Suricata on SELKS workshop

Ressource for the VM

- At least:
  - 4Gb of memory (5Gb recommended)
  - 2 cores
- Reason:
  - Elasticsearch

Download and start SELKS

- Download: http://dl.stamus-networks.com/selks/SELKS-4.0-desktop.iso
- Start it in virtualbox, vmware:
  - First interface for admin
    - Host network
  - Second one interface for sniffing:
    - Ethernet bridge
    - Promiscuous enable

Do the installation

- Select default installation
- User/Password: selks-user/selks-user
- Activate the interface

Connect to the GUI

- https://192.168.56.101/
  - user/password: selks-user/selks-user
- On physical box:
  - curl http://testmyids.com
- Go to
  - https://192.168.56.101/evebox/#/inbox
- Visualize the alerts

Upgrade (optional)

- Upgrade
  - sudo /opt/selks/Scripts/Setup/selks-upgrade_stamus.sh
- Reboot
  - Sudo reboot

Evebox: flow_id correlation & more

- Display all the events for the flow id corresponding to the alert
- Display IP report for the server

Alert with metadata

- Kibana
  - Do a donut of alerts count by category
  - Add a layer to the donut to display the http hostname

Signatures management (1/2)

- Disable rules
  - Is curl really a problem ?
  - Disable the rule
  - Test that it does not alert anymore
- Suppress rules
  - Is testmyids alert really a problem ?
  - Disable the alert for this specific server
  - Test that it does not alert anymore

Signature management (2/2)

- Thresholding
  - Do an apt-get update
  - Check the impact
  - Lower the noise by adding a threshold

DNS events

- Kibana analysis
  - Use Kibana to display the top 10 requested domain
  - Build a timeline with one line by request type
  - Save that in a dasboard
- Let’s jq your world
  - Check that you have */var/log/suricata/eve.json*
  - Use grep to extract the DNS query from it
  - Display a list of DNS requested name (rrname)
  - Use the shell to display a top of requested name

TLS events

- Kibana
  - Create a Pie with issuer DN with part size based on count
  - Duplicate the Pie to have splice size to be the number of unique certificates seen for each issuer

Flow events

- Kibana
  - Display volume of data per application layer

Write your own alert

- Write an alert that trigger when a let’s encrypt certificate is seen
- Update the alert to only alert if the server asked is a .com
- Kill the player exercise:
  - Use lua to update the alert so it only trigger for a certificate that is valid since less than one day

Conclusion

- Run your own Suricata
- Discover what happen on your network