

BUGGY

Cybersecurity Enthusiast — Aspiring RedTeam Operator

🌐 buggymaytricks.page ✉ contact@buggymaytricks.page

About

Aspiring Red Team operator and ethical hacker with **2+ years** of hands-on cybersecurity learning. Currently pursuing **Computer Engineering** and ranked in the **top 2% on TryHackMe** with 120+ labs completed. Focused on core offensive security concepts including web exploitation, privilege escalation, and system enumeration. Gained practical exposure through internships and CTFs, building a foundation in real-world methodologies. Actively building custom tools, sharing knowledge through technical content, and preparing for certifications like **CPTS** and **CJCA**.

Education

Sinhgad Academy of Engineering

B.E. Computer Engineering

September 2024 – May 2028

- Learning C, C++ , Python, Java, and Bash scripting, focusing on problem-solving.
- Practicing Object Oriented Programming, Getting hands-on Data Structures.
- Deep dive into Operating Systems

Experience & Achievements

Cybersecurity Intern

2024

ENCODERSPRO Private Limited

Remote

- Completed intensive Cyber Security training program covering advanced ethical hacking, OSINT, SIGINT, and digital forensics
- Developed real world botnet simulation framework for understanding malware C2 communications
- Analysed communication between bot and the C2 for better defenses

Cybersecurity Intern

March 2024 – April 2024

Threat Prism

remote

- Developed a Recon Automation for Info Gathering, Network Scanning and Web Pentesting.
- Built advanced phishing simulation frameworks for social engineering assessments

Capture The Flag(CTF) & Competitions

20xx – Present

TryHackMe, HackTheBox & Various Platforms

Remote

- **Top 2% on TryHackMe Globally** - Consistent high performance across 120+ red team focused labs
- **Hackfinity CTF** - Ranked 229th out of 4,309 participants in TryHackMe's flagship competition
- **Rise Get Set Hack** - Secured 85th position among 22,000+ participants nationwide
- Active participant in DamnCon CTF, NahamCon CTF, and international red team competitions

Featured Projects

ECSIP Botnet Simulation & Analysis | *Python, Network Analysis, Malware Research*

2025

- Developed comprehensive botnet simulation framework for red team operations
- Implemented wireshark network traffic analysis for studying advanced malware communication patterns
- Created a custom flask based C2 dashboard for controlling multiple bots
- Built cross-platform compatible bots for simulating and studying real world APT's
- Open-sourced on GitHub with detailed documentation for the cybersecurity research community

Hash-Verify | *Python, CLI, Cryptography*

2024

- Open-source file integrity verification tool supporting multiple hash algorithms
- User-friendly CLI interface designed for rapid file verification.
- Open-sourced on GitHub with detailed documentations

Active Directory Lab | *Windows Server, PowerShell, AD Exploitation*

2024

- Custom-built AD environment for practicing advanced red team techniques and attack paths
- Simulates real-world enterprise scenarios like Kerberoasting
- Implements lateral movement scenarios and post-exploitation persistence mechanisms
- Used for continuous skill development and red team technique validation

Technical Skills

Penetration Testing: Web Application Testing, Network PenTesting, Active Directory PenTesting
Programming Languages: Python, C, C++, Java, Bash, SQL
Security Tools: nmap, nessus, metasploit, burpsuite, nikto, ffuf, bloodhound, Impacket, CrackMapExec, responder
Reconnaissance & OSINT: Nmap, FFUF, Burp Suite, Shodan, Recon-ng, theHarvester
Operating Systems: Linux (Kali, Parrot, Ubuntu, Mint, etc), Windows

Certifications

Certified AppSec Practitioner (CAP)	2024
TCM Security - Practical Ethical Hacking - <i>Completed</i>	2024
Certified Junior Cybersecurity Analyst (CJCA) - <i>Currently Pursuing</i>	HackTheBox
Certified Penetration Testing Specialist (CPTS) - <i>Next Target</i>	HackTheBox

Community & Red Team Focus

Technical Blog Writing: Active blogger sharing red team techniques, setup blogs, tips and tricks, and security research insights
Open Source Contribution: Active GitHub contributor focusing on red team tools and offensive security research
Knowledge Sharing: Writing detailed CTF writeups, red team techniques, and whatever I learn
Interests: Red Team Operations, Advanced Persistent Threats, Malware Analysis, Cloud Security, Adversary Simulation