WhisperSuite: Ghost Operator Handbook

1. Introduction
WhisperSuite is a covert red team operations toolkit built for stealth, deception, and precision.
It is designed for high-impact simulations and advanced adversary emulation. Built in memory of Raven,
it represents a spirit that walks unseen, leaving only whispers behind.

2. Operational Doctrine
Ghost Operators adhere to strict stealth doctrine:
- Move silently, leave no trace.
- Persistence must not compromise secrecy.
- Blend into trusted flows: Active Directory, BLE devices, user impersonation.
- Prioritize payload polymorphism to evade pattern-based detection.
- Encrypt everything—leak nothing.

3. Setup & Deployment
Prepare your device:
- Load `WhisperSuite_Build` onto USB or Flipper Zero.
- Configure BLE broadcasting app (GhostWhisperer).
- Deploy `BLETrigger.ps1` or use Flipper USB injection.
- (Optional) Build & place `ghost_boot.iso` + `LinuxPDF.exe` if ephemeral VM scanning is desired.

4. Execution Phases
1) Trigger via BLE or USB (BLETrigger.ps1) or wormhole operator gating.
2) GhostResidency deploys modules: Logger, Seal, Hollow, Wormhole, Pivot.
3) Polymorph (GhostPolymorph) generates unique variants per host.
4) Commands are pulled from `.ghost.cfg` with signature validation.
5) Optionally, ExorcistMode and LinuxPDF virtualization can remove hostile or unwanted files in an ephemeral environment.

5. Command Reference
- LOG → Launch GhostLogger
- SEAL → Encrypt accessed files via GhostSeal
- EXFIL → Archive & stash payload using GhostHollow
- PIVOT → Attempt AD impersonation & lateral movement (GhostPivot)
- WIPE → Erase all traces of operation
- ANOINT / BIND / CLEANSE → ExorcistMode sub-commands for scanning and removal

6. Field Tactics
- Avoid launching during known audit windows.
- Physically plant BLE beacon near air-gapped terminals if required.
- Validate file clicks before sealing or exfiltrating.
- Use signed `.ghost.cfg` commands for control under surveillance.
- Use `LinuxPDF.exe --boot ghost_boot.iso` for ephemeral scanning if extra stealth is needed.

7. Deconfliction & Safety
- Never reuse polymorphic payloads.
- Enable Self-Destruct in GhostKey.dll for high-risk targets.

- Wipe logs using SilentBloom.ps1 after mission completion.
- Exfil into hidden USB paths with benign file names.
- Operator gating enforces no uncontrolled self-replication.

8. Appendices
- BLE Recon Cheat Sheet
- AD & Impersonation Command Cheat Sheet
- Signature Format (HMAC-SHA256)
- GhostTag Convention: per-user, per-host rotation
- Timestamp-based encryption logic reference
- Creating & Booting ghost_boot.iso with CreateGhostISO.ps1 & LinuxPDF.exe

GhostWhisper Suite – Operator Handbook (Updated 2025-03-29)
■ New Integrations:
- ExorcistMode (Anoint, Bind, Cleanse) for optional malware removal
- LinuxPDF virtualization (ghost_boot.iso) for ephemeral root-level environment
- AnomalyHunter & AnomalyDetector for advanced threat detection
- Wormhole protocol with defensive triggers & operator gating
- Polymorphic deployment across memory-only injection

For Raven.