Binary exploitation

Binary exploitation targets memory-safety bugs in compiled software: cases where a program reads or writes memory it should not, and an attacker uses that to corrupt the program and take control. This section explains the common classes, starting with how a booby-trapped file can overflow a heap buffer, and how each one is found and fixed.

HOW IT WORKS

01 Topics

- How Image-Based Heap Overflows Work: how a malformed image file overflows a heap buffer in an image decoder, and how a bad size calculation becomes an out-of-bounds write and code execution.

Scope a penetration test of your software.

securelayer7.net/learn/binary-exploitation

Open online