DEBARSHI KUNDU

Austin, Texas | debarshikundu0@utexas.edu | (512) 781-1946
github.com/debarshikundu | linkedin.com/in/debarshi-kundu-19145636/

PROFESSIONAL SUMMARY

Cybersecurity practitioner with hands-on experience in threat detection, incident response, and vulnerability management. Completed 200+ hours of security training across 6 industry certifications with proven ability to identify security threats, conduct penetration testing, and implement security controls. Strong technical foundation combining secure software development background with advanced cybersecurity training in SOC analysis, threat hunting, and security engineering. Actively seeking roles in Security Operations Center (SOC) analysis, penetration testing, security engineering, or incident response.

TECHNICAL SKILLS

Security Frameworks & Compliance: ISO/ANSI 17024, DoD Directive 8570.01-M, FISMA, PCI DSS, NIST Cybersecurity Framework, GDPR, HIPAA, OWASP Top 10
Network Security: Firewall Configuration & Management, IDS/IPS (Snort), VPN, SIEM (Splunk, Google Chronicle), Network Segmentation, Packet Capture Analysis, TCP/IP, DNS/DHCP
Cloud Security: AWS (EC2, Lambda, S3, VPC, IAM), Azure, GCP, Container Security (Docker, Kubernetes)
Incident Response & Vulnerability Management: Incident Handling & Triage, Digital Forensics, Threat Intelligence, Penetration Testing, Vulnerability Assessment & Remediation, Malware Analysis
Identity & Access Management: RBAC, MFA, PAM, Active Directory, IAM
Infrastructure & Systems: Windows Server & Client, Linux/Unix, Cisco IOS Routing & Switching, Virtualization (Hyper-V, VirtualBox), pfSense
Security Tools: Splunk, Wireshark, Nmap, Metasploit, Burp Suite, Nessus, ELK Stack, Kali Linux
Programming & Scripting: Python, Bash, PowerShell, C/C++, Java, JavaScript, HTML/CSS

PROJECTS

Cybersecurity Home Lab Setup

- Designed and deployed a comprehensive security testing infrastructure using VirtualBox with Ubuntu Server, pfSense firewall, Snort IDS, Kali Linux, and Metasploitable targets.
- Conducted virtual network security assessments identifying vulnerabilities across OWASP Top 10 categories, including SQL injection, cross-site scripting (XSS), and privilege escalation exploits.
- Simulated 15+ attack scenarios, including man-in-the-middle attacks, denial of service, and web application exploitation to develop hands-on incident response and threat mitigation skills.

TryHackMe Cybersecurity Challenges

- Completed advanced security labs covering network exploitation, web application vulnerabilities, privilege escalation, and Active Directory attacks.
- Earned full certifications in Presecurity and Introduction to Cybersecurity pathways, demonstrating proficiency in threat detection, log analysis, and security operations.
- Developed expertise in penetration testing methodologies, reconnaissance, enumeration, and post-exploitation following the industry-standard kill chain framework.

PicoCTF Capture the Flag Competitions

- Competed in 3 CTF events, solving 45+ challenges in cryptography, reverse engineering, binary exploitation, web exploitation, and digital forensics. Developed critical thinking and problem-solving skills applicable to real-world security scenarios.
- Developed critical thinking and problem-solving skills in identifying attack vectors, analyzing malicious code, and bypassing security controls applicable to real-world security scenarios.

Mibrary – Secure Web Application Development

- Led security implementation for the book exchange web application as part of CS373 Software Engineering course, ensuring secure authentication and authorization mechanisms.
- Collaborated in a 5-person Agile team to deploy Python/Flask backend with MySQL database, implementing SQL injection prevention, parameterized queries, and database encryption.
- Implemented Bootstrap UI framework and D3.js data visualizations while incorporating security controls including Content Security Policy (CSP) and cross-site request forgery (CSRF) protection.

Mastercard Cybersecurity Virtual Experience Program | Forage | September 2024

- Enhanced organizational security posture through deployment of quarterly phishing simulations and mandatory security education modules aligned with NIST Cybersecurity Framework.

J.P. Morgan Cybersecurity Virtual Experience | Forage | September 2024

- Analyzed large-scale fraud datasets in financial payment services to identify security patterns and anomalies
- Performed threat detection and incident response activities following NIST incident handling procedures, investigating and documenting findings in detailed incident reports.
- Evaluated security breaches involving unauthorized access and data exfiltration attempts, developing 8 comprehensive preventive security controls and remediation procedures.
- Delivered actionable recommendations to strengthen access controls, network segmentation, and monitoring capabilities, reducing organizational risk exposure by implementing defense-in-depth strategies.

J.P. Morgan Software Engineering Virtual Experience | Forage | April 2020

- Configured a secure local development environment implementing least privilege access controls, secure dependency management, and version control best practices for a financial trading application.
- Implemented JPMorgan Chase's Perspective library to create real-time data visualization dashboards with sanitized inputs and role-based access controls for financial trading operations.

EDUCATION

Cybersecurity & CySA+ Certification Program, Per Scholas | February 2026

Bachelor of Science in Computer Science, The University of Texas at Austin, Austin, TX | Graduated May 2022

Relevant Coursework: *Network Security, Cryptography, Digital Forensics, Secure Software Engineering, Ethical Hacking, Incident Response, Security Risk Management, Cloud Security Architecture*

CERTIFICATIONS

CompTIA Security+ (SY0-701) – Threats, Vulnerabilities, Architecture, Implementation, Operations, Governance, Risk, and Compliance (GRC)

ISC2 Certified in Cybersecurity (CC) – CIA Triad, Access Control, Incident Response, Network Security

AWS Certified Cloud Practitioner – Cloud Services, Security & Compliance, Deployment & Operations

Google Cybersecurity Certificate – Linux, Python, SIEM (Splunk, Google Chronicle)

ITIL v4 Foundation – Service Management, Technical Management Practices

TryHackMe SEC0 and SEC1 (Pre Security and Cyber Security 101) – computer fundamentals, operating systems, software basics, networking, how the web works, introductory security concepts, core security concepts, and essential security principles.

CySA+ (Cybersecurity Analyst) – In Progress | Expected August 2026