# Baning Philip Amponsah

| Grambling, LA | baningphilip1@gmail.com | LinkedIn.com/in/pabaning | GitHub.com/Alanperry1| www.pbaning.com |

## EDUCATION

**Grambling State University, Grambling, LA** ***Expected Graduation: May 2028***

Bachelors of Science in Computer Science & Cybersecurity | 3.64 GPA

## SKILLS & CERTIFICATIONS

**Skills**: Penetration Testing · Digital Forensics · SIEM Management · Threat Modelling · Secure Code Review · DevSecOps
**Languages:** Python · C++ · Bash · SPL · Java · JavaScript · SQL · PowerShell · YARA · KQL

**Frameworks:** STRIDE · NIST CSF · MITRE ATT&CK · OWASP Top 10 · OAuth 2.0 · Cyber Kill Chain · Diamond Model · PCI-DSS

**Tools:** Splunk · Metasploit · IBM X-Force · Postman · BurpSuite · SonarQube · OpenVAS · GitHub Actions · Microsoft Sentinel · Autopsy

**Certifications:** eJPTv2 (In Progress) · Security+ · AZ-900 · CAP· C3SA · CNSP · ISC$^2$ CC · Google CSP · IBM Cybersecurity Practitioner

## EXPERIENCE

**Application Security Engineer** ***May 2025 - Present***

BitLoop *Ruston, LA*

- Integrated security into CI/CD pipeline using GitHub Actions and YAML workflows, reducing security review time from 3 days to 2 hrs
- Conducted API pentesting with BurpSuite using OAuth 2.0 framework, patched auth flaws, blocking 1.2k+ malicious requests
- Performed secure code reviews on GitHub repos, identifying 50+ vulnerabilities including injection flaws and access control issues
- Automated security scanning pipeline using SonarQube and GitHub Action, detecting 871 vulnerabilities before production deployment

**Cybersecurity Research Assistant** ***Feb 2025 - Present***

Grambling State University *Grambling, LA*

- Conducted research on emerging cyber threats and adversary techniques, utilizing MITRE ATT&CK framework for threat analysis
- Developed threat models using CALDERA and ATT&CK Navigator to simulate adversary strategies and map potential attack pathway
- Integrated Threat Intelligence Platforms with STIX/TAXII protocols, reducing false positives by 60% and enhancing detection efficacy
- Optimized Atomic Red Team to simulate real-world adversary TTPs, enhancing threat detection and response capabilities

**Cybersecurity Forensics Intern** ***Jun 2024 - Sep 2024***

CFSS Cyber & Forensics Solutions *Remote*

- Led 6+ digital forensics investigations, analyzing 500+ GB of evidence, supporting 10+ cyber-crime cases.
- Implemented AWS EC2 and S3 services for VM deployment and secure artifact storage, reducing forensic workflow processing time
- Tracked 70+ cyber threats using Splunk and Wireshark, identifying 20+ attack vectors through proactive threat hunting
- Leveraged IDA Pro for reverse-engineering, improving threat detection accuracy and incident response capabilities by 70%

**Cybersecurity Engineer Intern** ***Jul 2023 - Nov 2023***

Ideation Axis *Accra, Ghana*

- Collaborated with 5-member team to conduct penetration testing, identifying and exploiting 45+ critical vulnerabilities
- Analyzed 10+ GB network logs with Wireshark, identifying 150+ critical anomalies to enhance threat detection.
- Optimized YARA rules for IDS systems, improving threat detection and reducing false positives by 45%.
- Utilized Splunk for log analysis and threat detection, creating custom queries and alerts, reducing incident response time by 60%

## PROJECTS

**Network Vulnerability Scanner** | Personal Project *(~50 hours)* - GitHub Repo ***Apr 2025 - May 2025***

- Built Python-based vulnerability scanner with Nmap and SQL Alchemy, optimizing network discovery with TCP connect scanning
- Utilized Flask REST API for vulnerability tracking, enabling automated workflows, reducing mean-time-to-resolution by 75%

**Malware Analysis** | Team Project *(~20 hours)* ***Jan 2025 - Feb 2025***

- Analyzed Zeus Trojan malware using static and dynamic analysis to identify propagation methods and trace execution flow
- Documented IOCs, refined YARA rules for Zeus variants to increase detection accuracy and reduce false positives

**AWS Automated Vulnerability Scanner** | Personal Project *(~15 hours)* ***Sep 2024 - Oct 2024***

- Configured and deployed Nessus on AWS for automated vulnerability assessment, identifying 30+ high-risk CVE and misconfiguration
- Strengthened cloud security by implementing IAM least privilege policies and optimizing VPC settings to reduce attack surface

## Activities

Industry Panel Discussion– Moderated panel on cybersecurity career opportunities and industry guidance for rising sophomores
VishwaCTF - Led a team of 4, securing 14th place by solving challenges in cryptography, web security and digital forensics
H4CKP13T 0X01 CTF - Completed 12 out of 18 challenges in diverse domains including web app pentesting and host evasion
Notion Hackathon – Developed a Notion-based interactive dashboard for SWE’s to track skill development and project milestones