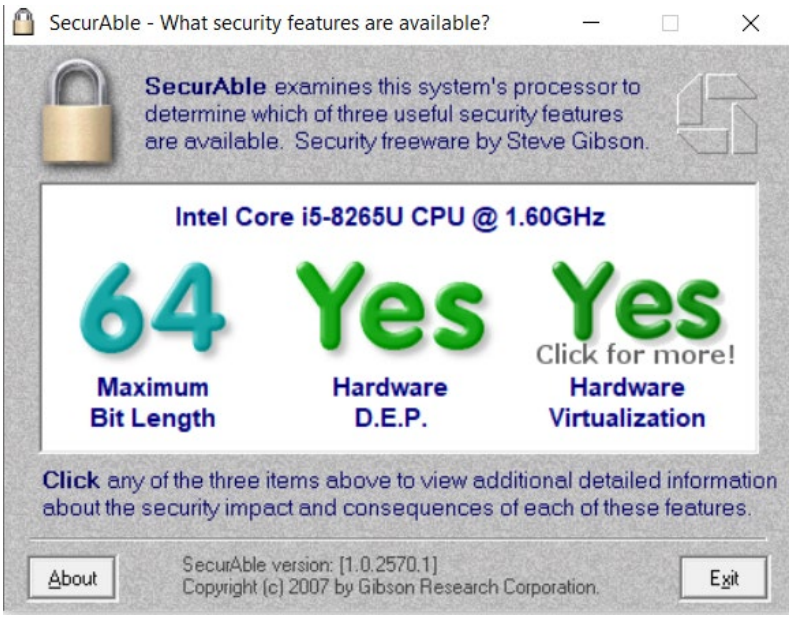
Muhammad Izham Bin Norhamadi
B032020039

Lab 5

1. Data Execution Prevention (DEP) prevent attackers from exploiting buffer overflow to execute malware because DEP prevents execution of code in memory area.



DEP NX supported on the hardware

2. No, Windows has already turned on DEP by default which is sufficient to prevent from virus and other threats, unless it's necessary to change it to troubleshoot problems that may be DEP-related.

3. To keep your computer safe and secure from attacks and malware.

4. An insecure web browser can lead to spyware being installed on your computer without your knowledge and stealing your data.

5.

- If there is a Flash setting in the browser, turning off running Flash is crucial for security as support for Flash was ended and it can be vulnerable to attacks.
- Don't save and autofill password. Autofill increases the chance of unauthorized access when the computer was used by more than one user.