Christopher Spankroy

Lake In The Hills, IL 60156 • 847-915-1416 • cspankroy@gmail.com • https://www.chrisspankroy.me

EXPERIENCE

onShore Security, Chicago, IL
DevSecOps Engineer (November 2023-present)
Worked on both internal and client-facing projects including:

- Maintained several Elastic clusters (diagnose issues, expand when needed, configure ingest pipelines/index templates, version upgrades)
- Deployed and maintained Elastic Agent/Elastic Defend EDR installations across several different clients
- Created dashboards and visualizations to display ingested logs in easily-viewable formats
- Configured several technologies such as Suricata, Sagan, syslog-ng, Snort, Filebeat, and others on IDS sensors that were placed in client environments to ensure proper traffic monitoring and successful log reception
- Performed tuning on detection rules and signatures to decrease false positives
- Developed new detection rules and signatures to add visibility to previously-unknown threats
- Created custom solutions for clients on a per-request basis (ingesting proprietary logs, creating unique protections, etc.)

onShore Security, *Chicago, IL*
Security Analyst (August 2021-August 2022)**; Senior Security Analyst** (August 2022-November 2023)
Worked with several clients to address their individual needs including:

- Correlated logs and alerts from several sources to identify potential threats in client environments
- Analyzed packet captures to identify potential issues
- Led incident response (IR) efforts when security incidents occurred
- Prepared and presented monthly security briefs that included security observations from many different sources
- Wrote several tools to interact with Elastic API to enhance the quality of reports given to clients
- Advised other security analysts on their investigations

University of Illinois at Urbana-Champaign, *Urbana, IL*
Software Engineering Intern (REU Participant) / Course Developer (August 2018—August 2019)
Successfully completed multiple projects to help improve introductory course curriculum:

- Created a new mobile application to enhance student interaction with university professors
- Developed kiosk interface with a Raspberry Pi to enhance user interaction with standard university technologies

Technologies Used:

- React Native
- Bluetooth Low-Energy Beacons (Estimotes)
- Android and iOS Native Development
- Web Development (React)

EDUCATION

Purdue University, West Lafayette, IN (August 2019 – May 2021)
Bachelor of Science in Cybersecurity; graduated May 2021; **GPA: 3.91**

Relevant Experiences:

- Conducted white-box physical penetration testing of public security devices as directed by the Purdue Homeland Security Institute
- Member of AITP (Association of Information Technology Professionals)

- Participated in multiple “Capture The Flag” (CTF) competitions, both as an individual and as part of a team. I developed reverse engineering and cryptography skills throughout these competitions.
- Member of a team that represented Purdue University in the *Collegiate Penetration Testing Competition* (CPTC) 2020
- Placed 1st place in Purdue’s *TracerFIRE* competition, which focuses on data and network forensics.
- Participated in the Department of Energy’s *CyberForce Competition: Warrior Edition*

University of Illinois at Urbana-Champaign, Urbana, IL (August 2017 – August 2019)
Completed 2 years of Computer Science curriculum; transferred to Purdue University

PROJECTS

pwn.college

- Earned a “blue belt” for 100% completion of a cybersecurity curriculum curated by Arizona State University known as “pwn.college”, which is focused on exploitation of x86-64 Linux platforms

Skills Learned

x86-64 assembly language • low-level Linux platform knowledge • kernel exploitation • SECCOMP escaping • ASLR/KASLR bypasses • low-level TCP/IP knowledge • C programming • reverse engineering with Ghidra • debugging with GDB • writing shellcode • ROP • respect for current security mitigations and how they are bypassed

homelab

- Obtained and configured a rack server to provide various production services and act as a testing ground for new things
- **Platforms/technologies used:** pfSense, OPNsense, VyOS, Proxmox, BIND (DNS), Docker containers, web hosting (NGINX, Apache), email hosting (postfix), IMAP (dovecot), Plex/Jellyfin, file sharing (Samba), IPsec VPNs, OpenVPN, various game servers, Elastic stack

CERTIFICATIONS (in order of date obtained, earliest to newest)

- **CompTIA Security+ (SY0-501)**
- **CompTIA PenTest+ (PT0-002)**
- **Palo Alto Networks System Engineer (PSE) Cortex Professional**
- **CompTIA CySA+ (CS0-003)**
- **Elastic Certified Engineer**

SKILLS & INTERESTS (in no particular order)

Linux exploitation • iOS security research and exploitation • IaaS (AWS, GCP, Azure) • VMware ESXi • Penetration Testing • VMware vSphere • Active Directory • Cisco IOS • OpenWRT • Linux (Ubuntu, Arch, CentOS, Debian) • Digital Forensics • Microsoft Windows Server • Pwntools • Autopsy • Wireshark • Volatility • Xcode • Android Studio • Metasploit • Python • JavaScript • Java • Bash scripting • C++ • C • Swift • Kotlin