Настройка Suricata на CentOS 7

2020, Feb 03

Настройка Suricata на CentOS 7

Предыстория

Проходим испытания на соответствие информационной безопасности, потребовали установить IDS\IPS для инспекции трафика. Самым популярным является Snort. Однако, его главный минус - однопоточность. Поэтому и появился suricata с поддержкой многопоточности и поддержкой правил формата Snort.

Решение

Пакет Suricata имеется в репозитории Epel. Версия 4.1, нас вполне устраивает. Устанавливаем пакеты, понадобится еще пакет с библиотекой PyYaml.

```
sudo yum install suricata python2-pyyaml -y
```

Необходимо изменить файл установок по умолчанию

```
cat <<"EOF" | sudo tee /etc/sysconfig/suricata
# The following parameters are the most commonly needed to configure
# suricata. A full list can be seen by running /sbin/suricata --help
# -i <network interface device>
# --user <acct name>
# --group <group name>

# Add options to be passed to the daemon
OPTIONS="--user suricata --group suricata"
EOF
```

По умолчанию сервис не параметризованнный, нужно это исправить. Создадим новый параметризованный сервис wpa_supplicant@.service

```
cat <<"EOF" | sudo tee /etc/systemd/system/suricata@.service
# /usr/lib/systemd/system/suricata.service
# Sample Suricata systemd unit file.
[Unit]
Description=Suricata Intrusion Detection Service on %I interface
After=syslog.target network-online.target systemd-tmpfiles-setup.service
Documentation=man:suricata(1)

[Service]
# Environment file to pick up $OPTIONS. On Fedora/EL this would be
# /etc/sysconfig/suricata, or on Debian/Ubuntu, /etc/default/suricata.
EnvironmentFile=-/etc/sysconfig/suricata
#EnvironmentFile=-/etc/default/suricata
ExecStartPre=/bin/rm -f /var/run/suricata.pid
ExecStart=/sbin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata
ExecReload=/bin/kill -USR2 $MAINPID

[Install]
WantedBy=multi-user.target
EOF
```

Включаем сервисы

```
sudo systemctl enable suricata@ens192.service
sudo systemctl start suricata@ens192.service
```

Нужно обновить базы suricata. У нас запрещено работать из-под root. Поэтому используем sudo. Более подробнее об обновление написано здесь.

```
export https_proxy=http://proxy.local:8888
export http_proxy=http://proxy.local:8888
sudo -E suricata-update
sudo -E suricata-update list-sources
sudo -E suricata-update enable-source ptresearch/attackdetection
sudo -E suricata-update enable-source oisf/trafficid
sudo -E suricata-update enable-source sslbl/ssl-fp-blacklist
sudo -E suricata-update
```

Смотрим логи сервиса

```
sudo journalctl -f -u suricata@ens192.service
```

Итог

В данный момент для меня это новая область. Но радует, что есть официальные государтсвенные требования, которые заставляют все АйТи-компании РК внедрять IDS\IPS-системы. Если будут новости, напишу позднее.

---

linux, centos, ips, ids, security, traffic, python, sudo

←
Используем spi-flash для загрузки с usb-storage на Orange Pi Zero Plus

Настройка Firecracker на CentOS 7
→