Kevin Figueroa

4993 Columbia Rd., Columbia MD 21044

Tel. 301.357.4609 kevinf.pr@gmail.com

Summary

An expert with over 19 years practiced as a Senior Security Specialist with a vast broad knowledge and focus on cyber security. As a seasoned practitioner my strength and emphasis is in enterprise IT security that includes network and web application penetration testing, vulnerability assessment analysis, intrusion detection and malware analysis, system and network hardening, and security research. My professional goals is to offer my on-going passion and expertise of technical and analytical knowledge on cyber security that an organization could benefit from and to help further enhance infrastructure protection against today's cyber threat.

Technical Skills

Certification:	CEH, ECSA, SANS Advance Network Forensic and Analysis, Security+, Network+, A+
Operating Systems:	UNIX, Linux Red Hat/ Ubuntu, Microsoft Windows 2012/2008/2003/2000/8/7/XP/9X/NT
Network/Security Tools:	BurpSuite, W3AF, Metasploit, Scapy, Netcat, Ettercap, SQLmap, SQLNinja, Nikto, Nmap, FireEye, ArcSight, LogRhythm, Sourcefire, Imperva, Splunk, IDA Pro, OllyDBG, Nessus, Kenna Security, Snort, TCPdump, Wireshark, TShark, MergeCap, Solar Winds, Cisco AMP & Firepower, GFI Network Security Scanner, Encase, Anti-viruses & Utilities to remove infections.
Languages:	Python, Bash
Database:	MySQL, MSSQL
Software:	Subversion, iPython Notebook, MS Office / Visio / Project, Dreamweaver, Adobe Photoshop CS
Hardware:	WatchGuard Firewall, Cisco 3600/2500 series Routers, Sourcefire 3D3800 & 3D2500 IDS, ISS GX4004 & GX5108 IDS appliance, Wireless Routers, Switches

CONFERENCE SPEAKING ENGAGEMENTS:

- InfoSec Connect KEYNOTE October 2018 ("Taking a Look At Security From The Mind Of A Hacker")
- Unallocated Space February 2017 ("Blinded by Big Data, Paralyzed by Analytics, Decipher by Machine Learning")
- NYCBug September 2009 ("Combining almost all security tool into the Power of One with Scapy")
- DEF CON 16 August 2008 (VLAN & Layer 2 Attacks)
- THE LAST HOPE July 2008 (VLAN & Layer2 Attacks)

Experience

3/2016 – Present **CNSI, MD**

Sr. Penetration Tester & Security Engineer

- Performing external network and web application penetration testing using Kali Linux, and other tools and frameworks to exploit the vulnerabilities discovered.
- Used tools to detect / exploit OWASP Top 10 Vulnerabilities with BurpSuite, SQLmap, Nikto, Dirbuster, Nmap, and fuzzing applications to discover potential security flaws.
- Conducting internal penetration testing from an insider threat perspective.
- Developing and performing IT system security scans, result analysis, vulnerability categorization, and dissemination of results.
- Researching escalated vulnerability issues, recommending remediation and/or mitigation solution to assisting system administrators with implementation.
- Providing an understanding and application of security governance and best practices.
- Support system administrators in the implementation of NIST, FISMA, and researching requirements for successful remediation of Plan of Action and Milestones (POA&M), recommending solutions, assisting system administrators and software engineers with implementation.
- Maintaining knowledge of technical and non-technical security regulations, interprets requirements, communicates with IT staff and senior management.
- Supporting secure system development lifecycles.

12/2015 – 3/2016 **Independent Security Consultant**

Security Consultant

- Lead customer engagements in providing security consultation in identifying and protecting customer's proprietary data by conduct a quantitative analysis on their vulnerabilities that potentially by exploited.
- Responsibility for conducting vulnerability risk assessment and penetration testing against the customer's network and web application using various tools within Kali Linux.
- Conducting social engineering attacks against corporate employees to simulate malicious threat actors attempting to extract information about the corporation.
- Reviewed, interpret and prioritize system vulnerabilities.
- Created tools using Python to automate basic enumeration task, correlate and extract information on suspicious ports and malicious traffic within logs, and setup Elasticsearch, Logstash, and Kibana for visualizations and representation of risk metrics to an environment.
- Research relevant threats and exploits currently being used in cyber attacks by threat actors or state sponsor attacks.

06/2015 – 12/2015 **Infor Corporation, TX**

Sr. Security Analyst

- Primary responsibility was managing and performing vulnerability assessments to over 50,000 servers.
- Responsible Verified finding and false positive by organizing meeting with various Product Directors in explaining each finding, gave recommendation on executing remediation action plan to ensure mitigation based on vulnerable findings.
- Completed primary objective by leading the initiative to automated schedule scan and manipulated of the results, which has increase productive 20% due to this automation process.
- Created custom prototype python program that streamline the manual process of manipulation result findings, which made it easier to management and executives to quickly understand each weakness within the corporations environment.

01/2015 – 6/2015 **ZeroFox, MD**

Director of Field Services

- Primary responsibility was managing a four man team performing deep dive analysis on malicious links posted via social media sites.
- Lead initiative on performing web application and network penetration testing and vulnerability assessment to verify finding and false positive.
- Performed manual exploitation technique against infrastructure and web application, and executing remediation and mitigation plans based on vulnerable findings.
- Created custom prototype python programs to integrate into ZeroFox's software platform.
- Responsible for performing incident response on breached customer.

