Akshat Pandey

+31 6 2619 3357 | akshatpandeymyself@gmail.com | Eindhoven, Netherlands
akshatpandey.com | linkedin.com/in/AkshatPandey1 | github.com/AkshatPandey1

Summary

Offensive-leaning security MSc candidate (Honors), comfortable across attack and detection. Hands-on with exploitation, intrusion detection, and protocol analysis through CTF challenges and honeypot research, with deep specialization in industrial control systems. Python and AWS/DevOps engineering background for building realistic test environments.

Education

Eindhoven University of Technology (TU/e) **Eindhoven, NL**
MSc. Information Security Technology *Sep. 2025 – Jul. 2027 (Exp.)*
- Coursework: Advanced Network Security, Intrusion Detection Lab, Applied Cryptography, Software Security, Verification of Security Protocols, Provable Security
- Selected for the Master Honors Academy, a competitive research-track honors program

University of Alberta **Edmonton, CA**
BSc. Computing Science (Software Practice Specialization, Co-op) *Sep. 2020 – Apr. 2025*
- Coursework: Operating Systems, Computer Organization/Architecture, Software Process/Product Management, Web Applications and Architecture, File and Database Management
- DevCon 2021 Hackathon Winner | International Country Scholarship

Technical Skills

Offensive Security: Metasploit, Burp Suite, Nmap, Wireshark, Kali Linux
Languages: Python, Bash, C, C++, Java, JavaScript, TypeScript, SQL
OT/ICS & Protocols: S7comm, Modbus, RPL/6LoWPAN, OpenPLC, Zeek, ICS/SCADA forensics
Cloud & DevOps: AWS (Glue, S3), Docker, Terraform, GitHub Actions, GitLab CI/CD
Databases: PostgreSQL, MongoDB, SQLite

Experience

Blackbuck Insights **Remote (Schaumburg, IL)**
DevOps Engineer, Co-op (AWS, Python, GitLab) *Jun. 2023 – Jul. 2024*
- Built **7 ETL pipelines** on **AWS Glue/S3** over TransUnion financial data, with **per-record schema validation**
- Built **GitLab CI/CD** quality gates (linting, tests) blocking non-compliant merges for an **8-person team**
- Wrote **PostgreSQL** transformations to standardize financial attributes feeding downstream reporting

University of Alberta **Edmonton, CA**
Teaching Assistant (C, Unix) *Jan. 2023 – Apr. 2023*
- Taught **C** and Unix tooling labs (**gdb**, **valgrind**), covering memory management and **memory-safety bugs**
- Graded assignments, ran plagiarism detection (**MOSS**), and held debugging office hours

Projects

High-Interaction VNC Honeypot TU/e – Master Honors Project
Python (asyncio), Docker, OpenPLC, FUXA, VNC/RFB *Sep. 2025 – Present*
- Building a high-interaction **VNC honeypot** that emulates an **HMI** to capture and study live attacker behavior
- Built a custom **asyncio RFB proxy** with protocol-level instrumentation that logs full attacker sessions

RPL Blackhole Attack & Defense TU/e – Advanced Network Security
C (Contiki-NG), Python, nRF52840, RPL/6LoWPAN, IEEE 802.15.4 *Feb. – Apr. 2026*
- Implemented a **rank-spoofing blackhole** attack and a **DAO-retransmission** defense on 3× nRF52840 boards
- Verified the defense detecting and blacklisting the malicious node via a **Python** SSH log monitor

Stuxnet ICS Forensic Investigation TU/e – Intrusion Detection Lab
Zeek, S7comm, Wireshark, ICS/SCADA Forensics *Feb. – Apr. 2026*
- Analyzed a Stuxnet ICS infection across a 4-subnet capture using **Zeek**
- Examined the attack path against a **Siemens S7-400 PLC**, the Stuxnet target class (**CVE-2010-2772**)

Interactive Portfolio with Embedded CTF Challenges Personal Project
Next.js, React, Tailwind CSS *2025 – Present*
- Designed **4 CTF challenges** (steganography, crypto, recon) as a live offensive-security demo at akshatpandey.com
- Published security write-ups, built in **Next.js** and deployed on **Cloudflare Pages**

Fingerprinting Automated ICS Scanning Tools TU/e – IST Seminar
Snap7/HoneyPLC, Conpot, S7comm, PROFINET, Metasploit, KVM/QEMU *Apr. 2026 – Present*
- Deployed **S7comm** honeypots (**HoneyPLC**, **Conpot**) to fingerprint automated ICS scanning tools
- Compiled a **100+ tool** S7comm inventory and analyzed the **Metasploit** and **ISF** scanning modules