BANING PHILIP AMPONSAH

Grambling, LA | baningphilip1@gmail.com | linkedin.com/in/pabaning | github.com/Alanperry1

EDUCATION

Grambling State University – Grambling, LA, USA Expected Graduation Date: **May 2028**
Bachelors of Science in Cybersecurity & Computer Science **| 4.0**/4.0 GPA
Relevant Coursework: Intro to Cybersecurity, Computer Science I, Computer Science II, Information Security

SKILLS & CERTIFICATIONS

- **Skills:** Vulnerability Assessment, Penetration Testing, Digital Forensics, Malware Analysis, SIEM Management, Threat Modelling, Cyber Threat Intelligence, Cloud Security
- **Languages**: Python, C++, SPL, Bash, SQL, PowerShell, JavaScript, YARA
- **Frameworks**: STRIDE, NIST CSF, MITRE ATT&CK, PCI-DSS, OWASP, Cyber Kill Chain, Diamond Model
- **Tools**: Splunk, Metasploit, Wireshark, Nmap, BurpSuite, Ghidra, IDA Pro, Autopsy, Nessus, IBM X-Force, OWASP ZAP, OpenVAS
- **Certifications:** eJPTv2(**In Progress**), Security+, C3SA**,** CAP, CNSP, ISC^2 CC, Google CSP

EXPERIENCES

Security Research Assistant Feb 2025 - Present
Grambling State University ***Grambling, LA***

- Conducted in-depth research, supervised by **Dr. Vasanth Iyer**, on emerging cyber threats, attack vectors, and advanced adversary techniques, utilizing **MITRE ATT&CK** and the **Cyber Kill Chain** frameworks for threat analysis.
- Developed and deployed threat models using **attack surface analysis** to simulate adversary strategies, leveraging tools such as **CALDERA** and **ATT&CK Navigator** to map potential attack pathways and reducing attack surfaces by **45%**.
- Integrated Threat Intelligence Platforms (TIPs) to aggregate and analyze high-fidelity Indicators of Compromise (IOCs), leveraging **STIX/TAXII** protocols, reducing false positives by **60%** and enhancing detection efficacy.
- Optimized **Atomic Red Team** to simulate real-world adversary tactics, techniques, and procedures (TTPs), enhancing threat detection and response capabilities.

Digital Forensics Intern June 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** services- **EC2** for VM deployment and **S3** for secure artifact storage, reducing forensic workflow processing time and enhancing evidence handling efficiency by **80%**.
- Leveraged **IDA Pro** to conduct malware analysis and reverse-engineering of exploits, improving **threat detection** accuracy and enhancing **incident response** capabilities by **70%.**
- Tracked **70+** cyber threats via network logs and artifact analysis utilizing **Splunk** and **Wireshark**, enabling the identification and mitigation of over **20+** of emerging security risks through proactive **threat hunting** and early detection techniques.

Cybersecurity Engineer Intern Jul 2023 – Nov 2023
Ideation Axis **Accra, Ghana**

- Collaborated with a **5**-member team to conduct **risk assessment** and **penetration testing**, identifying and exploiting **75+** critical vulnerabilities, enhancing system defenses by resolving security gaps to prevent potential exploits.
- Analyzed **10+** GB network logs with Wireshark, identifying **150+** critical anomalies to enhance threat detection.
- Monitored network traffic with **Splunk**, creating queries and alerts to track, reducing mean time to detect (MTTD) and respond (MTTR) to security incidents by **70%**.
- Optimized **YARA** rules for **IDS** systems improving threat detection and reducing false positives by **45%** leading to more accurate and timely incident responses.

PROJECTS

WIZARD| Personal Project **|** **Github Repo**

- Developed a Python-based USB drive sanitization program utilizing the **Gutmann algorithm** with three-pass randomization techniques to securely overwrite sensitive data, ensuring it is unrecoverable.
- Utilized OS-level **syscalls** to facilitate direct interaction with hardware components, ensuring efficient execution of low-level operations for secure data wiping and sanitization.

Reverse Shell Payload Generator| Personal Project **|** **Github Repo**

- Developed and obfuscated PowerShell reverse shell payloads, enhancing stealth and evasion with custom error messages and IP address encoding, ensuring successful exploitation in penetration testing.
- Automated payload delivery and execution using a batch file, enabling reverse shell connections on port 443, effectively **bypassing** antivirus and EDR's detection.

SSH Honeypot | Personal Project **|** **Github Repo**

- Developed and deployed honeypot on **AWS** to capture unauthorized login attempts and attacker credentials for threat intelligence and improving the detection of emerging attack vectors.
- Enhanced security monitoring with advanced IP filtering, traffic redirection, and customized prompts, leveraging AWS's cloud infrastructure for scalable and reliable data collection.

Malware Analysis | Team Project

- Analyzed **Zeus Trojan** malware samples using **static** and **dynamic** analysis to identify propagation and data exfiltration methods, tracing malware's execution flow and pinpoint malicious payloads.
- Documented **IOCs** and behavioral patterns to enhance threat intelligence while refining **YARA** rules for Zeus variants, increasing detection accuracy and reducing false positives.

AWS Automated Vulnerability Management |Personal Project

- Configured and deployed **Nessus** for automated vulnerability assessments on AWS-based systems, identifying and prioritizing high-risk **CVEs** and misconfigurations to enhance security posture.
- Strengthened cloud security by implementing **IAM least privilege policies**, configuring security groups, and optimizing **VPC settings**, significantly reducing the attack surface.

LEADERSHIP & ACTIVITIES

Team Lead (Team CyberArk)**,** VishwaCTF **(14th Place)**

- Led a team of 4 in a global cybersecurity competition, securing 14th place out of 130 participating teams by solving challenges in cryptography, web security, cloud forensics, reverse engineering, and digital forensics.

CTF Participant, H4CKP13T 0X01 CTF

- Successfully completed 12 out of 18 challenges in diverse domains including reverse engineering, mobile forensics, steganography, and host evasion.

Campus Ambassador, HBCUniverse

- Serve as the primary liaison at Grambling State University, promoting HBCU-related events to over 1000 students and achieving a 25% increase in participation and a 30% rise in program sign-ups through strategic outreach.

ORGANIZATIONS/CLUBS: ISC^2, Association of Computing Machinery, Blacks in Cybersecurity, Colorstack, NSBE, SECURE