download

PYTHON FOR NETWORK TRAFFIC ANALYSIS AUTOMATION

Mišo Mijatović
Security DevOps @ Sorint.SEC

python™

SORINT.SEC SORINT.lab

OBJECTIVE

There’s the need to automate tasks

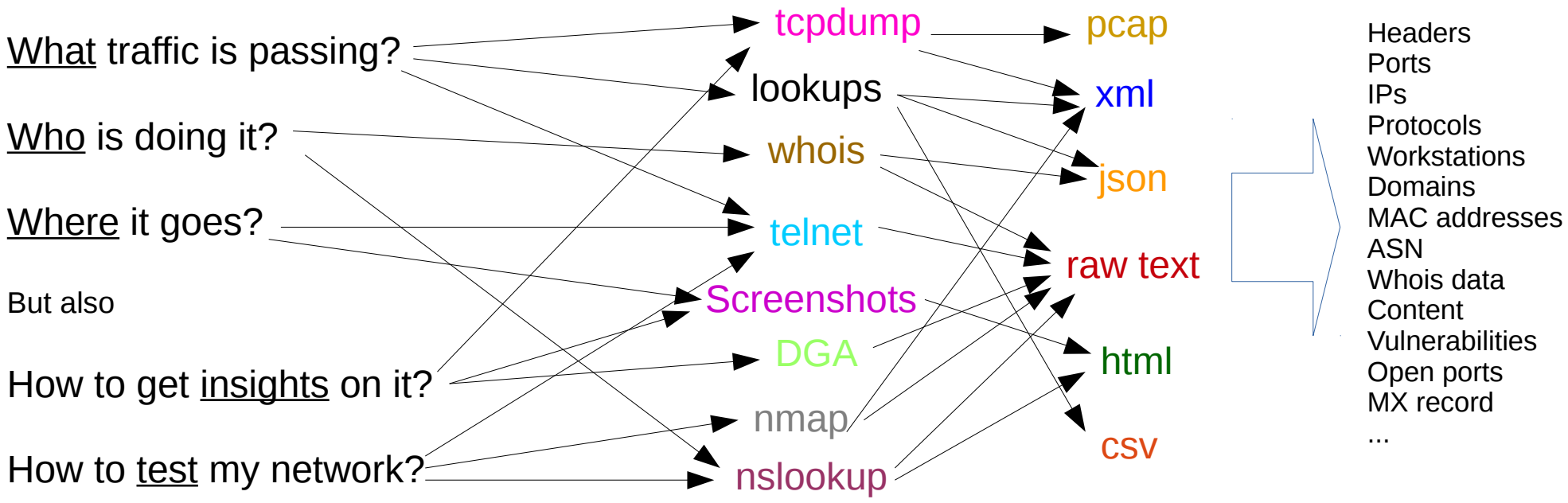
- demonstration on how to do it

- sponsorship of python as the tool to do it

- personal: have a feedback and new ideas, use cases

NETWORK TRAFFIC ANALYSIS: WHAT

Purpose: analyzing, get insighs on network data



TOOLS

socket
scapy
requests
urllib
whois
dnspython
nmap
smtp
imap
...

ENRICHMENT

Well known? → Alexa ranking

Strange? → DGA

Good/evil? → Threat Intelligence

What is it? → Cmdb, IPam

Else? → API lookups

Same problem as before:

- lots of stuff
- different inputs
- different outputs

How to make them cooperate?

ANALYZE

MariaDB FOUNDATION

HTML

splunk>

How many of the afermentioned tools are natively compatible with these on the left

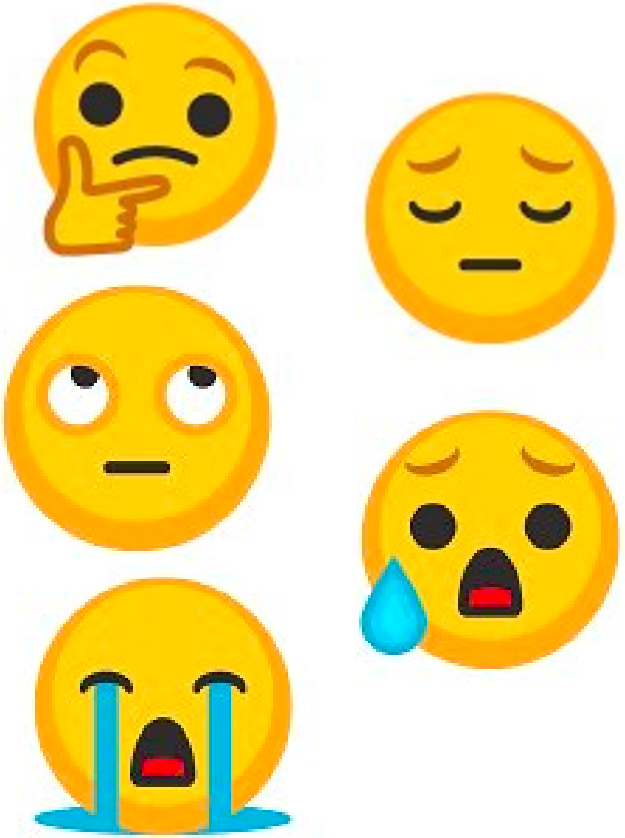
.

.

.

.

?



COOPERATE

- all the operations done by the existent tools and integration through scripting

- some operations done by the existent tools and some by the script

- all the operations done by the scripts

Today I am presenting the third option

DEMO
download
python™
SORINTsec
SORINTlab

CONTACTS & MORE

PYTHON

For references please see the demo code

Mišo Mijatović

mmijatovic@sorint.it

misomij@gmail.com

https://github.com/MisoMadao

DEMO HERE:

https://github.com/MisoMadao/download2018

download

Thanks!

mmijatovic@sorint.it

In collaborazione con:

BERGAMO CITTÀ DEI MILLE
COMUNE DI BERGAMO

SORINT SEC

SORINT lab