BLACK HAT C

LOW-LEVEL EXPLOITATION AND MALWARE ENGINEERING

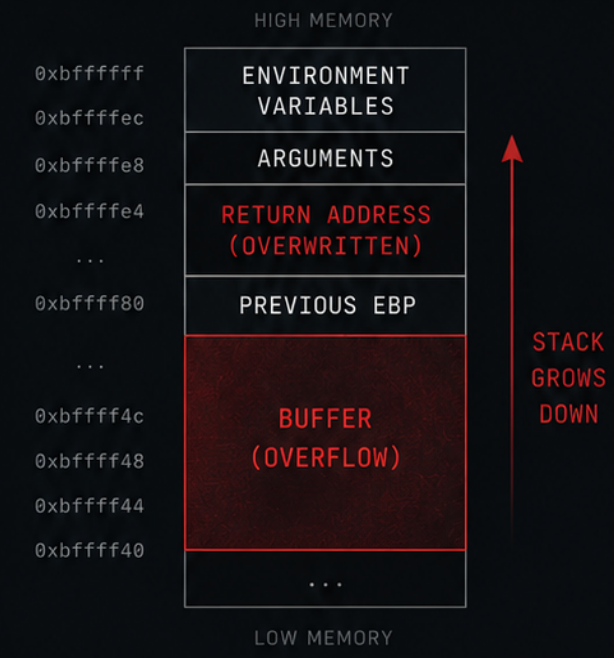
FROM BUFFER OVERFLOWS TO ROOTKITS:
A PRACTITIONER'S GUIDE

```c
#include <stdio.h>
#include <string.h>

void vuln(char *input) {
   char buf[64];
   strcpy(buf, input);
}

int main(int argc, char **argv) {
   vuln(argv[1]);
   return 0;
}
```

```
0x080484b6 <vuln+0>:    push   ebp
0x080484b7 <vuln+1>:    mov    ebp, esp
0x080484b9 <vuln+3>:    sub    esp, 0x50
...
0x080484e9 <vuln+83>:   ret
          // Control Over EIP
```



HANDS-ON CODE EXAMPLES

OFFENSIVE TECHNIQUES AND DEFENSIVE COUNTERMEASURES

EXPLOITATION, MALWARE, AND ROOTKITS

ETHICAL. LEGAL. ISOLATED LAB ENVIRONMENT.

SERGEY SOKOLOV

Black Hat C

Low-Level Exploitation and Malware Engineering

Steve T. Publications

This book is available at https://leanpub.com/blackhatc

This version was published on 2026-07-05

Contents

Low-Level Exploitation and Malware Engineering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

From Buffer Overflows to Rootkits: A Practitioner's Guide

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Introduction

The most useful perspective you can adopt as a security professional is the attacker's view of memory.

Most developers think about their code at the level of functions and data structures. The attacker has to think one layer lower: bytes on the stack, return addresses, process mappings, system call tables. If you want to understand modern exploits, rootkits, and malware patterns, you must be fluent in that lower-level view.

This book is an end-to-end treatment of how attacks are implemented in C and assembly on real systems. The through-line is simple:

- Start with a vulnerable program.
- Understand the underlying OS and hardware mechanics.
- Show exactly how control flow is hijacked.
- Add evasion, persistence, and stealth.
- For each technique, state the corresponding defenses clearly.

You will encounter concrete C code examples, annotated assembly snippets, and step-by-step walkthroughs that show how vulnerabilities are triggered and exploited in a controlled environment. The goal is not to impress with clever tricks; the goal is to make sure you can look at unfamiliar binary behavior and explain what it is doing and why.

How to use this book

- Prerequisites:
  - Working knowledge of C, including pointers, structs, and memory layout.
  - Comfort with a Linux command line and basic tools (gcc, gdb, objdump).
  - Familiarity with x86/x86_64 assembly is helpful but not required; key concepts are explained.

- Environment:
  - Use an isolated lab: a VM or container running a deliberately vulnerable target.
  - Do not run these examples on production systems.
  - Ensure your use is legal and authorized.
- Reading strategy:
  - Read Chapters 1–3 straight through to establish fundamentals.
  - Use later chapters as reference when encountering specific vulnerability classes, evasion techniques, or malware patterns in real work.

Ethical note

Several examples in this book demonstrate potentially risky behavior: shellcode execution, privilege escalation, kernel hooking, process injection, and stealth techniques. All are provided for educational and defensive engineering purposes. Every chapter that contains such material includes an explicit reminder to use it only in isolated, legal, ethical environments. If you are unsure whether your use is appropriate, assume it is not.

