**1.Suspicious ZIP or RAR File Downloads**

🔧 Step 1: Set up Attacker Server on Kali (to host a malicious file)

1. Create a fake ZIP/RAR file:
2. echo "test malware" > malware.txt
3. zip malware.zip malware.txt
4. Start an HTTP server:
5. python3 -m http.server 8080
6. Kali will now serve malware.zip at:
7. http:192.168.157.131//:8080/malware.zip

💻 Step 2: Simulate the Download on Windows 10 (Victim)

1. Open PowerShell or a browser on Windows.
2. Use PowerShell to simulate an external download:
3. Invoke-WebRequest -Uri "http://192.168.157.131:8080/malware.zip" -OutFile "C:\Users\Public\malware.zip"
4. This will leave logs of:
   * File creation
   * Network activity
   * Possibly the User-Agent string

Step 3: Set up Sysmon and Winlogbeat on Windows 10

A. Install Sysmon:

Sysmon64.exe -accepteula -i sysmonconfig.xml

Use a config like [SwiftOnSecurity’s Sysmon config](https://github.com/SwiftOnSecurity/sysmon-config)

Step 4: Analyze the Logs

A. File Creation Logs (Sysmon Event ID 11)

B. Network Connection Logs (Sysmon Event ID 3)

* Detect external HTTP download:

C. Look for Suspicious User-Agent

* If the download is via PowerShell:
* User-Agent: Mozilla/5.0 (Windows NT; ... PowerShell ...)
* Analyze proxy logs (if available) or use Wireshark on Kali to inspect the HTTP headers.

🧪 Step 5: Use Wireshark/Zeek on Kali (Optional)

* Run Wireshark with:
* ip.addr == <Windows-IP> && tcp.port == 8080
* You’ll see the HTTP GET request and response.
* Look at the User-Agent string in the request to identify unusual download behavior.