Alexander Sanabria

| asj5566773@gmail.com | 6785163517 | West New York, NJ | LinkedIn |

Dependable professional interested in a Security Analyst position that can apply analytical, technical, and innovation skills to support and guard organizations against security breaches.

TECHNICAL SKILLS

Security Tools: *Metasploit, Splunk, Burp Suite, SIEM, Wireshark, Nmap*
Networking: *Firewalls, NIST, MITRE ATT&CK Framework, SOC2, Active Directory, IDS/IPS*
Operating Systems & Programming Languages: *Linux, Bash, Windows, PowerShell, Python, JavaScript*
Other: *Kali, Parrot, Virtual Machines, Command Line, OSINT*

Certifications:
CompTIA Security+ (Obtained August 2023)
CompTIA Cybersecurity Analyst+ (Expected April 2024)

TECHNICAL PROJECTS

Final Project | "Beware Ransomware" | July/August 2023

- Used techniques and concepts learned over the course of bootcamp alongside teamwork to create a six-minute presentation video on the dangers of Ransomware.
- Skills used: Creating a phishing email & fake website, Using Python to modify a publicly available ransomware file, tested ransomware file on a virtual instance of Ubuntu, recorded and edited video footage of teammates describing ransomware and the preventative methods needed to remain safe from ransomware.

Career Preparation | "Units 4 (Python) & 7 (Splunk)" | June/July 2023

- Wrote Python scripts that could perform a variety of functions such as reading files, counting occurrences of elements, adding new lines/elements, rearranging/sorting text, putting results in a dictionary, as well as printing all results returned.
- Performed threat hunting challenges in Splunk using SPL alongside evidence and explanations of my solutions for each challenge.

Career Simulation | "Onboarding Runbook" | June 2023

- Collaborated with fellow students at Fullstack Academy to create a runbook for an IT team illustrating how to onboard new employees at a fictional company.
- Demonstrated how to create new users, groups, shared folders, and organizational units along with instructions on how to create and edit GPO's for current/new employees.
- Explained how to use Event Viewer as well as how to create Powershell scripts automating event and log viewing.
- Key Concepts: Windows Active Directory, Group Policy Editor, Event Viewer, Group Policy Objects, Role-Based Access Control, Powershell scripting

ADDITIONAL EXPERIENCE

TryHackMe: Junior Penetration Tester Job Pathway | January 2024

- Successfully engaged in realistic hands-on hacking exercises, honing skills in identifying vulnerabilities, exploiting them using ethical hacking techniques, and providing reports on findings.
- Demonstrated expertise in web and network vulnerabilities, proficiency with tools such as Burp Suite, Nmap, and Metasploit, and a comprehensive understanding of penetration testing techniques, including reverse and bind shells.

TCM Security Academy: GRC Analyst Master Class | February 2024

- Became knowledgeable on NIST Cybersecurity Framework and how the Identify, Protect, Detect, Respond, and Recover categories comprise and facilitate an information security program.
- Executed threat modeling exercise to determine higher likelihood threat events to inform cybersecurity risk modeling
- Developed Information Security policy to establish authorized access management and authenticator management for internal and third-party personnel.

LetsDefend: SOC Analyst Learning Pathway (Expected February 2024)
HacktheBox Academy: Job Pathway: Penetration Tester (Expected March 2024)

EDUCATION

Emory Cyber Bootcamp 05/23 - 08/23
Powered by Fullstack Academy

- Formed a solid foundation of computer knowledge including Windows client/server and various Linux distros
- Learned Python basics and Bash scripting as well as PowerShell cmdlets
- Practiced offensive techniques and how to mitigate these threats using blue team industry tools to align with cybersecurity frameworks such as NIST and MITRE ATT&CK
- Wrote and modified rule sets for IPS/IDS such as ACLs for firewalls based on parameters provided

- Used packet capture tools such as Wireshark to investigate traffic for Indicators of Compromise
- Performed simulated threat hunting by analyzing large data sets in Splunk
- Gained familiarity with a variety of tools including Splunk, Wireshark, Burp Suite, Metasploit, Nessus, Nmap, and ping/netstat

New York University

Bachelor of Arts in Global Liberal Studies with a Concentration in Politics, Rights, & Development 09/17 - 12/23

- Participated in discussion-based seminars, enhanced by experiential learning with visits to museums, theaters, and landmarks in multiple locations
- Completing major with a capstone independent research project, bringing together rigorous interdisciplinary studies and lively discussions in the classroom
- Graduating with unique global and interdisciplinary lenses for addressing the pressing challenges of our evolving world and contributing to creative solutions and effective social change

EXPERIENCE

Server | **Le Pain Quotidien** | New York, NY 05/21 – 07/21

- Maintained high standards of customer service during high-volume, fast-paced operations
- Communicated clearly and positively with coworkers and management.

Interpreter | **Primerica Financial Services** | Atlanta, GA 05/20 – 09/20

- Translated spoken presentations or speeches for multilingual audiences of 100-150 clients
- Researched industry-specific terminology, specialized dictionaries and translation tools for everyday use

Team Member | Shake Shack | New York, NY 08/18 – 05/19

- Correctly received orders, processed payments and responded appropriately to guest concerns.
- Adhered to established company procedures, guidelines, and policies at all times

PROFESSIONAL AFFILIATIONS

- **HtW (Hacking the Workforce) Fellowship Program,** attending biweekly meetings