

Andre Lima

RESEARCHER / RED TEAM SPECIALIST

Professional Summary

Researcher, **speaker** (Bsides Lisbon 2022, Bsides Oslo 2022 , 2023, 2026 , Sikkerhetsfestivalen 2023, 2024, 2025, TIBER-EU Provider Conference 2024, Bsides Kristiansand 2025, Vinterkonferansen 2026, Compliance Seminaret 2026, Bsides Hamburg 2026) and Red Teamer doing it (pentesting / red team) since 2011. Have worked in Portugal, Australia, and now settling with family in Norway (Oslo). My main areas of expertise are: Malware development for Red Teams, including Windows Kernel Rootkits, as well as bypassing EDRs; Reverse Engineering (WinDbg, IDA, x64dbg); Exploit development (bug hunting with WinDbg+IDA and writing remote exploits using python3); Red Team (cloud infrastructure setup and automation, and payload development and automation in C#/C++/C/assembly); Blackbox fuzzing, with qemu and developing my own emulators in C and Rust.

I mostly enjoy researching, figuring new things out, and publishing content at my blog https://medium.com/@0x4ndr3 and Youtube "jump call pop" channel.

Employment History

Red Team Leader, Telenor CyberDefence, Oslo

AUG 2025 — PRESENT

- Lead Red Team initiatives, ensuring technical quality assurance for all deliveries.
- Mentor team members, fostering career development and enhancing technical skills.
- Develop malware and conduct in-depth research to stay ahead of threats.
- Present findings at international conferences, showcasing expertise in Cybersecurity.

Team Leader in Cyber Ops - Senior Manager at Cyber & Digital Risk, Advisense, Oslo

NOV 2023 — AUG 2025

Leading a team of ethical hackers to improve and optimize penetration tests and red team engagements. Also doing research and payload development, focusing on EDR bypasses.

Manager in Risk Advisory Services (Red Team Operator), PwC Norway, Oslo

MAR 2022 — OCT 2023

- Windows Rootkit Development
- Windows malware and C2 development
- Research for AV bypass
- Red Team operation
- Infrastructure automation (terraform, ansible, python3)
- Payload generation automation (Roslyn, LLVM)

Senior Penetration Tester , Pure Security / Tesserent (Australia) https://pure.security/services/technical-assurance/, Melbourne

JUN 2017 — DEC 2021

- Reverse Engineering of Windows applications and internals
- Coordinate Red Team engagements
- Research and tool development
- Penetration Testing

Details

Oslo
Norway

NATIONALITY

Portuguese

Links

Presentations @ Conferences

Youtube channel: @0x4ndr3

Exploit-DB Shellcodes

Exploit-DB Papers

Twitter

LinkedIn

Blog

Personal website

Skills

- Leadership
- Communication Skills
- Research
- Fuzzing (blackbox)
- Maldev
- Reverse Engineering
- Exploit dev

Languages

- English
- Portuguese

Hobbies

Playing basketball, chess, tennis, and watching Formula 1.

- Physical recon and physical attack deployment

Team Leader Pentesting Team , Integrity S.A. (Portugal) , Lisbon

OCT 2016 — JUN 2017

- Coordinating team members
- Making sure analysis by different members render the same consistency throughout all clients' pentests done by the team
- Mentoring junior team members
- Guiding the creation of vulnerability templates for reporting
- Develop scripts (python+bash on github) that assist in guaranteeing consistency and efficiency throughout the pentesting process

Penetration Tester , Integrity S.A. (Portugal) https://keepitsecure24.com/, Lisbon

JAN 2011 — JUN 2017

Internship in Information Security Consulting , Integrity S.A. (Portugal) https://integrity.pt/, Lisbon

NOV 2010 — JAN 2011

Education

Undergraduate degree in Computer Science, Instituto Superior de Engenharia de Lisboa (ISEL), Lisbon

AUG 2003 — FEB 2009

Final project on monitoring system Nagios: https://www.andrelima.info/files/pfc.pdf

Speaking events - Conference presentations

Bsides Hamburg (Elbsides 2026), Hamburg, Germany

JUN 2026

Title: Pull the Plug: Kernel-Level Surgery to Blind EDRs

Modern EDR solutions are only as effective as the telemetry they can collect. This talk takes a methodical, kernel-level approach to understanding (and dismantling) every major sensor an EDR relies on to detect malicious activity. From ETW providers feeding threat intelligence data, to kernel callbacks registering process and image events, to minifilter drivers intercepting filesystem I/O, and WFP callouts gating network telemetry: each one is a wire that can be cut.
This is not an attack on Microsoft. It's a surgical dissection of Windows' own defensive instrumentation, from the perspective of a Red Teamer who needs operational silence. Through live reverse engineering of Windows internals and hands-on demos, attendees will leave with a concrete, layered plan for achieving full "sensor deprivation" against EDR products.

Vinterkonferansen 2026, Norway

JAN 2026

Title: Modern Advanced Cyber-Attacks (a practical demonstration) in 2026, and the Impact at the Threat Intel Level

Exploring how AI-powered systems, through relevant MCP servers, are transforming the threat landscape and what organizations need to know.

Sikkerhetsfestivalen 2025, Lillehammer

AUG 2025

Title: Malware detection... with type-1 hypervisors

In this presentation, I went through an explanation of how type-1 hypervisors work - more specifically Intel VT-X - and demoed a type-1 hypervisor (using HyperDbg) that transparently stopped an application from writing to memory (simulating malicious patching) and adulterating CPUID to trick applications into thinking they are running in a different environment.

