Exercise 1

CSCI - C437 | *Brandon Young*

Book Questions

1. A vulnerability is a specific exploit that can be taken advantage of. However, this does not inherently imply that the exploit will be taken advantage of. A risk however is created when a vulnerability exists and something is also ready and willing to exploit that vulnerability. Risk is a much more wholistic representation of the insecurities of a system, whereas vulnerabilities may not provide all the necessary information to make a decision.

2. We know the point at wich we consider our environment secure by evaluating the risks and evaluating the best steps towards mitigating those risks. We will never be completely secure, as new challenges and vulnerabilities will always arise. However if we can mitigate the most prominent attack options, we can consider ourselves reasonably secure.

3. You might use several layers:

    - External layer: Only scheduling necessary appointments, avoiding inviting large groups of individuals onto the premises, pen testing, vulnerability analysis
    - Building perimeter: Badge access, gates, security cameras, guards
    - Internal layer: Employee training, visitor procedures, pen testing, vulnerability analysis
    - Host layer: Authentication, antivirus, firewalls, password hashing, logging, auditing, pen testing, vulnerability analysis
    - Data layer: encryption, access controls, backup, pen testing, vulnerability analysis

4. In this case productivity will be severely inhibited, unless the use of a password manager is allowed, as users will have to remember these long confusing passwords, or, even worse, they will write them down.

Additional Questions

- Does IU Southeast have an Incident Response Plan for Computer Security? What is it? Where is it?
    - The policy can be found here. This policy states that when an incident is reported, a team of individuals will be created to help advise and take action to resolve the issue. They have created a toolkit for mitigating risks. In addition, they have created tools to help resolve the issues and improve security. The department being attacked is fully responsible for allocating the correct resources to the issue.