Aditya Dindi

Cyber Security Professional

+1 (303)-901-9459 | Email: adindi369@gmail.com | Website: https://adityadindi.com | www.linkedin.com/in/adityadindi

OSCP and Security+ certified Cybersecurity Professional with 3+ years of experience. Strong skills in conducting research and analysis in the threat hunting landscape to promote better cybersecurity practices and defenses. Developed programs in open source software to create logs for threat hunting. Good understanding of security methodologies, technologies, and best practices. Exceptional communication, presentation and interpersonal skills with proficiency at grasping new concepts quickly and productively.

Global finalist at the Collegiate Cyber Penetration Testing Competition (CPTC). Club Officer and Security+ Mentor in the CompTIA Student Chapter at the University of Texas at San Antonio.

Skills

Tools: Cobalt Strike C2 • Nmap • Burp Suite • Wireshark • Hydra • JohnTheRipper • Metasploit • Bloodhound • Mimikatz • CrackMapExec
Programming/Scripting Languages: Java, Python, Bash
Web Development: HTML/CSS, Javascript, Git/GitHub/GitLab
Github Page: Pyrus369 | ***Security Blogs / Writeups***: writeups.adityadindi.com

Experience

Defensive Cyber Operations, MITRE | May 2022 - Present

- Conducted research and analysis in the threat hunting landscape to promote better cybersecurity practices and defenses within corporate environments and contributed to the MITRE ATT&CK Defender program.
- Contributed to a MITRE ATT&CK Defender™ training course teaching a MITRE ATT&CK Technique and its sub-techniques with detailed Threat Research and Adversary Emulation testing.
- Developed Python programs to create logs for a Hands-On Threat Hunting testing environment (Elastic Stack / Kibana)
- Created a mapping capability to showcase process flow and decision making of MITRE ATT&CK techniques. Identified various paths ATT&CK techniques can take that helps identify adversary and benign behavior to build better analytic detections.

Penetration Tester, Government Agency (Classified) | 2023

- Conducted comprehensive penetration testing for sensitive government networks, systems and web applications, utilizing advanced methodologies to identify vulnerabilities and develop robust security solutions.
- Collaborated with cross-functional teams to analyze test results, prioritize risks, and develop appropriate mitigation strategies.
- Prepared a detailed report outlining findings, including identified vulnerabilities, recommended remediation measures, and potential impacts.

Education

University of Texas at San Antonio, TX | *Bachelor of Business Administration in Cyber Security*

- Cyber Security Lab (CSL) Red Team Operator and Infrastructure Engineer
- IoT Lab Researcher
- Vice President and Security+ Mentor at the CompTIA Student Chapter

Certifications

Offensive Security Certified Professional (OSCP)
Certified Red Team Operator (CRTO) [In-Progress]
CompTIA Security+ SY0-601
Microsoft Technology Associate: Security Fundamentals

Competitions

Member, Global Collegiate Cyber Penetration Testing Competition (*CPTC*), University of Texas at San Antonio (2022)

CPTC 2022: Global Finalist | 2nd place in Southeast Regionals

Member of the University of Texas at San Antonio's CPTC team. CPTC is a competition for college students to demonstrate their technical and business skills by conducting a full penetration test and finding vulnerabilities in a stimulated corporate network infrastructure. The team was responsible for responding to client questions while actively trying to find vulnerabilities and writing a professional report within a specific timeframe.

Captain, National Centers of Academic Excellence Cyber Games (*NCAE*), University of Texas at San Antonio (2022)

NCAE Cyber Games 2022: 3rd place in Regionals

Captain of the University of Texas at San Antonio's NCAE team. NCAE is a competition for college students where we learn about cyber competitions in an environment focused on teamwork, building confidence and growing our skills.