BRUNO DELNOZ

Offensive Cybersecurity Expert • Red Team • Ethical Hacker

30+ Years IT • 226+ Pentest Projects • Think Like Attacker

📍 Rochefort, Belgium • 📧 bruno.delnoz@protonmail.com • 📱 +32 456 882 457 💻 github.com/bdelnoz • 💼 linkedin.com/in/delnoz

OFFENSIVE PHILOSOPHY

Hacking isn't just technology - it's a mindset. 30 years of experience taught me that an attacker thinks differently: seeking blind spots, exploiting the unexpected, circumventing certainties. My strength? Combining technical expertise (226+ pentest projects) with human approach: OSINT, social engineering, reconnaissance. The code I've published (500+ GitHub stars) demonstrates this philosophy: offensive WiFi tools, privacy-first tools, behavioral analysis. A good red team doesn't just exploit CVEs - they think like the adversary to anticipate tactics.

RED TEAM MINDSET

Attacker Mindset

- □ **Think like adversary** : 30 years anticipating behaviors, circumventing defenses, exploiting blind spots
- □ **Permanent curiosity** : Daily CVE watch, exploring new vulnerabilities, testing system limits
- □ **Creative lateral thinking** : Finding unexpected vectors, combining vulnerabilities, chaining exploits
- □ **Systematic questioning** : "What if...?", challenging assumptions, testing every boundary
- □ **Relentless autodidact** : 30 years autonomous learning, hands-on experimentation, 500+ GitHub stars

Human Factor Security (OSINT & Social Engineering)

- □ **OSINT mastery** : Public information exploitation, passive reconnaissance, complete footprinting
- □ **Social engineering** : Psychological manipulation, phishing campaigns, pretexting, elicitation
- □ **Advanced reconnaissance** : Google dorking, Shodan, LinkedIn scraping, infrastructure mapping
- □ **Privacy-first approach** : Open source projects (Whisper local STT, zero cloud) demonstrate privacy understanding

Offensive Methodology

- □ **Kill chain execution** : Reconnaissance → Weaponization → Delivery → Exploitation → Installation → C2 → Actions
- □ **Persistence techniques** : Backdoors, rootkits, scheduled tasks, registry manipulation, service hijacking
- □ **Privilege escalation** : Kernel exploits, misconfigurations, credential dumping, token impersonation
- □ **Lateral movement** : Pass-the-hash, Kerberos attacks, SMB exploitation, network pivoting
- □ **Evasion & obfuscation** : AV bypass, EDR evasion, traffic encryption, covert channels

OFFENSIVE TECHNICAL SKILLS

WiFi Security (Production Tools)

- □ **cmd.airmon-dos v55** : Fast WiFi DoS + deauth attacks (GitHub public, Bash)
- □ **scripts-wifi-scan** : Complete airodump-ng automation suite, monitor mode, GPS, PCAP analysis
- □ **rtl88x2bu driver** : Custom WiFi driver (packet injection, AP mode, monitor mode, kernels 5.4-6.13)
- □ **Attacks** : WEP/WPA/WPA2/WPA3 cracking, Evil Twin, Rogue AP, KRACK, fragmentation attacks
- □ **Tools** : Aircrack-ng suite mastery, Wireshark deep packet inspection, Reaver/Bully WPS

Network Penetration Testing

- □ **Reconnaissance** : nmap NSE scripting, masscan, Shodan, DNS enumeration, OSINT gathering
- □ **Vulnerability scanning** : Nessus, OpenVAS, Nikto, custom scripts, CVE exploitation
- □ **Exploitation** : Metasploit Framework, custom exploits, buffer overflows, RCE chains
- □ **MitM attacks** : ARP spoofing, SSL stripping, DNS poisoning, session hijacking, credential capture
- □ **Packet analysis** : Wireshark expert, tcpdump/tshark, protocol dissection, traffic reconstruction

Application Security Testing

- □ **pentestAPK** : Android mobile app pentest (GitHub public)
- □ **Web attacks** : SQLi, XSS, CSRF, RCE, LFI/RFI, XXE, SSRF, deserialization
- □ **Tools** : Burp Suite Pro, SQLmap, OWASP ZAP, custom Python scripts
- □ **API security** : REST/GraphQL testing, authentication bypass, authorization flaws, rate limit bypass

Password Attacks & Credential Access

- □ **Cracking** : Hashcat GPU acceleration, John the Ripper, rainbow tables, wordlist generation
- □ **Credential dumping** : Mimikatz, LSASS extraction, SAM database, NTDS.dit, registry hives
- □ **Brute force** : Hydra multi-protocol, Medusa, custom scripts, timing optimization
- □ **Pass-the-hash** : NTLM relay, Kerberos attacks (Golden/Silver tickets), token impersonation

Offensive Scripting & Automation

- □ **Bash expertise** : 109+ production scripts, 25+ years experience, pentest workflow automation
- □ **Offensive Python** : 37+ projects, exploit development, custom tools, API abuse
- □ **NoXoZVorteX** : AI conversation analyzer (900+ convos) - data extraction capabilities demonstration
- □ **Payload creation** : Shellcode, obfuscation, polymorphic code, staged/stageless delivery

OPEN SOURCE PROJECTS (500+ GITHUB STARS)