06/2014 – 01/2015 **Federal Judiciary Commission, DC**

Web Application Penetration Tester / Sr. Security Analyst

- Primary responsibility was performing web application vulnerability assessment and verify false positive by performing manual exploit against the specified court web server.
- Responsible for monitoring and perform analysis on alert triggered events within FireEye, ArcSight, Imperva and Sourcefire while writing brief report on vulnerabilities with the potential exposure to exploitation.
- Perform deep dive analysis on malicious and non-malicious traffic using FireEye packet capture, Wireshark, Wget, and Splunk in correlation to gather evidence to verify false positive or true positive.
- Create ticket and court notification based on activity, which are deemed malicious, host infection beaconing to CNC server, and/or traffic attempting to compromise a court's server.
- Issue firewall block against IP address attempt malicious activity against web servers, servers, or host machines.
- Review e-mail header file submitted to the SOC based on judges or court employees that received Spam to their e-mail account.

09/2011 – 06/2014 **CompuCom System, Inc., TX**

Sr. Information Security Specialist

- Primary responsibility was to conduct vulnerability assessment scan, give an in-depth analysis report of my findings, which help to strategically defend against vulnerabilities that could exploit and comprise the customer's environment.
- Address the IDS and Firewall team to customized updates to signatures and ACL on appliances we supported.

- Lead a team that performed small periodical pen-test and was responsible for determining the measurable impact on systems, by conducting an in-depth analysis on port and protocols in order to determine the risk, vulnerabilities, and demonstrated the impact, which could cost the clients, if an attacker breach the client's infrastructure.
- Revised the company's SOC Service SOW, which included Firewall Management, IDS / IPS Management, Web Content Filtering, Vulnerability Assessment Scan, Threat Analysis Reports, Log Management, Security Management and Monitoring, Incident Response Management, Communications and Change Management, Identity and access Management, and Operational Management.
- Assigned a key role in teaching and mentoring teammates on best security practices and spoke on the newest cyber threats, there impacts, and the threat posed to our clients.
- Developed internal proprietary python scripted software to enhance the SOC's capabilities to quickly extract information needed from syslog files.

09/2010 – 2/2011 **Booz | Allen | Hamilton, MD**

Associate / Binary Reverse Engineer

- Primary responsibility was to reverse engineer Malware using IDA Pro and OllyDBG to give an in-depth analysis report of my findings, which help to strategically defend against malware by updating custom signatures to IDS and IPS appliances.
- Participated on a team that performed Penetration test and was responsible for determining the measurable impact on systems, by conducting an in-depth reverse engineering and protocol analysis on a specific software in order to determine the risk, vulnerabilities, and demonstrated the impact which could cost the clients millions of dollars and the possibility of confidential information being extracted out of there network.
- Created and presented a 1-hour presentation on best methods and tactical strategy analysis on Malware, the possible cost of the breach, and the impact to our clients and newly hired employees for Malware analysis department.
- Lead a research team in analyzing different aspects of Smartphone, market share, vulnerabilities, and exploits. This research demonstrated how businesses productivity could be affected if compromised.
- Assigned a leadership role for all new employees awaiting clearance. This position was key in assessing new employees' levels of experience, helped define each new employee skill set, and correlated each person's individual skills to task them on unclassified projects.
- Developed an internal proprietary Scapy software course in order to enhance employee's abilities to manipulate packets and give them a better understanding of different Internet Protocol.

01/2008-2/2010 **iTeam Technology Associates, NY**

Sr. Security Analyst / Consultant

- Primary role was to manage IT security operations by providing advisory decision to enhance security, which gave mitigating and preventive measure to threats, vulnerabilities, and risks infrastructure.
- Performed penetration tests on clients using some of the following tools as Metasploit, Scapy, Nessus, and Nmap.
- Generated technical report and strategic demonstration showing a reduction of attacks, which improved the management of the corporate Firewall, IDS, DNS, and network infrastructure to help mitigate risk and vulnerabilities from emerging security issues.
- Perform consulting services for Iron Guard Security and MAF Corp in the design and implementation one of the largest privately held security research labs in the country.
- Researched RFID technology and reported how cloning RFID affects security. Developed reusable python scripts to read numerous types of RFID tags.
- Perform security research on VLAN and Layer 2 security that has developed into two speaking engagements “HOPE” & “DEF CON” security conferences.

9/2007-01/2008 **Federal Reserve Bank, NY**

Security Engineer / Analysis Developer (Contractor)

- Develop confidential user documentation manuals base on NIRT (National Incident Response Team) standard policies pertaining to IDS installation, configuration and deploy process.
- Responsible for technical reports base on performing reverse-engineering analysis, which helped the development of tactical security on malicious URL, that targets the Federal Reserve Bank.
- Produced a research report on the concerns of VLAN attacks, how each attack can compromise the integrity of the banks VLANs and infrastructure, then finally illustrated how to mitigate these attacks.
- Responsible for tracking ISS and Sourcefire IDS deployed throughout different branches of the Federal Reserve Bank.
- Participated in the analysis of log files, to determine if any users or information security RSS news databases are having any connectivity issues or viewing NIRT s internal portal detailing the latest computer security vulnerabilities.

EDUCATION:

Cybrary, Online

All Web Application Micro-Certifications, Risk Management Micro-Certification, All Vulnerability Management Micro-Certifications 2107 – 2018

Career Center, New York, New York

MCSE, CCNA, CCNP, Security + Certification, Network +, A+ 2003 – 2004

New York University, New York, New York

Microsoft LAN Administration Certificate, 2001

Baruch College, City University of New York, New York, New York

Internet Technology Certificate, December 1997

Reference Available Upon Request