ZANDER WORK

zander@zanderwork.com
www.linkedin.com/in/zanderwork

Education

BS, COMPUTER SCIENCE (SECURITY) | Oregon State University | 3.87 GPA | Est. Graduation June 2021

- Key Courses: Intro to Digital Forensics, Operating Systems I and II, Systems Security, Cyber Attacks & Defenses, Social and Ethical Issues in Computer Science
- Leading a senior capstone project to design infrastructure for the Oregon Research & Teaching Security Operations Center (ORTSOC), a student-staffed Security Operations Center (SOC) designed to vocationally teach students how a SOC works and how to be a security analyst
- Member of Dr. Yeongjin Jang's research group (SSH Lab), focusing on system and software security vulnerabilities. Currently working on research projects targeting Apple iPhone/iOS, Intel CPUs, and Docker/container technology

Skills

Security	**Infrastructure**	**Programming**
• Malware Analysis (IDA Pro/Hex-Rays Decompiler, gdb, x64dbg)	• Virtualization (VMware vSphere, VMware Workstation, VirtualBox)	• C, C++
• Binary Exploitation (pwntools, angr)	• Cisco Networking (IOS)	• Python, *sh, PowerShell
• Vulnerability Scanning (Nessus, OpenVAS)	• Infrastructure as Code (Terraform, Ansible)	• HTML/CSS/JavaScript
• Network Security (Zeek, Wireshark, nmap)	• Containerization (Docker, Kubernetes)	• Django/Flask
• Log Management (Splunk, Elastic)	• Rapid Prototyping (Vagrant)	• x86 Assembly
		• Git

Work Experience

SECURITY ANALYST | Oregon State University Security Operations Center | October 2017 – Current

- Work with Zeek, Nessus, Splunk, and the Elastic Stack to perform network monitoring & analysis (max 100Gbps traffic)
- Design, deploy, and support production and development infrastructure
- Help lead incident response efforts by analyzing logs and performing forensic analysis on compromised Windows and Linux systems
- Develop automation to improve analysis efficiency by over 50%
- Monitor and respond to end-user phishing incidents
- Contribute to documentation and training materials for other team members

TECHNICAL INTELLIGENCE ANALYST INTERN | FireEye, Inc. | June 2019 – May 2020

- Deploy and integrate a sandbox environment for automated Android malware analysis for use across the entire company
- Analyze and process intelligence on financial crime threat activity to write reports for customers
- Profile and manipulate attacker Command & Control servers to learn more about their malware communications
- Hunt for and analyze malware samples from internal and external sources to support intelligence analysis
- Contributed to internal tracking of threat actors, malware samples/families, and TTPs
- Research published on the FireEye Blog: https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html

Activities/Awards

OSU Security Club (2017 - Current)	**NW Cyber Camp (2016 - 2019)**	**Recent Awards**
• Club president from 2017-2020, 250+ members	• Co-founded in 2016	• 3rd place, DOE Cyberforce Competition 2020 (remote, individual)
• Captain for competition teams (OSUSEC)	• 5 sessions with over 100 total participants	
• Work with industry partners to bring recruitment events and presentations to our club members	• Weekly management meetings	• 2nd place, Pacific Rim Collegiate Cyber Defense Competition 2020 (remote, team)
	• Work with local high schools for recruitment	
• Work with the College of Engineering to secure funding for competitions and tools	• Coordinate with industry partners to secure funding and guest speakers	