



Karl Biron



LOCATION Silicon Oasis, Dubai UAE	D.O.B 26/04/1991	DRIVING LICENSE LMV
E-MAIL karlbiron@yahoo.com	MOBILE NUMBER +971 56 474 5063	LINKEDIN www.linkedin.com/in/karlbiron

ABOUT ME

I am a Cyber Security professional with 5 years of experience in networking and information security as well as system administration and data center expertise. I am currently working in University of Dubai as a R&D Cyber Security Engineer. My role revolves around the implementation, configuration and maintenance of cyber-security tools and applications for information security lab projects funded by external entities. I am responsible for the design and development of scripts in both Windows and (especially) Linux environment for automated data acquisition, data sanitation, data processing, exploratory data analysis and then communicating data via smart and interactive visual reports. Moreover, I am also responsible for the seamless network and security operations of the information security labs through network architecture planning and implementation. I ensure to utilize best practices on my script/software development and network security architecture as well as abide by the organizations cyber-security standards thoroughly. One of my greatest contribution is designing entire projects to run on full automation using various scripts and applications that effectively increased efficiency and decrease overall required manpower.

WORK EXPERIENCE

Cyber Security Research & Development Engineer | University of Dubai

May 2018 - Current (Dubai, UAE)

- Developed, configured, and deployed security tools in the operations environment and performed test, audit, and other security measurement capabilities.
- Ability to write documentation for a variety of audiences, including technical & non technical personnel (eg. System & network administrators, software developers, senior managers, HODs and sponsors.)
- Knowledge and expertise in network and system penetration tools (NMAP, HPING3, MetaSploit, Enum4Linux, Hyena, ADEplorer, JackTheRipper, Cain & Abel, Responder, etc) and methodologies (NIST, OWASP, etc)
- Maintain awareness of emerging threats by actively attending and participating in InfoSec related events and conferences (eg. GISEC, HackIntheBox, IEEE conferences, etc)
- Knowledge and working experience on cyber attack stages (reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)
- Published international conference papers and has experience in speaking engagements at conferences
- Posses advanced knowledge and hands-on skill on Linux administration (Ubuntu, RHEL, SuSE, Solaris, etc).
- Strong grasp of scripting languages (eg. Linux-Bash, Perl, Python, Windows Batch and Powershell)
- Deep and extensive practical experience in REGEX concepts (GREP, SED, AWK, JQ and Xpath commands)
- Adept in Linux and Windows automation (Crontab, rc.local and start-up application, Windows Task Scheduler)
- Experienced in REST API using Curl command to extract specified content from a website.
- Capable of generating insightful and informative visualization graphs, maps and charts through MS PowerBI and Tableau.
- Experienced in vSphere administration with over a 100 clients (design, maintenance & troubleshooting)
- Experienced in a variety of open source HoneyPot tools from installation, configuration, deployment and maintenance.
- Working knowledge of vulnerability assessment (Nessus & Nikto) and penetration testing (VAPT)

- Experienced in Web server (Skipfish, HTTPRecon, ID Server, Hydra, SQL Map, etc) and Web application (WPScan, Vega, BurpSuite, etc) penetration tests.
- Capable of full intrusion detection system (IDS) installation and configuration (eg. Snort & Suricata).
- Broad knowledge of networking protocols (TCP, UDP, DNS, FTP, SMTP, DHCP, etc.)
- Experience performing network traffic analysis/packet-level analysis (Wireshark GUI, Tshark, Tcpdump, IPTables, Capinfos, and Dumpcap CLI)
- Able to install and configure Cuckoo Sandbox to automate Malware analysis and also able to sift through Malware obfuscation to find the underlying function and intent of a Malware using various tools (IDA Pro & OllyDbg).
- Capable of basic to intermediate Firewall (Cisco/Juniper/FortiNet) configuration of Policies and Objects (Static NAT Mapping, DHCP, etc) through both the web based interface as well as the CLI.
- Working experience with front and back-end web development languages (HTML, CSS, JavaScript, PHP, SQL)

Telecom & Data Center Engineer | Nahjtech

July 2015 - Feb 2016 (Abu Dhabi, UAE)

