Antonius – IT SECURITY RESEARCH BASED IN INDONESIA

bluedragonsec.com – blue dragon security vulnerability research

Antonius (w1sdom) is an it security researcher (hacker) based in Indonesia, focusing on low level vulnerability research (linux userland vulnerability, linux kernel vulnerability, android vulnerability, ios & mac os vulnerability) - combined with electronic,robotics & ai (deep learning) for security.

IT Security Researcher based in Indonesia. Linux Kernel. Android & IOS (vulnerability research & exploit development) Other Skills : electronic, intelligence device development, robotics, hardware hacking, counter surveillence device development, deep learning

Fuzzing Tools : syzkaller, honggfuzz, libfuzzer, spike, afl++, Jackalope, kAFL
Static Source Code Analysis : Smatch, Infer,Error Prone

Other capabilities : infrastructure pentest, web application pentest, etc…

Curriculum Vitae

https://github.com/bluedragonsecurity/docs/blob/main/antonius_curriculum_vitae.pdf

Legal Penetration Testing Track Record
- radical moslem web penetration testing (instructed by national agency of counter terrorism)
- esdm network pentest
- lippo group & meikarta pentest
- psdg pentest
- ksei pentest
- idnplay penetration testing
- gambling site penetration testing

etc …

Penetration Testing Track Record (before 2014) :
- foreign ISP intrusions (instructed by intelligence agency)
- indonesia & malaysia domain registrar intrusion
- some indonesian hacker's server & web intrusion
- some us hacker's server intrusion

etc ...

"highly capable intruder, silent intrusion, advanced persistent threat, nation state"

Data :
https://www.bluedragonsec.com
https://github.com/bluedragonsecurity
https://github.com/antoniusrobotsoft
https://bluedragonsec.com/docs/
https://bluedragonsec.com/docs-en/
https://bluedragonsec.com/var/robotic/
https://bluedragonsec.com/var/math/

https://bluedragonsec.com/var/ai/
https://medium.com/@w1sdom
https://www.youtube.com/antoniusringlayer
https://lore.kernel.org/all/?q=bluedragonsecurity
https://packetstorm.news/files/author/10292/1

cve discovery :
CVE-2026-23416 – linux kernel mseal invariant violation

https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.18.21
https://lore.kernel.org/all/CAK8a0jwWGj9-SgFk0yKFh7i8jMkwKm5b0ao9=kmXWjO54veX2g@mail.gmail.com/
https://www.cve.org/CVERecord?id=CVE-2026-23416

CVE-2026-27831 - rldns Vulnerable to Heap-based Out-of-Bounds Read

https://www.cve.org/CVERecord?id=CVE-2026-27831
https://github.com/bluedragonsecurity/rldns
https://github.com/bluedragonsecurity/rldns/security/advisories/GHSA-fv38-45j4-g9x4
https://github.com/bluedragonsecurity/rldns-1.3-heap-out-of-bounds-vulnerability-fixed-in-rldns-1.4
https://medium.com/@w1sdom/heap-based-buffer-over-read-vulnerability-in-rldns-1-3-5da3bccdc031

```
slab cross-cache confusion in skb_free_head
linux kernel 7.0.0-rc5, triggered via BPF_PROG_TEST_RUN with [redacted]
BPF_PROG_TYPE_SCHED_CLS.[redacted]
```

https://lore.kernel.org/all/CAK8a0jxC5L5N7hq-DT2_NhUyjBxrPocoiDazzsBk4TGgT1r4-A@mail.gmail.com/

remote heap based buffer underflow at buptlab dns relay server
https://medium.com/@w1sdom/remote-heap-based-buffer-underflow-vulnerability-at-buptlab-dns-relay-server-bac6505070a9

Antonius (w1sdom) – bluedragonsecurity.com is the first indonesian it security researcher (hacker) who discover and report linux kernel vulnerabilities with cve track record

known for :

xingyiquan linux kernel 2.6 & 3.x rootkit
https://github.com/bluedragonsecurity/xinyiquan-rc

Xingyiquan is legendary lkm rootk1t for linux kernel 2.6.x and 3.x developed in 2014

Developed by Antonius a.k.a w1sdom a.k.a Sw0rdm4n (@sw0rdm4n) a.k.a Ringlayer

www.bluedragonsec.com
https://github.com/bluedragonsecurity

THIS OLD LKM ROOTKIT FEATURED IN :

https://dl.acm.org/doi/fullHtml/10.1145/3458903.3458909
https://eprints.glos.ac.uk/4158/8/Detection%20of%20Malware%20and%20Kernel.pdf
https://github.com/skyw4tch3r/RootKits-List-Download
https://opensource.com/article/18/4/linux-filesystem-forensics
https://www.cs.nthu.edu.tw/~ychung/Journal/2021-IEEE-TC.pdf
https://malware-unplugged.blogspot.com/2015/09/linux-memory-diff-analysis-using.html
https://scispace.com/pdf/big-data-based-security-analytics-for-protecting-virtualized-38bvjtwpzr.pdf
and so on ...