Anthony Khoshrozeh

khoshrozeh.com | akhoshrozeh@gmail.com | LinkedIn | Github

Education

University of California, Los Angeles (UCLA) Los Angeles, CA
*Bachelor of Science in **Computer Science*** *Sep. 2019 – June 2022*
Relevant Coursework: Computer Security, Operating Systems, Computer Networks, Cryptography, Web Applications, Database Systems, Data Structures and Algorithms, Software Engineering, Computer Architecture and Organization, Programming Languages, Distributed Algorithms and Blockchains, Data Science, Graph Theory

Experience

Cyber Security Student Current

- Completed TryHackMe Junior Penetration Tester certification.
- Currently working towards Security+ certificate and TryHackMe Security Engineer certificate.
- Actively completing CTF challenges on HackTheBox and TryHackMe platforms.
- **Topics Studied:** OWASP Top 10, OS/Network Hardening, API Security, Privilege Escalation, Threat Modeling, Risk & Vulnerability Management, Network Reconnaissance, OSINT, SIEM, Vulnerability Research & Scanning, Defense Frameworks, Network Traffic Analysis, PKI

Junior Software Engineer Jan. 2022 – July 2022
StudioDev *Los Angeles, CA*

- Designed and implemented smart contracts for ERC-721 tokens with Merkle Tree authorization mechanism.
- Designed and implemented escrow software for Ethereum tokens which allows users to earn crypto while tokens are being staked.
- Built a cross-chain bridge that allows a cryptocurrency to be transmitted across different blockchain networks.
- Designed smart contract API for client usage, allowing for efficient client-side gateway querying.
- Wrote unit tests with Mocha framework to achieve 95% test coverage.
- Performed static analysis and fuzzing for code review and auditing.

Skills

Languages: Python, C/C++, SQL, Unix shell scripting, Java, JavaScript/TypeScript, HTML/CSS, Solidity
Security: Burp Suite, Nmap, Metasploit, Snort, Splunk, Wireshark, tcpdump, MITRE, Unified Kill Chain
Developer Tools: Git, Apache Tomcat, Docker, PostgreSQL, MariaDB, MongoDB
Frameworks/Environments: Linux/Unix, Node.js, React, Angular, Express, Mocha

Projects

Man in the Middle Attack Simulation | *Linux, ettercap, etterfilter, tcpdump, chaosreader*

- Simulated replay attack by analyzing traffic, capturing packets, ARP spoofing and generating ”fake” requests.
- Simulated insertion attack by performing ARP spoofing and executing regular expressions on targeted packets.

Web Application Exploits Laboratory | *C, Perl, PHP, MySQL*

- Performed code review and identified software vulnerabilities susceptible to buffer overflows, pathname attacks, and SQL injection attacks.
- Exploited and patched different vulnerabilities in a web server written in C, a CGI script written in Perl, and a MySQL-based application written in PHP.
- Wrote reports describing the findings and code changes made to repair the vulnerabilities.

Digital Forensics | *Linux, e2undel*

- Analyzed different disk images of compromised computer systems to detect the cause, recover lost data, and investigate the attacker’s identity.
- Used Linux tools like *grep, xargs, find* to investigate and analyze various log files for suspicious user behavior.
- Used password cracker John the Ripper to brute force passwords.

Router | *C++, Mininet*

- Developed a router that performs longest-prefix matching lookups and forwards Ethernet frames to the correct outgoing interface.
- Tested on Mininet (virtual network) and demonstrated its capability to handle Ethernet frames, IPv4 packets, and ICMP packets, achieving successful ping and file transfer between emulated hosts.