L2: Discussion 2 - Penetration Testing

#### **Purpose**

In this discussion, I would like you to get a better understanding of white box and black box testing.

#### **Tasks**

Please submit an original post focusing on the following questions and guidelines.

* Describe an example where you must use the Black Box approach to complete your penetration testing.
* Discuss why you would like to conduct White Box testing to supplement your penetration testing on your in-house web applications.

**Black Box:**

Black Box testing is essential for penetration testing your application when you want to test “”interactions between [application] components” or “interactions between the entire application or application system with its users, other systems, and the external environment.”[1]. This will supplement any White Box testing. An example of this would be testing user authentication. It is important to be sure that your system **only** allows correctly authenticated users access to the system. Thus, as a penetration tester, you would want to mimic the environment of a bad actor trying to gain access to the system. In order to do this, you would not be able to use information or code that is only accessible behind the scenes. You want to make sure that the application handles user acceptance or rejection end-to-end. This can only be done with Black Box testing.

**White Box:**

I work for a company that operates a federally funded research and development center for the government. We mostly prototype software. One of the most common concepts brought up in our security training (and also plastered on many walls throughout the campus) is to be aware of insider threats. White Box penetration testing can help mitigate or prevent these types of problems. Since White Box testing includes analyzing application source code, it can be used to identify potential compromising code an disgruntled employee can take advantage of. This may include providing direct access from personal accounts or allowing for a back door, unauthorized remote access. Some form of Grey Box testing (the combination of both Black Box and White Box testing) will ensure that your code is as safe as possible and that the system itself is as safe as possible

**References:**

1. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>