**Part 5 - Automated YARA Scanning**

In this section, we will **automate malware detection** using **YARA rules** within LimaCharlie. This enables **real-time scanning** of files and processes for **known threats**, such as **Sliver C2 implants**.

**Understanding YARA Scanning**

**What is YARA?**  
YARA is a tool used for identifying and classifying malware based on **textual or binary patterns**. Security professionals use YARA rules to detect **known and emerging threats** across **files, processes, and memory**.

Popular **YARA rulesets** include:

* [**VirusTotal YARA Rules**](https://virustotal.github.io/yara/)
* [**Nextron Valhalla**](https://www.nextron-systems.com/valhalla/)
* [**GitHub - YARA Rules**](https://github.com/Yara-Rules/rules)

**Lab Steps**

**1. Adding YARA Signatures for Sliver C2**

1. **Navigate to** Automation → YARA Rules in LimaCharlie.
2. **Click** Add Yara Rule.
3. **Create a rule named sliver** and paste this ‘YARA rule for Sliver’
4. **Create another rule named sliver-process** using **this YARA rule**.

**2. Setting Up YARA Detection Rules in LimaCharlie**

1. **Go to** Automation → D&R Rules.
2. **Create a rule for YARA file detections:**
3. **Create a second rule for YARA process detections:**

**3. Testing YARA Scanning**

1. **Open LimaCharlie**, go to **"Sensors"**, and select the **Windows VM sensor**.
2. **Run the following command** in the LimaCharlie **Sensor Console** to manually scan files in Downloads:

yara\_scan hive://yara/sliver -r C:\Users\sywtbsa\Downloads

1. **Check the console output** for a **positive detection**.
2. **Verify the detection in the "Detections" tab** in LimaCharlie.

**4. Automating YARA Scans for Suspicious Activity**

**Automatically Scanning Downloaded EXEs**

1. **Create a new D&R Rule in LimaCharlie.**

**Automatically Scanning Processes Launched from Downloads**

1. **Create another D&R Rule.**

**5. Testing the Automated YARA Rules**

**Scanning New EXEs in Downloads**

1. **Move the Sliver payload to another directory and back** to trigger detection:

cd ~\Downloads

Move-Item .\[payload\_name].exe ..\Documents\

Move-Item ..\Documents\[payload\_name].exe .\

1. **Check LimaCharlie’s "Detections" tab** for alerts.

**Scanning Processes Launched from Downloads**

1. **Terminate existing Sliver payloads:**

Get-Process [payload\_name] | Stop-Process

1. **Execute the Sliver payload to trigger detection:**

C:\Users\sywtbsa\Downloads\[payload\_name].exe

1. **Check LimaCharlie’s "Detections" tab** for:
   * **"Execution from Downloads directory"**
   * **"YARA detection in Memory"**

**Next Steps - Automating Threat Response**

With automated YARA scanning in place, consider **expanding detection & response rules** to:

**Terminate malicious processes immediately** upon detection.  
**Scan web server directories for webshells** using [**this YARA rule**](https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/core.webshell_detection.yara).  
**Detect and block CobaltStrike** with [**these YARA rules**](https://github.com/chronicle/GCTI/tree/main/YARA/CobaltStrike).  
**Automatically delete or quarantine malicious files**.