```
; EIP CONTROL
80  EC  24          sub     esp, 24h
8B  45  04          mov     eax, [ebp+4]
83  EC  08          sub     esp, 8
C7 45 FC 41 41 41 41  mov   dword ptr [ebp-4], 41414141h
...
C3                  ret
```

BUFFER OVERFLOW EXPLOITATION AND DEFENSE EVASION


```
BOOL IsBadReadPtr(VOID* p, UINT_PTR u)
{
  __try {
    volatile BYTE b = *(BYTE*)p;
    return FALSE;
  }
  __except(EXCEPTION_EXECUTE_HANDLER) {
    return TRUE;
  }
}
```

STEVE T.'

Buffer Overflow Exploitation and Defense Evasion

Steve T.

This book is available at
https://leanpub.com/buffer-overflow-exploit-defense

This version was published on 2026-06-19

Contents

Table of Contents

- Classic Techniques: Metadata Corruption, `unlink()`, Coalescing, UAF
- Advanced ptmalloc: House of Force/Spirit/Lore/Einherjar, Fastbin Dup, Tcache Poisoning
- Heap Spraying
- Windows Heap Internals (NT vs Segment Heap, LFH, Randomization)
- Recent Heap CVEs (CVE-2024-49138, CVE-2024-2961, CVE-2024-45492)

7. Format String Vulnerabilities: Exploiting Output Functions

   - Variadic Functions and the `printf` Family
   - Format Specifiers (`%x`, `%s`, `%n`, `%p`, `$`)
   - Information Leakage: Reading Stack, Heap, Arbitrary Memory
   - Arbitrary Memory Write (`%n`, `%hn`, `%hhn`)
   - Overwriting GOT/PLT, Return Addresses, Function Pointers
   - Direct Parameter Access for Precision Writes

8. Integer Overflows: The Silent Precursor

   - Integer Representation (Signed vs. Unsigned, Width)
   - Overflow, Underflow, Wraparound
   - Truncation and Sign Extension Errors
   - Exploiting Size Calculations (`malloc`, `memcpy`, loops)
   - Real-World Case Studies

9. Platform Defenses: Raising the Bar

   - Stack Canaries / StackGuard / SSP
   - Non-Executable Memory (NX / DEP / W^X)
   - Address Space Layout Randomization (ASLR)
   - Position Independent Executables (PIE)
   - Relocation Read-Only (RELRO: Partial vs. Full)
   - Control Flow Guard (CFG - Windows)
   - Control-Flow Integrity (CFI - Clang/LLVM)
   - Pointer Authentication (PAC) & Memory Tagging (MTE) - ARM
   - Intel Control-Flow Enforcement Technology (CET)
   - Source Code Hardening & Secure Libraries

10. Bypassing Stack Canaries

    - Information Leak Techniques

- Brute-Forcing Canaries (Forking Servers, Threaded Models, Low Entropy)
- Overwriting Saved Pointers Before the Canary
- Attacking Canary Generation/Checking Logic
- Partial Overwrites

11. Bypassing NX/DEP: Return-Oriented Programming (ROP)

- Reusing Existing Code Gadgets
- Finding Gadgets (ROPgadget, Ropper)
- Gadget Types and ROP Chain Construction
- `ret2libc` and Syscall Gadgets
- Stack Pivoting
- Sigreturn-Oriented Programming (SROP)
- Blind ROP (BROP)

12. Bypassing ASLR

- The Need for an Information Leak
- Calculating Base Addresses from Leaked Pointers
- Partial Overwrites
- Brute-Forcing (32-bit, specific server models)
- Exploiting Non-Randomized Components
- JIT Spraying / Scripting Engine Exploitation
- Side Channels (Cache Timing)

13. Bypassing CFI, CFG, and Advanced Mitigations

- Attacking CFG and CFI
- Counterfeit Object-Oriented Programming (COOP)
- PACMAN Attack (ARM PAC, Apple M1)
- TikTag Attack (Breaking ARM MTE)
- Attacking PAC/MTE (Tag Guessing, Data-Only Attacks)
- Jump-Oriented Programming (JOP) / Call-Oriented Programming (COP)
- Data-Only Attacks
- Return-to-CSU

14. The Holistic View: Combining Bypasses and Tooling

- Typical Exploit Chains (Info Leak □ ROP □ Shell)
- Exploit Development Workflow
- Debuggers (GDB+PEDA/GEF/Pwndbg, WinDbg)

Preface

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

How to Use This Book

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 1: Memory, Processes, and the Von Neumann Bottleneck

