Segurança em Redes de Comunicações

Intrusion Detection System

Suricata

IDS Deployment

1. Using a Linux VM connect to the internet as IDS, as root, install the Suricata service:

```
$ sudo su
$ apt install suricata
```

Stop and disable the start on boot of the Suricata service:

```
$ systemctl stop suricata
$ systemctl disable suricata
```

>> Analyze the default Suricata configuration file in /etc/suricata/suricata.yaml.

>> Analyze the included Suricata rules in /etc/suricata/rules/.

Note: Suricata must be run as a service in real world scenarios.

2. Create a file to add locally define IDS rules (named local.rules) in the default rules directory (/etc/suricata/rules/).

Edit the configuration file (/etc/suricata/suricata.yaml), look for the section that starts with “rule-files:” and add (at the bottom) an new entry pointing to the local.rules file:

```
rule-files:
 - botcc.rules
 # - botcc.portgrouped.rules
 - ciarmy.rules
…
# - ipsec-events.rules
# - kerberos-events.rules
- local.rules
```

Start Suricata from the command line:

```
$ suricata -c /etc/suricata/suricata.yaml -i enp0s3
```

3. Analyze the Suricata logs files “eve.json” and “fast.log” in the default log directory “/var/log/suricata/”.

Open a second terminal and start a continuous observation of the suricata fast-log file:

```
$ tail -f /var/log/suricata/fast.log
```

4. Edit local.rules by adding:

```
alert tcp 193.136.173.58 any -> $HOME_NET any (msg:"TCP Packets from www.ua.pt";sid:666671;)
```

Reload rules into Suricata:

```
$ kill -USR2 $(pidof suricata)
```

Using TCP pings, ping TCP port 443 of www.ua.pt, elearning.ua.pt, mail.ua.pt (with SYN flag):

```
$ hping3 -S -p 443 www.ua.pt
```

>> Analyze the Suricata alert log (fast.log).

Note: To install hping3: `$ apt install hping3`

5. Edit local.rules by editing the previous rule:

```
alert tcp [193.136.173.58,193.136.173.95] any -> $HOME_NET any (msg:"TCP Packets from UA";sid:666671;)
```

Reload rules into Suricata:

```
$ kill -USR2 $(pidof suricata)
```

Using TCP pings, ping www.ua.pt, elearning.ua.pt, mail.ua.pt:

```
$ hping3  -S -p 443 www.ua.pt
```

>> Analyze the Suricata alert log (fast.log).

6. Edit local.rules by editing the previous rule to only register the alarm when the TCP traffic originates from ports 80 and 443:

alert tcp [193.136.173.58,193.136.173.95] [80,443] -> $HOME_NET any (msg:"TCP Packets from UA strange ports";sid:666671;)

Reload rules into Suricata.

Using TCP pings, ping www.ua.pt, elearning.ua.pt, mail.ua.pt using ports 80, 443, 993.

```
$ hping3 -S -p 80 www.ua.pt
$ hping3 -S -p 443 www.ua.pt
$ hping3 -S -p 993 mail.ua.pt
```

7. Edit local.rules by adding a new rule to register an alarm when UDP messages contain the ASCII text “SRCATTACK”:

alert udp any any -> any any (msg:"Message from SRCATTACK";**content: "SRCATTACK";**sid:666672;)

Reload rules into Suricata.

Using UDP pings, ping www.ua.pt with the data string “SRCATTACK”:

```
$ hping3 --udp -d 64 -e “SRCATTACK” www.ua.pt
```

>> Analyze the Suricata alert log (fast.log).

8. Edit local.rules by adding a new rule to register an alarm when TCP messages are received from Russia IP addresses:

alert tcp any any -> $HOME_NET any (msg:"With love from Russia";**geoip:src,RU;**sid:666673;)

Reload rules into Suricata.

Using TCP pings, ping rt.com Russian server (82.202.190.90):

```
$ hping3 -S -p 443 82.202.190.90
```

>> Analyze the Suricata alert log (fast.log).

9. Edit local.rules by adding a new rule to register an alarm after 10 TCP messages from the same flow are received from Russia IP addresses:

alert tcp any any -> $HOME_NET any (msg:"Measuring HATE from Russia";geoip:src,RU;**flowint: rucount, +,1;**sid:666674;noalert;)

alert tcp any any -> $HOME_NET any (msg:"HATE from Russia";geoip:src,RU;**flowint: rucount, +,1;flowint:rucount,>,10;**sid:666675;)

Reload rules into Suricata.

Using TCP pings, ping rt.com Russian server (82.202.190.90):

```
$ hping3 -S -p 443 82.202.190.90 --keep
```

>> Analyze the Suricata alert log (fast.log).

10. Edit local.rules by adding a new rule to register an alarm after 3 or more TCP messages from the same source (any flow) within 30 seconds are received from Russia IP addresses:

alert tcp any any -> $HOME_NET any (msg:"With REAL HATE from Russia";geoip:src,RU;**threshold: type threshold, track by_src, count 3, seconds 30**;sid:666676;)

Reload rules into Suricata.

Using TCP pings, ping rt.com Russian server (82.202.190.90):

```
$ hping3 -S -p 443 82.202.190.90
```

>> Analyze the Suricata alert log (fast.log).

11. Using the Suricata rules manual: https://suricata.readthedocs.io/en/suricata-6.0.0/rules/index.html design additional rules.