Justin R. Lew

(718) 506-6340
justinlew1000@gmail.com
LinkedIn Profile - https://www.linkedin.com/in/justinrlew/
Personal Website - https://justinrlew.github.io/index/

I'm a highly motivated graduate with a Bachelor of Science degree in Cybersecurity and Information Assurance! I'm also certified in multiple CompTIA tracks (PenTest+, CySA+, Security+, etc.), with hands-on experience in IT support, help desk troubleshooting, and web development. Over time, I've gained excellent communication skills with a proven ability to work well in a team. I'm also highly adaptable with a customer-centric mindset, and ready to apply technical knowledge while further developing my cybersecurity expertise.

I’m passionate about protecting digital environments and staying up-to-date with emerging security practices. If you’re looking for someone who’s dedicated, adaptable, and ready to hit the ground running, feel free to connect—I’d love to explore how I can add value to your organization.

Bachelor of Science, Cybersecurity and Information Assurance
Western Governors University, Graduate of the Class of 2024

Experience

IT Support Specialist Webster Bank *(May 2024 – Nov 2024)*

- Provided courteous customer service by actively listening to user concerns.
- Offered reassurance through technical resolutions while maintaining a positive rapport.
- Provided technical assistance to employees, addressing hardware, software, and device-related issues both in-person and remotely.
- Installed, configured, and updated software to ensure optimal performance and security.
- Managed support tickets through the helpdesk system, prioritizing and resolving issues in a timely manner.
- Escalated more complex problems to senior team members, ensuring a smooth handoff and resolution.
- Conducted brief training sessions on cybersecurity best practices, enhancing overall user awareness.

Service Desk Analyst **Queens College, City University of New York** *(Jan 2024 – Apr 2024)*

- Provided attentive customer service by responding to technical issues with a friendly, patient attitude.
- Ensured users felt heard and supported throughout the troubleshooting process.
- Answered user calls and emails, logging all issues into the ticketing system for tracking and resolution.
- Assisted with basic troubleshooting tasks, such as resetting passwords and helping users navigate software applications.
- Escalated more complex technical problems to senior team members or Tier 2 support.
- Followed step-by-step instructions provided by the team to resolve recurring technical issues.
- Learned company systems and procedures through hands-on experience and training sessions.

Technical Support Specialist ***Queens Library*** *(Sep 2023 – Dec 2023)*

- Delivered personalized customer service by explaining technical solutions in a straightforward and empathetic way.
- Prioritized making users feel confident and at ease with resolving their issues.
- Provided excellent customer service by explaining technical solutions in simple, user-friendly terms, achieving a 95% customer satisfaction rating.
- Responded to over 30 daily user inquiries via phone, email, and ticketing systems, delivering fast and efficient resolutions to technical issues.
- Diagnosed and resolved software, hardware, and network connectivity issues for a variety of enterprise tools and systems.
- Documented recurring issues and resolutions in the knowledge base to improve team efficiency and reduce resolution time for common problems.
- Supported onboarding of new hires by setting up workstations, configuring accounts, and ensuring seamless system access.

Help Desk Technician Tier 1 **Queensborough Community College** *(May 2023 – Aug 2023)*

- Provided compassionate and patient customer service by delivering technical assistance to employees in an approachable manner.
- Maintained a friendly and professional attitude when assisting users, providing a positive experience.

- Answered user calls and emails, logging all issues into the ticketing system for tracking and resolution.
- Assisted with basic troubleshooting tasks, such as resetting passwords and helping users navigate software applications.
- Escalated more complex technical problems to senior team members or Tier 2 support.
- Followed step-by-step instructions provided by the team to resolve recurring technical issues.
- Learned company systems and procedures through hands-on experience and training sessions.

Certifications

- CompTIA PenTest+ (Aug 2024)
- ISC2 CCSP: Certified Cloud Security Professional (Aug 2024)
- CompTIA CySA+ (Jun 2024)
- CompTIA Security+ (Oct 2023)
- CompTIA Project+ (Apr 2024)
- CompTIA Network+ (Sep 2023)
- CompTIA A+ (Jul 2023)
- ITIL 4 Foundation - IT Service Management (GR671577319JL) (Oct 2023)
- ISC2 SSCP: Systems Security Certified Practitioner (Feb 2024)
- LPI Linux Essentials (Dec 2023)

Extracurricular Activities

- Cyber Club Member

Actively participated in discussions and practiced hands-on cybersecurity concepts

Awards & Achievements

- Excellence Award

Awarded for exemplary work in Managing Information Security coursework

Technical Skills

Programming and Development

- Programming Languages: Python, SQL, Bash, PowerShell
- Web Development: HTML, CSS, JavaScript
- Microsoft Office

Tools

User and Identity Management
Active Directory (AD) • Okta • LDAP (Lightweight Directory Access Protocol) • Duo Security

Ticketing and Helpdesk Systems
ServiceNow • Jira Service Management • Zendesk • Freshdesk • Spiceworks

