GEETANSH ADITYA

Cybersecurity Engineer - Offensive Security Focus

geetanshaditya2005@gmail.com +91-9352095862 geetanshaditya.in Bengaluru, Karnataka

Summary

An offensive security enthusiast with expertise in Red Teaming, Reverse Engineering and Malware Development. Skilled in exploit development, memory loader engineering, and AV/EDR evasion techniques. Active contribution to open-source red team tools and engaging in real-world CTFs and bug bounty programs. Experienced in Linux environments, Bash and PowerShell scripting, and stealth operation in adversary simulations. Passionate about learning both attack and defense, currently sharpening my blue teaming tactics. Currently seeking red or blue team roles to apply offensive capabilities, reverse engineering insight, and real-world adversary simulation in production environments.

Projects

BloodProxy

Developed a custom MitM reverse proxy tool for red teaming, enabling TLS interception via forged certificate injection, similar to Burp Suite.

DozerNet

A stealthy process injection framework for simulating botnet behavior and orchestrating controlled DoS attacks during red team assessments.

GhostForge

A windows payload generator which can bypass any AV/EDR solution useful for red and purple team exercises

MemPEeler

A custom memory loader which revives packed executables by dumping, reparing IAT and making it executable

Education

BTECH CSE (Cybersecurity) 2025 - Present
Alliance University

Higher Secondary (PCM) 2020 - 2022
Delhi Public School

Skills

Cybersecurity Domains:
Red Teaming, Blue Teaming, Adversary Simulation, Malware Analysis, Reverse Engineering, DFIR, OPSEC, Privilege Escalation, Post-Exploitation

Tools & Frameworks:
Metasploit, Burp Suite, Nmap, Wireshark, Zeek, Velociraptor, Sysmon, BloodHound, ImHex, CrackMapExec, Suricata, CyberChef, YARA, ELK Stack

Scripting & Payload Dev:
Python, Bash, PowerShell, C, Custom Reverse Shells, AV/EDR Evasion, Automation of TTPs, Linux Internals, Windows API Abuse

Reverse Engineering & Malware Analysis:
Static & Dynamic Analysis, Ghidra, x64dbg, Shellcode Crafting, Custom Packers, Memory Dumping, IAT Fixing, API Hooking, AMSI Bypass, Obfuscation

Platforms & Labs:
TryHackMe, Hack The Box, PwnTillDawn, DetectionLab, MalwareBazaar, Penathon CTFs

Other Domains:
Web Exploitation, Network Recon, Active Directory Attacks, Threat Hunting, Log Analysis, Forensics, Detection Rule Writing (Sigma/YARA)

Key Achievements

ContinuumCon 2025: CTF Rank #4
ContinuumCon CTF 2025, a blue team based CTF focued on DFIR, Threat Hunting, Reverse Engineering, Malware Analysis and more. With hundreds or participants I managed to secure the 4th rank.

All India Rank 1 - PwnTillDawn 2025
International red team-style CTF simulating real-world attack chains.

Pentathon: All India CTF Rank #41
Secured first place in a national CTF, demonstrating strong collaboration, fast learning and practical offensive security skills under real-world challenge scenarios.

Certification

Certified in Cybersecurity (CC) by ISC2 - 2025

Cisco Ethical Hacker Badge - Cisco Networking Academy, 2025 (Skills Badge)