Yara

YARA

Yara is used to identify and classify malware samples. Using YARA, an analyst can create patterns of malware families based on textual or binary patterns.
Rules consist of set of strings and boolean expressions. Yara is multi platform.
Install YARA on Kali Linux
    apt-get install yara
    https://github.com/InQuest/awesome-yara

To create a yara rule
    yara myrule.yar dir_name

    The rule must consist of rule name and condition

YARA Conditions
    Meta
        Adding description- Similar to commenting
        `desc`

    Strings
        Can use strings for searching a specific text or hex content
        Hello world checker

            rule helloworld_checker {
                strings:
                    $hello_world = “Hello World!”
                    $hello_world_l = “hello world!”
                    $helloo_world_u = “HELLLO WORLD!"
            }

    Conditions
        Condition checking

            rule conditioncheck{
                condition: true

                condition:
                    $hello_world <= 10
            }

Modules
    Cuckoo Sandbox
    Python PE

Yara Tool : Loki
    python Loki/loki.py -p malicious_file_location

Yara Tool : yarGen
    python3 yarGen -m file_location --excludegood -o new_rule_file_location
        Eg: python3 yarGen -m /home/h4ck/Desktop/THM/malfiles/ --excludegood -o /home/h4ck/Desktop/THM/malfiles/rule.yar
Yara Tool : Valhalla
    It's an online tool