anatomicys@gmail.com
Research Blog
Github

Yordan Stoychev

Passionate security researcher driven by the desire for improvement and the chase for knowledge. Always ready to deep dive into any code base and research alike. Experienced in analysing and exploiting complex vulnerabilities. Broad spectrum of skills and experience, from conducting web penetration tests to writing complex kernel exploits.

EXPERIENCE

OtterSec — *Security Researcher*

February 2025 - Present

PricewaterhouseCoopers Bulgaria — *Penetration Tester*

Associate | April 2024 - January 2025

- Enhanced the internal infrastructure of the offensive security team.

Intern | September 2023 - March 2024

- Familiarised myself with a wide range of targets.
- Gained experience working on engagements alone and as a part of a team.

ACHIEVEMENTS

First place in Cyber Security Challenge Bulgaria 2024

Finishing first place out of all players competing

First place in Cyber Security Challenge Bulgaria 2023

Finishing first place out of the junior players competing and second out of all players

ARTICLES

Conquering the memory through io_uring - Analysis of CVE-2023-2598

https://anatomic.rip/cve-2023-2598/
https://github.com/ysanatomic/io_uring_LPE-CVE-2023-2598/

Conquering a Use-After-Free in nf_tables: Detailed Analysis and Exploitation of CVE-2022-32250

https://anatomic.rip/cve-2022-32250/
https://github.com/ysanatomic/CVE-2022-32250-LPE/

Abusing RCU callbacks with a Use-After-Free read to defeat KASLR

https://anatomic.rip/abusing_rcu_callbacks_to_defeat_kaslr/

CVE-2022-1015: A validation flaw in Netfilter leading to Local Privilege Escalation

https://anatomic.rip/cve-2022-1015/
https://github.com/ysanatomic/CVE-2022-1015/

Dissecting the Linux Firewall: Introduction to Netfilter's nf_tables

https://anatomic.rip/netfilter_nf_tables/

TECHNICAL SKILLS

Skilled in binary exploitation and reverse engineering.

Strong background in C and Python.

Experienced with x86 and ARM Assembly.

Knowledgeable on the inner workings of the Linux kernel.

Experienced in kernel (Linux) and browser engine (V8) exploitation.

Experienced in conducting web, internal, external and infrastructure penetration tests.

AWARDS AND HONOURS

First Bulgarian National Cyber Security Team

Awarded by the Minister of e-Government on the 19th of December 2023

CERTIFICATES

HTB Certified Penetration Testing Specialist

HTBCERT-8F60354B99 - Issued in October 2024

Burp Suite Certified Practitioner

EF22FD5EBBC5F0D0 - Issued in March 2024

TALKS

Ghetto Superstar - BSides Sofia 2024

A talk on state-of-the-art Linux rootkits, stealth and evading EDR/XDR. Complete evasion of Wazuh in the live demo.

Linux Implants and Evasion - CSCB Conference 2024

A short talk on Linux Kernel implants and evasion of forensic methods.

EXTRA-CURRICULAR ACTIVITIES

Captain of the Bulgarian National Cyber Security Team

Represented Bulgaria at the European Cyber Security Challenge since 2023

Bulgaria’s nomination for Team Europe 2024

Competing in CTFs with “Perperikon”

Ranked number 1 in Bulgaria, top 50 globally. Founding member.

Competing in CTFs with “Organizers”

Ranked top 10 globally. Member since September 2024.

EDUCATION

Mathematics and Informatics, High School of Mathematics "Dr Petar Beron", Varna

September 2018 - May 2023