

VERITAS — COMPLETE v1.0

The witness that cannot be bribed.

GitHub: <https://github.com/priyajyadav8-crypto/veritas>

Kali Bug Tracker: <https://bugs.kali.org/view.php?id=9695>

Proof — Diamorphine Rootkit Detected

```
[*] /proc readdir sees: 191 processes [*] Brute force scan finds: 726 PIDs [*] Known
threads: 725 [!] 1 HIDDEN PROCESS(ES) DETECTED! [!] PID 9201 - sleep - sleep 1000
VERDICT: COMPROMISED - anomalies detected Rootkit: Diamorphine Kernel:
6.12.88+deb13-amd64 (Debian 13) ps could not see PID 9201. Veritas caught it.
```

Environment

Item	Value
Dev OS	WSL2 Ubuntu — kernel 6.6.114.1-microsoft-standard-WSL2
Test OS	Debian 13 GNOME in VirtualBox
Test Kernel	6.12.88+deb13-amd64
Rust	Nightly toolchain
eBPF Library	Aya (pure Rust)
Binary	2.7MB static musl — no dependencies
GitHub	https://github.com/priyajyadav8-crypto/veritas
eBPF probe	tracepoint on syscalls/sys_enter_getdents64

Build Commands

Build eBPF:

```
cargo +nightly build --package veritas-ebpf --target bpfel-unknown-none -Z
build-std=core
```

Build debug:

```
cargo build --package veritas
```

Build static release:

```
cargo build --package veritas --target x86_64-unknown-linux-musl --release
```

Run:

```
sudo ./target/debug/veritas --diff
```

JSON:

```
sudo ./target/debug/veritas --json
```

Push:

```
git add . && git commit -m 'message' && git push
```

Complete Feature List

- [ok] eBPF loads and attaches to kernel via tracepoint
- [ok] Three-method hidden process detection with thread filtering
- [ok] Hidden network socket detection via inode cross-reference
- [ok] Hidden file detection and critical path checks
- [ok] LD_PRELOAD injection check
- [ok] Rootkit module name scanning
- [ok] Critical path permission checks
- [ok] Suspicious path detection
- [ok] PID 1 maps scan for injected libraries
- [ok] --diff flag (human readable output)
- [ok] --json flag (machine readable, pipeline ready)
- [ok] --processes --network --fs individual flags
- [ok] Full JSON report with verdict field
- [ok] 2.7MB static binary via musl (no dependencies)
- [ok] Man page (veritas.1)
- [ok] README on GitHub
- [ok] GPL-2.0 license
- [ok] PROOF: Diamorphine PID 9201 caught on Debian 13 kernel 6.12
- [ok] Submitted to Kali Linux bug tracker

How to Resume in New Chat

Upload this PDF to Claude and say: Resume building veritas from this progress PDF. Open WSL2 and navigate to ~/veritas.

Confirm environment:

```
cd ~/veritas && cargo build --package veritas && sudo ./target/debug/veritas --diff
```