Nazariy Buryak

0852675261 | nazarburyak21@gmail.com | LinkedIn | GitHub | Portfolio Website

EDUCATION

South East Technological University | Carlow, Ireland

- ***Ordinary B.S. in CyberCrime and IT Security*** – current avg. grade 72%

Portlaoise College | Portlaoise, Ireland

- ***Leaving Certificate***

Certifications:

- ***DevSecOps Certificate*** *TryHackMe - issued May 2025*
- ***Security Engineer Certificate*** *TryHackMe - issued May 202*
- ***AWS Certified Solutions Architect Associate Course*** *Digital Cloud Training - issued August 2025*

TECHNICAL SKILLS

Languages: Terraform, Python, HTML, CSS, Java, Go, JavaScript, C, PHP

Cloud & DevOps: AWS, GCP, Azure, Kubernetes, Docker, Jenkins, Git, SonarQube

Security Tools: Wireshark, Nmap, BurpSuite, Metasploit, Hydra, OWASP ZAP

Networking: VLAN setup and segmentation, trunk/access port configuration, DHCP scope configuration, STP/RSTP tuning and loop prevention, ACLs/security hardening, switch/router troubleshooting

Databases: PostgreSQL, MongoDB, MySQL

Operating Systems: Linux, Windows, macOS

SOFT SKILLS

- Effective communication
- Event participation
- Analytical thinking
- Calm under pressure
- Problem solving

RELEVANT EXPERIENCE

Cohort | Carlow, Ireland **Sep. 2025 - Present**

-Cloud Infrastructure & DevOps Engineer

- Designing and building AWS cloud environment for an ambitious project, setting up networks, databases, caching, routing, containerization while also making infrastructure secure and scalable for future application growth.
- Working on building secure CI/CD pipeline, implementing DevSecOps principles for analysis using SonarQube and adding Jenkins for better testing and automation.

Amazon Web Services | Zurich, Switzerland **Sep. 2025**

-Event Participant

- Developed skills in securing systems, identity frameworks, and CI/CD pipelines (GitLab, Kubernetes, AWS), including global network solution design.
- Gained hands-on experience through CTFs, card games, and expert-led sessions, applying attack/defense strategies and safety protocols for autonomous agents.

PROJECTS

GhostState **Jan. 2026**

- TUI-based security and governance tool for AWS written in Go; scans cloud infrastructure in real-time to identify "Ghost" resources (unused/shadow IT) and "Risk" assets (critical vulnerabilities), featuring hexagonal architecture for multi-provider extensibility.

WAFPierce **Feb. 2026**

- CLI & GUI Python WAF/CDN fingerprinting and bypass validation tool for pentesting across cloud providers. It detects 17+ WAFs and 12+ CDNs, runs 35+ bypass/evasion techniques with baseline heuristics (status, size, hashes), and outputs Markdown reports.

GhostWeights **Jan. 2026**

- Go-based pentesting tool for AWS that detects unsanctioned AI workloads ("Shadow AI") and risky AI service exposure across cloud environments.

AWS Image Detector **Aug. 2025**

- Serverless image analysis system using AWS Lambda, S3, Rekognition, and DynamoDB. Automatically detects and labels objects in uploaded images.

TCP_Recon_Tool **Dec.2025**

- Command-line Python reconnaissance tool that probes targets, enumerates services and HTTP applications, inspects TLS, fingerprints web stacks, and outputs machine-readable JSON reports for further analysis.

Find more on my GitHub or Portfolio Website