**Part 2: Setting Up the Environment and Launching Sliver C2**

Part 2 focused on creating a simulated lab environment and launching the Sliver C2 framework, enabling me to simulate real-world attack scenarios and enhance my practical skills as a SOC analyst. Here's a breakdown of what I accomplished and the skills I acquired:

1. **Lab Environment Setup:**
   * Created a virtualized lab environment using Linux and Windows virtual machines, mimicking a real-world network environment.
   * Configured network settings to establish communication between the Linux and Windows VMs, ensuring an isolated and secure environment for conducting security experiments.
2. **Sliver C2 Framework:**
   * Installed and configured the Sliver C2 framework, a powerful command-and-control platform used in security testing and red teaming exercises.
   * Gained hands-on experience with launching and managing C2 sessions, executing commands on compromised systems, and exploring sensitive processes for further analysis.
3. **Practical Attack Simulation:**
   * Leveraged the Sliver C2 framework to simulate real-world attack scenarios, allowing me to understand the attacker's perspective and develop the ability to detect and respond to malicious activities effectively.
   * Acquired practical skills in identifying and exploiting vulnerabilities, gaining insights into common attack vectors and techniques employed by adversaries.
4. **Threat Hunting and Analysis:**
   * Developed the ability to analyze telemetry data and identify indicators of compromise (IOCs) within the Sliver C2 framework.
   * Gained proficiency in identifying suspicious activities, anomalous behaviors, and potential security breaches through the analysis of telemetry generated during simulated attacks.



