





# Arsalan Husain

 [LinkedIn](#) |  978-460-4978 |  arsalanhusain15@gmail.com |  [GitHub](#)

## Skills

---

**Technical Skills:** SIEM | Azure Sentinel | Splunk | Kali Linux | Wireshark | Active Directory | Tcpdump | Bash | Python |

**Functional Skills:** | Crossteam Collaboration | Leadership | Problem-Solving | Time Management | Critical Thinking |

## Education

---

### Cybersecurity Bootcamp

Columbia University

New York, NY, USA

08/2022 - 02/2023

- 24 Week Cybersecurity Bootcamp Certificate
- Preparation for Security+ Certification
- Grade: 98%

## Cybersecurity Projects

---

### Detecting & Mitigating a Real Threat in Splunk | <https://tinyurl.com/4s2y2yak>

- Utilized **system logs** to monitor and detect attacks on company infrastructure.
- Established baseline behavior to evaluate system alarms in the event of a breach due to unusual behavior.
- Derived actionable insights to enhance prevention strategies based on **generated reports from Splunk**.
- Provided crucial evidence for incident response and ensured compliance with security policies.

### Exploiting S3 Bucket Vulnerabilities in AWS | <https://tinyurl.com/yc87yyby>

- Used **AWS CLI** to examine the bucket's contents and discovered sensitive information.
- Identified a significant finding in the form of a ".git" directory within the bucket.
- Accessed and extracted data from a specific commit that contained sensitive files.
- Located and retrieved "access keys.txt" file with AWS access and secret keys.
- **Configured an AWS profile** to match the extracted access and secret keys.

### Azure Virtual Honeypot to Log RDP Brute Force Attacks | <https://tinyurl.com/4vyh7sb7>

- Used **Azure Sentinel (SIEM)** and connected it to a live virtual machine acting as a honey pot.
- Observed live attacks (RDP Brute Force) from all around the world.
- Used a custom **PowerShell script** to look up the attackers Geolocation information and plot it on the Azure Sentinel Map.

## Certifications

---

- CompTIA Security+ Completed May 2023
- Coursera: Analyze Network Traffic with TCPDump
- Coursera: Microsoft Windows Defender and Firewall for Beginners
- HackTheBox: Windows Event Logs & Finding Evil
- Currently pursuing CompTIA Network+ - Estimated Completion by December 2023

## Work Experience

---

### Talent Acquisition Coordinator

EOS Accountants LLP

New Jersey

07/2021 - Present

- Collaborated closely with key stakeholders to implement and enforce security protocols within the recruiting process, safeguarding sensitive candidate information and mitigating potential risks.
- Implemented and established recruiting programs from inception, including the system architecture, infrastructure and process.  
**Saving \$150,000 for the firm within 2 years.**
- *Developed and created technical documentation for all best practices, policies, and procedures.*

### HRIT Analyst

C&S Wholesale Grocers

New Hampshire

07/2019 - 03/2021

- Managed Windows administration and Active Directory functions for the HR team, ensuring smooth operations and system stability.
- Implemented and managed user accounts, security groups, and access controls within Active Directory, data integrity and privacy.

## Other Education

---

### Bachelor of Science

Virginia Tech

Blacksburg, VA, USA

08/2015 - 05/2019

- Major in Business Management and Human Resources
- Clubs: Virginia Tech Fencing Team Captain