Naimur Rahman

30/1, Road 3, Block C
Banasree, Dhaka, Bangladesh
(+880) 1728389090
(+63) 9083570715
naimurrahman04@gmail.com
https://www.linkedin.com/in/naimur-rahman-417a2a1a8/

Cybersecurity Engineer experienced in vulnerability assessment, penetration testing, security analysis, malware analysis, and software development, seeking new opportunities to leverage skills and expertise to enhance organizational security.

EDUCATION

Daffodil International University, Daffodil Smart City, Ashulia, Dhaka — *B.Sc. in Software Engineering.*

In spring 2019 I started my Bachelor of Science (B.Sc.) in Software Engineering **(Major in Cyber Security)**, at Daffodil International University, Dhaka, Bangladesh. **CGPA:3.59 out of 4**.

Al-Amin Academy School & College, Chandpur — *Higher Secondary Certificate (HSC) in science*

2018 Higher Secondary Certificate (HSC) in Science, Al-Amin Academy School & College, Chandpur, Chittagong **GPA: 3.25 out of 5.00**.

Al-Amin Academy School & College, Chandpur — *Secondary School Certificate (SSC) in science*

2015 Secondary School Certificate (SSC) in Science, Al-Amin Academy School & College, Chandpur, Chittagong **GPA: 4.81 out of 5.00.**

EXPERIENCES

12 April 2024- Started Working as Senior System Security Engineer (offensive security) at Cyber Security Department at **DigiPlus Interactive Corp** and worked on security various fields of cybersecurity.

1. Vulnerability Assessment and Penetration Testing:

   Identified and assessed vulnerabilities in IT infrastructure and applications, taking proactive measures to address them. Conducted penetration testing to simulate real-world attacks, ensuring the organization's security readiness.

2. Malware Analysis:

   Conducted in-depth analysis of malware, including behavior, code, and characteristics, to enhance detection and prevention strategies. Developed effective strategies to mitigate the risks posed by various types of malicious software.

CERTIFICATIONS & ACHIEVEMENTS

1. **Certified Ethical Hacker (CEH)**

   4 April 2021 Certified Ethical Hacker certificate through an examination administered by EC-Council.

2. **C)VA: Certified Vulnerability Assessor**

   4 April 2021 Certified Vulnerability Assessor certificate through an examination administered by mile2.

3. **Windows Forensics**

   15 January 2021 Windows forensics authorized by Cyber Security Center

4. **Burp Suite: In-Depth Survival Guide**

   21 June 2022 authorized by Udemy.

5. **Linux Command Line**

   20 October 2020 is authorized by Coursera and offered through Coursera.

6. **Technical Support Fundamentals**

   21 Feb 2021 Technical Support Fundamentals are authorized by Google and offered through Coursera.

7. **Intro to Bug Bounty Hunting and Web Application Hacking**

   22 September 2022 authorized by Udemy.

8. **OSINT: Content Discovery**

   2 September 2022 authorized by Udemy.

9. **Spoken English Course**

   11 Oct. 2019 I got certificates for the" Spoken English Course". by Daffodil International Professional Training Institute with an "A" grade.

10. **Computer Office Application**

    15 December. 2019 I got the certificate for" Computer Office Application". from Bangladesh Technical Education Board Dhaka with an "A+" grade.

3. Threth Analysis:

Conducted comprehensive threat analyses to assess potential security threats and their impact on the organization. Informed decision-making processes for security measures and risk mitigation strategies based on threat assessments.

4. Digital Forensics

Conducted thorough investigations into security incidents by collecting, analyzing, and preserving digital evidence. Utilized forensic tools and techniques to retrieve data from compromised systems, including recovering deleted files, analyzing logs, and identifying attack vectors. Performed root cause analysis to determine how breaches occurred and collaborated with legal and incident response teams to support ongoing investigations. Prepared detailed forensic reports outlining findings and recommendations for remediation, ensuring adherence to industry standards and legal requirements for evidence handling and chain of custody.

29 June 2023- Started Working as Advance Cyber Security Engineer at Network Security Department at **ITCOM (Philippines)**and worked on various field of cyber security.