Remote Access and Troubleshooting
TeamViewer • Microsoft Remote Desktop • Chrome Remote Desktop • LogMeIn • AnyDesk

Virtualization and Cloud Management
VMware vSphere • Hyper-V • AWS Management Console • Microsoft Azure Portal • Spiceworks

Endpoint and Device Management
Microsoft Intune • Jamf • PDQ Deploy

Network Monitoring & Analysis
Wireshark • Nmap

Firewall & Intrusion Detection
pfSense • Cowrie

Vulnerability Scanning & Exploitation
Metasploit • Nessus • OpenVAS

SIEM
Splunk

Password Cracking & Authentication
Hydra • John the Ripper • Hashcat

Phishing & Security Awareness
GoPhish • Have I Been Pwned

Projects

1. **Windows Active Directory Virtual Lab**

This project demonstrates the deployment and management of an Active Directory environment in a virtual lab. It includes setting up a domain controller, configuring DNS, managing users and groups, implementing Group Policy Objects, and integrating a client machine.

GitHub Repository - https://github.com/JustinRLew/Active-Directory-Virtual-Lab

---

2. **Remote Desktop Protocol (RDP) – Real-Time Walkthrough**

This project shows my ability to assist users in setting up and troubleshooting three popular remote desktop tools:

- Microsoft Remote Desktop Protocol
- Chrome Remote Desktop
- TeamViewer

GitHub Repository - https://github.com/JustinRLew/Remote-Desktop-Protocol-Project

---

3. **SIEM Monitoring with Splunk**

This project demonstrates the implementation of a Security Information and Event Management (SIEM) system using Splunk. The purpose of the project is to monitor a simulated network, detect security threats, and respond to incidents in real-time. This project showcases deploying and configuring a SIEM solution, creating detection rules, visualizing data, and automating alerts.

GitHub Repository - https://github.com/JustinRLew/SIEM-Monitoring-Splunk

---

4. **Phishing Simulation Tool**

This project involves building a phishing simulation tool using a custom HTML front-end interface, SendGrid, a Python Flask backend API, and Postman for testing API requests to demonstrate phishing attack methodologies.

GitHub Repository - https://github.com/JustinRLew/Phishing-Simulation-Tool

5. **Brute-Force Attack Simulation**

This project is a Python-based brute force attack simulation that demonstrates how brute force attacks work. The script attempts to guess passwords by hashing and comparing them to a stored hash.

GitHub Repository - https://github.com/JustinRLew/Brute-Force-Attack-Simulation

6. **Honey Pot – Creation & Deployment**

This project involves setting up a medium-interaction SSH honeypot using Cowrie to detect and analyze unauthorized login attempts, particularly brute-force attacks. The honeypot logs attacker behavior and provides insights into attack methods and the threat landscape.

GitHub Repository - https://github.com/JustinRLew/Honey-Pot-Creation-and-Deployment

7. **Personal Firewall & Network Monitoring**

This project demonstrates how to configure a personal firewall and monitor network traffic on a Windows system. Windows Defender Firewall, PowerShell, Wireshark, and Nmap were used to enhance system security and analyze potential threats.

GitHub Repository - https://github.com/JustinRLew/Personal-Firewall-and-Network-Traffic-Monitoring

8. **Password Strength Checker**

Created a web-based password strength checker that evaluates passwords in real-time based on NIST guidelines. It provides visual feedback, displays password strength, and offers recommendations for improving password security.

GitHub Repository - https://github.com/JustinRLew/Password-Strength-CheckerPassword Strength Checker

Password Strength Checker App - https://justinrlew.github.io/Password-Strength-Checker/

---

9. **Founder and Blockchain Developer - CrustCoin (CRST)**

Founder and Creator of CrustCoin (CRST):

CrustCoin is an ERC-20 utility token developed as a blockchain-based solution for decentralized financial services. Designed to power Bank-as-a-Service (BaaS) platforms, CrustCoin integrates features like savings accounts, staking rewards, and community-driven governance. Its deflationary tokenomics and focus on scalability, security, and accessibility position it as a foundational layer for fintech innovation.

- **Key Features:** Blockchain-based savings, staking rewards, and governance mechanisms.
- **Tokenomics:** Deflationary model with a fixed supply of 1 billion tokens.
- **Built On:** Ethereum using OpenZeppelin libraries, with a React.js-based wallet interface.

Private GitHub Repository:

(Demonstration Video Available Upon Request)

This project demonstrates ability in Solidity, smart contract development, decentralized finance (DeFi), and blockchain integrations for fintech applications.

---

10. **Crypto Exchange Penetration Testing Toolkit**

The Crypto Exchange Penetration Testing Toolkit is designed to test and identify security vulnerabilities in cryptocurrency exchanges.

Targets common exploits:

1) API vulnerabilities (e.g., weak token validation, unauthorized access)
2) Improper input validation (e.g., SQL injection, XSS attacks)
3) Weakness reporting with severity rankings and recommendations.

Private GitHub Repository:

(Demonstration Video Available Upon Request)

Languages

English • Spanish • Chinese