Ibrahim Odat

PhD Candidate | Cybersecurity, AI & Autonomous UAV Systems Engineer

Contact Information

- **Phone**: (248) 237-5426
- **Email**: ibrahimodatt@gmail.com
- **Location**: Michigan, USA
- **Website**: 3odat.github.io
- **LinkedIn**: linkedin.com/in/ibrahim-odat

Professional Summary

Cybersecurity professional with 3+ years of experience designing and implementing Offensive Security strategies, AI-driven Threat Detection solutions, and Penetration Testing protocols for autonomous systems. Expert in leveraging Machine Learning and Deep Learning frameworks to automate vulnerability discovery, conduct comprehensive security assessments, and harden UAV and embedded system defenses. Currently pursuing a Ph.D. in AI-augmented Autonomous Systems Security, with published research on machine-learning–based threat mitigation.

Skills

- **Cybersecurity:** Penetration Testing, Vulnerability Assessment, MITRE ATT&CK, OWASP Top 10, NIST Frameworks, Endpoint Detection & Response (EDR), Security Information & Event Management (SIEM**).**
- **AI & LLM:** Model Fine-Tuning, Prompt Engineering, Knowledge Distillation, Ollama Integration, Autonomous Systems
- **Tools & Platforms:** Kali Linux, Metasploit, Wireshark, Nessus, Nmap, Docker, ROS2, PX4 Autopilot, Gazebo, YOLOv8
- **Programming & APIs:** Python, Bash, SQL, REST APIs, Flask, PHP
- **Cloud & IAM:** AWS Security, Active Directory, Okta, Multi-factor Authentication (MFA), Zero Trust Architecture

Work history

Cybersecurity Researcher | Oakland University | Jan 2022 – Present

- Led Penetration Testing and Vulnerability Assessments on PX4 Autopilot systems to identify buffer overflows, session hijacking, and MAVLink protocol exploits, improving security resilience by 80%.
- Conducted Firmware Analysis and Security Assessments for Foscam IoT cameras, uncovering critical flaws and reducing unauthorized access risk by 90%.

- Architected and deployed AI-driven Threat Detection pipelines using Machine Learning models, LLM fine-tuning, prompt engineering, and Ollama integration—automating anomaly detection and cutting manual analysis time by 60%.

- Executed Man-in-the-Middle (MITM) and brute-force attack simulations to validate and strengthen encryption protocols, optimize Intrusion Detection System (IDS) configurations, and enhance incident response readiness.

Cybersecurity Specialist | ZADD | Jan 2021 – Jan 2022

- Secured Windows Domain environments using TSplus Remote Desktop Servers, significantly limiting lateral movement and reducing unauthorized access vectors.

- Integrated Artificial Intelligence (AI) security models into enterprise translation platforms, decreasing false-positive alerts by 35%.

- Conducted 120+ Vulnerability Scans with Nessus, ensuring full compliance with NIST SP 800-171 and bolstering audit readiness.

- Managed and optimized security infrastructure—including Intrusion Detection and Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs), Firewalls, Data Loss Prevention (DLP), and Security Information and Event Management (SIEM) solutions.

Penetration Tester | Futuretec Security Solutions | Jan 2020 – Jan 2021

- Executed 200+ Web Application and API Penetration Tests using Burp Suite and SQLMap, reducing assessment cycle time by 40% and uncovering critical SQL injection and authentication bypass vulnerabilities.

- Remediated Open Web Application Security Project (OWASP) Top 10 risks—including Injection, Broken Authentication, and Security Misconfiguration—to ensure client compliance with PCI DSS and ISO 27001 standards.

- Developed and maintained custom Python-based security testing frameworks and automation scripts, streamlining vulnerability discovery and reducing manual effort by 50%.

- Authored comprehensive technical reports and delivered remediation recommendations to C-level stakeholders, elevating overall client security posture and awareness.

- Collaborated with cross-functional development and DevOps teams to integrate security testing into the Software Development Life Cycle (SDLC), minimizing regression risks and accelerating secure release cycles.

Projects

- **PX4 Autopilot Session Hijacking Exploit**: Exploited session hijacking vulnerability in PX4 Autopilot software to elevate user privileges to system level; validated and proposed mitigation strategies. Technologies: PX4 Autopilot, MAVLink, MAVSDK, Python.

- **Foscam Camera Security Showcase**: Presented at Black Hat Arsenal on authentication bypass and memory-corruption exploits in Foscam IoT cameras; influenced adoption of firmware encryption standards. Technologies: IoT Firmware Analysis, Python, Metasploit.
- **Multi-Agent UAV Coordination Framework**: Designed LangGraph-based orchestration for two PX4 drones, enabling peer-to-peer WebSocket communication, dynamic task delegation, and real-time feedback. Technologies: LangGraph, LangChain, FastAPI, WebSockets, MAVSDK, Python.
- **Autonomous Traffic Simulation for UAV Surveillance**: Integrated ROS2 (Humble) and Gazebo Ignition to simulate realistic highway traffic with moving vehicles and pedestrians; built ROS2 control interfaces for end-to-end testing. Technologies: ROS2, Gazebo Ignition, CARLA-style scenarios, Python.
- **YOLOv8 Object Detection Pipeline**: Implemented real-time object detection within ROS2 for autonomous drone vision; achieved >95% accuracy on simulated traffic datasets. Technologies: YOLOv8, ROS2, Python, NVIDIA Jetson Nano.

Education

Doctor of Philosophy (Ph.D.) in Computer Science & Informatics | Oakland University, Rochester, MI | Expected Dec 2028

- **Research Focus:** Securing Autonomous Systems through AI Integration

Master of Science (M.S.) in Cybersecurity | Oakland University, Rochester, MI | May 2022 – Dec 2023 | GPA: 4.0/4.0

- **Publication:** Net-GPT: LLM-Empowered MITM Chatbot for UAV Security.

Certifications and Training

- Certified Ethical Hacker (**CEH**) – **EC-Council**, 2023.
- eLearnSecurity Junior Penetration Tester (**eJPT**) – **INE**, 2022.
- Fortinet Network Security Expert Level 1 (NSE 1) & Level 2 (**NSE 2**) – **Fortinet**, 2021.