# ANTONIUS

*IT Security Researcher · Electronic Engineer · Roboticist · AI/ML Practitioner*

antonius@bluedragonsec.com | bluedragonsec.com
github.com/bluedragonsecurity | Tangerang, Indonesia
Twitter: @bluedragonsec | Medium: @w1sdom | 0x00sec: w1sdom

## PROFESSIONAL SUMMARY

Multi-disciplinary security professional with 10+ years of hands-on experience spanning offensive security research, Linux kernel exploitation, hardware engineering, robotics, and applied AI/ML. Founder of Blue Dragon Security, an independent research page conducting advanced vulnerability research, 0-day discovery, and custom security hardware development in collaboration with intelligence-aligned organizations in Indonesia.

Recognized CVE discoverer with active contributions to the Linux kernel security community via LKML and direct maintainer engagement. Combines deep expertise in low-level systems — from kernel internals and x86 exploitation to RF hardware and custom IoT fabrication — with modern deep learning capabilities, producing a rare cross-disciplinary profile across both offensive and defensive security domains.

## CORE COMPETENCIES

| | |
|---|---|
| **Offensive Security** | Linux Kernel Exploitation, Heap Exploitation, ROP Chains, SMEP/SMAP/KASLR Bypass, x86/x64 Assembly, Fuzzing (Syzkaller), CVE Research & 0-day Discovery |
| **Kernel / Systems** | Linux Kernel Internals (SLUB Allocator, VMA/mm, io_uring, mseal), LKM Development, KASAN/KCOV, GDB/GEF, QEMU Lab Environments |
| **Hardware & RF** | PCB Design & Fabrication, RTL-SDR / HackRF / BladeRF, SIM Card Attacks, Custom Intelligence Hardware, IoT Device Fabrication |
| **Robotics** | Autonomous Robot Design & Programming, Embedded Systems, Sensor Integration, Motor Control, Custom Robotic Platforms |
| **AI / Deep Learning** | Deep Learning (TensorFlow/PyTorch), Computer Vision, Transformers, Mamba, AI-assisted Security Tooling |
| **Programming** | C, C++, Python, x86/x64 Assembly, Java (android studio), PHP, JavaScript, Rust (analysis) |
| **Platforms** | Linux (primary), Freebsd, Android (security research), IOS, QEMU, ARM/x86 embedded systems |
| **Other Skills & Knowledges** | Math, chess, playing musical instruments (guitar fingerstyle & keyboard), martial art (muay thai, taekwondo, boxing, bjj) |

## CVE DISCOVERIES & VULNERABILITY RESEARCH

| CVE / Finding | Description | Year |
|---|---|---|
| `CVE-2026-23416` | Linux Kernel mm/vma.c:830 — VM_WARN_ON_VMG invariant violation via mseal(2) spanning VMAs with mixed VM_SEALED states. Affects Linux 6.17 through 7.0-rc5. Discovered via Syzkaller fuzzing; fix acknowledged and submitted by Lorenzo Stoakes (Oracle) within hours of disclosure. | *2026* |

| | | |
|---|---|---|
| **LiteDNS OOB Read** | Out-of-bounds read vulnerability in LiteDNS server. Full PoC, CVSS analysis, and responsible disclosure completed. | *2026* |
| **buptLab dns_relay** | Remote heap-based buffer underflow in buptLab dns_relay_server. PoC exploit demonstrating remote trigger without authentication. | *2026* |
| **CVE-2026-27831** | Heap based buffer over read in rldns dns service | *2026* |

**Ongoing Research:** Active Syzkaller fuzzing campaigns on Linux 7 rc5 targeting io_uring ZCRX, io_uring BPF_TOKEN, mseal syscall. Multiple UAF and slab-out-of-bounds crashes identified; Netfilter UAF (nf_hook_entry_head) under investigation.

## PROFESSIONAL EXPERIENCE

### IT Security Researcher

**Blue Dragon Security (bluedragonsec.com)** · *2023 – Present* · *Tangerang, Indonesia*

- Lead original vulnerability research: kernel fuzzing with Syzkaller, PoC development, CVE reporting, and responsible disclosure to Linux kernel maintainers
- Conduct advanced kernel exploitation: ROP chain development, heap UAF exploitation (SLUB), SMEP/SMAP/KASLR bypass on Linux 5.15 and 6.x/7.0 in QEMU lab environments
- Design and fabricate custom intelligence hardware: counter-surveillance equipment, RF interception devices, specialized IoT security sensors for field deployment
- Develop deep learning models for security applications including anomaly detection and computer vision on embedded/edge devices
- Build and publish autonomous robot platforms and custom IoT devices (YouTube: robotsoft, antoniusringlayer)
- Publish technical security research on Medium (@w1sdom), 0x00sec, Packet Storm Security, CXSecurity, and bluedragonsec.com