1. Monitoring and Handling Threats (SANGFOR CC):

Proactively monitored and managed security threats within the organization's network using SANGFOR CC security solutions. Identified, analyzed, and responded to various security incidents, ensuring minimal impact on operations.

2. Malware Analysis:

Conducted in-depth analysis of malware, including behavior, code, and characteristics, to enhance detection and prevention strategies. Developed effective strategies to mitigate the risks posed by various types of malicious software.

3. Managing and Implementing DRM (FASOO):

Administered and deployed Digital Rights Management (DRM) solutions provided by FASOO to safeguard sensitive digital assets. Controlled access and managed permissions to protect intellectual property and confidential information.

4. Vulnerability Assessment and Penetration Testing:

Identified and assessed vulnerabilities in IT infrastructure and applications, taking proactive measures to address them.
Conducted penetration testing to simulate real-world attacks, ensuring the organization's security readiness.

5. Handling EDR and SIEM:

11. **Practical Ethical Hacking**
    12 February 2023 authorized by TCM security.
12. **Secure 13 positions on National Cyber Drill 2022**
13. **12-13 Jul 2022 -** Secure 13 positions on National Cyber Drill 2022 (**BGD e-GOV CIRT CTF Ground**). https://cyberdrill.cirt.gov.bd/scoreboard
14. **External Pentest Playbook**
    20 September 2024 authorized by TCM security.
15. **Practical API Hacking**
    21 September 2024 authorized by TCM security.

TECHNICAL SKILLS

1. Penetration testing

2. Vulnerability Assessment

3. Digital Forensics

4. Malware Analysis

5. Sandboxing

6. SEIM
7. Dark and Deep Web Analysis

8. Endpoint Detection and Response (EDR)

9. Linux

10. Information Security & Risk Management

11. Web Development

12. Security Analysis

PROGRAMMING SKILLS

1. C Programming

2. PHP

3. Python

4. HTML

5. CSS

6. JAVA

PROJECTS

1.SNMPS — This script is created to simplify "find and discovering live host" and "NMAP scan" (nmap contain -T4 -A (everything) - p- (all ports) -

Managed and maintained Endpoint Detection and Response (EDR) solutions to detect and respond to threats on individual endpoints.
Effectively utilized Security Information and Event Management (SIEM) tools to centralize security event data analysis.

6. Threat Analysis:

Conducted comprehensive threat analyses to assess potential security threats and their impact on the organization.
Informed decision-making processes for security measures and risk mitigation strategies based on threat assessments.

25 Jul 2021- Started Working as a Cyber Security Engineer at Security Operations at **Enterprise InfoSec Consultants (EIC)** and worked on various projects in reputed banks and organizations with more than **2 years of experiences**.

The Banks and organizations I have worked with:
1. International Finance Investment and Commerce Bank Limited (IFIC).

I conducted a comprehensive black box penetration testing of the server and web application using the OWASP ASVS checklist as a framework.

2. DUNCAN brothers LTD.

I conducted a gray box approach to both internal and external penetration testing of the system, covering web application, API, Workstation, and AD testing. This approach simulated an attack by a threat actor with some prior knowledge of the internal system architecture.

3. United Commercial Bank (UCB).

I conducted black box internal and external penetration testing focused on server testing, along with a dark web analysis to monitor the system's online presence in hidden areas of the internet where cybercriminals operate.

4. Uttara Bank LTD.

I performed Vulnerability Assessment and Penetration Testing (VAPT) on the Core Banking System (CBS), workstations, servers, web applications, and APIs as part of the project.

5. Lanka Bangla Finance Limited (LBFL).

As part of the project, I performed a Vulnerability Assessment (VA) on the network devices, servers, and workstations within the scope of PCI DSS.

