MUNI NITISH KUMAR YADDALA

+1 (404) 451-4193 | nitish.yaddala@gmail.com | Atlanta, Georgia, USA | linkedin.com/in/nitish-yaddala/

EDUCATION

Georgia Institute of Technology | **CGPA:** 3.50 / 4.00   **Aug 2022 – Dec 2023**
Master of Science in Cybersecurity - Information Security   *Atlanta, GA*
Relevant Coursework: Introduction to Information Security, Network Security, Secure Computer Systems, Applied Cryptography

SRM Institute of Science and Technology | **CGPA:** 9.49 / 10.00   **Jul 2018 – May 2022**
Bachelor of Technology in Computer Science Engineering   *Chennai, TN*
Relevant Coursework: Computer Networks, Network Security, Advanced Programming in Python

SKILLS

Programming: Python, Bash, HTML, CSS, JavaScript, SQL

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

Tools: Burp Suite | Wireshark | Metasploit Framework | Nmap | Snort | Netcat | John the Ripper | Nikto | Immunity Debugger | Ghidra | Virtualbox | VS Code | MS Office Suite

Miscellaneous: Penetration Testing | Web Application Security | Vulnerability Assessment | Network Security

PROFESSIONAL EXPERIENCE

HP Inc.   **Feb 2022 – Jul 2022**
Penetration Tester Intern | Kali Linux, Burp Suite, sslscan, SSL Labs   *Bangalore, KA*
- Identified and reported 20 vulnerabilities across 6 applications using Burp Suite and Kali Linux tools, and suggested mitigations.
- 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**
Networking Intern | Wireshark   *Sriharikota, AP*
- Secured 35% attack surface reduction on the subnet by closing 30 unused ports on 20 devices, including FTP and TELNET.
- Improved subnet's performance by identifying choke points, using Wireshark and a custom tool, leading to a 20% performance boost.

PROJECTS

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 web-target probing tool with HTTP/HTTPS support, yielding 98% target status determining accuracy.
- Enhanced output design for better target interpretation, boosting comprehension by 40%.

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.

Enhanced Virus Evasion | *Windows, ProRat, VirusTotal, PolyCrypt*   **Jul 2021**
- Developed a virus with a 58/67 anti-virus detection rate, demonstrating encryption technique effectiveness.
- Enhanced detection evasion by 35% and outwitted 33 out of 69 antivirus programs using PolyCrypt.

ACCOMPLISHMENTS

IDOR Vulnerability - State Government Website   **Feb 2023**
- Discovered an Insecure Direct Object Reference (IDOR) vulnerability in a state government website, demonstrating cybersecurity efforts to protect sensitive user data for over 500 individuals.

Flipkart Grid 3.0 - Information Security Challenge   **Jul 2021**
- Led a team of 3 to secure semi-finalist rank in the national competition, outperforming over 3000 teams.

CERTIFICATIONS

Practical Ethical Hacking (PEH): TCM Security | Certified Ethical Hacker (CEH): EC-Council | Certified Network Defender (CND): EC-Council | Shields Up: Cybersecurity Virtual Experience Program: AIG | Certified in Cybersecurity (CC): (ISC)² | Introduction to Cybersecurity: Cisco

EXTRACURRICULAR ACTIVITIES

NAHCOMM CTF 2023: Led an impressive CTF comeback, securing 867th out of 2631 teams, despite joining late. **Jun 2023**

Red Team Hacker Academy's CTF: Achieved a top 5 ranking out of 50 teams by implementing innovative strategies, resulting in a remarkable success rate of 65%. **Apr 2021**

Infysec & Zybeak Technologies CTF: Ranked 10th out of 62 teams in the CTF Competition, showcasing proficiency in penetration testing, vulnerability assessment, and security skills. **Oct 2020**