Malayan Colleges Laguna
A MAPÚA SCHOOL

REVISION NO.:	00
REVISION DATE:	May 10, 2016

DAILY JOURNAL

IMPORTANT INFORMATION

- INCLUDE TASK ASSIGNMENTS OR MOVEMENTS, REFLECTION ON THE DAY'S NEW LEARNING, ACCOMPLISHMENT, CHALLENGES FACED AND HOW YOU RESPONDED, OBSERVATIONS AND RECOMMENDATIONS ON THE IMPROVEMENT OF SYSTEMS / OPERATION / MANAGEMENT, ETC.
- SCANNED COPIES OF THIS FORM SHALL BE SUBMITTED ON A WEEKLY BASIS THROUGH APPROVED LMS.
- HARD COPIES OF THIS FORM SHOULD BE COMPILED AS PART OF THE STUDENT'S PORTFOLIO.

DATE	May 23 - May 27 2022	AREA ASSIGNMENT	ATA
TASK	Becoming an Ethical Hacker module	SHIFT/TIME	8:00 AM - 5:00 PM

In the first few part of this module, I learned about structured ethical hacking which starts in reconnaissance and foot printing where we gather information about our target like remote access capabilities, determining network range and what security mechanism are in place. This is followed by scanning where I learned how to do ping sweep to identify live hosts on the network and once a live host is identified we can now use NetScan to send TCP or UDP packets to determine the firewall rules on the target system and use shell to redirect output and input for remote access. I also learned about different techniques and tools that we can use to obtain access to restricted access to a system or user information such website mirroring using HTTrack to create a copy of the entire website so that we can analyze and look for clues, directories and exposed user credentials by inspecting html and javscript codes. Additionally, I also learned how to hijack a web sessions by capturing user cookies using WireShark on public networks and then we can now use TamperMonkey and inject this cookie to our own browser to gain access to user account without their user credentials. I also learned about URL parameter manipulation, cross-site scripting wherein we inject our own javascript to HTML elements to perform harmful actions like redirection to a harmful website, automatically downloading of malware, accessing or cookies from our web browser and sending it to a repository. SQL injection was also discussed though this can be a powerful attacks that may show us information from the database that might not be accessible through normal means, many developers are now aware of this and they are utilizing the use of parameterized query to prevent such attacks. I also learned how to perform a denial of service attack by putting heavy load on HTTP serves to exhaust their resource pool and limit access to the website using GoldenEye. I also learned to how crack wi-fi passwords using a combination of Wireshark and FernWi-Fi Cracker. I also learned how to perform steganography and NTFS Alernate Data Streaming to hide malwares in plain files like picture and text file to avoid detection. Overall, this module was the best for me so far because by learning how to these attacks work and how to perform them, I now have an idea on how to protect the software or system that I will be creating in the future

TRAINEE'S SIGNATURE