Krutarth Panchal

CIS 450

Week 4 - Fuzzing with Spike (Book)

1. What is the purpose of Spike?

The purpose of spike is to find the potential vulnerabilities of a program (example: Vulnserver) that are acceptable to buffer overflow attack by fuzzing TCP application. The process of throwing packets of data in a system or system component from a purpose of crashing or overflowing is known as fuzzing.

1. How does Spike work?

Spike send data in random and large set of arrays of data to find either the system crashes or overflow and response interaction with a vulnerable program or variable. We can use *gerenic\_send\_tcp* command to pass fuzzing data to the corresponding protocols data on program like Vulnserver to determined either it will be crashed or buffer over.

1. What is the purpose of Vulnserver?

Vulnserver is a windows TCP server that run on port 9999 by default. It is specifically designed to be exploited which can be used to determine the vulnerabilities like buffer overflow in the test environment.

1. What is Fuzzing?

Fuzzing is a powerful testing technique to detect vulnerabilities and bugs in software, networks, and even hardware. It works by throwing a ton of unexpected, random inputs/data at a system to see how it reacts. More like poking and testing the system to see if it breaks in any unexpected ways.

1. Vulnserver can be used to identify unpatched target systems. (T or F)

True