SECURITY TESTING

Tyler O’Riley

CSD370 Assignment 7.2

09/11/2023

1. SCANNING

Scanning is a method used to assist in identifying various parts of a system. It can cover a plethora of categories including OS ID, System Functionality, and System Vulnerabilities. You can think of scanning as pre planning where you are evaluating how a system even works, how it runs, and areas that may need to be monitored initially.

1. ATTACK SURFACE EVALUATION

The Attack Surface are all points of access within a system. Being a broad idea, you can think of it as identifying all points where information comes in, and where it exists. These points can be both internal and external but are the primary sources where unauthorized users may attempt to enter from.

1. INTEGRATION TESTING

Integration tests are used “wholistically” when verifying a system. Just as each part of a system is separate, they are all moving as a unit as well. This test aims to ensure the overall system is functioning at an optimal level and meeting its basic requirements.

1. CRYPTOGAPHRIC VALIDATION

Cryptography is one the most important assets for a system. It provides encryption, keys, randomly generated access numbers, etc. The importance of this validation comes as two factors. Choosing the right form of cryptography is important as you need to ensure the algorithms it provides are safe and secure. The second is to implement the cryptography to your system correctly and effectively as to not cause errors down the line.

1. SIMULATIONS

Simulating can be thought of as testing similar to how you would test new code before implementing it in a master branch for a system. Simulations assist developers by testing the programs function in a separate production environment so as to not affect the functioning primary program. This helps with costs and to not disrupt customer experience with the working product.

1. PENETRATION TESTING

Unlike passive scan methods or methods that evaluate a software structure, Penetration Testing involves human knowledge to evaluate the strength of a program or update. An example company would have their development group who creates the new program or updates and then a secondary group whose job is to test it. This group of individuals have a task to test the structure of this data and try and penetrate it to the best of the knowledge and skills they have access to.

1. FUZZING

Fuzz testing is a method of trying to brute force access into a system. The verbiage stems from the abundance of inputs attempted to try and find exploits and errors within a program. The goal of this test is to identify where a program might be vulnerable to input errors and data streams attempting to gain access to the system.

1. FAILURE MODES

Fault testing is the primary tool when thinking about Failure Modes in code. The primary use is to attempt specific code that is designed to cause failure within a system. The goal of this testing is to identify lingering “dead” code that is still in the program but no longer actively runs. This is important in the event the dead code affects any future updates.

1. REGRESSION TESTING

Regression testing is the tool utilized to test how new patch updates may impact previous versions of a system. This process can be tedious and time consuming as variance across each old version may react differently to the patch.

1. CONTINUATION TESTING

As the name implies, continuous testing is an imbedded process that is constantly scanning a system to identify business risks, redundancy, and support the development cycle by providing data to help speed up production.