

Krishna Vamshi Katta Rokkaiah

• (301)-728-4227 • [LinkedIn](#) • krish789@terpmail.umd.edu

EDUCATION

Master of Engineering, Cybersecurity

May 2021

University of Maryland, College Park

Courses: Hacking of C Programs and Unix Binaries, Penetration Testing, Reverse Software Engineering, Network Security, Digital Forensics and Incidence Response, Cloud Security

Bachelor of Engineering, Information Science and Engineering

Aug 2019

Dayananda Sagar College of Engineering, Bangalore

Courses: Unix System Programming, Computer Network and Cyber Security, Wireless and Mobile Networks

CERTIFICATIONS AND SKILLS

- **Certified Ethical Hacker v10 (CEH):** Certified by EC-Council.
- **A+ and N+:** Recognized as a Computer Hardware and Network Engineer.
- Currently pursuing Offensive Security Certified Professional (OSCP).
- **Networks Tools:** Cisco Packet Tracer, Snort, Wireshark, Nmap, Splunk.
- **Security Tools:** Qualys, Nessus, IDA, Metasploit, httpRecon, Burp-suite, GDB.
- **Programming:** C, C++, Java, Python, Assembly, Bash Scripting, PowerShell.
- **Assurance:** Familiar with PCI-DSS, HIPAA, ISO 2700x, Threat Modeling.
- **Cloud:** Essentials of Amazon Web Services (AWS) and Microsoft Azure.

EXPERIENCE

Hindustan Aeronautics Limited, Bangalore

Jun - Jul 2018

Intern

- Acquainted with real-time implementation of Enterprise Resource Planning (ERP) systems.
- Devised strategies for organizing Online Exam System throughout 5 modules of HAL, Bangalore.
- Led a team of 2 and collaborated with 5 employees of IT department to develop and formulate a design project for implementation of Online Exam System.

PROJECTS

Reversing Slammer Worm

Oct – Dec 2020

- Utilized GDB and IDA to inspect 32-bit binary of Slammer worm in detail.
- Studied structure of packet to determine malware's payload and technique used to propagate worm.

Honeynet on a Windows Domain

Jul – Aug 2020

- Deployed and configured a Windows domain consisting of 5 Windows and Unix-based systems to simulate a company environment along with an external pfSense firewall.
- Setup Artillery honeypot on a Windows Server 2016 to monitor folders and blacklist specified IP addresses.
- Implemented Cowrie honeypot on an Ubuntu client in order to fake a filesystem and log SSH commands over a connection.

Windows Forensic Analysis

Mar – May 2020

- Examined given Windows image using Autopsy to search for hidden and important information.
- Extracted and decrypted files to review contents for further inquiry.
- Correlated data obtained from Wireshark packet captures and Autopsy to obtain final flag.

Heap Exploitation [Unsafe Unlink and Overlapping Chunks]

Oct – Dec 2019

- Led a team of 3 to analyze and demonstrate Overlapping Chunks exploit techniques in 32-bit machine.
- Executed shellcode (8 bytes) by corruption of GOT table and heap overflow using GDB.
- Demonstrated and devised strategies for mitigating heap exploits in real life situations.

EXTRA CURRICULARS

- Awarded runners-up in Business Marathon conducted by IEDC, DSCE.
- Competed in regional level volleyball and football competitions at KVS, India sports meets.