Krutarth Panchal

CIS 450

Week 5 - Simple Buffer Overflow

1. What is Exploit-DB? What OS do the exploits target?

The Exploit Database is an archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

The exploits are target mainly for Windows OS.

1. What is Searchsploit and its purpose?

Searchsploit” is a command-line search tool for Exploit-DB, which also allows us to bring a copy of Exploit-DB. The purpose of the Searchsploit is to perform detailed offline searches ion out local machine for the locally saved repositories.

1. What is a Buffer Overflow?

Buffer overflow is a condition when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer.

1. What tool can be used to generate shell code?

“mfvenom” tool can be used to generate the shell code.

1. The tool in question #4 cannot be used to generate in-memory payloads? (T or F)

False

1. (Industry Research) Navigate to the following link: <https://cve.mitre.org/cve/search_cve_list.html>.

Search for buffer overflow in the list of vulnerabilities. How many Total CVE Records do you see?

There are 15006 CVE Records that matches when searched for Buffer Overflow.

1. What are at least three different stack-based overflow vulnerabilities found?

Classic Buffer Overflow, Format String Vulnerability, Integer Overflow, Stack Smashing.

1. What are at least three different heap-based overflow vulnerabilities found?

Double Free, Use-After-Free, Heap Spraying

1. Network devices like routers are not subject to overflow vulnerabilities. (T or F)

False

1. Buffer overflow vulnerabilities simply cannot lead to remote code execution. (T or F)

False