### Security Curriculum Developer & Trainer

**Brimob — Collaboration** · *2026* · *Indonesia*

- Designing Security Researcher Master Class covering: Kernel Exploitation (UAF, ROP, SMEP bypass), Hardware Hacking, Web Security, and Network Penetration Testing
- Providing hands-on lab environments and exploit development training for intelligence agency personnel
- Training materials published (subset) at github.com/bluedragonsecurity/docs in Indonesian and English

### IT Security Researcher & Penetration Tester

**BNPT (**National Counter Terrorism Agency**)** · *2013 – 2015* · *On Site / Indonesia*

- Network security assessments, protocol analysis, and infrastructure hardening recommendations
- Custom security tool development: fuzzers, OSINT frameworks, exploit scaffolding

### IT Security Researcher

**Codewall Security** · *2012 – 2013* · *Remote / Indonesia*

- Network security assessments, protocol analysis, and infrastructure hardening recommendations
- Custom security tool development: fuzzers, OSINT frameworks, exploit scaffolding

### Electronic Engineer & Robotics Developer

**Independent / Contract Projects** · *2013 – Present* · *Tangerang, Indonesia*

- Design and manufacture custom PCBs for robotics, IoT, and intelligence hardware applications

- Build fully autonomous robot platforms with sensor fusion, computer vision, and real-time motor control
- Create AI-powered embedded systems combining deep learning inference with custom hardware for field deployment

## NOTABLE PROJECTS & PUBLICATIONS

### Kernel Security Research

- (CVE on progress) Linux Kernel 7.0 VMA/mseal bug discovered via Syzkaller; acknowledged and patched by Lorenzo Stoakes (Oracle) on the same day as disclosure via LKML
- Linux Kernel ROP Exploit Chains — Fully working ROP chains on Linux 5.15 and 6.x with SMEP bypass, developed and verified in QEMU/GDB/GEF lab
- Dirty Pipe Variant Research — Extended CVE-2022-0847 with custom dirtypipe2.c exploring variant attack surfaces (bluedragonsec.com/files/dirtypipe2.c)
- Linux Kernel 7.0-rc1 – Linux Kernel 7-rc3 Vulnerability Documentation — github.com/bluedragonsecurity/Linux_Kernel_v7.0-rc1_Vulnerabilities

### Intelligence Hardware & IoT Devices

- Custom counter-surveillance hardware for intelligence agency deployment: RF detection, signal analysis, and covert monitoring devices — designed and fabricated in-house
- Hacking hardware tools: custom-built devices for physical penetration testing and red team operations
- IoT security research platforms: custom-fabricated embedded sensors for field security assessments
- Robotics portfolio: multiple autonomous robot designs documented at youtube.com/antoniusringlayer and youtube.com/robotsoft

### Software & Security Tools

- Android security app — persistent background screen capture with FTP upload and MediaProjection API token handling
- Custom Syzkaller syzlang descriptions for io_uring ZCRX and mseal syscall fuzzing campaigns

### Published Security Research

- Technical articles on Medium (@w1sdom): kernel exploitation techniques, CVE deep-dives
- Exploit publications on Packet Storm Security and CXSecurity: packetstorm.news/files/author/10292/1
- 0x00sec community contributions: SEH exploitation, Linux ret2user and arbitrary function pointer call techniques
- Documentation portal: bluedragonsec.com/docs — userspace exploitation (ASLR/PIE bypass), kernel exploitation, IT security training materials

## TECHNICAL EXPERTISE — DEEP DIVE

### Kernel Exploitation & Modern Mitigations Researches :

- Bypass techniques: KASLR, FG-KASLR, SMEP, SMAP, KPTI, CR4 pinning, SLAB_FREELIST_RANDOM, Stack Canaries
- Linux 7.0 mitigation landscape: ML-DSA post-quantum module signing, stricter eBPF verifier, BPF SELinux token for io_uring, FineIBT documented attack surface
- Fuzzing infrastructure: Syzkaller with custom syzlang, KASAN/KCOV-enabled kernels, multi-VM QEMU campaigns, 46K+ coverage edges achieved

### RF, Hardware & Intelligence Devices:

- RTL-SDR, HackRF,protocol reverse engineering
- SIM card security: cloning research, protocol-level attack analysis
- wifi hacking device development

## ONLINE PRESENCE & VERIFICATION

| | |
|---|---|
| **Security Research** | bluedragonsec.com \| github.com/bluedragonsecurity \| cve.org (search: bluedragonsecurity) |
| **Publications** | packetstorm.news/files/author/10292/1 \| cxsecurity.com/author/antonius/1 \| medium.com/@w1sdom |
| **Community** | forum.0x00sec.org/u/w1sdom \| sw0rdm4n.wordpress.com |
| **Hardware / Robotics** | youtube.com/robotsoft \| youtube.com/antoniusringlayer |
| **Code Repositories** | github.com/bluedragonsecurity \| github.com/antoniusrobotsoft |

## EDUCATION & CERTIFICATION

| | |
|---|---|
| **Education** | none |
| **Certification** | none |