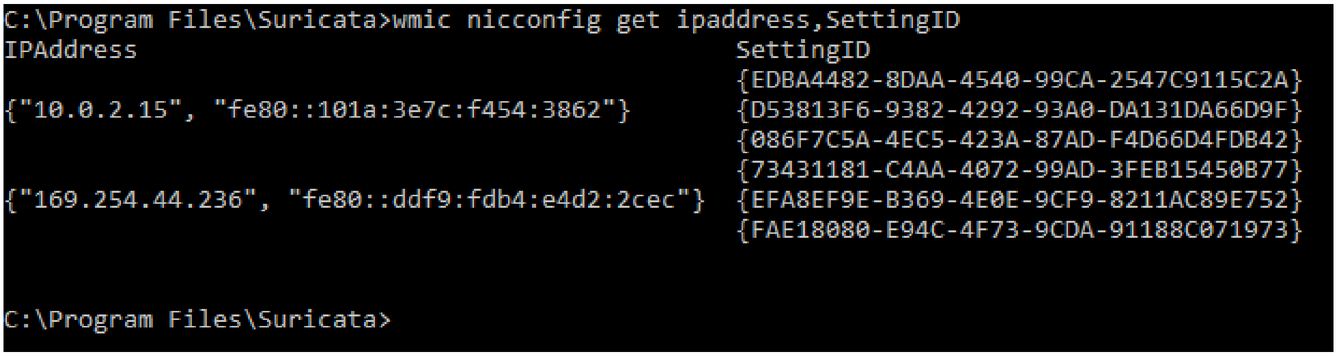
```
28/8/2018 -- 11:33:05 - <Info> - Using 1 live device(s).
28/8/2018 -- 11:33:05 - <Info> - using interface \Device\NPF_{D53813F6-9382-4292-93A0-DA131DA66D9F}
28/8/2018 -- 11:33:05 - <Info> - Running in 'auto' checksum mode. Detection of interface state will require 1000 packets.
28/8/2018 -- 11:33:05 - <Info> - Found an MTU of 1500 for '\Device\NPF_{D53813F6-9382-4292-93A0-DA131DA66D9F}'
28/8/2018 -- 11:33:05 - <Info> - Set snaplen to 1524 for '\Device\NPF_{D53813F6-9382-4292-93A0-DA131DA66D9F}'
28/8/2018 -- 11:33:05 - <Perf> - NIC offloading on \Device\NPF_{D53813F6-9382-4292-93A0-DA131DA66D9F}: Checksum IPv4 Rx: 0 Tx: 0 IPv6 Rx: 0 Tx: 0 LSOv1 IPv4: 0 LSOv2 IPv4: 0 IPv6: 0
28/8/2018 -- 11:33:05 - <Info> - RunModeIdsPcapAutoFp initialised
28/8/2018 -- 11:33:05 - <Config> - using 1 flow manager threads
28/8/2018 -- 11:33:05 - <Config> - using 1 flow recycler threads
28/8/2018 -- 11:33:05 - <Notice> - all 3 packet processing threads, 4 management threads initialized, engine started.
28/8/2018 -- 11:33:06 - <Info> - No packets with invalid checksum, assuming checksum offloading is NOT used
```

**NOTE:**

If you need to run Suricata on a 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*



```
C:\Program Files\Suricata>wmic nicconfig get ipaddress,SettingID
IPAddress                                       SettingID
                                                {EDBA4482-8DAA-4540-99CA-2547C9115C2A}
{"10.0.2.15", "fe80::101a:3e7c:f454:3862"}      {D53813F6-9382-4292-93A0-DA131DA66D9F}
                                                {086F7C5A-4EC5-423A-87AD-F4D66D4FDB42}
                                                {73431181-C4AA-4072-99AD-3FEB15450B77}
{"169.254.44.236", "fe80::ddf9:fdb4:e4d2:2cec"} {EFA8EF9E-B369-4E0E-9CF9-8211AC89E752}
                                                {FAE18080-E94C-4F73-9CDA-91188C071973}


C:\Program Files\Suricata>
```

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 example:

*C:\Program Files\Suricata>suricata.exe -i \\DEVICE\\NPF_\{D53813F6-9382-4292-93A0-DA131DA66D9F\}*

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

## More Info and Documentation

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

https://suricata.readthedocs.io/en/latest/what-is-suricata.html