Robinson Acosta

Robinsonacosta1@gmail.com | 914-837-7586 | LinkedIn: /robinson-acosta | GitHub: /racosta | Website: racosta.io

Summary:

Cybersecurity professional with 7.5 years of experience working both professionally and academically within the cybersecurity domain. Possess both technical and management skills, program/project management and a keen ability to learn new skills and technologies. Interested in offensive/application security engineering and in the process of becoming a lab member for NYU's Osiris Labs.

Education:

New York University: Tandon School of Engineering, *NYC, NY* **Jan 2021 - Sep 2023**
MS, *Cybersecurity (NSA Center of Academic Excellence)* | ***GPA: 3.49***
The College of St. Rose, *Albany, NY* **Graduated - May 2020**
BS, *Cybersecurity* | *Minor: Business Administration* | ***GPA: 3.64*** | *Honors:* ***Cum Laude***

Professional Certifications:

Offensive Security Certified Professional (OSCP) **Expected: January 2023**
CompTIA Security+ (SYO-601) **September 2022**

Relevant Technical Skills:

Programming/Scripting Languages Python | C/C++ | HTML | CSS | Bash | JavaScript | PHP | LaTeX
Tools Splunk | QRadar | Qualys | Burp Suite | CrowdStrike | Wireshark | Nmap | Metasploit | Ncat | IDS/IPS | Firewalls
Database Development & Management SQL | MySQL
Operating Systems Linux (Kali, QubesOS, ParrotOS, Ubuntu, Debian) | Windows | MacOS
Virtualization & Cloud AWS | GCP | Docker | Kubernetes | VirtualBox | VMWare | O365
Miscellaneous UAV Building, Piloting, & Photography | 3D Modelling & Printing | PC Building | Soldering
Languages Spanish- Fluent | Italian- Intermediate

Relevant Work Experience:

TIAA Broomfield, CO **Nov 2022 –Present**
Information Security Engineer II

TIAA Charlotte, NC **June 2022 – Sep 2022**
Information Security Incident Response Specialist Intern

- Investigated and triaged various cybersecurity related events to determine risks and potential impact to TIAA.
- Assessed user submitted phishing emails for malicious content to protect the company from the most ordinary form of social engineering attacks.
- Leveraged security tools such as Splunk (SIEM), endpoint, crowdstrike, and various OSINT tools to preform investigations to defend against internal/external threats that aimed to infiltrate company emails, data, and users.
- Investigated threat alerts for external IP scanning, typo squatting, audit log clearing, public source code detections, etc.
- Analyzed firewall logs, PCAPS, IDS alerts, Anti-malware alerts, Host Intrusion Prevent System, and server and application logs to investigate events and incidents for anomalous activity and produce reports of findings.
- Documented investigations and remediation steps thoroughly within Archer for case management and auditing.

Imagine Communications Denver, CO **November 2021 – Jan 2022**
Information Security Intern

- Supported activities related the administration of security policies and processes, governance and risk management program, RFPs/contracts, third-party vendors, and compliance frameworks.
- Assisted with audits and penetration testing to ensure compliance with security policies and processes.
- Supported activities related to internal phishing campaigns, security announcements, and security awareness training for new hires and contractors.
- Led efforts to research, demo, and contract negotiations for various GRC platforms to aid in SOC 2 compliance campaign to C-Suite level executives based on business problems and requirements.
- Leveraged security tools such as SIEM and vulnerability scanners to monitor assets and secure environment.
- Managed a project consisting of system engineering from a security standpoint involving the remediation of 102 servers hosting various legacy applications to present risk mitigation strategies and licensing costs to C-Suite level executives.
- Preformed CSIRT activities, from ad- hoc vulnerability scanning, sending out company wide InfoSec updates, to the logging and documentation of assets for scans and their results. Additionally participated in tabletop exercises with C-Suite level executives.

- Acted as a security liaison for weekly tuning calls with IBM for SIEM monitoring rules that were added and reported metrics directly to the CISO.

