# Major Project Tasks:

1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and Windows 7 machine and find the open/closed ports and services running on machine

   Hacker Machine : Windows 10
   Victim machine : Kali Linux and Windows 7

2. Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc.,
   Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks

   Hacker Machine : Kali Linux
   Victim machine : Windows XP / Windows 7

3. Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and

   Hacker Machine : Kali Linux
   Victim machine : Windows XP / Windows 7 / Windows 10

4. Perform SQL injection Manually on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections

5. Try to perform Bypass Authentication on https://demo.testfire.net and mention the payload which you used to bypass and mention preventive steps to avoid this attack

6. Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned

7. Perform DOS attack on Windows 7 virtual machine and see the difference in performance of victim machine and mention the preventive measures to avoid DOS attack

**Note:**

1. Write a Document with on each task along with screenshots and after attack mention the solutions to avoid those attacks
2. Use Only Virtual Machines to perform the tasks
3. Don't try these attacks on real-time environment, we won't be responsible for any misuse
4. Create a New lab with all the Operating system and practice on that
5. Refer Internet resources for solutions and complete the project within given date.