Malware Analysis

Assignment 2

Objective: To set up a sandbox environment and run a malware sample with monitoring similar to Process Monitor, here is a detailed approach suitable for your Kali Linux and Windows VM-based malware analysis lab:

Step 1: Set Up a Sandbox Environment

- Use virtualization software like VMware or VirtualBox to create a dedicated Windows VM because Process Monitor runs on Windows.
- Install a clean Windows OS in the VM and take a snapshot to revert to a clean state after analysis.
- Isolate the VM network (host-only or no network) to prevent malware escape.
- Install malware analysis tools in the VM such as Process Monitor (Procmon) from Sysinternals, Wireshark for network monitoring, and a sandbox program like Sandboxie or Firejail for Linux sandboxing if needed.

Step 2: Run Process Monitor

- In the Windows VM, run Process Monitor (Procmon.exe).
- Clear existing logs (Ctrl + X) to start fresh.
- Configure filters to only focus on your malware sample process (filter by Process Name).
- Start capturing events (file system, registry access, network calls, process/thread activity).
- Execute the malware sample inside the VM.
- Let it run for enough time to trigger behaviors.
- Stop capturing (Ctrl + E).

Step 3: Monitor Behavior

- Observe logs for suspicious activity including:
    - Files created, modified, or deleted by malware.
    - Registry keys added, deleted, or changed for persistence.
    - Network connections or DNS queries attempted.
    - Process spawning or injection behaviors.
- Use filters in Procmon to focus on relevant events tied to the malware.

Step 4: Document Suspicious Behavior

- Save the Procmon captured event logs (File → Save).
- Note down suspicious file and registry changes with their timestamps.
- Log any unusual network communication attempts or external IPs contacted.

- Document any persistent techniques used by malware (auto-run registry keys, scheduled tasks).
- Take screenshots or export logs for thorough documentation.

Additional Tools on Kali Linux

- Use Wireshark or tcpdump for network traffic capture.
- Use Linux alternatives to Procmon like ProcMon for Linux or tools like strace, auditd for monitoring processes on Linux side.

Summary

Step	**Description**
Create VM sandbox	Isolated Windows VM with clean snapshot
Install Procmon	Sysinternals Process Monitor for Windows
Start monitoring	Clear old logs, set filter on malware process
Run malware sample	Execute inside VM, capture behaviors
Analyze logs	Observe file, registry, network suspicious activity
Document findings	Save event logs, note suspicious behaviors

This method combines the best practice of dynamic malware analysis, giving you visibility into file system, registry, and network activities safely.