- Conducted site surveys to identify site issues such as required iron work, cable routes and length, equipment, ODF and DCDB allocation, fiber connector types and delivery access.
- Installed Ciena racks with proper ground and top support in various site conditions such as raised floor, concrete floor, and cables running from overhead or underground.
- Laid and patched fiber optical cables from equipment to ODF and vice versa.
- Laid and terminated power, earth and fiber optical cables.
- Prepared RJ45 cables for COLAN, ILAN and/or craft port (remote commissioning)
- Used Power Query of Microsoft Excel to collate data from multiple Excel files that presents an overall report of a project.
- Created floor-plans using Microsoft Visio and AutoCAD to identify Rack, Line Fiber ODF, Client Fiber ODF, DCDB location and the proposed cable routes.
- Used Microsoft Excel to tabulate Power Running Lists and Fiber Running List (Internal and External).
- Familiar with Ring Networks (ROADM and ILA sites).
- Completed several training of Ciena web courses for equipment such as 6500 32-Slot and 14 Slot, 5430 and 5410 and Ciena Ethernet switches.
- Familiar with Ciena circuit packs such as WSS, MLA, SRA, XLA and etc.

IT & Systems Administrator | Netlynx Technology

June 2012 - June 2014 (Singapore)

- Monthly maintenance and file/folder housekeeping of Interactive Voice Response System (IVRS) and Automated Recall and Monitoring System (ARMS) that has prevented and minimized customer on-site faults and emergencies.
- Quality assurance of various automation and communication products that significantly lowered the rate of the company's return of defective products. (Testing power and looking for common faults).
- Minimized server down-time by responding to faults and emergencies at customer site to analyze and rectify problems.
- Maintained and updated batch manufacturing records (using MS Excel) of log books that proved to be useful in times of searching for a faulty batch.
- Experienced with a variety of sever installation and setup including Windows Server 2003, 2008, 2012 and Windows 7&8.
- Configured and tested GSM modems to be installed in customer site.
- Conducted incident response and disaster recovery in emergency fault situations.
- Experience with Cisco routing and switching protocols (OSPF, EIGRP, BGP, STP, etc.)
- Involved in several on site installations be it in teams or alone.
- Managed regular endpoint security (Symantec) patch maintenance for many of our clients.

ACADEMIC QUALIFICATIONS

- 2014-2018** Bachelor of Science in
Computing and Information Systems
University of Dubai, UAE
- 2009-2012** Diploma with Merit in
Media and Communication Technology (Telecommunication)
Temasek Polytechnic, Singapore
- 2006-2008** GCE 'O' Levels
Saint Patrick's School, Singapore

AWARDS/CERTIFICATE

- Aug 2020** EC-Council Ethical Hacking Leaderboard, 2nd Place for August 2020
- July 2020** Certified Ethical Hacker [CEH] Practical Exam (20/20)
- Apr 2020** Certified Ethical Hacker [CEH] Knowledge Exam (120/125)
- Nov 2018** HackInTheBox Conference Training (Modern Malware Warfare)
- Nov 2018** University of Dubai's BSc Graduate (Summa Cum Laude)
- Nov 2017** University of Dubai's Deans Highest Honor (CGPA: 3.99)
- Nov 2016** University of Dubai's Deans Highest Honor (CGPA: 4.00)
- Nov 2015** University of Dubai's Deans Highest Honor (CGPA: 4.00)
- Oct 2014** IELTS (Band 8 out 9)
- Apr 2014** Cisco Certified Network Associate (CCNA)
- Feb 2014** Cisco Certified Entry Networking Technician (CCENT)
- Mar 2012** Diploma with Merit in Media and Communication Technology
- Mar 2012** Temasek Polytechnic Honor's List (top 10% of the graduating cohort)
- Jan 2012** Merit Award Certificate for Major Project (top 5% of Engineering School)
- Dec 2011** IPv6 Basic Course Certification

PROFFESIONAL SKILLS

- Practice good interpersonal and communication skills.
- Proficient in English, verbal and written.
- Possess good analytic and problem-solving skills.
- Able to work to a high degree of detail.
- Worked independently, as well as in teams.
- Conducted weekly meetings and generated minutes of meeting.
- Planned and organized task delegation and distribution among the part time and internship team members to increase productivity and their technical proficiency.
- Have the ability to break down and explain complex information security problems to technical and non-technical team members.

PUBLICATIONS (As First Author)

Aug 2020

A Big Data Fusion to Profile CPS Security Threats Against Operational Technology
World of Wireless, Mobile and Multimedia Networks 2020 Conference in Cork, Ireland

Aug 2019

Data Science Tools for Crime Investigation, Archival, and Analysis
International Workshop on Pervasive Healthcare 2019 Conference in Leicester, UK