

Felix Guerrero Jr.

Email : felixguerrero12@gmail.com

Mobile Phone : (443) 666 4032
website : <https://area1337.com>

Summary

Dedicated Problem Solver, looking for Red Team role. Strong background in networking, system administration, and network security.

Professional Experience

Salesforce, Herndon, VA, USA Feb 2018 – Current
Incident Response Handler

- Respond to security incidents in a production environment, such as investigating and remediation possible endpoint malware infections and mitigating e-mail borne threats such as spam and phishing.
- Provide executive communications to leadership on high severity incidents.

MKA Cyber, Fairfax, VA, USA Dec 2016 – January 2018
Lead Security Analyst

- Perform network and host-based security analysis using ingested logs to assist with computer incident investigations.
- Develop operational day to day scripts to assist in the automation of tasks.
- Interpret vulnerability scan results to provide client's with detailed security posture.
- Accumulate and vet indicators of compromise for the threat intelligence program.
- Utilize ticketing system to create and escalate actionable reports on suspicious network events.
- Educate and guide junior security operators to move the mission forward.
- **Toolset:** Security Onion (NSM), TCPdump, Splunk Enterprise Security, Jira and Confluence, Slack, Snort Intrusion Detection System (IDS), BRO IDS, DNSRecon, Dirb, Nikto, Metasploit, MSFVenom Nmap, Nessus, SQLMap, TCPdump, SSH, Vagrant, VMWare, NCat/NC

EmeSec Incorporated, Chantilly, VA, USA Jan 2016 – Dec 2016
Network Security Analyst

- Train recent hires on the basics of network intrusion, environment and rules of engagement.
- Monitor network intrusion detection systems to identify anomaly incident events.
- Creation of detailed technical reports based on intrusions events.
- Provides assistance in computer incident investigations.
- **Toolset:** Shodan, Snort, TCPdump, VirusTotal

RH2RU - Capture The Flag Professional Team, Internet, Worldwide September 2016 – Current
Team Captain & Web Pentester Lead

- Advise and guide team in upcoming events.
- Oversee communications and recruiting processes.
- Manual Packet Inspection using known industry tools.
- Fuzz testing.
- In charge of managing cloud infrastructure instances.
- **Toolset:** DNSRecon, Dirb, Nikto, Kali Linux, Metasploit, MSFVenom NMAP, Nessus, SET, SQLMap, TCPdump, SSH, Vagrant, VMWare, NCat/NC, Docker, Volatility, Hashcat, John the Ripper, Hydra, Kippo Honeygot, Grep, Mimikatz, Recon-ng

Aplura LLC, Towson, Maryland, USA May 2015 – Jan 2016
Security Consultant Intern

- Install, configure, and maintain infrastructure services such as databases, backup systems, and communication systems in a both virtual and hardware environment.
- Maintain user access and system security through various tools.
- **Toolset:** SaltStack, MySQL, SSH, Logger, BareOS, Spacewalk, Atlassian Tools : (Bamboo, Hipchat, Jira, and Confluence), Nginx HTTPD, VMware Fusion, Syslog-ng, Splunk

Certifications

Offensive Security Certified Expert (OSCE)
Offensive Security Certified Professional (OSCP)
Red Hat Certified System Administrator : Nov 2016 | EX200
 Certified Ethical Hacker v9 +: Feb 2016
 CompTIA Security +: June 2013 | SY0-301, JK0-018
 CompTIA Network +: September 2013 | N10-005, JK0-019

Education

Towson University, Towson, Maryland, USA June 2013 – June 2016
 Bachelor of Science in Information Technology

The Community College of Baltimore County, Catonsville, Maryland, USA January 2010 – June 2013
 Associate of Science in Information Systems Security

Volunteer

Y of Central Maryland, Baltimore, Maryland, USA June 2015 – August 2015
 Computer Science Teacher

Assist students understand the basic concepts of algorithms, conditions, functions, and loops by creating a mental connection to what they already know. They were required to investigate different problem-solving techniques and discuss societal impacts of computing and the Internet.

Honors and Activities

PwnEIP –
 SOHOpelessly Broken CTF - (2nd Place) - Def Con, 2018
 Parsons and Friends CTF - (2nd Place) - ParsonsCyber, 2018

Towson University : Cyber Club, Towson, Maryland, USA June 2013 – September 2015
 Linux Security Engineer
 Mid-Atlantic Cyber Defense Competition (3rd), 2015
 National Collegiate Cyber Defense Competition, 2014
 Mid-Atlantic Cyber Defense Competition (1st) 2014
 National Cyber League (24th/400), 2014
 CSAW 15'

Languages

English: Native language.
 Spanish: Fluent (speaking, reading, writing).