# SIT111 - Task 2.2P

I am Iflal Iqbal. I am from Negombo, Sri Lanka and I am 21 years old. I am a student at CICRA campus who is conducting a bachelor's degree in cyber security willing to enhance my knowledge and skills in cyber field. I am excited about pursuing a career as a professional penetration tester. My goal is to contribute to the field of cybersecurity by testing the security of systems, networks and applications and identifying possible vulnerabilities in it. I strongly believe that by becoming a penetration tester, I can help organizations and individuals strengthen their security measures and protect against potential cyber threats.

I have acquired a wide variety of vital skills along the way that are extremely applicable to the penetration testing industry. These abilities have given me the capacity to evaluate and improve system, network, and application security with effectiveness.

Knowing the fundamentals of network security is one of my strong points. I am quite knowledgeable in encryption methods, protocols, and network design. With this knowledge, I can spot weaknesses and put strong security measures in place to fend off possible attackers. I also know everything there is to know about ethical hacking techniques. My abilities to conduct penetration tests, spot flaws, and take advantage of vulnerabilities in safe settings have improved. With this knowledge, I can mimic actual cyberattacks and offer practical advice on how to improve an organization's security posture.

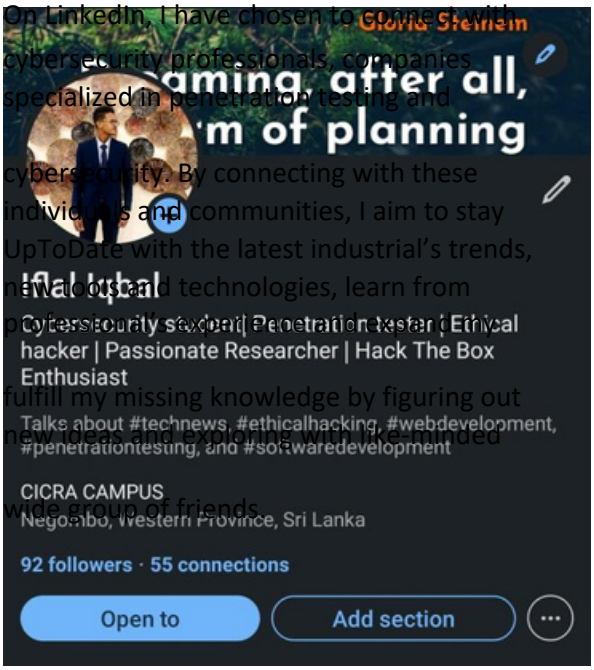
I have a great deal of experience with vulnerability assessment and risk analysis. I have extensive experience finding security holes and assessing their possible consequences through comprehensive examinations. I am able to efficiently assess and reduce risks, making sure that systems are safe from possible attacks, by utilizing industry-standard frameworks and tools like ISO27001, MITRE ATT&CK, and Metasploit.

Analytical and problem-solving abilities are essential to my work as a penetration tester. I have an excellent eye for detail and am skilled at breaking down complicated systems to find weak points. This enables me to create creative fixes and suggestions to fortify security measures. My proficiency with a variety of security tools and technologies, including as EvilGnix, FatRat, Beef, and Nmap, further improves my capacity to carry out thorough security assessments and offer clients insightful information.

In addition, I have worked toward obtaining pertinent certifications to enhance my technical knowledge. The Advanced Certificate in Networking and System Administration (ACNSA), Cyber Threat Intelligence (CTI101), Certified Cyber Security and Ethical Hacking (CCSEH), and Ethical Hacking Expert (EHE) are among these certifications. I'm working toward the Practical Ethical Hacking (PEH) certification right now. Which going to make me enhance me in the path of advancement and lead me to a professional level.

Looking ahead, I have set my sights on acquiring additional certifications including Certified Ethical Hacker (CEH), Certified Network Defender (CND), Certified Hacking and Forensic Investigator (CHFI), Certified Security and Information Officer (CSIO), and Offensive Security Certified Professional (OSCP). These certifications will provide me with advanced expertise in hacking methodologies, network defense, digital forensic investigation, and information security management.

Ultimately, my goal is to work for prestigious penetration testing companies like Google or other industry leaders. I am attracted to their commitment to cutting-edge security practices and the opportunity to contribute to securing complex systems and protecting user data. With my skills, certifications, and dedication to continuous learning, I am confident that I can make a valuable contribution to these organizations and thrive in the dynamic and challenging field of penetration testing.




On LinkedIn, I have chosen to connect with cybersecurity professionals, companies specialized in penetration testing and cybersecurity. By connecting with these individuals and communities, I aim to stay UpToDate with the latest industrial's trends, new tools and technologies, learn from

cybersecurity and industrial groups related to

professional network. Also, LinkedIn helps me

people and having a talk with them to have a

fulfill my missing knowledge by figuring out

wide group of friends.

During my personal learning time, I came across John Hammond, a cybersecurity researcher specialized in penetration testing. I was impressed by his approach to cybersecurity and his commitment to deliver high quality information to the public. His thoughts on continue learning, staying ahead of emerging threats and following ethical hacking policies perfectly aligns with my career values.

Also, during my research, I came across CISO2CISO Global Cyber Security Group, this group provides most complete reference & news, toolbox & networking related things for cyber technical and C-levels which helped me a lot in my research where I found legitimate resource to refer for. Its main objective is to build a large network of professionals with knowledge and experience in information security to share information receiving and giving help to the whole community of people interested in information security. Additionally, I am also interested in participating in industry-based communities like open web application security projects (OWASP) which offer valuable resources, knowledge and networking opportunities for professionals in cybersecurity field.

To further develop my skills and knowledge in network security, ethical hacking, and penetration testing, I actively engage with online platforms such as TCM Security, EC-Council, and Offensive Security. These platforms offer comprehensive courses and training programs that allow me to stay updated with the latest industry practices and methodologies. By leveraging these resources, I gain in-depth knowledge of advanced hacking techniques, network defense strategies, and the latest tools and technologies used in the field.

To enhance my practical skills, I participate in Capture the Flag (CTF) challenges on platforms like TryHackMe, HackTheBox, Hacker101, and the Web Security Academy. These challenges provide real-world scenarios where I can apply my knowledge in a hands-on environment, solving complex problems and exploiting vulnerabilities. Engaging in CTF challenges not only sharpens my technical skills but also fosters critical thinking, problem-solving, and teamwork abilities, which are essential in the field of cybersecurity.

Additionally, I actively participate in cybersecurity competitions to gain further hands-on experience and enhance my skills. These competitions often simulate real-world scenarios, allowing me to test my abilities in a competitive setting. By actively participating, I can further develop my proficiency in areas such as penetration testing, incident response, and secure coding.

Moreover, within my degree program, I pursue relevant units that complement my cybersecurity knowledge. These include subjects like network security, database management systems (DBMS), cryptography, and cybersecurity management. These units provide a solid theoretical foundation, enabling me to understand the underlying principles and concepts that drive effective cybersecurity practices.

By combining online courses, CTF challenges, cybersecurity competitions, and relevant units in my degree program, I am continuously expanding my skills and expertise in network security, ethical hacking, and penetration testing. This multifaceted approach ensures that I am well-prepared to tackle real-world cybersecurity challenges and contribute effectively to organizations in need of robust security measures.