TANMAY SHARMA

sharma.tanm@northeastern.edu | [LinkedIn](#) | [GitHub](#) | [Portfolio](#)

Education

Northeastern University — **September 2024 – Present**
Master of Science in Cybersecurity — *Boston, MA*

Coursework: Network Security, Linux Administration, Cryptography, Binary Exploitation, Shell Scripting

SRM Institute of Science and Technology — **September 2020 – July 2024**
Bachelor of Technology in Computer Science and Engineering — *Chennai, India*

Coursework: Operating Systems, Computer Architecture, Data Structures, Algorithms, Computer Networks

Experience

CyberspACe securiTy and forensIcs lab (CactiLab) — **March 2024 – Present**
Research Member — *Boston, MA*

- Collaborated on reverse engineering the EdgeTPU driver on Pixel devices, analyzing its interaction with firmware, which enhanced the lab's understanding of hardware security layers.
- Analyzed FirmXRay software by OSUSecLab, focusing on baseaddresssolver.java module, to identify how base addresses are resolved and features extracted, improving vulnerability assessment capabilities in embedded firmware.

Institute for Plasma Research (IPR) — **September 2023 – November 2023**
Network Systems Trainee - Cybersecurity — *Gandhinagar, India*

- Designed and deployed a secure, cost-effective network of Raspberry Pi-based access points, creating a dedicated wireless-to-wireless VPN/Wi-Fi solution for an isolated laboratory of 25–30 plasma physicists, enabling seamless and secure intra-lab communication.
- Implemented advanced encryption and security protocols, reducing network vulnerability by 60% and ensuring compliance with stringent research data protection standards, critical for sensitive plasma research experiments.
- Optimized network performance through real-time monitoring and custom configuration, achieving 99% uptime and improving data accessibility for researchers, which enhanced collaboration and accelerated experimental workflows by 30%.

Projects

Secure Instant Messaging System | *Python, SRP, ECDH, TCP Sockets* — **January 2025 – April 2025**

- Engineered a terminal-based secure chat system leveraging SRP for password-authenticated key exchange, ECDH for secure key derivation, and AES-GCM for end-to-end encrypted messaging, enabling confidential and authenticated real-time communication among users, developed as part of the CY6740 course - Network Security.
- Designed and implemented robust message rate limiting and online user listing features to enhance system integrity and user experience, reducing potential abuse vectors by 80%.
- Developed a socket-based client-server-client architecture supporting encrypted command-based interactions, strengthening the platform's resilience against network-based attacks.

DuckyScript Payloads for Flipper | *DuckyScript, HID Injection, FLipper Zero* — **February 2025 – Present**

- Engineered and maintained a comprehensive repository of advanced DuckyScript payloads and submodules for Flipper Zero, enabling HID-based attacks across Windows and Linux environments.
- Streamlined red team operations and ethical hacking workflows for the cybersecurity community by curating modular BadUSB exploits, credential harvesters, exfiltration scripts, and penetration testing utilities.

Platform for Azure Response & Security Event Correlation | *Azure, AMA, Azure Sentinel* — **November 2024**

- Designed and deployed a cloud-based SIEM using Azure Sentinel, Log Analytics, and a Windows VM to collect and monitor security events in real time.
- Integrated Windows Security Events via Azure Monitor Agent (AMA), enabling centralized log analysis and scalable threat detection across virtual infrastructure.

Technical Skills

Languages: C/C++, Python, Linux x86 Assembly (32bit/64bit), Bash, PowerShell, DuckyScript, SQL
Security Tools: Metasploit, Wireshark, GDB Debugger, Ghidra, Nikto, Burp Suite, Nmap
Technologies: Cryptographic Protocols, SSL/TLS, IPsec, OAuth, Docker, Git, Linux Administration
Security Domains: Penetration Testing, Vulnerability Analysis, Binary Exploitation, Network Security, Incident Response

Certifications & Achievements

Certifications: NSE 1-8 | Palo Alto Fundamentals of Network and Cloud Security | PNPT by TCM Security (In Progress) | CompTIA Security+ (In Progress)
Achievements: SimSpace Cyber Cup 2025 - Top 6 Finalist