KEVIN HAMZAJ

kvnhamzai@gmail.com | 2163968768 | **WWW:** www.linkedin.com/in/kevin-h-574253360 |
WWW: https://keviswicked.github.io/KevinsCyberPortfolio/

Summary

I am a Cybersecurity Professional with a Masters Degree in Cybersecurity and Data Privacy. I am always improving and building my skills through hands on labs and projects set to challenge my skills

Skills

- Understandings in network technologies, TCP/IP stack, network protocols, and IT infrastructure
- Experienced with basics in Nmap, Wireshark, Metasploit, John the ripper, Nikto, Nessus, Splunk, SIEM, IDS, automation and encryption techniques
- Keen ability to identify vulnerabilities, threats, and attacks to information systems, and recommend countermeasures
- Knowledgeable on Linux including the basics of linux kernel. Writing shell scripts
- Adept and Familiar with Azure and AWS Active Directory environment
- Solid understanding of programming concepts and hands on experience in Python, SQL
- Security frameworks, controls, design principles
- Knowledgeable about HIPAA and privacy
- Basic understanding of the OWASP Top 10

Education

Cleveland State University | Cleveland, OH | 05/2024

Master of Legal Studies: Cybersecurity And Data Privacy

- Graduated summa cum laude
- Ethical Hacking, Capstone Project : Provides technical security skills needed to make informed, risk-based decisions in an operational context. This hands-on, lab-based course aligns with the Certified Ethical Hacker certification with additional labs focused on malware analysis in virtual environments.

Cleveland State University | Cleveland, OH | 05/2022

Bachelor of Science: Health Sciences

Rocky River | Rocky River, OH | 06/2016

High School Diploma

- Google Cyber Security Certificate : Includes Linux, MySQL and Python hands-on labs
- Comp Tia Security + (September 2025)
- Comp Tia Network + (October 2025)
- AWS Cloud Practitioner (October 2025)

Practical Projects

Ethical Hacking Labs From Capstone

- Conducted network traffic analysis and ARP spoofing using Wireshark and Kali Linux to intercept FTP credentials and transferred files.
- Cracked Windows LM/NTLM hashes with Cain and brute-force attacks; cracked Linux shadow passwords using John the Ripper.
- Performed vulnerability scanning and enumeration using Nessus, OpenVAS, and Nmap NSE scripts to identify CVEs such as CVE-2006-3439 and CVE-2008-4250.
- Exploited real-world vulnerabilities via Metasploit modules (e.g., vsftpd backdoor) and confirmed root-level access through shell commands.
- Detected and exploited web application vulnerabilities (XSS, SQLi, RFI, Path Traversal) in DVWA and PentesterLab environments using Burp Suite and OWASP ZAP.
- Documented exploitation steps, technical findings, and security best practices in lab reports and post-engagement debriefs.

AWS Security Monitoring Project

- Implemented secure storage and management of sensitive credentials using AWS Secrets Manager.
- Enabled CloudTrail logging to monitor and audit all secret access activity.
- Created CloudWatch metric filters and alarms to automatically detect and alert on unauthorized or suspicious secret access.
- Configured SNS notifications for immediate real-time security alerts to stakeholders.

AWS Security – Threat Detection with GuardDuty

- Performed simulated attack scenarios (e.g., SQL injection, command injection, credential exfiltration) against a demo web application to generate realistic security events.
- Enabled and configured Amazon GuardDuty to monitor for malicious activity, including malware uploads and IAM key misuse.
- Validated detection capabilities by triggering GuardDuty findings in real-time and analyzing alerts for unauthorized access, credential exfiltration, and malware threats.
- Demonstrated end-to-end incident response, from threat detection through investigation and remediation.

AWS Security – Encryption Project

- Implemented data-at-rest encryption for DynamoDB using AWS KMS and customer-managed keys (CMK).
- Configured and managed IAM roles and KMS key policies to enforce granular encryption and decryption permissions.
- Verified secure data access by testing user permissions, demonstrating enforcement of security best practices.

Home Soc Honeypot Lab in Azure

- Gained hands-on experience in network monitoring, log correlation, and threat intelligence analysis, simulating real SOC workflows.
- The lab provided a practical foundation in intrusion detection, alert triage, and cyber threat hunting in a low-cost, self-managed environment.
- Created a VM and a VN in Azure and configured Log Analytics Workspace, forwarded logs and integrating with Sentinel
- Querying failed login attempts and visualizing attack sources, built an attack map to track real time hacker activity

Azure Active Directory project

- Completed a hands-on project on Secure Access with Azure Active Directory through Coursera, focusing on implementing secure identity and access management in a cloud environment
- Gained practical experience configuring Azure AD, including user and group management, Single Sign-On setup, and Multi-Factor Authentication enforcement.
- Applied Conditional Access policies to manage access based on risk levels, device compliance, and user roles. Developed foundational skills in securing cloud-based applications and aligning with zero-trust security principles.

Phishing Simulation

- Completed a phishing simulation where I served as an analyst on MasterCard's Security Awareness Team
- Helped identify and report security threats such as phishing
- Analyzed and identified which areas of the business needed more robust security training and implemented training courses and procedures for those teams

Cybersecurity Job Simulation

- Completed a job simulation involving the role of a cybersecurity generalist, specializing in fraud detection and prevention for Commonwealth Bank's Cybersecurity team.
- Developed skills in building data visualization dashboards using Splunk to uncover patterns and insights in historical

customer data, aiding in fraud detection.

- Demonstrated the ability to respond effectively to cybersecurity incidents, including notifying relevant teams, collecting information, containing and stopping attacks, and aiding in recovery efforts.
- Enhanced security awareness expertise by designing infographics promoting best practices for secure password management, following Australian Cybersecurity Centre advice.
- Acquired practical experience in penetration testing, assessing the security of web applications, identifying vulnerabilities, and providing recommendations for remediation to bolster cybersecurity defenses.

AWS Networking Basics

- Created and hosted a static website on Amazon S3, configuring bucket policies and permissions for secure public access.
- Visualized data using Amazon QuickSight, building interactive dashboards to transform raw data into actionable insights.
- Implemented cloud security best practices using AWS IAM, managing users, roles, and policies to enforce least-privilege access and protect AWS resources.
- This project strengthened my skills in cloud storage, data analytics, and security, while providing a practical understanding of AWS architecture and governance.

Chronicle SIEM – Introduction & Single Event Rules

- Gained hands-on experience with Chronicle Security Information and Event Management (SIEM) platform, part of Google Cloud.
- Developed and tested Single Event Rules using YARA-L for threat detection and security alerting.
- Analyzed security logs and investigated potential threats using Chronicle's built-in tools and dashboards.
- Demonstrated foundational knowledge in SIEM architecture, rule writing, and log correlation to enhance security operations.

Virtual Private Cloud in AWS

- Built a custom VPC in AWS by designing subnets, route tables, and attaching internet gateways to support cloud resource deployment.
- Configured and secured VPC traffic flow by implementing security groups and network ACLs to control and monitor network access.
- Deployed resources across multiple Availability Zones to ensure high availability and improve fault tolerance within the VPC.