6. Meghna Bank LTD.

I conducted both Malware Analysis and Vulnerability Assessment and Penetration Testing (VAPT) on the

O(OS))
https://github.com/naimurrahman04/snmaps

2. BDCTF — CTF platform to solve CTF challenges. This platform is created with HTML, CSS, BOOTSTRAP, AND PHP. **http://bdctf.unaux.com/**

3. MEDICAREHELPDESK — MEDICAL HELP DESK to Help someone find blood and doctors. This platform is created using HTML, CSS, BOOTSTRAP, AND PHP. **http://medicarehelpdesk.ezyro.com/**

4. EVANDERBD — Multi-vendor ECommerce website. This platform is created using WordPress. **https://evandarbd.com/**

5. D&M — This website is created for clients. **https://github.com/naimurrahman04/**

6. Load-testing— This code appears to be a script for testing the response times of a list of URLs. **https://github.com/naimurrahman04/Load-testing**

7. mac-forensic— Help us to do mac-book forensic. **https://github.com/naimurrahman04/mac-forensic**

8. s3_operations.py — This script is designed to perform various operations on AWS S3 buckets and generate a report based on those operations. **https://github.com/naimurrahman04/s3_operations**

9. s3_operations.py — This script is designed to perform various operations on AWS S3 buckets and generate a report based on those operations. **https://github.com/naimurrahman04/s3_operations**

GitHub links-

https://github.com/naimurrahman04/

PERSONAL SKILLS

Languages

English language – Moderate proficiency. Fluent in speaking, Decent in reading and writing.
Bangla language – Native Fluent in speaking, Decent in reading and writing.
Hindi - Moderate proficiency. Fluent in speaking.

X-Factors

Great Communicator: Excellent verbal and written communication skills Ability to explain complex technical concepts to non-technical stakeholders. Effective collaboration with cross-functional teams

network device, web application, and server within the scope of PCI DSS as part of the project.

7. ABG Technologies.

I conducted a Vulnerability Assessment and Penetration Testing (VAPT) on the network devices and servers using a white box approach as part of the project.

8. Midland Bank Limited

I conducted a Vulnerability Assessment and Penetration Testing (VAPT) on the web application to identify and address potential vulnerabilities as part of the project.

9. Pathao

As part of the project, I conducted a Vulnerability Assessment and Penetration Testing (VAPT) on the payment service system's web application to identify and address potential vulnerabilities.

15 Jan 2021-Windows Forensic workshop organized by Cyber Security Center, Daffodil International University.

01 Jan 2021-Working on freelancing platforms like fiverr.com freelancer.com as a Web developer, Penetration tester, and Malware Analyst.

01 Jan 2021- Started Working as Campus Ambassador in the paid task and conducted Vulnerability Assessment on their website.

KEY DELIVERABLES

1. Specialized in public and private corporate security systems.
2. Utilized dynamic and static malware analysis tools like Cuckoo Sandbox, joe Sandbox, Malware Bazaar, Vmray, Any.run, Fireeye and VirusTotal etc. to detect and analyze malicious software.
3. Deployed and configured SEIM and SOC solutions to monitor and respond to security events in real-time.
4. Conducted threat intelligence analysis to proactively identify and mitigate potential cyber threats.
5. Commanding knowledge of VAPT concepts and best practices.
6. Extensive experience with White Box, Grey Box and Black Box penetration testing.
7. Experience with common automated VAPT tools such as Nessus, Burp Suite, and Trustwave etc.
8. Proficiency with other common attack tools and frameworks such as Wireshark, Kali, Metasploit, etc.

Early Learner: Passion for learning and staying up to date with the latest trends and technologies. Proven track record of acquiring new skills quickly. Eager to take on new challenges.

Creative Thinking: Ability to approach challenges from multiple angles. Think outside the box to find innovative solutions.

Enthusiastic Researcher: Understanding the importance of staying informed about the latest threats Continuously research and stay up to date on new vulnerabilities and exploits. Use research to inform threat intelligence and mitigation strategies Enthusiastic Researcher

Naimur Rahman.

SIGNATURE

9. Expert understanding of the difference between a vulnerability assessment and a penetration test in the context of assessment scope, objectives, and deliverables.
10. Prepared detailed VAPT reports for executives, including technical findings, risk prioritization, and actionable recommendations for mitigation.
11. Support the technical implementation of ongoing security requirements, including access control and technical audits.

Assessed security risks and reported them to the cyber security team for strategic patching.