Zhekun Hu

zhekunhu@gmail.com 904-515-6302 https://zhekunhu.xyz/
https://www.linkedin.com/in/zhekunhu/ https://github.com/huzhekun

Education

Computer Science at UC Davis (B.S.)

- Sep. 2017 - Dec. 2021

Skills

- Metasploit, Nmap, DIRB, Burp Suite
- SSL/TLS, PKI, GCP, AWS, DNS, TCP/IP, Apache, Nginx, Linux & Windows System administration
- C, C++, Python2, Python3, SQL, Java, Bash, Go

Relevant Coursework

- ECS 154A - Computer Architecture
- ECS 150 - Operating Systems
- ECS 140A - Programming Languages
- ECS 153 - Computer Security
- ECS 162 - Web Programming
- ECS 160 - Software Engineering
- ECS 152A - Computer Networks

Relevant Work Experience

- **Thinvent Corp. (08/2018 - 09/2018)**
  - (Corporate Software Solutions in China)
  - Position: Systems administration Intern
  - Tasks performed:
    - Maintaining and supporting a custom database solution.
    - Working with a support team to coordinate access.
    - Deploying custom software solutions.

Clubs

- **Davis Cyber Security Club (09/2018 - 12/2021)**
  - Vice President
    - Responsible for managing officers and coordinating club activities such as attending CTF's, events, and conferences.
    - Provide technical assistance at workshops for tools such as nmap and ssh, shell utilities for log analysis such as grep and piping, as well as writing bash scripts and deploying reverse shells.
- **Aggie Gaming (10/2019 - 12/2021)**
  - President
    - Responsible for hosting, maintainence, and upkeep of club infrastructure, presently hosted on a VPC on GCP. Infrastructure includes web server and discord bot, both with over 4 months of continuous uptime.
    - Maintained and hosted Minecraft server with custom DNS records and 2 continuous months of uptime.
    - Responsible for managing officers and organizing community events.

Personal Projects

- Personal Kubernetes Cluster And Website
  - Created custom kernel for PS4s to serve as fully functional Kubernetes Nodes
  - Registered own domain and set up DNS entries
  - Custom Pod with Nginx Hosting and CI/CD sidecar container pulling content from Git
  - Deployed Ingress rules and Auto Certificate Provisioning
- Wireless VR Solution
  - Flashed and configured OpenWRT on Wi-Fi Access Point to connect to a VR headset wirelessly from a connected PC using DFS channels.
  - Ran DHCP server and gateway outside of router
- 3D Printer Hardware Modifications
  - Troubleshot hardware errors on an Arduino control board on a PWM pin
  - Modified both hardware and firmware source code to reconfigure pin layout

Class Projects

- Java Stream Based Github Comment Analyzer (ECS 160)
  - Wrote Java Program to analyze CSV of Github comments via Stream filters and collectors.
- C thread scheduler (ECS 150)
  - Wrote Thread scheduler with preemption in C using provided user thread library.
- REST API in NodeJS (ECS 162)
  - Wrote REST API to retrive and write data into a MySQL database using NodeJS.

CTF Experience

- Reconnaissance
  - Used Nmap to identify running services that may hold vulnerabilities
  - Utilized Dirb to find hidden management interfaces and directories on webservers
  - Searched for common CVEs
- Webapp Enumeration
  - Burp Suite
    - Capture HTTP traffic to and from the backend
    - Enumerate, or fuzz webapp API calls to find potential code execution vulnerabilities
    - Manipulate POST requests to insert malicious parameters
  - Injection Attacks
    - Took advantage of XSS and CSRF vulnerabilities to extract credentials from other clients
    - Utilized SQLi to bypass authentication and exfiltrate secrets from databases
- DNS
  - DynDNS
    - Learned how to compromise a DynDNS server when given credentials
    - Updated DNS records to register personal machine under organization domain
- Privilege escalation
  - Automated search with LinPEAS to identify potential privilege escalation vectors
  - Manually searched to find credentials on the file system
  - Exploited SUID executables and sudo-allowed commands by manipulating input parameters to gain root access
- DOE Cyberforce Competition Regional Champion (Nov. 2019)
  - Competed against top universities such as UC Berkeley and defended a network consisting of 9 Windows Servers, Unix machines and industrial controllers with no security breaches.