Hello,

My suricata config is working fine as in if I start a Nmap scan with Suricata's VM IP address, suricata shows alert but the problem is that it does not show alerts when I do a scan on another Virtual Machine (in the same subnet as my Suricata's VM). Can anyone help me? I've been trying to resolve that issue with no success.

Thanks

History

#1 - 05/19/2020 10:06 AM - Victor Julien
- Tracker changed from Bug to Support
- Priority changed from Immediate to Normal

Can you please leave the priority set to normal? Thanks.

#2 - 05/19/2020 10:08 AM - Andreas Herz
- Status changed from New to Feedback
- Assignee set to Little Yu

Hi,

please stop setting Support Tickets to Immediate priority. Also please provide more details about your setup as requested in other issues created by you or it's rather hard to help you.

#3 - 05/19/2020 01:36 PM - Little Yu

I'm sorry, not gonna do it again.

I'm on Suricata 4.1.2 version and my suricata.yaml setup is as follow:

`HOME_NET : "[192.168.0.0/24]"
EXTERNAL_NET : "!$HOME_NET"

As for rules, I'm using emergingthreats rules that are available with suricata-update so those lines are also not commented in suricata.yaml

default-rule-path: /etc/suricata/rules
rule-files:
- suricata.rules

And when I start Suricata : suricata -c /etc/suricata/suricata.yaml -i enp0s3

It shows that it is working fine and rules are enabled.

As for the alerts, I did a nmap scan on the virtual machine where Suricata (192.168.0.34) is. The alerts show up fine in fast.log but when I do an nmap scan on another virtual machine (192.168.0.39), there's no alert showing up in fast.log

#4 - 05/19/2020 08:08 PM - Andreas Herz

Did you ensure that the routing/mirroring of the traffic is forwarded to that interface?
If you run `tcpdump -nn -vv -i enp0s3 host 192.168.0.39` do you see that traffic?

#5 - 05/20/2020 08:22 AM - Little Yu
Andreas Herz wrote in #note-4:

Did you ensure that the routing/mirroring of the traffic is forwarded to that interface? If you run ` tcpdump -nn -vv -i enp0s3 host 192.168.0.39` do you see that traffic?

I did not do that, seeing as I'm running both of those virtual machines using VirtualBox, how exactly can I configure port mirroring without a switch?

And when I run the command, it shows this:

```
tcpdump.JPG
```

#6 - 05/26/2020 08:24 PM - Andreas Herz

I don't know if Virtualbox offers such a functionality but at least from the dump it's rather clear that the traffic you want to monitor is not seen, so that's something you need to fix within your virtual network setup.