WhisperSuite Test Execution Log – GhostISO + LinuxPDF

Timestamp: 2025-03-29 10:14:58
Environment: Operator End-to-End Flow
Self-Destruct: Disabled

1. **BuildDeployWhisper**

   - Successfully compiled GhostKey.dll, WraithTap.exe (Release|x64)

   - Packaged modules and stagers to \WhisperSuite_Build

   - Polymorph completed → Payload variant: GhostKey_R19.dll, WraithTap_R19.exe

2. **CreateGhostISO.ps1**

   - Located oscdimg.exe in E:\WhisperSuite\Tools\CreateGhostISO

   - Copied TinyCore + isolinux → E:\WhisperSuite\Tools\CreateGhostISO\boot\isolinux

   - Command:

     ```mathematica
     CopyEdit
     E:\WhisperSuite\Tools\oscdimg.exe
       -bE:\WhisperSuite\Tools\CreateGhostISO\boot\isolinux\isolinux.bin
       -h -lGHOST_BOOT -m
       E:\WhisperSuite\Tools\CreateGhostISO
       E:\WhisperSuite\Tools\CreateGhostISO\ghost_boot.iso
     ```

   - **[✓]** ghost_boot.iso successfully generated

3. **GhostWhisperBootstrap**

   - Modules loaded: GhostResidency, ExorcistMode, GhostLogger, Wormhole, LinuxPDF_Emu, LinuxPDF_Runtime, etc.

   - **[AnomalyHunter]** scanned system drive; no critical anomalies found

   - Operator Menu → Option [5] selected: "Run GhostLinux VM"

4. **LinuxPDF.exe**

   - Args: `--boot="E:\WhisperSuite\Tools\CreateGhostISO\ghost_boot.iso"`

   - Found qemu-system-x86_64.exe

   - **[LinuxPDF]** Launch QEMU with: `-m 512 -cdrom "ghost_boot.iso" -boot d -enable-kvm`

5. **QEMU Boot**

   - Booting `ghost_boot.iso` → TinyCore + isolinux

- **ghost_script.sh** auto-invoked in ephemeral environment

- **Anoint** Phase: Found 12 suspicious binaries in /tmp/test; logged to /home/tc/ghost_ops_log.txt

- **Bind** Phase: Suspended 2 processes named suspiciousd

- **Cleanse** Phase: Overwrote & removed 4 .exe artifacts

- Exorcism complete; VM shut down

6. **GhostResidency** (host)

   - Received `COMMAND=LOG` from .ghost.cfg

   - [GhostLogger] monitoring user interactions…

   - Found ghost user opened `C:\Sensitive\report.docx` at 10:33:02

   - [GhostSeal] created `loot_20250329_GK.enc.zip`, dropped hidden at `C:\Users\RedTeam\AppData\Local\Temp\.logs\.hidden\`

7. **Wormhole Listener**

   - Operator triggered Start-WormholeListener for memory-based lateral pivot

   - Valid ephemeral credentials from domain GhostTag_R19

   - Uncontrolled replication gating enforced

8. **Exfil + Cleanup**

   - Operator placed `COMMAND=EXFIL` in .ghost.cfg → GhostHollow stashed final loot

   - [SilentBloom.ps1] run → logs, keys, temp artifacts wiped from disk

   - All tasks removed, mission complete

Final State

- The ephemeral TinyCore environment in QEMU performed anoint/bind/cleanse.

- Host side sealed and exfiltrated with no permanent footprints.

- System cleaned after final command.

- Operator stands by for next mission.