Mohammad Khabir Uddin

Merivalkama 1H as 72,  
02320 Espoo, Finland.  
Mobile : +358 46 5647293

Email: masumndc1@gmail.com

Skype: md.khabir.uddin

Github: https://github.com/masumndc1/zim

Linkedin : https://www.linkedin.com/in/mohammad-khabir-uddin-a9a67114

Professional Certification

1. **E|CSA (Eccouncil Certified Security Analyst)**

Certification Number: **ECC93298374538**

Exam date: **21th December,2013**

2. **C|EH (Certified Ethical Hacker)**

Certification Number: **ECC961022**

Exam date: **22th of April,2011**

Technical Knowledge

System Administration

* Hands-on working experience on System Administration and configuration knowledge on **firewall(iptables,pf)**,**Squid**,**Sendmail**,**Postfix**,**Apache**,**Nginx,HaProxy,bind9**,**DNSSec**,**DHCP**, **FTP**, **LVM,RAID,MySQL,MariaDB, OpenSSL, Openswan, Strongswan VPN, git** etc on **Red hat Linux, CentOS, Debian, Ubuntu, OpenBSD, FreeBSD, NetBSD and Archlinux operating system.**
* Knowledge on **Networking** and **package management** on **Solaris 10** OS**.**
* Apt on limiting users and processes by **Selinux** and **AppArmor**.
* Working knowledge on configuration management tool **Ansible** and **Saltstack.**
* Working knowledge on **Bash scripting** and **Python**.

Cloud

* Knowledge on cloud computing using **Openstack** (Keystone,glance,rabbitMQ,Nova,Nova-compute and horizon) and Amazon web service **AWS** (EC2,ELB,Auto Scaling, CloudWatch, IAM, CloudFormation, CloudTrail etc).

Containers and orchestration

* Working knowledge on **Linux container** and networking using **LXC,Vagrant**,**Docker**,**Docker Swarm** and **Docker Compose**.
* Apt on container management using **Kubernetes.**
* Apt on cloud deployment and management using **Packer** and **Terraform**.

IDS/IPS

* Hands-on Network based Intrusion Detection System **(NIDS)** using **Snort, Suricata.**
* Hands-onHost based Intrusion Detection System **(HIDS)** using **OSSEC, AIDE.**

Virtualization

* Apt on Vmware ESXi and Vsphere and virtualbox.
* Apt on Kernel-based virtual machine (KVM).

Identity Access Management (IAM)

* Working experience on freeradius, freeipa on Unix based OS.

Security

* I have experience on **Network Security operations, monitoring and management** along with vast knowledge on **TCP/IP, packets analysis (Wireshark,Tshark,Xplico, tcpdump** etc**)** and **IPS/IDS** tools **(Snort,psad)** along with other security tools (**Nmap,Nessus, Nexpose, OpenVAS, Metasploit, Burp suit** etc) included in **Backtrack/ KaliLinux/ Blackbuntu** security distro.
* Network security monitoring using security distro **SecurityOnion**.
* I have also expertise and experience on **maintenance of the security policy**, **standards and procedures**, **review firewall rules**, **recommend required actions, penetration testing and vulnerability assessment.**

SIEM

* Apt on log management using rsyslog in Unix operating system.
* Hands-on knowledge in Splunk.
* Hands on Knowledge in ELK (**Elasticsearch,logstash** and **Kibana**).

Computer Networking

* Experienced on **routing** (**OSPF,RIP,EIGRP,BGP** and static etc) and **switching** using **cisco,juniper** routers,switches**.**
* Apt on opensource networking systems using quagga, vyatta, VyOS in linux.
* Knowledge on Software defined Networking (**SDN**) using openvswitch, openflow and opendaylight.

Firewall

* Hands on experience of providing network security, access-control, policy build-up, routing, switching, natting, filtering, User Authentication, configuring vpn (ipsec), load balancing etc using **cisco ASA, juniper SRX** and **MX,** **Checkpoint, PaloAlto, fortigate, pfsense, Astaro Linux** and **Mikrotik.**
* Hands on experience on natting, gateway, redirection, access control, traffic shaping, bandwidth management using **Pf** on **OpenBSD, FreeBSD, NetBSD** operating system.

Bandwidth Managemet

* Knowledge on **Bandwidth Management** in Mikrotik, **HTB** in Linux, **ALTQ** on BSD operating systems.

Wireless Networking

* Knowledge on **Wireless Networking** configuration and WEP,WPA security techniques.

Monitoring

* Monitoring infrastructure using **Nagios** and **grafana**.

Academic Qualifications

**Session 2003-2007: B.Sc. in Electronics and Communication Engineering (ECE)**

Khulna University, Khulna, Bangladesh.

Secured 3.37 CGPA out of 4.00 with Telecommunication major.

Working experience

1. Working as **Developer,Network Security** in **L M Ericsson,Jorvas,Finland** from 12th of march,2018.

2. Worked as **Senior Officer** (promoted from Officer) at Information Technology Department in **Prime Bank Limited,Dhaka, Bangladesh** from 12th May, 2010 to 15th May, 2016. Duration: 6 years.

3. Worked as **Asst.System Administrator** in **Media & Multimedia**, **Dhaka, Bangladesh** one of the fastest growing ISP in Bangladesh from 15th April,2008 to 5th May, 2010. Duration: 2 years.

Personal info & Interest

I started learning Linux and Cisco Networking and switching during my B.Sc level back in 2006. Through the year I have devoted myself to learn various firewalls,routing and other linux and BSD operating systems. My **eight** years of practical experiences on networking and system and security administration skills helped me a lot to become **C|EH(Certified Ethical Hacker)** then **E|CSA (Eccouncil Certified Security Analyst)** certified**.** I had also conducted **vulnerability assessment** and **penetration testing** for organizations.Most of the time now, beside my job, I spend cracking vulnerable OS(Kioptrix, pWnOS etc) by tools included in Kali Linux (Metasploit, nmap, nessus, openvas etc). Firewalling(juniper, cisco ASA, paloalto etc) and automation (shell scripting, ansible, saltstack) intrigue me also. I also like to learn new things and some of my works can be found on my github account.