Ali Hussain

Career Objective: To contribute in making the world a peaceful and connected eco system. And invest my Cyber security and internet governance skills in solving the future cyber security challenges of world.

Summary:

I am a Cyber Security technology research professional having in depth knowledge of emerging Cyber Threats and detection technologies, innovation, and latest trends in the area of Internet Governance in different sectors.

With over 4 years of experience in the Anti Malware professional services, research and training industry at different levels, I am working with a number of International organizations.

With in-depth practical knowledge of web traffic categorization, CVE Analysis, CVE Hunting, APTs, Generic Malware Detection Engines, Reverse Engineering of Bot-Net families, Identification of Novel malicious behavior and digital forensics. I also have keen interest in Internet Governance Issues, Role of ICT as enabler in Society.

Hands on research and analysis experience on Fireeye NX appliances

I have excellent research & analysis skill coupled with strong understanding of multistakeholder community.

Contact Details

[redacted]

Distinctions and Services I can offer to Information Security Research Team

In addition to job at Ebryx (Pvt) Ltd did following extra activities totally self-motivation based:

1) Active member of The Multi-Stakeholder Steering Group (MSG) of APrIGF since Feb 2016
2) Attended SANOG 27 as fellowship member selected from Pakistan in Feb 2016
3) Participated in planning and organizing premium cyber security conference Cyber Secure Pakistan (CSP) 13-15 2)
4) Volunteer work with Pakistan information security association (PISA) and Lead regional chapter
5) Love Agile way of working and talking with security professionals
6) Trainee at Digital Forensic training for Law enforcement officers in Pakistan
7) Cloud and Virtualization Training and Certification

I can contribute in following area:

Give assistance in advanced and comprehensive vulnerability testing and risk analysis

Attack categorization based on attack vectors and type of infection social engineering, denial of service and malware analysis e.g. CVE sample classification out of web traffic and web exploit vector identification

Security components and architecture review E.g. utilizing windows internals knowledge to predict future threats landscape exploit and challenges in implementing defense.

Latest malware sample behavior based malware analysis (virtual machine based) and reverse engineering and exfiltration tracking using callbacks. E.g. Malware analysis of widows and computer network based malwares and tracking malware families using Snort rules.

Final Year Project | UnderGraduate BE | Software based Bittorrent Caching Solution for Internet Service providers (ISP)

As undergraduate final year thesis, we have developed a software based Torrent caching solution that enable ISP to cache bittorrent protocol data and serve for subsequent redundant requests. Key feature of our software are; don't pose much delay, smartly utilize open source technologies, scalable and innovative approach to solve industry problem. We deployed at local ISP, NaYatel Pvt Ltd, in Islamabad, Pakistan

Educational Qualifications

Degree/Diploma	University/Board/Institute	Year Attended
Bachelor of Information & Communication System Engineering	National University of Sciences and Technology (NUST), Islamabad, Pakistan	[redacted]

Work Experience: Specialization; Threat analysts, Automation and Research

Lead Regional Chapter | Pakistan Information Security Association (PISA)| December 2015 to Present

I am Information Security Analyst and Internet Public Policy researcher. Leading Regional Chapter at PISA and Visiting Forensic Investigator at PISA – CERT. Actively involved in general Cyber Security awareness of community in Pakistan.

Currently working on our National IGF in Pakistan.

Lead first Internet Summit of Pakistan in 2016 and organizer of Cyber Secure Pakistan 2013-2015

Participated in past three OIC Cyber Drills on behave of Pakistan from PISA Platform

Senior Malware Research Engineer | Ebryx, Pakistan | December 2015 to Present

Advance patch guard analysis of web FNs and product's features deep analysis to find our root cause of detection loss. R&D of window 10 x86/x64, port various security tools to window 10 x86/x64 and Cuckoo based lab setup to compare existing tools with cuckoo detection.

Windows 10 security architecture review and penetration testing and managing team.

Malware Research Engineer| Ebryx, Pakistan | June 2012 to December 2015

- Analysis of zero day attacks, analyzing weekly web exploit attacks and binary attacks to check for false positives, unique malware behaviors through the analysis of many malicious toolkits samples, sample development as POC for proposed various techniques, Gained complete expertise in behavior of all types of malwares in wild, windows shellcode writing malicious pcap analysis and experience in the following areas (exe, dll, Java, Flash and PDF). Also conducted 2 training sessions of company wide network security team
- Experience of dissecting and analyzing samples in debugger.
- Extracting the forensic footprints of Malware and the Incidents of data theft. Classification of malware families.
- Understanding of various file format exploited in wild and exploitation techniques used in 0 days In depth windows internals architecture and binary execution
- Experience of anti-reverse engineering and anti-debugging techniques Developed ROP, Shellcode samples for both x86 and x64 Developed samples for QA of bugs verification and general R&D tasks

Certifications and Trainings:

Name of Certification: **Security and Privacy Awareness Training**
Certification authority : FireEye, Inc., License AH3621291020150212190A
Dates Starting October 2015

Name of Certification: **Cloud And Visualization hand on Workshop**
Certification authority : South Asian Network Operators Group (SANOG)

Name of Certification: **CompTIA Security+**
Certification authority : Cybrary-IT, License (Training)
Dates Starting March 2016

Name of Certification: **Python for Security Professionals**
Certification authority : Cybrary-IT, License (training)
Dates Starting August 2015

Name of Certification: **Metasploit**
Certification authority : Cyberary-IT, License (Training)
Dates Starting May 2015

Honors & Achievements

1) Fellowship winner of SANOG 27 conference and workshop
2) Core planning and organizing committee member at Internet Summit of Pakistan 2016 (ISP'16)
3) Received souvenirs of appreciation for best performance in academic year NUST-SEECS, Islamabad
4) Runner up NASCON 2012 held at FAST-NU Islamabad
5) Appreciation by NaYatel CEO for successfully completing "Bittorrent Caching Solution at ISB Corporate Network"
6) Awarded 100% Scholarship by Government of Pakistan through National ICT R&D fund for graduation from National University of Science and Technology (NUST)
7) Acknowledged and appreciated by NUST as well as National ICT R&D Fund for achievements in FAST-NU Islamabad

Website links: http://seecs.nust.edu.pk/news_events/nascon2012/index.php
http://ictrdf.org.pk/stories/?p=20

Reference:

[redacted]

[redacted]

[redacted]