BALAJI G

Cybersecurity Professional | Red Team & Purple Team Specialist

📍 Coimbatore, Tamil Nadu, India | 📧 balajigpro121@gmail.com | 🌐 Portfolio = demonjokerwarrior.github.io |

💻 GitHub = https://github.com/demonjokerwarrior| TryHackMe = https://tryhackme.com/p/Demonwarrior121

🎯 PROFESSIONAL SUMMARY

Cybersecurity professional specializing in Purple Teaming, Malware Development (MalDev), and Adversary Simulation with proven success in competitive and real-world environments. Winner of the Tamil Nadu Police Hackathon and International CTF competitions, demonstrating advanced capabilities in offensive security, exploitation, and threat analysis. Certified in CompTIA Security+, with deep expertise in network security, cloud security, and system-level attack techniques. Actively conducting Red Team training programs, mentoring learners in practical cybersecurity and offensive methodologies.

📌 KEY HIGHLIGHTS

- **Offensive & Defensive Synergy:** Strong experience bridging offensive and defensive security through a Purple Team mindset.
- **Controlled Exploitation:** Proven ability to design, execute, and analyze cyber attacks in controlled environments.
- **Low-Level Knowledge:** Strong foundation in system internals, custom payload engineering, and offensive tooling.
- **Mentorship:** Active contributor to hands-on cybersecurity learning, training, and community development.

🧠 CORE EXPERTISE & SPECIALIZATIONS

- 🔴 **Offensive Security (Red Team):** Adversary Simulation, Kill Chain Execution, RAT Development, Payload Engineering, Privilege Escalation, Post-Exploitation, Defense Evasion, Persistence Techniques.
- 🔵 **Defensive Security (Blue Team):** Threat Detection, Traffic Analysis, Incident Investigation, Log Analysis, Network Monitoring, Attack Identification.
- 🟣 **Purple Teaming:** Attack-Defense Alignment, Detection Engineering, Gap Analysis, MITRE ATT&CK Mapping & Validation.
- 🌐 **Security Domains:** Malware Development (MalDev), Network & Wireless Security, Cloud Security Fundamentals, TOR & Dark Web Intelligence/Reconnaissance.

🛠️ TECHNICAL SKILLS

- **Programming & Low-Level:** C (Windows Internals, DLL Payloads, API Evasion), Python (Automation, Security Tools, Flask, SocketIO), JavaScript (Frontend Integration).
- **Tools & Frameworks:** Kali Linux, Wireshark (Advanced PCAP Analysis & Extraction), Git/GitHub, PyAutoGUI.
- **Systems & Infrastructure:** Linux System Administration, Windows Architecture, Network Routing & Switching.

💼 PROFESSIONAL EXPERIENCE

Cybersecurity Instructor – Red Teaming | *Self-Directed / Remote*

[Month, Year] – Present

- Design and deliver hands-on Red Team training programs covering system exploitation, malware basics, and network attacks.
- Train students in real-world attack scenarios, actively improving their practical cybersecurity and defensive skills.
- Build structured learning paths, including WiFi attacks, RAT concepts, and network exploitation methodologies.
- Enable learners to perform complex CTF-style problem-solving and execute structured attack simulations.

🧪 KEY PROJECTS

🔐 **Demons Firewall GUI** | View on GitHub

- Engineered a Python-based firewall management system with an integrated, user-friendly web interface using HTML, CSS, and Bootstrap.
- Implemented real-time traffic monitoring, packet filtering, and control mechanisms.
- Successfully bridged backend security logic with frontend visualization for immediate threat assessment.

🧠 **Stealth Reverse Shell (Windows DLL Payload)**

- Developed a custom reverse shell in C utilizing socket-based communication protocols.
- Implemented stealth execution techniques and advanced obfuscation strategies to bypass standard detections.
- Demonstrated a deep understanding of low-level Windows behavior, memory management, and modern attacker tradecraft.

📡 **Network Forensics & PCAP Analysis**

- Conducted deep packet inspection and network traffic analysis using Wireshark.
- Successfully extracted hidden artifacts, payloads, and nested files (ZIPs/binaries) from complex PCAP datasets.
- Applied forensic methodologies aligned with real-world incident response investigations

and elite CTF challenges.

🤖 **AI-Based Automation & Screen Interaction**

- Built scalable automation systems utilizing Python and PyAutoGUI.
- Enabled real-time screen interaction and intelligent, automated task execution.
- Simulated human user behavior to test security controls and streamline automation workflows.

🏆 ACHIEVEMENTS & CERTIFICATIONS

🎓 Certifications

- **CompTIA Security+** – Industry-recognized certification covering network security, threat management, and risk mitigation
- **Certified Cyber Security Educator Professional** – RedTeam Leaders
- **Certified Ethical Hacker & Bug Bounty Hunter** – Cyfotec
- **Offensive Security Specialist** – TryHackMe

🏆 Achievements

- 🥇 **Award Winner – Tamil Nadu Police Hackathon**
  - Recognized for strong practical cybersecurity skills and real-world problem solving
- 🌍 **Winner – International Capture The Flag (CTF) Competition**
  - Demonstrated advanced capabilities in exploitation, reverse engineering, and network security
- 🎯 **Top 100 Rank – Offensive Security "Art of Hacking" Event**
  - Ranked among **Top 100 out of 2000+ participants** in a highly competitive global offensive security challenge conducted by Offensive Security

---

🎯 CTF & Competitive Participation

- 🧠 **Participant – Yukthi CTF (Government of Tamil Nadu Initiative)**
  - Competed in national-level challenges covering cryptography, forensics, and exploitation

---

🔥 Professional Recognition

- Active contributor in **offensive security labs and competitive environments**
- Consistent performer in **hands-on cybersecurity challenges and adversarial simulations**
- Demonstrates strong **practical, real-world security mindset aligned with Red/Purple Team operations**

🎓 EDUCATION

BSC Computer science with cyber security Rathinam college of arts and science Echanari, Coimbatore