**Name :** **Naeyna Alam**

**Position :Cyber Security**

**Professional Summary**

Having over 6 plus years of experience in Information Security Analyst with expertise in incident management, unauthorized access, viruses and a wide range of vulnerabilities and threats. Well-versed in direct and remote analysis with strong critical thinking communication and people skills. Able to thrive in fast-paced and challenging environments where accuracy and efficiency matter.

**Education**

Master of Science in Information Technology

Minnesota State University, Mankato, MN

Bachelor of Science in Electrical and Electronics Engineering

American International University-Bangladesh (AIUB), Dhaka, Bangladesh

**Technical Skills**

|  |  |
| --- | --- |
| Security& Networking: | IDS/IPS, Identity & Access Management, Data Security, Firewall, WAF, Proxies, DDoS, Cloud Security, Advanced Wireshark, Threat Analysis, Endpoint Security, Metasploit, Splunk, Sentinel, Risk Management, Security Research, Kali Linux. |
| Programming Language | C, C++, PLSQL, Java |
| DBA,QA & Testing | Oracle SQL, Microsoft Access, MSSQL, QlikView, Azure, SQL injections, System testing, Unit testing |
| Virtual Machines | VMware and VirtualBox |
| Technologies/ Concepts and Tools | HTML, XML, CSS, Trello, JIRA |
| Certificate | Graduate Certificate in Database Technology |

**Related Course Work**

• **Information Warfare** - Worked with network traffic capture using Wireshark, network scanning using net cat and Nmap. Worked with network analysis, malware analysis, and incident response. For each lab we submitted a report describing how we analyzed the situation and what helped us to let that one-person work on it. Studied basics of configuring and reviewing IDPS tools, SIEM tools, Antivirus, etc.

• **Mini Thesis** - The paper addressed some of the risks that corporate offices are experiencing, the basic concepts and importance of prioritizing cybersecurity risks with some data collected from previous surveys, and the actions executive board members should be taking to safeguard against risks.

• **Self Study –** Taking Udemy and Cybrary courses like malware fundamentals, network security fundamentals, SOC analyst training, CYSA+ certification training, etc.

**Professional Experience**

**Technical Consultant (Cyber security) Aug 2017 – Till Date**

**CRT, Mankato, MN**

* Reviewed and provided feedback on network firewall syslogs and web activity logs for unusual activities.
* Worked with the Service Desk and FootPrints to remedy issues located during vulnerability scanning.
* Investigated security violations and breaches; provides analysis summary to management and recommends alternative courses of action when possible.
* Updates System Security Plans (SSP) Using NIST 800-18 as a guide to develop SSP, Risk Assessments and Incident Response Plans.
* Collaborated with teammates, managers, and other senior engineers to develop and implement process improvements regarding the detection, investigation, containment, recovery, and eradication of security events.
* Utilized my knowledge, skills, experience and tools in countering malicious code attacks such as viruses, malware, spyware, adware, worms, Trojan horses, root kits and all other abnormal activities on computer systems and on the network.
* Performed regular systems and network vulnerability scans using Qualys; identify and remediate potential risks and coordinated patch and vulnerability management with the Vulnerability Risk Management (VRM) team.

**Teaching Assistant Aug 2016 - May 2017**

**Minnesota State University, Mankato**

* Assisted faculty to develop class material for students and the course lab for the security course.
* Evaluated and provided feedback to students during the lab work.

**Information Analyst Aug 2014 - July 2016**

**Bit / Mascot Pty Ltd, Dhaka, Bangladesh**

* Worked in a group of 3 security analysts to provide excellent service & report to CISO/Team Lead.
* Performed initial incident investigation/response.
* Analyzed security alerts/incidents and tickets for malicious traffic and events on the network.
* Monitored and analyzed firewall logs of active users to ensure any risks are responded to

immediately.

* Evaluated web application firewall (WAF) configurations.
* Utilized strong TCP/IP networking skills to isolate and diagnosed network issues.
* Identified & evaluated potential threats and vulnerabilities on company network.
* Performed & Investigated Forensic Imaging.
* Preformed pen-testing in existing web applications and reported to DevOps team.
* Executed vulnerability scans of all technology assets on a regular basis.
* Ensured secure disposal and destruction of data of any electronic media containing confidential information.
* Performed risk assessments to help create optimal prevention and management plans.
* Made recommendations for mitigating identified risks with Systems & Network team.

**IT Analyst. Jan 2013 - Jun 2014**

**Brandable, Dhaka, Bangladesh**

* Resolved any technical issues over the phone, and/or in person.
* Communicated daily basis with system administrators to ensure data integrity when completing a DMCA, SOC, Malware and Phishing tickets.
* Worked with web development team to investigate security vulnerabilities.
* Performed patching of about all machines.
* Executed vulnerability scans of all Information Technology assets.
* Troubleshooting printers, network connectivity, windows, Linux and MacOS hardware & software system.
* Reinstalled software programs or adjusted settings on existing software to fix machine malfunctions