Jonathan Vargas

Penetration Tester

BASIC INFO

Address
San Antonio, TX

Phone Number
(210) 550 - 6119

Website
Linkedin.com/in/JonathanSec/

Email Address
11JonathanVargas11@gmail.com

CERTIFICATIONS

CRTO
Zero-Point Security
October 2022

OSCP
Offensive Security
January 2021

Security+
CompTIA
August 2020

TECHNICAL PROFICIENCIES

- Red Team Operations
- Infrastructure Pentesting
- Web Application Security Auditing
- Social Engineering
- Digital Forensics
- Antivirus Evasion
- Reverse Engineering
- Exploit Development
- Vulnerability Assessment Reporting
- Physical Security Assessments
- Active Directory

SOFT SKILLS

- Teaching
- Presentation
- Leadership
- Public Speaking
- Client Relations
- Mentorship

AWARDS

DEFCON CTF Winner
DEFCON
August 2022

Contributed a pivotal role in EY's first place victory at DEFCON's biomedical hacking competition, in which a small team of EY red team operators solved more biomedical security challenges than over 100 competing teams worldwide.

Top 5% of CTF Teams
Hack The Box Cyber Apocalypse
April 2021

Led a CTF team comprising of nine other security enthusiasts from around the world. Our team ranked in the top 5% of participating teams by effectively tackling a series of cyber security challenges during the Cyber Apocalypse CTF.

PROFESSIONAL SUMMARY

I am proficient in planning and executing red team operations, discovering flaws and weaknesses in enterprise computer networks, and chaining together vulnerabilities to perform full domain takeovers of corporate environments. I have two years of experience in performing every stage of the cyber attack life cycle in industries such as healthcare, manufacturing, financial institutions, and energy. I am committed to devising effective mitigation techniques at operational and strategic levels in order to ensure our private data remains private.

EDUCATION

The University of Texas at San Antonio
BBA - Cyber Security
(August 2017 - May 2021)
3.72 GPA

The University of Texas at San Antonio
BBA - Information Systems
(August 2017 - May 2021)
3.72 GPA

EXPERIENCE

Penetration Tester
Ernst & Young
(July 2021 - Present)

- Plan and execute adversary simulation operations for large corporate clients in various industries by applying knowledge of red team operations, command and control frameworks, and engagement planning.
- Perform each stage of the cyber attack life cycle from reconnaissance to full domain takeover, whilst evading defenses and keeping OPSEC considerations at the forefront.
- Executed internal, external, web application, and red team operations for over 20 corporate clients.
- Developed and carried out social engineering campaigns with the purpose of convincing employees into divulging sensitive information about the organization via spoofed phone calls and email messages.
- Delivered physical security audits at corporate locations to demonstrate various methods in which an outsider threat can gain access to company resources without authorization.
- Researched the latest exploit trends and gave internal talks on cyber threat intel
- Mentored batches of newly on-boarded security analysts who were interested in learning more about penetration testing and how to leverage educational resources to hone their craft

Cyber Security CTF Organizer
Self-Hosted
(August 2020 - August 2020)

- Executed an open capture-the-flag competition for members of the Try Hack Me and Hack The Box ethical hacking communities. Two teams of five members were tasked with exploiting a remote server, gaining access, then establishing tighter security controls in order for the opposing team to fail at breaching entry.
- Assembled a collection of three exploitable machines containing vulnerabilities in line with the Open Web Application Security Project's (OWASP) top ten security risks.
- Researched real-world security compromising incidents and integrated recent exploits into the competition's vulnerable machines.

SQL Developer
Ward North American
(February 2020 - August 2020)

- Optimized MS SQL reporting scripts for lower data retrieval latency
- Debugged live SQL reports for database inconsistencies.
- Collaborated with various department managers to build a data management system that fits the department's requirements.
- Creatively devised functions of exporting and aggregating business data to adjust for the company's changing data management practices.

President
UTSA Swing Dance Society
(May 2019 - May 2020)

- Headed a student-led organization to preserve the social dance and culture of the swing jazz era
- Orchestrated weekly dance instruction
- Cultivated a Board of Executives
- Partnered with community and intercollegiate organizations

IT Intern
Ward North American
(March 2019 - February 2020)

- Spearheaded the development of aggregation software to understand sales trends
- Developed two complex SQL and JDBC algorithms to fully automate corporate budget analysis
- Inspired the prototyping of Ward University: a learning management system for small corporations
- Collaborated closely with cloud service provider to ensure network reliability
- Offered expert IT troubleshooting and consultation for software and hardware solutions
- Gained experience using Wireshark to monitor network activity and identify network issues
- Developed automated emails to be sent out to customers and agents

PROJECTS

Penetration Testing Blog
https://vargasportfolio.github.io

Developed a simple online CV detailing my past penetration testing engagements, cyber attack methodologies, and CTF writeups.

Self-Hosted Cloud Solutions

Researched the benefits and utility of virtualized micro-services in order to deploy a network of Docker containers for remote file system management. By configuring Docker volumes, networks, images, and containers using Portainer, I was able to effectively host my own Nextcloud storage platform from a home lab.

Cyber Apocalypse CTF
https://www.hackthebox.eu/cyber-apocalypse-ctf-2021

Organized a global team of ten cyber security enthusiasts to participate in Hack The Box's Cyber Apocalypse CTF. By rotating shifts, we were able to tackle dozens of security challenges for 24 hours each day for five days. As a result, the team ranked in the top 5% of teams out of 4,740 worldwide

Aero CTF
https://ctftime.org/event/1224

First team-based CTF experience in cracking real-world cyber security puzzles in a Jeopardy-style format. Exposed to diverse methodologies for handling digital forensics incidents, network vulnerability assessment, reverse engineering, and web application security flaws