MUNI NITISH KUMAR YADDALA

nitish.yaddala@gmail.com Atlanta, USA LinkedIn Github Portfolio

EDUCATION

Georgia Institute of Technology | CGPA: 3.5/4.0 **Aug 2022 – Dec 2023**
Master of Science in Cybersecurity—Information Security *Atlanta, USA*
Relevant Coursework: Introduction to Information Security, Network Security, Secure Computer Systems, Computer Networks, Applied Cryptography, Secure Internet Infrastructure

SRM Institute of Science and Technology | CGPA: 3.8/4.0 **Jul 2018 – May 2022**
Bachelor of Technology in Computer Science Engineering *Chennai, India*
Relevant Coursework: Computer Networks, Network Security, Advanced Programming in Python

PROFESSIONAL EXPERIENCE

HP Inc. **Feb 2022 – Jul 2022**
Penetration Tester Intern | *Kali Linux, Burp Suite, OWASP Top 10, SSL Labs* *Bangalore, India*
- Identified and reported 20 vulnerabilities in 6 applications using Veracode's SAST reports and DAST, mainly utilizing BurpSuite.
- Proposed tailored mitigation strategies for discovered vulnerabilities, leveraging insights from the application team.
- Gained expertise in OWASP Top 10 vulnerabilities through hands-on testing and research, improving future penetration tests.

Indian Space Research Organization (ISRO) **Nov 2019 – Dec 2019**
Network Engineer Intern | *Wireshark, Custom tool* *Sriharikota, India*
- Reduced attack surface on the subnetwork by closing 30 unused ports on 20 devices, including FTP and TELNET.
- Monitored 30 network assets with the custom tool to maintain performance and prevent downtime.
- Enhanced network performance by analyzing traffic, using Wireshark, to identify choke points.

SKILLS & CERTIFICATIONS

Languages: Python | HTML | CSS | JavaScript

Operating Systems: Kali Linux | Windows | Ubuntu | Parrot Security

Tools: Burp Suite | Wireshark | Metasploit Framework | Nmap | Netcat | John the Ripper | Nikto |WinPEAS | LinPEAS | sqlmap | Immunity Debugger | DirBuster | ffuf |Responder |PsExec | dnsrecon | hashcat | sublist3r | Mimikatz | Nessus | impacket | BloodHound | VS Code | MS Office 365

Miscellaneous: Penetration Testing | Web Application Security | Network Security | Vulnerability Assessment | Threat Mitigation | Active Directory | Computer Networking

Certifications: Certified Network Defender (CND): EC-Council | Certified Network Defender (CND): EC-Council | Certified in Cybersecurity (CC): (ISC)² | OSCP: Offsec (Pursuing)

PROJECT EXPERIENCE

Honeypot+ | *Python, Snort, htop, VS Code, Ubuntu, VirtualBox* **Aug 2023 - Dec 2023**
- Developed a lightweight tool emulating 30 services, optimizing resource usage and ensuring user-friendly deployment.
- Enhanced security by integrating with Snort IDS, actively detecting attacks on various services.
- Actively streamlined logs to a designated website for centralized analysis, ensuring minimal resource consumption.

System Call Hooking and Malicious String Detection | *Python, Linux kernel programming, VS Code, Ubuntu, VirtualBox* **Oct 2023**
- Developed a system call hook in the Linux kernel to log new directory paths and systematically captured parameters for 21 syscalls.
- Automated collection of system call invocations for a target binary in Python, streamlining the analysis process efficiently.
- Designed a Python system call analysis framework, trained on 100 non-malicious inputs, and validated for maliciousness detection.

Binary Exploitation | *Ghidra, Python, VS Code, Metasploit, Kali Linux, Bash, Ubuntu, VirtualBox* **Sep 2023**
- Discovered and exploited overflow vulnerabilities in three binaries employing reverse engineering techniques like pattern creation, precise offset calculation, and custom payloads.
- Automated exploitation with Python's 'pwn' package, managing binaries, inputs, & capturing outputs for efficient workflows.
- Analyzed binary code to identify vulnerable functions and exploitable conditions, demonstrating a practical grasp of low-level programming concepts, enhancing overall system security.

CMS v2.8 Exploitation: Gaining Shell and Root | *Nmap, Metasploit, Kali Linux, Virtual Box, GTFObins, LINPEAS* **Aug 2023**

- Conducted an intensive Nmap scan, unveiling open ports 22, 80 (leading to directory discovery at /navigate), and 53.
- Exploited Navigate CMS v2.8, achieving a shell and www-data user access, followed by privilege escalation attempts.
- Detected 3 SUID-enabled PHP files, allowing privilege escalation, and used 1 to maintain escalated privileges using GTFObins.

WebPulse | *Python, Kali Linux* **May 2023**

- Developed and tested a comprehensive web-target probing command line tool, featuring user-friendly functionality, and supporting both HTTP and HTTPS protocols, resulting in high accuracy rate in determining target status.
- Designed dynamic output formatting, visually distinguishing target validity and status stages, significantly enhancing user comprehension compared to previous versions.

Denial-of-Service (DoS) | *Wireshark, HOIC, LOIC, Windows, Kali Linux, Metasploit Framework, VirtualBox* **Sep 2021 - Oct 2021**

- Executed DoS attack using HOIC and LOIC, reducing machine performance by 75% through TCP and UDP packet flooding.
- Performed successful SYN flood attack, diminishing target machine performance by 50% with Metasploit's synflood module.

Making a virus undetectable | *Windows, ProRat, VirusTotal, PolyCrypt* **Jul 2021**

- Developed and implemented advanced polymorphic encryption techniques to evade anti-virus detection, resulting in an evasion rate of about 50% of a virus created using ProRat.
- Generated a virus using ProRat with high detection rates of 58 out of 67 available anti-virus programs at VirusTotal, leveraged in proving the effectiveness of the encryption techniques utilized.
- Leveraged PolyCrypt to encrypt viruses and decrease detection rates by 35% from initial testing results, successfully avoiding detection by 33 out of 69 available anti-virus programs at VirusTotal.

Network Designing | *Windows, Packet Tracer* **Aug 2020 – Sep 2020**

- Developed a custom network design featuring limited IP addresses and efficient subnetting techniques to avoid IP address wastage.
- Implemented a network security plan, utilizing access control lists and subnetting to restrict unauthorized access.
- Restricted internet access to the 7th department by using the access control list to block ports 80 and 443.

EXTRA-CURRICULAR ACTIVITIES

Identified an IDOR Vulnerability in State Government Website

- Discovered an Insecure Direct Object Reference (IDOR) vulnerability in a state government website, posing risks of horizontal privilege escalation and unauthorized access to sensitive user data.

Flipkart Grid 3.0 - Information Security Challenge

- Led a team of 3 to secure semi-finalist rank in the national competition, outperforming over 3000 teams.

BSidesPhilly 2023 Conference

- Participated in BSidesPhilly 2023, fostering cybersecurity awareness, research, and networking in the Philadelphia region.

NahamCon CTF 2023

- Led a late-entry CTF team to achieve the top third percentile.

Red Team Hacker Academy's Capture the Flag Competition

- Achieved a 65% success rate, securing 5th place among 50+ teams, overcoming intricate challenges in the competition.

Infysec and Zybeak Technologies Capture the Flag Competition

- Competed in the CTF Competition demonstrating expertise in penetration testing and vulnerability assessment.