Legacy Activity) Threat Hunting With YARA

In this activity you'll use YarGen and YARA to perform a basic threat hunt, identifying the presence of any malicious artifacts after an incident occurred and a system was compromised. Below is a brief and the files you'll need to complete the exercise. You can complete this activity as many times as you want, but you'll need to score 70% or higher to pass.

CHALLENGE SCENARIO

An employee clicked a link in a phishing email and downloaded malware to their system, which wasn't detected by the anti-virus or endpoint detection and response solution. We need to check if the malware made copies of itself to ensure the attacker's have persistence and can continue working to complete their objectives. We've collected a copy of the initial file that was downloaded from a packet capture. Use yarGen.py to create a detection rule for this binary, and then use YARA to audit the copy of the user's files we've provided you. Report on your findings, and let us know if this malware is hiding anywhere else.

Download the file below and transfer it to your Kali virtual machine, then read the "READ ME.txt" file inside. Good luck hunter.

Download "BTL1_Hunting_With_YARA.zip"

CHALLENGE SUBMISSION

[YARA General Questions 1/4] We want to generate a YARA rule using yarGen.py. The terminal is open in the location of yarGen.py and the malicious file is inside a directory named 'MALICIOUS' on the Desktop of the root user and we want to name the rule "YARARule.yara", saving it in the same location as the terminal. What is the command we want to use ?

Hint

Check