Sachin Banjade

Euless, TX | SachinBanjade@my.unt.edu | 330-701-0611 | linkedin.com/in/sachin-banjade-345339248 | github.com/sbanjade | sachinbanjade.com

Professional Summary

Entry-level Security Analyst and Computer Science student with hands-on experience in network traffic analysis, Linux security, authentication and access control testing, and system-level analysis. Proficient in Wireshark, Linux CLI, Nginx, OpenSSL, and security hardening practices. Demonstrated understanding of incident detection, SIEM concepts, vulnerability assessment, and secure system design. Pursuing a role in cybersecurity to apply technical skills in protecting organizational assets and infrastructure.

Technical Skills

Security Domains: Network Security, SIEM, Incident Response, Authentication & Authorization, Access Control, Privilege Escalation Concepts, Vulnerability Assessment, Risk Management, Security Hardening, Least Privilege Principle
Networking: TCP/IP, HTTP/HTTPS, SSL/TLS, Port Analysis, Packet Capture & Analysis, DNS, Firewall Concepts
Tools & Platforms: Wireshark, Hydra (controlled environments), Nginx, OpenSSL, Linux CLI, Git, Bash Scripting
Operating Systems: Linux/Unix (processes, permissions, signals, file descriptors), Windows
Programming / Scripting: Python (automation, scripting), Bash, SQL, C

Education

University of North Texas Denton, TX
Bachelor of Science in Computer Science *Expected May 2026*

- Relevant Coursework: Operating Systems, Networks, Systems Programming, Data Structures, Database Systems

Certifications

Google Cybersecurity Professional Certificate Feb 2026
Google / Coursera

- Automate Cybersecurity Tasks with Python
- Sound the Alarm: Detection and Response
- Assets, Threats, and Vulnerabilities
- Connect and Protect: Networks and Network Security
- Tools of the Trade: Linux and SQL
- Play It Safe: Manage Security Risks
- Foundations of Cybersecurity

SQL Essential Training 2025
LinkedIn Learning

Security Projects

Web Application Security: HTTP vs. HTTPS Traffic Analysis | *Wireshark, Nginx, OpenSSL, Linux* 2025

- Deployed and configured an Nginx web server on Linux to simulate real-world credential transmission scenarios.
- Captured and analyzed HTTP network traffic using Wireshark; identified and documented plaintext credential exposure vulnerabilities.
- Implemented SSL/TLS encryption using OpenSSL and reconfigured the server for HTTPS on port 443, eliminating credential exposure.
- Verified encrypted traffic integrity through packet inspection and TCP stream analysis, confirming successful mitigation.
- Produced findings report demonstrating the risk of unencrypted communications and effectiveness of HTTPS enforcement.

Authentication and Access Control Security Lab | *Linux, Hydra, Bash* 2025

- Designed and executed controlled tests of Linux file permission enforcement and authorization controls to identify misconfiguration risks.
- Conducted ethical brute-force password testing using Hydra against SSH in an isolated environment; documented attack vectors and countermeasures.
- Demonstrated the distinction between authentication and authorization and enforced privilege boundaries using role-based access principles.
- Applied security hardening techniques including least privilege, SSH key-based authentication, and account lockout policies.

Unix System Call and Performance Analysis | *C, Linux, Bash* 2025

- Performed in-depth analysis of Linux system calls including fork, exec, kill, ptrace, and sync to understand kernel-level process behavior.
- Examined process creation lifecycle, memory allocation (sbrk), CPU affinity scheduling, and file descriptor management.
- Benchmarked system call overhead using read/write operations with varying chunk sizes; identified performance bottlenecks relevant to endpoint monitoring.
- Applied findings to strengthen understanding of malware behavior, rootkit techniques, and incident response at the OS level.

Relevant Experience

Student Assistant Youngstown, OH

Youngstown State University *2022 – 2024*

- Maintained accurate documentation and handled sensitive academic records in compliance with data privacy requirements.
- Demonstrated strong attention to detail and confidentiality practices in a structured academic support role.
- Collaborated with faculty and staff to ensure secure and efficient information management workflows.

Key Competencies

Threat Detection | Vulnerability Assessment | Security Monitoring | Log Analysis | SIEM | Incident Response | Network Traffic Analysis | Packet Analysis | Security Hardening | Risk Management | Access Control | Identity & Access Management (IAM) | Penetration Testing Concepts | Scripting & Automation | Linux Security | Compliance Awareness (NIST, CIS Controls)