Daniel Andrade

Offensive Security Specialist | OSCP Certified

CONTACT & PRESENCE

Website: d4ni.me
LinkedIn: linkedin.com/in/anbapdan
GitHub: github.com/AnBapDan
Email: dani7andrade@protonmail.com
Location: Remote Available • Global Opportunities

SUMMARY

OSCP certified offensive security specialist with hands-on expertise in penetration testing, red team operations, and vulnerability research across embedded systems, aerospace, and critical infrastructure. Ability to identify exploitable vulnerabilities through advanced attack methodologies including post-exploitation, lateral movement, and Active Directory exploitation. Currently conducting security assessments for critical aerospace systems.

PROFESSIONAL EXPERIENCE

CYBERSECURITY EXPERT (Offensive Security)

Freelancer Cybersecurity Consultant @ **Osmium** | Remote | August 2024 – Present
Assessed a defense-in-depth embedded Linux distribution for the aerospace sector, engineering a hardened OS baseline from the ground up using Yocto Project. Worked on the full security lifecycle: from initial threat modeling to final implementation to delivering a "secure-by-design" platform that strictly enforces integrity and isolation in hostile environments.

Key Technical Achievements:

- Hardened Boot Chain: Implemented a full Hardware Root of Trust using Secure Boot and U-Boot signature verification within Yocto build recipes to prevent unauthorized code execution and firmware tampering.
- Immutable Root Filesystem: Deployed DM-Verity for transparent block-level integrity checking, ensuring the OS remains tamper-proof and audit-compliant in production environments.
- Resilient & Atomic Updates: Engineered a RAUC-based Secure OTA system with atomic A/B partitioning, cryptographic bundle signing, and automated rollback mechanisms to guarantee fail-safe patching even during power loss.
- Custom SELinux Policy Development: Translated threat models and aerospace security requirements into fine-grained SELinux policies, mapping user workflows and service behaviors into strict type enforcement rules and role-based access controls contexts.
- Zero Trust Access Control: Enforced a Zero Trust model with SELinux in Enforcing mode, utilizing custom policies to confine each service to minimal required permissions, eliminating lateral movement and reducing attack surface.
- Threat Modeling & Security Architecture: Conducted comprehensive TARA reviews using STRIDE and OWASP methodologies, translating theoretical attack vectors into concrete kernel hardening, policy enforcement, and userspace defenses.

- Build System & Supply Chain Security: Implemented secure Yocto build recipes with cryptographic verification, signed artifacts, and reproducible builds to ensure end-to-end integrity from source to deployment.

Technologies Used:

Embedded Linux (Yocto,Petalinux) | Kernel analysis tools | Custom exploitation development | Network assessment tools | Cryptographic vulnerability analysis

UNIVERSITY RESEARCHER – Cybersecurity & Blockchain Security

Researcher @ **Instituto de Telecomunicações** | Aveiro, Portugal | August 2020 – December 2023
Researched cryptographic security, consensus mechanism vulnerabilities, and attack vectors in COMSOLVE- a decentralized peer-to-peer energy trading platform using blockchain technology for renewable energy communities.

Key Technical Achievements:

- Blockchain Architecture: Implemented Hedera Hashgraph as the foundational consensus layer for immutable transaction settlement and audit trails, ensuring cryptographic integrity across all energy exchanges.
- Distributed Microservices Ecosystem: Built a gRPC-based microservices infrastructure enabling asynchronous, high-throughput communication between autonomous services (Transactions, Meters, Gateway).
- Payment & Settlement Engine: Developed the Transactions microservice to process real-time peer-to-peer energy payments with Hedera smart contracts, ensuring atomic settlement and dispute resolution.
- IoT Metering Integration: Engineered the Meters microservice to aggregate real-time energy consumption data from distributed smart meters, feeding accurate usage metrics into the settlement pipeline.
- API Gateway & Orchestration: Designed a RESTful Gateway exposing the entire REC (Renewable Energy Community) platform as a unified API, abstracting blockchain complexity for external integrations and frontend clients.
- Master's Research & Publication: Authored thesis on blockchain-based Renewable Energy Communities, contributing peer-reviewed research on decentralized energy markets and DLT scalability in IoT-heavy environments.

Research Areas:

Blockchain consensus mechanism security | P2P network attack vectors | Cryptographic protocol analysis
Energy trading platform security | Distributed systems threats | Transaction validation architecture

Technologies:

Blockchain platforms (Ethereum, Hashgraph) | Cryptographic libraries | P2P networking | Smart contract analysis

Contributions:

Raised and helped resolve issues `#1990` and `#1976` in the Hedera JavaScript SDK, improving reliability of client network configuration and error handling for downstream integrators.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP)

Credential: `https://www.credential.net/e022ed3e-0318-4ff5-9e2d-a263d37fd5b6`
Date Earned: [05/2024]
Advanced hands-on penetration testing certification requiring successful exploitation of live systems in controlled lab environment. Demonstrates mastery of reconnaissance, vulnerability identification, exploitation, and post-exploitation techniques across diverse attack scenarios.

Core Competencies

- **Offensive Security:** Penetration testing, red teaming, exploit development, vulnerability research,

post-exploitation, lateral movement, privilege escalation, Active Directory exploitation, payload development

- **Tools & Frameworks:** Metasploit, Burp Suite, Mimikatz, Bloodhound, Impacket, Hashcat, John the Ripper, Ghidra, custom Python/C tooling
- **Embedded & OS Security:** Embedded Linux hardening (Yocto, Petalinux), SELinux, secure boot, DM-Verity, U-Boot, cryptographic validation
- **Blockchain & Distributed Systems:** Blockchain/DLT security, smart contracts, consensus and P2P security, cryptographic protocols
- **Infrastructure & Networking:** Active Directory, network penetration testing, Linux administration, system hardening, network reconnaissance, OSINT

EDUCATION

Master's in Cybersecurity

Universidade de Aveiro | Portugal | 2021–2023

Bachelor of Science in Computer Engineering and Telematics

Universidade de Aveiro | Portugal | 2018–2021

High School

Escola Secundária Dr. Joaquim de Carvalho | Figueira da Foz, Portugal | 2014–2017

LANGUAGES

Portuguese — Native Proficiency

English — C1 Proficiency (CEFR Level)

- Listening: C1 | Reading: C1 | Writing: C1 | Spoken Production: C1 | Spoken Interaction: C1