# JAMES FLORES

linkedin.com/in/jamesfloresjr

## PROFESSIONAL EXPERIENCE

**US Air Force Reserves** — **San Antonio, TX**
**Incident Responder** — **09/2019 - 06/2022**

- Utilized EnCase and Tanium to investigate and perform incident response activities
- Conducted analysis to identify indicators of compromise (IOCs) on the network
- Facilitated vulnerability scanning by automating the surveying of firewall rules, processes, services, autorun directories, etc. with PowerShell scripts
- Responded to security events and initiated triage of devices by collecting and sending data to the appropriate departments

**Malware Analyst** — **06/2022 - Present**

- Analyzed malware and exploits to support the 33rd Network Warfare Squadron AFIN-SOC
- Looked at malicious PDFs to identify anomalies such as embedded URLs and JavaScript code
- Performed memory forensics and malware reverse engineering of suspected malicious files to verify if system compromise occurred

**CACI International Inc.** — **San Antonio, TX**
**System Administrator** — **06/2020 - Present**

- Created multiple PowerShell scripts to automate tedious administrator tasks
- Deployed downstream/upstream WSUS servers onto multiple networks
- Used Nutanix to create servers and manage virtual desktop infrastructure
- Created and deployed gold images using Citrix
- Ran SCAP and Nessus scans to implement STIG compliance and mitigate vulnerabilities

**CNF Technologies** — **San Antonio, TX**
**System Administrator** — **10/2019 - 06/2020**

- Pushed scripts through group policy which allowed for the automation of daily routines
- Accompanied Quality Assurance team by running through processes and correcting any issues
- Updated certificate revocation list weekly, allowing the use of two factor authentication for our development network

**US Air Force** — **San Antonio, TX**
**System Administrator** — **09/2015 - 09/2019**

- Provided IT support ranging from password reset to the installation and removal of IT equipment
- Replaced 400+ systems, installed CAT5, and installed various telecommunication equipment
- Accomplished administrative tasks on Windows and Linux systems

## CERTIFICATIONS

- CompTIA Security+ ce
- CompTIA Linux+ (Powered by LPI)
- Certified Linux Admin (LPIC-1)
- GIAC Certified Forensic Analyst

## EDUCATION

Associate of Applied Science in Cyber Security

Bachelor of Science in Computer Science, Projected 2023

## TECHNICAL SKILLS

- Python
- PowerShell
- Java
- JavaScript
- Ghidra
- PeStudio
- x64dbg
- Process Monitor
- AutoRuns
- RSAT
- Tanium
- Devo
- Encase
- Volatility
- Nutanix