Offensive Security Tools

- □ **cmd.airmon-dos v55** : Fast WiFi DoS automation (deauth, scan, recon) - github.com/bdelnoz
- □ **scripts-wifi-scan** : Complete Kali WiFi scanning suite (airodump-ng, GPS, PCAP)
- □ **pentestAPK** : Android application security testing
- □ **scan_security** : Security scanning suite (ClamAV, rkhunter, ports, processes)
- □ **rtl88x2bu** : Custom WiFi driver (injection, monitor, AP mode)

Privacy & OSINT

- □ **braveVTTextension v3.0** : Whisper local STT (100% privacy, zero cloud, 9+ languages) - privacy-first approach demonstration
- □ **NoXoZVorteX v2.7** : 900+ AI conversations analyzer (skill extraction, OSINT capabilities)
- □ **regles_contextualisation V110** : 98 master rules prompt engineering - LLM manipulation understanding

Infrastructure Hardening (Defense = Attack Knowledge)

- □ **iptables firewall** : SystemD auto-boot, strict rules - understanding defenses to better bypass them
- □ **usb_enc** : LUKS USB encryption automation
- □ **ssh_control** : SSH hardening & monitoring

RELEVANT EXPERIENCE

Freelance Consultant AI/ML & Security (2024-2025)

- **11 production applications** : Privacy-first AI tools, security conversation analysis
- **500+ GitHub stars** : Community recognizes offensive/defensive code quality
- **Open source contributions** : Pentest knowledge sharing, WiFi security, privacy tools

Axway Software - Senior Consultant (2007-2018, 11 years)

- **40+ middleware projects** : Integration expertise, API security, authentication (OAuth/SAML/JWT)
- **Infrastructure security** : Critical flow protection, transit encryption, PKI management
- **Certified trainer** : Security knowledge transmission, best practices, threat modeling
- **Multi-country** : France (Ministry of Finance under Macron), Belgium, Luxembourg, international

COMPLEMENTARY TECHNICAL SKILLS

Linux Systems (30+ years)

- **Kali Linux mastery** : Daily environment, complete customization, all pentest tools
- **Debian/Ubuntu** : Server administration, hardening, package management
- **Kernel** : Driver compilation, modules, performance tuning, kernel vuln exploitation

Languages & Frameworks

- **Bash** : 25+ years expert, 109+ production scripts, complete pentest workflow automation
- **Python 3** : 37+ projects, exploit development, web scraping, API abuse, ML/AI integration
- **JavaScript/Node.js** : Browser extensions, XSS payloads, prototype pollution
- **C/Assembly** : Shellcode, buffer overflows, reverse engineering, exploit primitives

Infrastructure & Cloud

- **Containers** : Docker escape techniques, privilege escalation, misconfigurations
- **CI/CD** : GitHub Actions, pipeline poisoning, secret extraction
- **Cloud** : AWS/Azure basics, S3 misconfigurations, IAM privilege escalation

Crypto & Forensics

- **Encryption** : LUKS, GPG/PGP, SSL/TLS, cryptanalysis basics, weak crypto detection
- **Forensics** : Memory analysis, disk imaging, timeline reconstruction, artifact recovery
- **Reverse engineering** : Ghidra, IDA Pro, binary analysis, malware dissection

CERTIFICATIONS & CONTINUOUS TRAINING

- **CCSP (in progress)** : 6 courses completed - Cloud security, cryptography
- **Autodidact** : 30 years autonomous learning, daily CVE watch
- **CTF participant** : Capture The Flag competitions, HackTheBox, TryHackMe
- **Bug bounty** : Ethical hacking, responsible disclosure, vulnerability research

VALUE PROPOSITION

Authentic Hacker Mindset

- □ **30 years experience** : Not theoretical - production tools used daily (WiFi, pentest, OSINT)
- □ **Think like attacker** : Portfolio demonstrates real offensive approach, not just compliance
- □ **Open source proof** : 500+ GitHub stars prove security community recognition

Rare Skills

- □ **Advanced WiFi offensive** : Production tools immediately deployable (cmd.airmon-dos, custom drivers)
- □ **Privacy-first approach** : Deep confidentiality understanding (Whisper local, zero cloud)
- □ **AI security** : Emerging expertise in prompt injection, LLM manipulation, AI adversarial attacks
- □ **Scripting mastery** : Pentest workflow automation, custom tools, rapid prototyping

Pragmatic Approach

- □ **No bureaucracy** : Autodidact, concrete solutions, measurable results
- □ **Knowledge transmission** : Certified Axway trainer, comprehensive project documentation
- □ **Adaptability** : 30 years tech evolution - mainframes → cloud → AI → quantum (next)
- □ **Ethics** : Responsible disclosure, open source contribution, privacy respect

ADDITIONAL INFORMATION

- □ **Location** : Rochefort, Belgium - Immediate availability
- □ **Languages** : French (native), English (professional - technical reading/writing C1)
- □ **GitHub** : github.com/bdelnoz - Public portfolio demonstrating skills
- □ **Web portfolio** : bdelnoz.github.io - Detailed technical CV
- □ **Security clearance** : Available upon request

30 Years IT • 226+ Pentest Projects • 500+ GitHub Stars • Think Like Attacker
📍 Rochefort, Belgium • 📧 bruno.delnoz@protonmail.com • 📱 +32 456 882 457 💻 github.com/bdelnoz • 💼 linkedin.com/in/delnoz