**4. External Beaconing or C2 Communication**

* Outbound HTTP or HTTPS traffic at a repeating interval.
* Use custom domain or IP.
* Detect it using Winlogbeat logs, Wireshark, or Zeek.

Step-by-Step Guide

Option 1: Simulate Beaconing Using PowerShell (Windows → Kali)

On Windows 10 VM:

1. Run PowerShell as Administrator.
2. Use this loop to send HTTP GET requests every 10 seconds:

while ($true) {

Invoke-WebRequest -Uri "http://192.168.157.131:8080" -UseBasicParsing

Start-Sleep -Seconds 10

}

Replace 192.168.157.140 with your Kali Linux VM’s IP

This mimics a common malware beaconing pattern.

Option 2: Start Listener on Kali (C2 Server Sim)

On Kali Linux VM, start a simple HTTP server:

sudo python3 -m http.server 8080

This listens on port 8080, and you’ll see the incoming beacons from Windows.

Detection

Use Wireshark (on Kali or any VM in same virtual network):

1. Start capturing on the interface (e.g., eth0).
2. Filter:
3. ip.addr == 192.168.157.140
4. Look for regular intervals of HTTP requests → this is beaconing.

Use Sysmon + Winlogbeat (on Windows):

1. Look for logs where powershell.exe accesses the internet:
   * Sysmon Event ID 1 (process creation)
   * Sysmon Event ID 3 (network connection)