Himanshu Dahal

Artesia, CA | +1 (657) 271–7656 | himanshudahal123@gmail.com |
https://www.linkedin.com/in/himanshu-dahal/

Professional Summary

Analytical BSIT student at Westcliff University (graduating April/May 2026) with a concentration in Cybersecurity. Experienced in vulnerability management, digital forensics, and incident response through extensive labs and coursework aligned with CompTIA CySA+. Skilled in Linux troubleshooting, authentication flows, and secure application development. Adept at applying frameworks such as CIA triad, MITRE ATT&CK, and OWASP Top 10 to real-world scenarios. Seeking a Cybersecurity Analyst internship to contribute to threat detection, risk mitigation, and compliance initiatives.

Education

Bachelor of Science in Information Technology (BSIT)

Westcliff University, Irvine, CA: Expected April/May 2026

- Concentration: Cybersecurity
- Relevant Coursework: Threat & Vulnerability Management, Software & Systems Security, Security Operations & Monitoring, Digital Forensics & Incident Response, Compliance & Assessment

Technical Skills

- Security Frameworks: CIA triad, DAD triad, MITRE ATT&CK, Kill Chain
- Tools: Wireshark, Nmap, Metasploit, Burp Suite, SIEM/SOAR platforms
- Programming/Web: HTML, CSS, JavaScript, Python, Express.js, MongoDB, React, Bootstrap
- Systems: Linux (Fedora, Mint, Kali), Windows Server
- Cybersecurity Practices: Vulnerability scanning, incident response playbooks, forensic evidence collection, patch management, system hardening
- Soft Skills: Collaboration, troubleshooting, analytical reporting

Cybersecurity Coursework & Projects

- Threat & Vulnerability Management (CYB 400): Applied MITRE ATT&CK framework, developed enterprise patch management plan, performed system hardening and centralized logging.
- Software & Systems Security (CYB 401): Configured SIEM/SOAR tools, performed asset discovery and vulnerability scanning, applied CVSS scoring to validate vulnerabilities.
- Security Operations & Monitoring (CYB 402): Executed incident response playbooks, conducted forensic evidence collection and root cause analysis, configured infrastructure vulnerability scanning.
- Digital Forensics & Incident Response (CYB 403): Applied file analysis, DNS/IP reputation checks, and network sniffing; performed vulnerability assessments; conducted web and cloud vulnerability scans.
- Compliance & Assessment (CYB 404): Performed labs on XSS, SQLi, CSRF, directory traversal; applied SSDLC and OWASP Top 10 practices; conducted privilege escalation and misconfiguration labs; analyzed cloud infrastructure vulnerabilities.

Experience

- Collaborated on cybersecurity labs simulating incident response playbooks, including detection, containment, eradication, and recovery.
- Applied digital forensics techniques such as file analysis, DNS/IP reputation checks, and forensic evidence collection to investigate simulated breaches.
- Configured and analyzed outputs from SIEM/SOAR tools to automate threat detection and streamline incident response.
- Conducted vulnerability scanning and patch management planning, reducing false positives through CVSS scoring and context awareness.
- Facilitated group collaboration and technical communication in coursework projects, ensuring clear documentation and evidence-based reporting.
- Troubleshot technical issues in Linux and web development environments, validating solutions step-by-step for reliability.

Certifications

- CompTIA Security+: In progress