Yara

## 📓 **Notes – Yara**

**Lab Name:** Yara

**Summary:**  
**Yara** is a pattern-matching tool used to identify and classify malware by searching for specific strings, patterns, and characteristics in files or memory.  
It’s often called the “**grep** for malware” and is widely used in threat hunting, incident response, and malware research.

### **Task 1 – Introduction**

* Yara helps analysts detect malware families based on known patterns.
* Works with **Yara rules** that define what to look for.

### **Task 2 – What is Yara?**

* Open-source project by VirusTotal.
* Scans files or processes for matches against rule sets.

### **Task 3 – Deploy**

* Available on Linux, Windows, and macOS.
* Installed via package manager or compiled from source.

### **Task 4 – Introduction to Yara Rules**

* Rules contain:
  + **Meta:** Information about the rule (author, date, purpose).
  + **Strings:** Patterns to search for (text, hex, regex).
  + **Condition:** Logic for when the rule matches.

### **Task 5 – Expanding on Yara Rules**

* Can use wildcards, regular expressions, case sensitivity, and file size checks.
* Multiple string matches can be required for detection.

### **Task 6 – Yara Modules**

* Extend functionality (e.g., PE module for parsing Windows executables, ELF module for Linux binaries).

### **Task 7 – Other Tools and Yara**

* Yara integrates with many tools:
  + **VirusTotal**
  + **CAPE Sandbox**
  + **Cortex** (for enrichment in TheHive)

### **Task 8 – Using LOKI and its Yara Rule Set**

* **LOKI** is a free IOC scanner that uses Yara rules for endpoint scanning.
* Detects suspicious files, processes, and network artifacts.

### **Task 9 – Creating Yara Rules with yarGen**

* **yarGen** helps generate Yara rules from malware samples automatically.
* Avoids hardcoding overly specific strings to improve detection across variants.

### **Task 10 – Valhalla**

* Commercial Yara rule feed maintained by Florian Roth.
* Updated with high-quality detection rules for emerging threats.

**Practical Takeaway:**

* Yara is essential for **malware hunting and detection engineering**.
* Custom rules allow SOCs to detect threats missed by antivirus.
* Rule writing requires balancing specificity (avoid false positives) and generalization (catch more variants).

**Tools/Commands Used:**

* yara sample\_rule.yar suspicious\_file.exe
* LOKI scanner CLI
* yarGen for rule generation

