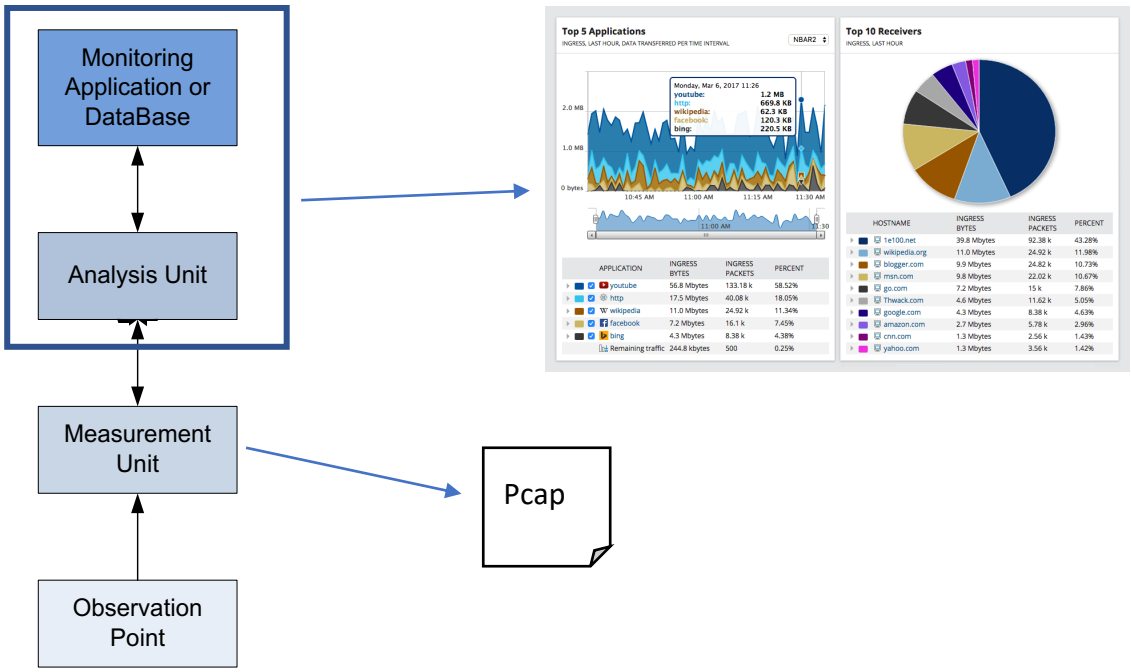
Mini-Projet : Network Monitoring
Enseignant : Zujany SALAZAR
Contact : zujany.salazar@montimage.com, zujany@gmail.com (emergency)

Pcaps files: https://github.com/zujany/paris7-network-monitoring-project

Description

During this mini-project you will perform offline monitoring of a network. You will work in the Analysis unit and Monitoring Application of the Network Monitoring process. Measures were already done in a single observation point, and you will correlate them to obtain meaningful information, generate plots, make rules to deploy alerts when detecting specific behaviors in Suricata, and finally generate a report with your conclusions.



Activities

In the further steps you are suggested to use **Python's libraries NFStream, Pandas, and Matplotlib.** Nevertheless, if you prefer working with other tools that can provide you the same results, it is perfectly valid.

1.1 **Prepossessing the data:** Using Python NFStream extract specific features of your pcap file, and get them into a pandas dataframe or a cvs file. TShark could also help you to extract more fields of your pcap.

1.2 **Generate plots:** Once you have the data ready to be process, generate plots that contain the following information of you pcap file

- What are the used communication protocols in the transport layer? (e.g. TCP, UDP, SCTP)
- What are the most used application protocols? (e.g HTTP, FTP)
- Who is sending/receiving data? What are their MAC addresses?
- Traffic volume per time, incoming and outgoing flows (Here you must use TShark to extract the timestamp and the size of the packets)
- Who (what IP address) is sending more volume of traffic?
- 3 other plots you consider relevant

Be sure to make different types of charts: line graphs, bar graphs and histograms, pie charts, and Cartesian graphs, etc.

1.3 Perform Security Analysis with Suricata:

1.3.1 Process your pcap file with all the default rules of Suricata activated, and analyze the results. Explain.

- Notice that, in general, alerts starting by "SURICATA" do not correspond to security incidents but to traffic that is not conform to the standards or that Suricata cannot parse
  - After installing Suricata you must make sudo suricata-update to charge all the default rules
  - The alerts of your rules will be in the file fast.log

1.3.2 Make 3 new rules that trigger new alerts. Explain what you wanted to detect and show pictures of the alerts. Do not forget to send the code of the rules too. The rules can be very simple, for example:

This rule will trigger an alert for each tcp messages, in which the payload contains the string "yahoo"

```
alert tcp any any -> any any (msg:"My own rule"; content:"yahoo"; nocase;
classtype:policy-violation; sid:1; rev:1;)
```

Check Adding your own rules for more information.

With all the information you already collect from your plots, the Suricata alerts, and maybe Wireshark, perform an analysis of the network:

- What were the people we captured the traffic from doing? were they sending emails? working remotely? watching a movie?
- What country are they in?
- Analyze and explain with details the plots you made
- Are you using Deep Packet Inspection? Explain

- Are you performing passive or active monitoring? Explain
- A security incident occurred while they were doing this activity? Explain (Spoiler alert: yes!)
- Could you provide the MAC address of the infected computer?
- Are you using signature-based security monitoring techniques or performing anomaly detection? Explain
- Who (IP and/or MAC address) you think is the attacker and why?
- What type of attack is this? And what principle of security (i.e., confidentiality, integrity, and availability.) is it attempting to violate?

Teams work

You can make this project individually, in pairs, or in groups of 3.

Deliverables

Students must return by email before December 22, 2021 11:59 p.m

- A pdf file with the answers of the Activity section, the images of the generated plots, and the images of the Suricata rules and alerts. Your pdf file must be the story of what's happening in your pcap file, more detailed is you story, higher will be your note. I advise you to write the document in English, but you can do it French as well.
- The code of the Suricata rules you made

Email content:

- Subject : [M2-Universite-de-Paris] Monitoring projet
- Recipient: zujany.salazar@montimage.com
- Don't forget to put the group members in the email
- Don't send an empty email with only the files attached, it's rude ☹
- An acknowledgment of receipt will be sent to you before December 28, 2021. If you do not receive an acknowledgment, please contact me to verify that I have received your mini-project

References and useful readings:

- NFStram https://github.com/nfstream/nfstream
- TShark https://www.wireshark.org/docs/man-pages/tshark.html

- Pandas https://pandas.pydata.org/docs/user_guide/index.html#user-guide
- Suricata https://suricata.readthedocs.io/en/suricata-6.0.1/what-is-suricata.html
    - Rule Management with Suricata-Update https://suricata.readthedocs.io/en/suricata-6.0.0/rule-management/suricata-update.html
    - Suricata Rules https://suricata.readthedocs.io/en/suricata-6.0.1/rules/index.html
    - Making sense out of Alerts https://suricata.readthedocs.io/en/suricata-6.0.1/make-sense-alerts.html
    - Adding your own rules https://suricata.readthedocs.io/en/suricata-6.0.0/rule-management/adding-your-own-rules.html