Kais Rafie, journal#1, ASPS

8th November:

- Made the proposal with Ibrahim in the afternoon
- At night, I went on https://www.kali.org/get-kali/#kali-installer-images
  to install a kali iso file for a virtual machine. I made sure to not experience the same mistake as before, having viruses from the machine by accident. So I searched for a clean machine and could not. I asked Ibrahim to send me his file and he sent it using mega.nz
- Later that day we decided to set up OpenVAS, and were not able to.

  We watched a video, https://youtu.be/0CZBN9DnDCg?si=1oD0kGYYnl2IYLz9 , but were not able to follow their steps. Then tried to watch another video, https://youtu.be/OUiRTv4Q80c?si=3coKPXZmtQfXB9gw , and could not either. We got tired and decided to leave it to the next day.

9th November:

- In the morning at 9am and until 2pm, I tried to solve our problem with OpenVAS, which was that we were unable to find the required dependencies nor the installation files were able to locate it automatically.
- We gave up on OpenVAS and decided to find an alternative. Our choices were OpenSCAP, Wazuh, and Nessus.
- We decided to use Nessus at the end because it had what we needed and easy to set up.
  - To install Nessus, I watched a video, https://youtu.be/TbpfX07NoV4?si=Wfpp5r-l05sKO4sJ , but I had some issues setting up my email with them. So I asked ChatGPT to help.
  - It gave me some commands to work with instead of following the video.
    - sudo /opt/nessus/sbin/nessuscli adduser
    - sudo /opt/nessus/sbin/nessuscli fetch --register <activation_code>
    - sudo systemctl start nessusd
    - sudo systemctl status nessusd
    - Open a web browser and go to https://localhost:8834/
    - **Enter your Admin Username and Password**:

13th November:

- We received the teacher's feedback on the proposal and decided to modify it accordingly.
  - We added a MIT license because it is a research project

- We decided to post bone the creation of the automatic scripts until we understand what we need to do

15th November:

- I wanted to create my virtual machine victim after a long week. And asked Ibrahim for his version, we previously decided on using Windows XP, one of the most vulnerable machines that exists now, and like before I asked him to send me his iso file on mega.nz
- I went on https://web.archive.org/web/20240000000000*/windows%20xp%20product%20key , but could not find any product key that the windows xp machine accepted and decided to ask Ibrahim how he did it. He gave me a product key that he used and found on internet archive as well.
- I set up my machine and its network to host-only
- I set kali's network to NAT to be able to connect to the internet to update and upgrade
- Then I discovered that I cannot make my two machines communicate because of the internet setup, I tried pinging both their ip addresses on each other but could not. I asked ChatGPT if there is a possibility to make them communicate and it told me to tweak the VMware configuration file
- In the file vmnetnat.config, under [incomingtcp] write "2222 = [other machine's ip address:22]" I changed the numbers later to be able to use other tools that did not work on the port 2222 and 22, instead I changed them both to 4444.
- I delayed my today's work till the next day.

16th November:

- I called Ibrahim to work on the project, and I set up my machine with him to change his machines configurations. And he sent me some videos to watch later to be able to use one for the tools.
- Then, I went on ChatGPT to ask it guiding questions about creating an automatic script. We had previously decided on making a script for kali linux that would open the internet temporarily, update and upgrade, then cease the connection again.
    - ChatGPT told me to use methods like we do in Python. So I went on https://www.shellscript.sh/functions.html , to learn more about the way to write methods. And it was as expected.
    - I asked ChatGPT on how to open the internet and if it was possible to write such a script, but it gave me the whole script on how to achieve my goal
        - Create a .sh file and write the following methods

        - Write a method internetOn, inside write “iptables -F OUTPUT
        - Write another method internetOff, inside write “iptables -A OUTPUT -o th0 -j DROP” and “iptables -A OUTPUT -o wlan0 -j DROP”
        - Call the internetOn method then write “apt update && apt upgrade -y”
        - Finally call the internetOff.
        - I decided to just write
        - “internetOff() {
        - iptables -A INPUT -j DROP
        - iptables -A OUTPUT -j DROP
        - }”
        - Instead of the things after researching about iptables in https://www.geeksforgeeks.org/iptables-command-in-linux-with-examples/ , and asked ChatGPT if my script would work, and it confirmed that it would. Just to isolate the machine better just in case.
    - I close this day by having the script executed on boot by adding it to the ~/.bashrc of my machine.