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

1.1 Revisiting Process Memory Layout

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

1.2 Virtual Memory, Paging, and Permissions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 1: Memory, Processes, and the Von Neumann Bottleneck (Continued)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

1.3 CPU Architecture Basics: The Registers Guiding Execution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

1.4 The C Language Memory Model: Power and Peril

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

1.5 Why Buffer Overflows Happen: The Missing Check

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

1.6 The Code/Data Equivalence: Enabling Execution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

1.7 Quantitative Analysis: The Scale of Memory Corruption Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Prevalence of Memory Safety Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Industry-Specific Data

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Historical Trend

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 2: Stack-Based Buffer Overflows: The Canonical Exploit

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.1 Detailed Stack Frame Anatomy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

x86 (32-bit) Calling Conventions (cdecl, stdcall):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

x64 (64-bit) Calling Conventions (System V AMD64 ABI - Linux/macOS, Microsoft x64 - Windows):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.2 Function Prologues and Epilogues

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Typical x86 Prologue (with Frame Pointer):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Typical x86 Epilogue (with Frame Pointer):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Typical x64 Prologue (System V, with Frame Pointer):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Typical x64 Epilogue (System V, with Frame Pointer):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.3 Overwriting the Return Address: Seizing Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Example Payload Structure (Conceptual):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.4 Vulnerable Functions Revisited

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.5 Crafting the First Payload: NOP Sleds and Shellcode Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Payload Structure:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Example (Conceptual x86):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.5.1 Real-World Stack Overflow Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

The Morris Worm (1988) — fingerd Buffer Overflow

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

SQL Slammer (2003) — UDP Buffer Overflow

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Code Red Worm (2001) — IIS ISAPI Overflow

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.6 Finding Buffer Addresses: The Elusive Target

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.7 Variations: Beyond the Simple Overwrite

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.8 Quantitative Analysis: Stack Overflow Prevalence and Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Prevalence Statistics (2010–2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Industry Breakdown

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Historical Trend

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Mitigation Effectiveness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.8 Quantitative Analysis: Stack Overflow Prevalence and Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Prevalence Statistics (2010–2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Industry Breakdown

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Historical Trend

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Mitigation Effectiveness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

2.8 Quantitative Analysis: Stack Overflow Prevalence and Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Prevalence Statistics (2010–2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Industry Breakdown

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Historical Trend

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Mitigation Effectiveness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 3: Shellcoding Craftsmanship

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.1 Principles of Position-Independent Code (PIC)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.2 Common Shellcode Goals

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.3 Writing Basic Shellcode: Linux (x86/x64 Syscalls)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Key Concepts:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Example: x64 Linux `execve("/bin/sh", ["/bin/sh", NULL], NULL)`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.4 Writing Basic Shellcode: Windows (API Resolving)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Key Concepts:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Example Snippet (Conceptual x86 - Finding Kernel32 Base):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.5 Dealing with Bad Characters

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Identifying Bad Characters:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Avoiding Bad Characters:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.6 Encoders, Decoders, and Simple Polymorphism

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Common Encoder Example (XOR):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.7 Staged Shellcode

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

3.8 Quantitative Analysis: Shellcode Metrics and Real-World Measurements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Shellcode Size Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Bad Character Prevalence

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Encoder Effectiveness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Staged Shellcode Communication Metrics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 4: Heap-Based Buffer Overflows: The Unstructured Frontier

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

4.1 Heap vs. Stack Dynamics: A Tale of Two Memories

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

4.2 Heap Allocator Internals: Focus on dlmalloc/ptmalloc

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Core Components:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

4.3 Classic Heap Exploitation Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

4.4 Advanced Heap Exploitation (`ptmalloc` specific)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

4.5 Heap Spraying Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

4.6 Windows Heap Internals: NT Heap, Segment Heap, and LFH

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Windows Heap Architecture Evolution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

The Low Fragmentation Heap (LFH)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Randomization (Windows 8+)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Practical Heap Exploitation on Windows

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

4.7 Recent Heap-Related CVEs: Real-World Impact

CVE-2024-2961: glibc iconv() Buffer Overflow (Tcache Poisoning)

CVE-2024-45492: libexpat Integer Overflow (Heap Buffer Overflow)

CVE-2026-25897: ImageMagick Sun Decoder Integer Overflow

4.8 Quantitative Analysis: Heap Exploitation Complexity and Success Rates

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Exploitation Success Rate by Technique (2015–2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Allocation Size Distribution (Linux, glibc 2.31+)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Fragmentation Metrics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Vulnerability Prevalence

