Whisper Suite Operator Mission Brief

OBJECTIVE:
- Deploy implant via USB or BLE to compromised target.
- Optionally run ephemeral scanning in LinuxPDF VM with ghost_boot.iso.
- Trigger logging, encryption, and exfil via remote .ghost.cfg.
- Retrieve encrypted archive via hidden drop or USB.

FIELD CHECKLIST:
[ ] USB contains WhisperSuite_Build (including GhostKey.dll, WraithTap.exe)
[ ] If ephemeral scanning is desired, also includes ghost_boot.iso + LinuxPDF.exe
[ ] Target machine is live and accessible
[ ] (Optional) Shell.exe running (for injection)
[ ] .ghost.cfg with valid commands (LOG, SEAL, EXFIL, PIVOT, etc.)

RED TEAM FLOW:
1. Launch `GhostWhisperBootstrap.ps1` from USB
2. Use operator menu to select desired actions or run ExorcistMode
3. Wait for command execution (up to 2 min for pulses)
4. Collect loot archive from hidden folder (or ephemeral VM logs if used)
5. If needed, drop .ghost.cfg with COMMAND=WIPE to scrub

STAGE COMMANDS:
- COMMAND=LOG → Begin ghost user file logging
- COMMAND=SEAL → Encrypt logged file interactions
- COMMAND=EXFIL → Archive + drop encrypted loot
- COMMAND=WIPE → Remove all traces of operation
- ExorcistMode → (ANOINT/BIND/CLEANSE) to forcibly remove hostile data in memory or ephemeral VM

Stay stealthy. For Raven.