#### **Testing Procedure**

1. **Malware Preparation:**
   * Collect malware samples in a secure manner. Store them on an encrypted USB drive or a secure cloud storage location that you can access from the VMs.
2. **Environment Setup:**
   * Start each VM from its clean snapshot.
   * Update Malwarebytes, REMnux, and Flare VM tools to the latest versions.
   * Disable any shared folders between the host and the VMs to prevent accidental escape of malware.
   * On the Windows VMs, disable Windows Defender or any other antivirus software besides Malwarebytes to prevent interference.
3. **Testing:**
   * **On Malwarebytes VM:** Install malware samples one at a time, scan with Malwarebytes, and note the detection and removal process.
   * **On REMnux and Flare VM:** Use the tools available within these VMs to analyze the malware samples for behavior, network activity, and any changes made to the system.
4. **Logging and Documentation:**
   * Document every step taken during the testing, including installation of tools, malware behavior observations, and any issues encountered.
   * Use the logging features of REMnux and Flare VM to capture detailed analyses of the malware samples.
5. **Clean-up:**
   * After testing each malware sample, revert the VMs back to their clean snapshots. This ensures no residual malware remains.
6. **Review and Analysis:**
   * Compile and analyze the data collected during the testing. Compare the effectiveness of Malwarebytes against the in-depth analysis capabilities of REMnux and Flare VM.

#### **Post-Testing**

1. **Secure Storage of Malware Samples:** Ensure all malware samples are securely stored or destroyed according to best practices.
2. **Final Review:** Consolidate findings, observations, and any recommendations for future testing.
3. **Report Preparation:** Prepare a detailed report based on the testing procedure, findings, and analysis.