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Exploitation by Platform

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 5: Format String Vulnerabilities: Exploiting Output Functions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.1 Variadic Functions and the `printf` Family

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.2 Format Specifiers: The Language of `printf`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.3 The Vulnerability: Broken Trust

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Incorrect Code:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Correct Code:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Exploitation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.4 Information Leakage: Reading Process Memory

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.5 Arbitrary Memory Write: The Power of `%n`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Example (Conceptual): Write `0xdeadbeef` to address `0x12345678`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Using `%hn` and `%hhn` for Precise Writes:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Example: Write `0x1234` to address `TargetAddr` (using `%hn`)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Direct Parameter Access (`%N$n`)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.6 Exploitation Targets for Arbitrary Write

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.7 Mitigations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.8 Real-world Context

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

5.9 Quantitative Analysis: Format String Vulnerability Impact and Detection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Prevalence Statistics (2010–2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Format String Exploitability by Platform

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Detection Effectiveness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Format String Payload Size Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Format String Mitigation Adoption

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 6: Integer Overflows: The Silent Precursor

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.1 Integer Representation Fundamentals

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.2 Overflow, Underflow, and Wraparound: Crossing the Limits

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.3 Truncation: Losing Precision

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.4 Sign Extension Errors: Misinterpreting Signs

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.5 Exploitation Scenarios: From Bad Math to Memory Corruption

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.6 Real-world Case Studies (Brief Mentions)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.7 Detection and Prevention

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.8 Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

6.9 Quantitative Analysis: Integer Overflow Prevalence and Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Prevalence Statistics (2010–2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Industry Breakdown

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Historical Trend

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Detection Effectiveness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Integer Overflow → Buffer Overflow Correlation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Part 2: Modern Defenses and Bypasses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 7: Platform Defenses: Raising the Bar

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.1 Stack Canaries / StackGuard / Stack Smashing Protector (SSP)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.2 Non-Executable Memory (NX / DEP / W^X)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.3 Address Space Layout Randomization (ASLR)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.4 Position Independent Executables (PIE)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.5 Relocation Read-Only (RELRO)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.6 Control Flow Guard (CFG - Windows)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.7 Control-Flow Integrity (CFI - Generic/Clang)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.8 Pointer Authentication Codes (PAC - ARM)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.9 Memory Tagging Extension (MTE - ARM)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.10 Source Code Hardening & Secure Libraries

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.10 Intel Control-Flow Enforcement Technology (CET)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Shadow Stack (SHSTK)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Indirect Branch Tracking (IBT)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

CET Effectiveness Against ROP/COP/JOP

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.11 Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

7.12 Quantitative Analysis: Mitigation Effectiveness and Adoption Rates

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Global Mitigation Adoption Rates (2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Mitigation Effectiveness in Practice

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Exploit Chain Complexity by Mitigation Profile

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Historical Evolution of Mitigation Deployment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Cost-Benefit Analysis of Mitigations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 8: Bypassing Stack Canaries

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

8.1 Leaking the Canary Value

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Methods for Leaking:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Payload Construction after Leak:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

8.2 Brute-Forcing the Canary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Factors Affecting Feasibility:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Brute-Force Payload Structure (Byte-by-Byte):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

8.3 Overwriting Targets Below the Canary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Potential Targets:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

8.4 Attacking Canary Generation or Checking Logic

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

8.5 Partial Overwrites and Data-Only Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

8.6 Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 9: Bypassing NX/DEP: Return-Oriented Programming (ROP)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.1 The Principle: Reusing Existing Code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.2 What is a Gadget?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.3 Finding Gadgets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.4 Gadget Types and Their Roles

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.5 ROP Chain Construction: Orchestrating Gadgets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Stack Layout Example (Conceptual x64 - Call `func(arg1, arg2)`):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.6 Controlling Function Arguments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.7 `ret2libc`: Calling Library Functions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.8 Syscall Gadgets: Direct OS Interaction

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.9 Stack Pivoting: Changing the Stage

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.10 Advanced ROP: Sigreturn-Oriented Programming (SROP)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.11 Blind ROP (BROP)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.12 Conclusion: The Ubiquity of ROP

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

9.13 Quantitative Analysis: ROP Chain Metrics and Real-World Performance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ROP Chain Length Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ROP Gadget Availability by Module

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ROP Chain Reliability Factors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ROP vs. Direct Syscall Comparison

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ROP Chain Construction Time by Experience Level

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 10: Bypassing Address Space Layout Randomization (ASLR)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.1 The Crucial Role of Information Leaks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.2 Common Sources of Information Leaks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.3 Leveraging Leaked Pointers: Calculating Base Addresses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.4 Partial Overwrites: Exploiting Low Entropy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.5 Brute-Forcing ASLR: A High-Cost Gamble