Gaming Insomniacs Inc. Schenectady, NY **February 2019 – Aug 2019**
Senior Developer Intern

- Implemented the utilization of Amazon Web Services for setting up company services.
- Tested and deployed programs and applications while troubleshooting, debugging, and improving the programs.
- Collaborated with management and various departments to identify end-user requirements and specifications.
- Assisted in the creation of an online database for implementation of statistical tracking of players and teams.
- Managed and led a team of less-experienced interns. Additionally, taught programing in python and basic web development.

Brewster Technology Brewster, NY **January 2016 – June 2016**
Information Technology Intern

- Provided support to Windows Server 2003/2008/2008R2/2012/2012R2, Windows 7/XP and Windows 8/8.1; set share and NTFS permissions. Provided support to MS Office Suite additionally.
- Set up testing center's computers for the utilization of testing and certification testing services. Upgraded and managed testing station's hardware and software.
- Troubleshooted and setup switches and routers (Cisco & Patch panel management).
- Set up and supported remote Windows, Apple, and Linux end-users with GoToMyPC, both RSA soft and hard tokens, and Citrix.
- Manage Active Directory accounts and groups; create and manage new users/email IDs for contracted clientele.
- Troubleshooted network issues using TCP/IP diagnostics tools such as ping, netstat, pathping, tracert, nslookup, hostname, ipconfig, etc.

Tudor Investment Corp Greenwich, CT **October 2015 – Dec 2015**
Information Technology Intern

Relevant Projects/Self Learning/Github: **Note: There are more projects, just not enough space.**

Lucerne [Private Repo]

- Currently building a project that leverages various microservices on Google Cloud Platform to web crawl Github repos via API and Gitlab projects that were most recently posted to scan them and extract secrets. Written in Golang.

Application Security Projects [Private Repo]

- With ASLR turned off preformed Buffer Overflow attacks on both 32-bit and 64-bit programs by using GDB to debug to locate the distance between the buffers start and the return address. Then implemented countermeasures like StackGuard, and the use of Non-executable stack protection.
- Preformed various attack against a Django Web Application. Preformed XSS, CSRF, SQLI and CMDI with the use of SqlMap, and Burp suite. Wrote scripts to automate the process of checking the presence of vulnerabilities and implemented secure coding practices to mitigate the attacks.
- Leveraged CIS Benchmarks guides for SQL, Docker and Kubernetes to take a containerized web application and remediate failing security controls.
- Android Studio deployment of same gift card site in Kotlin, implemented the proper usage of intents, and secured REST API communications via HTTPS, implement authorization controls, remove all unnecessary permissions from Android manifestos to ensure privacy.

Network Security Projects [code]

- Scapy programs to sniff and spoof ICMP echo request and echo reply packets in transmission from a specified source IP address to a targeted destination source IP.
- Various Scapy programs used to preform Arp cache poisoning to preform various MITM attacks against TelNet and Netcat to change packet payloads.
- Implementation of TCP traceroute using Scapy in python to reveal the IP address of routers leading to a specified destination IP and counts the number of hops away it is.
- Various Scapy programs used to sniff and spoof RST packets to terminate a TCP connection between two victims using telnet, an attack for TCP session hi-jacking and an attack for creating a reverse shell on a victim using TCP session hi-jacking.
- Various Scapy programs used to preform Arp cache poisoning to preform various MITM attacks against TelNet and Netcat to change packet payloads.

Computer Networking Projects [code]

- Using the python socket library implemented the following various programs: an icmp pinger, smtp server, traceroute and a web server in python.

RePy Reference Monitor [code]

- Reference Monitor using the security layer functionality in RePy V2. Used to implement proper access control and input validation when reading and writing files. This reference monitor was then tested and improved after creating various attack cases.

MAC Address Changer Script [code]

- Automation of ifconfig CLI commands. Used to return current MAC address for an interface and assignment of a new user defined MAC address for the interface chosen. Used mainly when pentesting in Kali Linux VM's.

HackTheBox/Cybrary/ImmersiveLabs/Overthewire/Etc

- Practice exploitation, investigative, and detective techniques etc. in HacktheBox. Cybrary, OverTheWire, Immersive Labs, CTFs and Cyber ranges.