Kismat Kunwar

Cyber Security Graduate Student
kismatkunwar89@gmail.com | West Haven, CT | +1 203-410-6691 | linkedin.com/in/kismatkunwar

EDUCATION

Master's in Cyber security (GPA: 3.9) *August 2024 - Present*
University Of New Haven *West Haven, CT, US*

- **Relevant Courses:** Enterprise Network and Design, Windows and Linux Network Administration, Network Defense, Threat Hunting and Incident Response, Intermediate C Programming, AI & CyberSecurity

Bachelor's in Cyber security, First Class Honors (GPA: 3.96) *May 2020 - June 2023*
Coventry University *Coventry, UK*

- **Relevant Courses:** Advanced Networking , Advanced Digital Forensics, Penetration Testing, Python, System Security

TECHNICAL SKILLS & CORE COMPETENCIES

- **Cybersecurity & Threat Intelligence:** Incident Response, Threat Hunting, Vulnerability Management, Risk Mitigation, Network & Application Layer Security, Digital Forensics, Penetration Testing, Threat Landscape Analysis
- **Security Tools:** CrowdStrike Falcon EDR, Rapid7 InsightVM, Nessus, Wireshark, Burp Suite, Metasploit, Sysinternals Suite, Autopsy
- **System & Network Administration:** Windows Server, Active Directory, Group Policy (GPO), PowerShell, DNS, DHCP, TCP/IP, VLANs, OSPF, NAT, Access Control Lists (ACLs), Port Security , Routing , Switching
- **Cloud, OS & Programming:** Microsoft Azure (IaaS, PaaS, SaaS), Azure Entra ID, Windows, Kali Linux, Ubuntu; Python, C, C++
- **Artificial Intelligence** Langchain , LangGraph, Retrievel Augmented Generation(RAG)
- **Professional Competencies:** Analytical & Problem-Solving Skills, Teamwork & Collaboration, Written & Oral Communication, Leadership & Initiative, Adaptability in Fast-Paced Environments
- **Certifications:** (ISC)^2 Certified in Cybersecurity (CC), Cisco Certified Network Associate (CCNA), Microsoft Certified: Azure Fundamentals (AZ-900)

EXPERIENCE

Provost Research Assistant *West Haven, CT*
Tagliatela College of Engineering - University of New Haven *September 2024 - Present*

- Researched anti-forensics techniques in digital forensics by analyzing Windows artifacts and their inconsistencies, developing standardized artifact structures using CASE/UCO ontology to improve forensic tool interoperability and accuracy in incident investigations.
- Engineered LLM prompts (GPT-4, DeepSeek, Gemini) to automate artifact standardization workflows, reducing manual definition time by 30% while achieving 100% semantic accuracy and 70% syntactic validity in compliance with CASE/UCO specifications.

Security Support Intern *Kathmandu, Nepal*
Raechal Enterprise Pvt Ltd *May 2023 - March 2024*

- Developed and documented threat detection use cases, enabling client-facing demos of CrowdStrike EDR that drove a 25% increase in new enterprise client acquisitions and renewals for our MSSP in Nepal.
- Configured and supported CrowdStrike Falcon EDR deployments for commercial banking clients, ensuring endpoint protection, threat detection, incident response, and PCI DSS compliance.
- Provided tier-one support for CrowdStrike EDR and ManageEngine Endpoint Central (MFA), resolving $\sim$15 tickets per week and collaborating with SOC analysts on endpoint and identity security.
- Deployed ManageEngine Endpoint Central multi-factor authentication (MFA) across client networks, strengthening identity and access management and building expertise with Active Directory.

PROJECTS

- **Reliable, Scalable Network Design:** Designed and implemented a redundant, scalable network for Network Hats company (170 users across 6 departments) using a three-tier architecture (access, distribution, core layers). Improved performance and security with OSPF, STP, HSRP, EtherChannel, VLANs, VLSM, firewalls, ACLs, VPN, port security, DHCP snooping, and AAA server integration. 80% emulated on Cisco Packet Tracer.
- **Malware Research & Development:** Researched APT evasion techniques, developed malware, and increased detection evasion by 90% on Windows systems using Metasploit and Cobalt Strike for command-and-control simulations.
- **Windows Server & Client Lab Setup:** Built a virtualized lab environment using VMware, deploying Windows Server 2022 and Windows 10 clients. Configured Active Directory, DNS, DHCP, Group Policy, file and print services, IIS, FSRM, WSUS, and automated admin tasks with PowerShell. Demonstrated full system administration workflow from clean OS install to advanced server roles and secure client integration.