Pim Beune

Enschede | pim (at) beune (dot) dev | beune.dev | pim-beune | beune

Experience

Coöperatieve Rabobank U.A., Ethical Hacker — Utrecht, the Netherlands — Sept. 2024 - Present

- In the Red Team of Rabobank, I perform various Red and Purple team exercises for the bank and its subsidiaries.
- Developed Beacon Object Files (BOFs), shellcode loaders, persistence techniques, initial access methods, and cookie dumping techniques.
- Designed and deployed OPSEC-friendly C2 infrastructure to be used in operations.

Tesorion Operations B.V., Ethical Hacker — Leusden, the Netherlands — Feb. 2023 - Jul. 2024

- In the Red Team of Tesorion, I performed black- and gray-box penetration tests, phishing simulations and Red Team assessments.
- Deployed a C2 infrastructure to be used in Red Team assessments.
- Contributed to developing Tesorion's phishing framework.
- Developed custom tooling to enumerate sessions in an Active Directory environment, whose output is BloodHound-compatible.

Certifications

UDRL and Sleepmask Development — Certificate

- This course focuses on developing custom User-Defined Reflective Loaders (UDRLs) and Sleepmask components for Cobalt Strike, teaching students low-level Windows internals, memory evasion, reflective loading, module stomping, sleep obfuscation, ROP chains, and call stack spoofing techniques. The course is aimed at experienced red teamers and malware/tool developers who already understand C, Windows APIs, and Cobalt Strike internals.

BOF Development & Tradecraft — Certificate

- This course focuses on creating Beacon Object Files (BOFs) for Cobalt Strike and other C2 frameworks. It teaches Windows API usage, COFF/position-independent code, Aggressor scripting, and operational BOF development through hands-on projects like ransomware simulation, UAC bypasses, and Kerberos ticket harvesting. It is aimed at practitioners with some C/C++ and Windows internals experience who want to build custom in-memory tooling and understand offensive tradecraft at a deeper level.

Offensive Security Exploit Developer — Certificate

- Description from Offensive Security: Certified OSEDs possess the expertise to craft their own shellcode and develop custom exploits from the ground up, allowing them to analyze vulnerabilities and circumvent standard Windows security mitigations. They are capable of: Bypassing fundamental mitigations like DEP and ASLR, leveraging format string vulnerabilities, and identifying flaws in binary applications to build tailored exploits.

Mastering WinDbg — Certificate

- Description from Trainsec: WinDbg is a powerful Microsoft debugger that can debug both kernel and user mode programs. The main features of using WinDbg in both user and kernel mode, with and without source code, are demonstrated in this course.

Malware Development Course Certificate

- Description from Maldev Academy: A module-based course featuring over 200 continuously updated modules and challenges that cover beginner, intermediate, and advanced malware development techniques.

Offensive Phishing Operations Certificate

- Description from Maldev Academy: A module-based course providing in-depth training on secure phishing infrastructure deployment and advanced evasion strategies to bypass modern phishing detection mechanisms.

Offensive Security Web Expert Certificate

- Description from Offensive Security: Certified OSWEs possess a solid and hands-on knowledge of white-box web application assessments. They have demonstrated their expertise in reviewing advanced web app source code, identifying vulnerabilities, and exploiting them. OSWEs are capable of exploiting web applications with sophisticated chained attacks that leverage multiple vulnerabilities, and using innovative and lateral thinking to find unique ways to exploit web vulnerabilities. They are also equipped to support web development teams in building and maintaining secure-by-design web applications.

Training Offensive Entra ID (Azure AD) and Hybrid AD Security Certificate

- This training enables participants to analyze, attack, and secure Microsoft Entra ID and hybrid setups from modern threats.

Red Team Operator Certificate

- Description from Zero-Point Security: Individuals with the Red Team Operator badge have proven their expertise in adversary simulation, command and control, engagement planning, and time management. They are capable of executing each phase of the attack lifecycle, from initial compromise to full domain takeover, data hunting, and exfiltration, all while maintaining OPSEC awareness and evading defenses.

Offensive Security Certified Professional Certificate

- Description from Offensive Security: OSCP-certified individuals have demonstrated the ability to utilize persistence, creativity, and perceptiveness to identify vulnerabilities and execute organized attacks within strict time constraints. They demonstrate proficiency in various tasks, including information gathering, script development, exploit analysis, and conducting diverse attacks such as remote and local privilege escalation, client-side exploits, and web application vulnerabilities. Their expertise extends to utilizing tunneling techniques for network pivoting. OSCP holders are known for their innovative thinking and efficient time management, making them highly effective in cybersecurity roles.

CVEs

CVE-2024-53615 Jan. 2025
Exploit Link

- A command injection vulnerability in the video thumbnail rendering component of Karl Ward's `files.gallery` v0.3.0 through 0.11.0 allows remote attackers to execute arbitrary code via a crafted video file.

Education

MSc **University of Twente**, Computer Science — Sept. 2021 - Jul. 2023

- Weighted average grade: 7.7
- Topics such as: Cryptography, Cyber Risk Management, Software Testing and Reverse Engineering, Internet Security, Software Security, Security Services for IoT, & Secure Cloud Computing
- Thesis: *Lightweight Public Key Infrastructure for IoT.* URL

BSc **University of Twente**, Computer Science — Sept. 2018 - Jul. 2021

- Weighted average grade: 7.0
- Topics such as: Computer Systems, Network Systems, Software Systems, Algorithms, Automata, Calculus, Discrete Mathematics, (Linear) Algebra & Statistics.
- Research project: *Classifying the Network Capacity of the Dutch IPv4 Address Space.* URL

Skills

Malware development: Developed several loaders in Rust capable of bypassing modern EDR solutions. Conducted research and implementation of persistence and evasion techniques to enhance operational security.

Technologies: Docker, Nginx: I am hosting a number of web services, among self-made full-stack applications. Passionate Linux user for many years.

Languages: Dutch (native), English (proficient)