Kismat Kunwar

kismatkunwar89@gmail.com • linkedin.com/in/kunwarkismat

Education

Master's in Cyber Security (GPA: 3.9), University of New Haven — Aug 2024 – Present

Bachelor's in Cyber Security, First Class Honors (GPA: 3.96), Coventry University — May 2020 – Jun 2023

SKILLS

Cybersecurity	Incident Response, Threat Hunting, OSINT/Recon, Vulnerability Assessment, Web App Exploitation, Privilege Escalation, Penetration Testing
Security Tools	CrowdStrike Falcon EDR, Rapid7 InsightVM, Nessus, Nmap, Wireshark, Burp Suite, Metasploit, CrackMapExec, Kerbrute, Impacket, Snort, Elastic Stack (ELK), Sysinternals, Autopsy
Systems/Networking	Windows Server, Active Directory, GPO, PowerShell, DNS, DHCP, TCP/IP, VLANs, OSPF, NAT, ACLs/Firewall Hardening, Port Security, Routing, Switching
Cloud/OS/Code	Azure (IaaS, PaaS, SaaS), Azure Entra ID, Windows, Kali Linux, Ubuntu; Python, C, C++
AI/Agents	LangChain, LangGraph, Retrieval Augmented Generation
Certifications	(ISC)2 CC, Cisco CCNA, Microsoft Azure Fundamentals (AZ-900)

EXPERIENCE

Provost Research Assistant — Sep 2024 – Present

Tagliatela College of Engineering - University of New Haven — *West Haven, CT*

- Researched anti-forensics in Windows artifacts; defined standardized structures with CASE/UCO to improve forensic tool interoperability and investigation accuracy.
- Engineered LLM prompts (GPT-4, DeepSeek, Gemini) to automate artifact standardization, cutting manual definition time by 30%.
- Delivered first-author research: applied full methodology, authored initial sections, and presented at ICDF2C (International Conference on Digital Forensics and Cyber Crime) with emphasis on validation.

Security Support Intern — May 2023 – Mar 2024

Raechal Enterprise Pvt Ltd — *Kathmandu, Nepal*

- Built detection use cases and demos for CrowdStrike EDR, contributing to 25% more enterprise client acquisitions/renewals.
- Configured and supported Falcon EDR for banking clients; strengthened endpoint protection, IR, and PCI DSS compliance.
- Resolved 15 EDR/MFA tickets weekly and deployed Endpoint Central MFA, coordinating with SOC analysts for identity security.

PROJECTS

- **Flamingo Neck Networks Internal Pentest (Course Lab).** Simulated internal test (10.248.1.0/24, ICS excluded). Default Postgres creds → RCE; guest-as-admin → Pass-the-Hash to full AD compromise; 9 findings (2 Critical) with remediation and topology.
- **VectorProbe (In Progress).** Automated Nmap/Searchsploit/enum4linux-ng recon with exploit correlation, AD-aware enumeration, and Markdown reporting.
- **Threat Intelligence Platform (In Progress).** Flask app aggregating AbuseIPDB, OTX, VirusTotal, and GreyNoise with risk scoring, MITRE ATT&CK mapping, and PDF/CSV/JSON exports.
- **Malware Research and Development.** Researched APT evasion techniques and simulated C2 using Metasploit and Cobalt Strike, achieving high evasion on Windows testbeds.
- **Reliable, Scalable Network Design.** Designed a redundant three-tier network for 170 users across six departments with OSPF, STP, HSRP, EtherChannel, VLANs, VLSM, firewalls, ACLs, VPN, port security, DHCP snooping, and AAA server integration; 80% emulated in Cisco Packet Tracer.