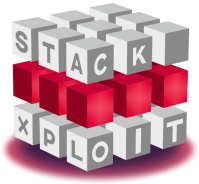
StackXploit
Exploiting Stacks in Linux

Section	Topics To Be Covered
Assembly Language	• Introduction to Assembly Language • Assembly Instruction Format • Basic Assembly Instructions • Addressing Modes
Fundamentals of Program Execution Flow	• Calling Convention • Memory Layout of a C Program • Understanding Call Stack and Stack Frame
Reversing the Code	• Getting Familiar with IDA • Reversing to System Shell with IDA • Analyzing and Exploiting RAND Function • Cracking the seed
Insights into Integer Overflow Vulnerabilities	• Understanding Integer Overflow • Integer Overflow In Action
Arbitrary Memory Exploitation	• Arbitrary Read • Exploiting Arbitrary Write
Buffer Overflow	• Understanding Buffer Overflow • Controlling RIP Register



StackXploit
Exploiting Stacks in Linux

Section	Topics To Be Covered
Bypassing Stack Canary Defenses	• Understanding Stack Canaries • Defeating Stack Canaries
Shellcoding	• Understanding System Calls & Generating a Custom Shell Code • Exploiting Binary Using Shellcode • Seccomp Bypass Tactics for Shellcode Execution • Buffer Size Dynamics in Shellcode Execution
Format Strings	• Introduction to Format Strings • Arbitrary Read Using Format String Vulnerability • Arbitrary Write Using Format String Vulnerability • Overwriting GOT using Format String Vulnerability • Exploiting Format String Vulnerability • Exploiting Format String Vulnerability with FINI_ARRAY
Return Oriented Programming	• Understanding Return-Oriented Programming • Hands-on ROP: From Gadget Hunt to Shell Access • Bypassing PIE using ROP gadgets • Leveraging Ret2libc in ROP Exploits • Understanding Stack Pivoting • Stack Pivoting in Action
RET2CSU	• RET2CSU
SIGRETURN Oriented Programming	• Understanding SROP