The rest of the book now moves from fundamentals to advanced topics: memory layout and calling conventions, stack overflows, format string bugs, heap exploitation and use-after-free, shellcoding, bypassing ASLR/DEP/canaries, position-independent code, anti-analysis tricks, kernel rootkits, and modern malware development patterns. Each chapter closes with a defensive summary so you can translate what the attacker can do into what your systems should enforce.

Chapter 1: The Attacker's View of Memory and Execution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

A Minimal Vulnerable Program

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Process Layout: Text, Data, Heap, Stack

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

ELF Format and Why It Matters

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

x86/x64 Registers and the Call Stack

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

How a Function Call Really Works (Calling Conventions)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

From Source to Assembly: Tracing One Example

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Segmentation, Paging, and Virtual Memory

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: Why You Must Know This

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chapter 2: Buffer Overflows–The Classic Weapon

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Anatomy of a Stack Buffer Overflow

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Controlling the Return Address

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Finding the Offset: Fuzzing with Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

NOP Sleds and Shellcode Placement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

A Complete Exploit Walkthrough (Linux, x86)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Return-to-libc: Exploitation Without Shellcode

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: Stack Canaries, ASLR, and Hardening Trade-offs

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chapter 3: Format String Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

How printf Parses Its Arguments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Leaking the Stack with %x and %p

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Overwriting Arbitrary Memory with %n

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

A Realistic Exploit Example

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chained Format String Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Real-World Example: CVE-2024-29510 in Ghostscript

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: Safe Formatting and Static Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chapter 4: Heap Exploitation and Use-After-Free

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

How the Heap Is Managed (ptmalloc / glibc Basics)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Off-by-One and Heap Overflows

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Use-After-Free: The Concept

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Exploiting UAF via Struct Overwrite

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Fastbin Attacks: A Concrete Walkthrough

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: Hardened Allocators and Sanitizers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chapter 5: Shellcoding–Code That Runs Anywhere

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Constraints of Shellcode (No Null Bytes, No Fixed Addresses)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Writing a Simple execve("/bin/sh") on Linux (x86)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Writing a Simple execve("/bin/sh") on Linux (x86_64)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Reverse TCP Shellcode: Connecting Back

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Position-Independent Tricks (Self-Referencing RIP, Syscall Stubs)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Encoding and Decoding Payloads

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Embedding Shellcode in C Exploits

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: DEP/NX, CFG, and Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chapter 6: Bypassing Protections–ASLR, DEP, Canaries

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

ASLR: How It Works and Where It Leaks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Information Leaks via Pointers and CRT

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

ROP Chaining (Return-Oriented Programming)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Bypassing DEP with ROP

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defeating Stack Canaries (Leak + Reuse)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: Full Mitigation Stacks and SECCOMP

Chapter 7: Position-Independent Code and Exploit Engineering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Static vs Dynamic Linking

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Position-Independent Executables (PIE)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

GOT/PLT Overwrites as an Attack Vector

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Leveraging libc Offsets in Exploits

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Combining Leaks, ROP, and GOT Hijacking

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: RELRO, BindsNow, and Full Hardening

Chapter 8: Anti-Analysis Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Detecting Sandboxes and VMs (CPUID, Timing, Artifacts)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

String Obfuscation and Encrypted Payloads

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Packed Binaries and Custom Unpackers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Anti-Debugging Tricks (PTRACE, Timing, sysenter tricks)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Flow Obfuscation and Control Integrity

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: Dynamic Analysis Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chapter 9: Rootkits–Hiding in the Kernel

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Userland vs Kernel Rootkits

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Inline Hooking System Calls (Linux Example)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Modifying the System Call Table (Conceptual)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Hiding Processes, Files, and Network Sockets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Driver-Based Persistence on Windows (Conceptual)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: Integrity Checking, eBPF, and PatchGuard

Chapter 10: Malware Development Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Process Injection Techniques (CreateRemoteThread, APC Injection)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Reflective DLL Loading

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Living Off the Land (LOLBins and Scripts)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Command and Control (C2) Channel Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Fileless Persistence and Memory-Only Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: EDR, Telemetry, and Behavioral Detection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Chapter 11: Putting It All Together–A Controlled Case Study

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

The Lab: Dockerized, Isolated Test Environment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Target Service with Multiple Flaws

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Step-by-Step Exploit Development

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Adding Evasion and Persistence Layers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Post-Exploitation View

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: How a Hardened System Would Resist This

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Defensive Note: How a Hardened System Would Resist This

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/blackhatc.