Mario Alberto Ibarra

(562) 922 9225 www.marioibarra.me
ibarramario94@gmail.com www.linkedin.com/in/ibarra-mario/
Downey, California

Education and Certification

California State Polytechnic University, Pomona **2013 - Present**
B.S. in Computer Information Systems, Information Assurance Pomona, California
Expected Graduation – December 2017

CCNA Cyber Ops – Cisco Certified Network Associate Cyber Ops

Skills

- Python, Bash, Java, HTML/CSS, Regex
- Linux, Windows, Android
- Incident Response and Handling Methodologies
- Endpoint Threat Analysis / Network Intrusion Analysis
- SIEM, IDS/IPS, Splunk, Snort, Wireshark PCAP Analysis
- Penetration Testing Methodologies
- Kali Linux (Metasploit, nmap, Nessus, OpenVAS)
- Digital Forensics Analysis
- Forensics Toolkit (FTK), EnCase, SANS Investigative Forensic Toolkit (SIFT)
- Ticketing Software / Service Desk Software
- Microsoft Office (Word, Excel, Access, PowerPoint, Visio)

Experience

Business Data Links **January 2017 – March 2017**

IT Support Intern **Pomona, California**

- Provided customer support to a variety of end user questions and problems through phone and email.
- Created SOP's for office equipment and software.
- Responsible for installing, testing, and maintaining VMware ESXi on over 15 servers.
- Produced daily reports on 40 customer servers to ensure vital services were functional.
- Solved daily customer and internal tickets through FreshDesk customer support software.
- Troubleshoot office equipment including employee workstations and issues on customer servers.
- Utilized VNC and Remote Desktop to access company and customer computers remotely.
- Successfully trained new interns on job functions and on how to use VMware ESXi.

Projects

Penetration Testing Lab **March 2017 – Present**

- Deployed an ESXi box with pfSense, Kali Linux, SIEM with Splunk, IPS with Snort, and vulnerable virtual machines.
- Practiced manual penetration testing without Metasploit use by performing Reconnaissance, Enumeration, Exploitation, Privilege Escalation, and Reporting.
- Practiced Intrusion Detection and Incident Analysis by inspecting IDS/IPS logs after exploiting a vulnerable machine and identifying/analyzing suspicious behavior.