Bsides Kristiansand 2025, Kristiansand

JUN 2025

Title: EDR Evasion 101: in a professional hacker Red Team

In this session, I dived into practical techniques for bypassing both static and dynamic analysis within modern Endpoint Detection and Response (EDR) solutions. I started by exploring how to select the right programming language to outmaneuver automated detection, then shifted gears to writing my own x86_64 assembly that stays under the radar. This talk is intended as a foundational guide - leaving the deeper complexities of kernel and hypervisor development for more advanced sessions - so attendees can walk away with a solid “101” understanding of EDR evasion.

Sikkerhetsfestivalen 2024, Lillehammer

AUG 2024

Title: High performance fuzzing

Showed how to develop a fuzzer by writing my own, start with a simple but obviously slow implementation, and start adding techniques to it to make it faster and faster. These techniques require a deep technical understanding of how the Operating System works, but also how the CPU works. I'll be giving detailed explanations about how to use all CPU cores, how to make sure no time is wasted in the kernel (syscalls), and why is that important, but also write your own fuzzing emulator and how to write faster assembly code that will speed it up. The results in speed will be mind blowing! This will all be put into context at the beginning of the talk, in order for you to understand that speed is, however, just one variable in designing a great fuzzer.

Bsides Oslo 2023, Oslo

SEPT 2023 — SEPT 2023

Title: Red Team (infrastructure & payload dev) automation

In this presentation, I went through details of automating Red Team infrastructure with Terraform/Ansible and a Python3 wrapper, its security, as well as the automation of payload generation and auto-rewriting of existing code with Roslyn for existing C# projects (Rubeus, Sharphound, Seatbelt, etc). I also went through the DevOps setup to auto build and retrieve the artifacts. The slides can be found here and more details on the presentation, here. As soon as the video is available, I'll share as well.

Sikkerhetsfestivalen 2023, Lillehammer

AUG 2023

Title: **Advanced malware in 2023. How prepared are you?** (30m)

The talk aimed to address the maturity level of companies in Norway in a world where cyber warfare seems to be the new standard, while the country holds very relevant infrastructure that must be kept safe for obvious reasons. I addressed defensive teams (Blue Teams) and people responsible for the security of their companies, and question how prepared they are for new trends of attacks, including malware running in the Windows kernel, and even at a lower level, and analyze how more and more malware are slowly getting into this more advanced stage. The presentation included practical demos of some of the advanced capabilities that such malware possesses, while running trusted proof-of-concepts developed internally through research.

The slides can be found here.

Bsides Lisbon 2022, Lisbon

NOV 2022

Title: **Windows Kernel Rootkit for Red Teams** (45 m)

Description: Adding on to the presentation in Bsides Oslo in May, I've added a brief section on Bring Your Own Vulnerable Driver (**BYOVD**), as well as show a new command and control mode where the keylogger is used to control the driver. **After the keylogger is enabled, if any user in any session types 666 <enter>, it will interpret whatever is typed before the next <enter> and will execute the command. The slides and video can be found here**.

Bsides Oslo 2022, Oslo

MAY 2022 — MAY 2022

Title: **Life in the Windows Kernel for Red Teams** (45 m)

Description: In this presentation, Andre will go through details of not only things to consider when developing in the kernel but, most importantly, things to consider when developing malware for the Windows kernel. He'll explain synchronization when the Operating System is not cooperating with you, Direct Kernel Object Manipulation (DKOM), and finally show demos on a rootkit he's constantly developing, doing the following: **Hide a process by PID; Hide a process by name (full name > 15 characters); Hide a process by name whenever it's created; Hide a driver/rootkit; Elevate privileges from any process given their PID; Auto attaching to all and new RDP sessions and keylogging each of them. Slides and video can be found here.**

TIBER-EU Provider Conference, Düsseldorf

NOV 2024

Title: **Not all TIBERs are made equal - The rare ability to develop advanced malware in 2024**

Spoke at the TIBER-EU Provider Conference held at Deutsche Bundesbank in Düsseldorf. I showcased some advanced malware development capabilities, and emphasized their critical role in testing clients concerned about state-sponsored threats. At the same time, I challenged my peers to rethink some common practices, like the overemphasis on password-grabbing phishing campaigns.

Slides: here

Certifications

Offensive Security Exploit Developer (OSED)

JUN 2021 — PRESENT

https://www.credential.net/bcec194d-a199-455c-9719-5851fbaa7be2

eLearnSecurity Certified Reverse Engineer (eCRE)

APR 2020 — PRESENT

https://andrelima.info/files/ecre.pdf

Offensive Security Certified Professional (OSCP)

JUL 2015 — PRESENT

https://www.credential.net/d49fc58e-6bb3-4236-ac10-029cba9dd5a9

x86_64 Assembly Language and Shellcoding on Linux Expert (SLAE64)

FEB 2018 — PRESENT

https://andrelima.info/files/slae64.pdf

ISC2 Associate CISSP

MAY 2011 — MAY 2012

Do reach out for validation, please.

Courses

Windows Kernel Rootkits (by Bruce Dang), Offensivecon 2019

FEB 2019 — FEB 2019

Fuzzing for Vulnerabilities, Huntress Labs (BlackHat USA 2018)

AUG 2018 — AUG 2018

Hypervisor Development for Security Researchers, Offensivecon 2023

MAY 2023 — MAY 2023