> Suricata 是一个免费和开源，成熟，快速且强大的网络威胁检测引擎。
>
> Suricata引擎能够进行实时入侵检测（IDS），内联入侵防御（IPS），网络安全监控（NSM）和离线pcap处理。Suricata使用强大而广泛的规则和签名语言检查网络流量，并具有强大的Lua脚本支持来检测复杂的威胁。通过YAML和JSON之类的标准输入和输出格式，与现有SIEM，Splunk，Logstash / Elasticsearch，Kibana和其他数据库之类的工具的集成变得毫不费力。

安装

```
# Recommended dependency
apt-get install libpcre3 libpcre3-dbg libpcre3-dev build-essential libpcap-dev   \
                libnet1-dev libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev \
                libcap-ng-dev libcap-ng0 make libmagic-dev         \
                libgeoip-dev liblua5.1-dev libhiredis-dev libevent-dev \
                python-yaml rustc cargo

#  Binary packages - Ubuntu
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
# `jq` help with displaying information from Suricata’s EVE JSON output
sudo apt-get install suricata jq

# Verify Installation
sudo suricata --build-info
sudo systemctl status suricata
# Outputs:
● suricata.service - LSB: Next Generation IDS/IPS
   Loaded: loaded (/etc/init.d/suricata; bad; vendor preset: enabled)
   Active: active (exited) since 二 2021-05-25 15:29:42 CST; 2min 27s ago
     Docs: man:systemd-sysv-generator(8)

5月 25 15:29:42 ubuntu systemd[1]: Starting LSB: Next Generation IDS/IPS...
5月 25 15:29:42 ubuntu suricata[39360]: Starting suricata in IDS (af-packet) mode... done.
5月 25 15:29:42 ubuntu systemd[1]: Starte™£d LSB: Next Generation IDS/IPS.

# update rules: merge the lastet rules to /etc/suricata/rules/*
suricate-update
```

网卡配置

`vim /etc/suricata/suricata.yaml`

本例中，网卡为 `ens33`

```
# Linux high speed capture support
af-packet:
  - interface: ens33
    # Number of receive threads. "auto" uses the number of cores
...
...
# default rules
default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
```

修改完成后重启服务 `systemctl restart suricata`

测试

使用 `2100498` 规则进行测试。规则可在 `/var/lib/suricata/rules/suricata.rules` 查看：

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; classtype:bad-unknown; sid:2100498; rev:7; metadata:created_at 2010_09_23, updated_at 2010_09_23;)
```

`tail` 查看 `fast.log` 文件，运行 `curl http://testmynids.org/uid/index.html` 。可看到log文件中，增加到了监测内容。

```
# path of log files
fastlog_file:"/var/log/suricata/fast.log"
log_file:"/var/log/suricata/suricata.log"
statistics_file:"/var/log/suricata/stats.log"

suricata tail -f fast.log
# Outputs:
05/25/2021-17:10:53.943090  [**] [1:2013028:5] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.205.6:50856 -> 13.225.103.101:80
05/25/2021-17:10:54.040108  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 13.225.103.101:80 -> 192.168.205.6:50856
```

```
curl http://testmynids.org/uid/index.html
# Outputs:
uid=0(root) gid=0(root) groups=0(root)
```

> 参考：
>
> https://suricata.readthedocs.io/en/latest/