MOHITH
TUMMALAPALLI

CRTP, Security+

+91 79866 33983 ☎
mohith.tummalapalli@outlook.com ✉
Rajahmundry, Andhra Pradesh ◉

About Me

A passionate blue teamer, certified with CRTP and SC-900 working in both Offensive and defensive fields combating threats. Exploring the operating systems while also focusing on Active Directory misconfiguration s and abuses. Currently deep diving hunting into understanding and adversary tradecraft.

Skills

- Microsoft XDR
- Threat Hunting
- Malware Development
- Security Operations (SOC)
- OSINT
- WINAPI Programming - C/C++
- Threat Intelligence
- Active Directory

Certs / Badges

- Comptia Security +
- Microsoft SC-900: Microsoft Security, Compliance, and Identity Fundamentals
- Altered Security - CRTP (Certified Red Team Professional)
- Pentester Academy
- PentesterLab
- Ace Responder
- TryHackMe
- AttackDefense Labs
- HacktheBox
- PortSwigger Labs
- BlueTeam Labs Online

Professional Links

GitHub | LinkedIn | Twitter/X

Work Experience

2022
10 months

Cyber Security Intern | DreamBig IT Solutions

- Generated malware samples with different capabilities for Windows using C++.
- Created and maintained lab environments for launching CTFs on AWS and VMWare environments.
- Authored numerous challenges from different domains in cyber for the students to easily understand underlying security concepts.
- Assisted in Penetration Tests and Vulnerability assessments.
- Worked on Application Security, Network security, Reverse engineering and malware analysis.

Education

2020-2023

B.TECH IN COMPUTER SCIENCE AND ENGINEERING
Alliance University | Bengaluru

2016-2019

DIPLOMA IN COMPUTER SCIENCE AND ENGINEERING
Lovely Professional University | Jalandhar

Projects

CYBERWHIZ

CyberWhiz is a gamified cyber security education platform. I've contributed in generating CTF challenges for cryptography, hashing and OSINT challenges on this platform.

WINAPI Repository

I've noted down my journey into the world of WINAPI coding. A series of programs used to create and manage - processes, threads, objects and various other windows kernel objects. A collection of C++ programs to help understand windows internals and operating system concepts.

Sentinel

A ML backed proxy based web application firewall. A trained model to distinguish between benign and malicious web traffic. Written in Python to understand HTTP traffic and nuances of attack vectors and payloads.

Real Estate - Price Analysis

Performed price and trend analysis on the past 10 years data of real estate data and derived insights into future trends and price predictions on various factors. Dataset used was from Kaggle.

Dynamic Sky

A MySQL and IIS based ASP web application that fetches data from weather API and displays weather conditions across Indian regions.