Zhangchi Wang

Los Angeles,CA • wangzhangchi1995@hotmail.com • (412) 616-6095 • /in/zhangchiwang

Information Security Analyst with knowledge and experience in both offensive and defensive cyber security. Core strengths include vulnerability scanning and management, risk identification and assessment, and customer communications and presentations. Deep analytical and troubleshooting skills with multiple certifications and a graduate engineering degree.

Security Solution Design & Implementation • Penetration Testing • Cyber Threat Intelligence Analysis
Risk Mitigation Planning • Security Risk Assessment • Report/Presentation Development

EDUCATION & CERTIFICATIONS

Master of Science, Electrical & Computer Engineering, University of Pittsburgh - Pittsburgh, PA GPA: 3.18/4 (Dec 2018)

- Served as Research Assistant Fall 2017 focused on dependable embedded system development.

Bachelor of Science, Electrical Engineering, Harbin Institute of Technology - China GPA: 3.23/4 (2017)

Associate of (ISC)2 for CISSP (April 2019)
Offensive Security Certified Professional (OSCP) (March 2019)
Cisco Certified Network Associate Routing & Switching (CCNA) (August 2018)
ABB 800xA System User Certification – Basic Level (August 2016)

PROJECT & LAB WORK

- Connected to OSCP virtual machine environment via VPN for training in a simulated real world scenarios. Completed ~500 hours of training in OSCP program.
- Developed a personal and pragmatic pen test methodology. Successfully exploited 36 of 40 machines in lab environment during training and 4 out 5 in 24 hours during exam.
- Wrote a vulnerabilities description, detailed the exploitation process step by step, and developed a mitigation strategy recommendation report for the 14 machines exploited in the lab and exam environment.
- Established personal lab environment for CCNA training that included three Cisco Catalyst routers and three Catalyst switches, and VOIP phones to support a mid-size enterprise network.

SKILLS

Penetration testing: Vulnerability scanning and exploitation, mitigation strategy, Metasploit framework, Powershell Empire, Cobalt Strike, Burp suite, SQLmap, Nessus
Threat analysis: Malware reverse engineering, malware development, threat hunting, Network traffic monitoring and analysis, IDS/IPS and firewall configuration, pfSense/Endian firewall, Snort IDS, Splunk SIEM
Other: Scripting (Python, Bash), AWS, Google Cloud, Windows /Linux administration, Cisco router/switch configuration
Languages: Mandarin Chinese (Bilingual Proficiency)

EXPERIENCE

Cyber Security Engineer, Gurucul Solutions, LLC - El Segundo, CA June 2019 - Now
Gurucul provides the on-prem or SaaS GRA product for enterprise level security analytics and related services.
Hired into a hybrid role that includes responsibilities for project management, security analysis, research, and IT operations.

- Led projects with Sallie Mae and McKinsey with responsibility for managing client communications, reviewing security risk investigation reports, advising clients on findings to improve threat modeling methods, evaluating client data, parsing and automating data ingestion into GRA, and reporting status.
- Completed GRA product setup that includes server provisioning, data ingestions, creating use cases, and evaluating system outcomes.
- Perform threat research to identify security trends and share findings with internal analysts.
- Stood up a pentesting lab to simulate advanced cyberattacks using custom and open source tools. Report results to product teams to inform product strategy.
- Contributed to IT infrastructure management and GRA upgrade initiatives for large clients including Bayer, Starbucks, CVS, and State Farm. Developed tools to simplify product integrations, automate processes, and monitor Linux servers. Achieved 99.9% uptime.