# FAATIH ADEKUNLE KAJOGBOLA

## Cybersecurity Professional & Game Developer

Garrus31@gmail.com   +353 870 303 133   Dublin, Ireland   linkedin.com/in/renegade-studios

github.com/Garrus-31   garrus-31.github.io/

## PROFESSIONAL SUMMARY

Game Developer and Cybersecurity Specialist with 3+ years of combined experience designing engaging games and securing applications. Proven track record in developing interactive, educational cybersecurity games that improve knowledge retention by 12%, and leading cloud security projects that enhance system defenses. Skilled in C++, Python, Unreal Engine, penetration testing, and secure coding practices. Known for bridging creative development with robust security solutions to deliver innovative and safe user experiences.

## EDUCATION

**MSc, Cybersecurity**                                                                                                    *2025*
**National College of Ireland**
Dublin, Ireland

**B.Eng, Chemical Engineering**                                                                                  *2022*
**University of Ilorin**
Kwara State, Nigeria

## TECHNICAL SKILLS

**Programming Languages**

C++   Python   JavaScript   Blueprint

**Game Engines & Tools**

Unity   Unreal Engine

**Cybersecurity**

Penetration Testing   Network Security   Threat Analysis
Vulnerability Assessment

**Tools & Technologies**

Git   Docker   AWS   Linux   Wireshark   Metasploit
Burp Suite

## FEATURED PROJECTS

**CyberKnights**                                                                                                            *2025*
**Solo Developer | Unreal Engine 5, Cybersecurity Education**
- Developed a gamified cybersecurity learning module using Unreal Engine to teach core concepts.
- Designed interactive gameplay elements to make learning more appealing and rewarding for users.
- Conducted a user study with 19 players to measure learning gains against a conventional control group.
- Achieved a significant 12% increase in cybersecurity knowledge retention among participants.

**Demo | Itch.io**

**Cloud Security Project**                                                                                          *2025*
**Team Leader | AWS, MySQL, Network Security**
- Set up, configured, and secured an AWS EC2 instance running a LAMP stack and a WordPress site.
- Employed security monitoring and analysis tools, including Wireshark, OWASP Zap, DataDog, and CloudWatch.
- Implemented a SIEM solution for centralized log management and threat detection.
- Enhanced security posture by configuring SSL, 2FA, access control, and anti-spam protocols across all components.

**Demo**

**Secure Application Development Project**                                                      *2025*
**Solo Developer | Java, Application Security**
- Conducted a manual code review and security testing using SonarQube and Snyk on a vulnerable Java application.
- Identified and addressed critical security flaws, including SQL injection and hardcoded credentials.
- Successfully remediated all issues, raising the application's Reliability score from an E to an A.
- Enhanced the overall security posture by implementing robust password encryption and fixing all identified vulnerabilities.

**Demo | GitHub**

### Crypt Raider
**Solo Developer | Unreal Engine 5, C++**                              *2024*
- Developed an UE5 project focused on dynamic level interaction and advanced lighting systems.
- Created a system using overlapping actors and tags to trigger essential in-game actions.
- Solved complex event triggering challenges using overlapping actors, tags, line traces, and hits.
- Explored and implemented UE5's advanced Nanite geometry and Lumen lighting systems.

**Demo | Itch.io**

### Open World RPG Project
**Solo Developer | Unreal Engine 5, C++**                              *2024*
- Designed an ambitious open-world RPG level using UE5 sculpting and foliage tools.
- Programmed multiple enemy types with unique movesets from a single master AI controller class.
- Managed and populated a massive open world level to combine skills gained over the years.
- Overcame significant optimization challenges for smooth gameplay with numerous active enemies and foliage.

**Demo | Itch.io**

## CERTIFICATIONS & TRAINING

### Certification in Unreal Engine 4 Blueprint Development                 *Udemy | 2022*
Credential ID: UC-f9af9c19-3b25-4751-a393-b0c3afaf9137

### Certification in Unreal Engine 5 Blueprint Development                 *Udemy | 2023*
Credential ID: UC-cfb1085f-e1ba-441f-8db1-a9d5f9c0f795

### Certification in Oracle Cloud Infrastructure Foundations                 *Oracle | 2023*
Credential ID: 100330997OCIF2023CA

### Cybersecurity Training Diploma                 *Femtech IT Institute | 2024*
Credential ID: FITI/24/TW/3260

### Certification in Unreal Engine 5 C++ Development                 *Udemy | 2024*
Credential ID: UC-d101d091-19de-4519-ac64-83d5d544b225

## PROFESSIONAL EXPERIENCE

### Junior Cybersecurity Analyst                 *January 2023 – December 2023*
**Nigeria Extractive Industries Transparency Initiative**
Abuja, Nigeria
- Conducted daily threat monitoring and log analysis using SIEM tools to detect and respond to security incidents.
- Performed routine vulnerability scans and penetration testing on internal and cloud-based network infrastructure.
- Prioritized and reported critical security flaws and application vulnerabilities to senior management for immediate remediation.
- Developed and enforced security policies and procedures, maintaining compliance with mandated industry security standards.
- Managed and maintained security tool performance, ensuring firewalls, antivirus, and IDS/IPS systems were fully operational.

*Key Achievement: Developed an automated reporting script (Python) for monthly vulnerability assessments, which streamlined the reporting process, saving approximately 10 hours per month.*

### Cybersecurity Intern                 *June 2020 - May 2021*
**Standard Organization of Nigeria**
Abuja, Nigeria
- Participated in hands-on penetration testing exercises, documenting findings using tools like Burp Suite and Metasploit.
- Assisted senior team members in the remediation of low-to-medium severity vulnerabilities identified in internal systems.
- Provided essential end-user security awareness training, focusing on phishing and strong password practices.
- Managed and updated security tools and systems, including antivirus software and firewalls, ensuring maximum protection and uptime.
- Conducted bi-weekly security inspections to ensure compliance with the organization's network security mandates.

*Key Achievement: Implemented a new asset inventory system for network devices, increasing the accuracy of security audits and facilitating faster patch management cycles.*