Sedat Altun

Santa Clara • 650-963-6972
altunsedat63@gmail.com
www.linkedin.com/in/sedat-altun630800

Qualifications Summary

- Dedicated and ambitious professional with a strong foundation in information technology and a passion for enhancing cybersecurity measures. Profound knowledge of **cybersecurity concepts**, including **threat detection**, risk assessment, encryption, and network security protocols **IPSec** and **VPNs**, **TLS** and **SSL**, **Kerberos**, **OSPF authentication**, **SNMPv3**, and **SSH.**
- Proficiency with industry-standard security tools and software, such as firewalls, intrusion detection systems (IDS), antiviruses, and vulnerability assessment tools including **Nmap**, **Wireshark**, **Splunk, NoSQL,** and **Linux Kernels**.
- Proven ability to collaborate effectively within **cross-functional teams**, contributing insights to enhance overall cybersecurity posture

Education

California State University, East Bay; Hayward, CA Expected Graduation: **May 2026**

- BS in Computer Science
- Double Minor in Data Science and IT Management
- Relevant Coursework: Security and Info Assurance, Data Structures and Algorithms, Computer Architecture, Analysis of Algorithms, Programming Language Concepts.

Experience

You-Think(Web Development)

Intern ***November 2020 - February 2021***

- Developed a professional website as a final project using **CSS, HTML, JavaScript, Bootstrap, React, and NoSQL databases**.
- Applied full-stack technologies, including **HTML, CSS, and JavaScript** to develop and optimize a company website. Increased end-user experience by implementing new features to the company's website, such as an improved search bar, more free-flowing graphics, and smoother page transitions.

Clarusway Bootcamp(Cyber Security)

April 2022-October 2022

- Engineered an advanced Intrusion Detection System(**IDS)** leveraging **Metasploit** in a **Kali Linux** environment, enhanced through comprehensive packet analysis with **Wireshark** to identify and mitigate potential threats extensively.
- Masterfully executed a simulated password attack utilizing Hydra against a secured file, uncovering critical vulnerabilities and developing robust countermeasures to strengthen security defenses.
- Employed **Netcat** and Wireshark in a strategic analysis of packet flows across various ports and machines, significantly enhancing network traffic insights and security posture.
- Established a dedicated **Ubuntu** machine for controlled hacking simulations, employing Wireshark to monitor network activity meticulously, effectively assessing and optimizing **security protocol efficacy**.

Projects

- **Rubber Ducky Project** ***August 2023-December 2023***
  - Contributed to the 'Rubber Ducky Project' with Dr. Levent Ertaul, assessing the Rubber Ducky USB keystroke injection tool's security implications through experiments. Evaluated system vulnerabilities and countermeasures, documenting and reporting findings
- **Raspberry Pi Hacking Tool** ***January 2024-Present***
  - Engaged in the 'Raspberry Pi Hacking Tool initiative, utilizing the device for cybersecurity penetration tests. Explored its application in network security breaches, developing preventative measures against potential vulnerabilities.
  - Extended the project scope by incorporating the Raspberry Pi as an application tester within Android Studio, conducting focused analyses on its effectiveness against network defenses. Documented and strategized based on findings, broadening the understanding of its multifaceted role in cybersecurity.

Technical Proficiencies

Programming Languages: Python, Java, C++, SQL, JavaScript | **Version Control**: Git, GitHub
Networking Tools: Wireshark, Nmap | **Virtualization**: VMware, VirtualBox

Operating Systems: Windows, Linux (Ubuntu, Kali), MacOS