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.6 Exploiting Non-Randomized Components

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.7 Chaining Leaks: Multi-Stage Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.8 Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

10.9 Quantitative Analysis: ASLR Entropy and Bypass Feasibility

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ASLR Entropy by Platform and Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ASLR Bypass Feasibility by Entropy Level

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Information Leak Effectiveness by Vulnerability Type

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ASLR Bypass Success Rate by Method (Real-World Data)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact of ASLR on Exploit Development Time

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 11: Bypassing CFI, CFG, and Advanced Hardware Mitigations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.1 Bypassing Control Flow Guard (CFG - Windows)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.2 Bypassing Control-Flow Integrity (CFI)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.3 Bypassing Pointer Authentication Codes (PAC - ARM)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.4 Bypassing Memory Tagging Extension (MTE - ARM)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.5 JOP/COP: Alternative Code Reuse

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.6 Return-to-CSU (`__libc_csu_init`)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.5 Counterfeit Object-Oriented Programming (COOP)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Core Concept

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

COOP Payload Structure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Practical Bypass of CET Shadow Stack

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.6 PACMAN: Speculative Execution Oracle for ARM Pointer Authentication

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

The Core Insight

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

PACMAN Gadget Structure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Attack Mechanics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.7 TikTag: Breaking ARM Memory Tagging Extension with Speculative Execution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Background: MTE

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

TikTag Gadgets: TIKTAG-v1 and TIKTAG-v2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Attack Results

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Response from Arm and Google

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Implications for MTE

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

11.8 Conclusion: The Ever-Shifting Battlefield

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 12: The Holistic View: Combining Bypasses and Tooling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.1 Typical Exploit Chains: The Sum of Parts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.2 Exploit Development Workflow: A Systematic Approach

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.3 Using Debuggers Effectively

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Debugger Usage Strategy:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.4 Leveraging Disassemblers/Decompilers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Usage Strategy:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.5 Exploit Frameworks (pwntools)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.6 Fuzzing for Bug Discovery

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.7 Automated Exploit Generation (AEG) Concepts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

12.8 Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Part 3: Beyond the Basics and Future Trends

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 13: Architecture Specifics and Kernel Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

13.1 Architecture Specifics: ARM/AArch64 Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Key Architectural Differences:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact on Exploitation Techniques:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

13.2 Introduction to Kernel Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

User Space vs. Kernel Space:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Kernel Memory Layout:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Kernel Attack Surface:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Common Kernel Bug Classes:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Kernel Mitigations:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

13.3 Basic Kernel Exploit Concepts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Payload Example: Privilege Escalation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

13.4 Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Chapter 14: The Shifting Landscape and Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

14.1 The Rise of Memory-Safe Languages

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Rust: The Leading Memory-Safe Systems Language

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Other Memory-Safe Languages

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Limitations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

14.1.5 Recent CVE Trends: Active Exploitation in 2024–2025

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

14.2 Managed Runtimes (JVM, .NET, Python, Ruby, etc.)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

14.3 WebAssembly (Wasm) Security Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

14.4 Hardware-Level Security Evolution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

14.5 The Continuous Arms Race: What's Next?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

14.6 Final Thoughts: The Primacy of Secure Development

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Appendix A: Glossary of Terms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Appendix B: Common Syscall Tables (x86, x64, ARM32, ARM64)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

B.1 x86 (32-bit) Syscall Convention

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Common x86 Syscalls:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

B.2 x64 (64-bit) Syscall Convention

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Common x64 Syscalls:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Important Considerations:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

B.3 ARM64 (AArch64) Syscall Convention

Common ARM64 Syscalls:

ARM64 Shellcode Example: `execve("/bin/sh", NULL, NULL)`

Appendix C: Useful Debugger Commands for Exploit Development

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

C.1 GDB + Extensions (PEDA/GEF/Pwndbg)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Process Control & Execution:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Breakpoints:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Memory Examination:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Register Manipulation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Stack Analysis:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Disassembly:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Analysis (Extensions - Commands may differ slightly):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

ASLR/PIE/Mitigation Info (Extensions):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Searching Memory:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Scripting & Automation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

C.2 WinDbg (Windows)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Process Control & Execution:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Breakpoints:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Memory Examination:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Register Manipulation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Stack Analysis:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Disassembly:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Heap Analysis:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Module/Memory Info:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Searching Memory:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Symbols:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

C.3 Final Note

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

Appendix D: Further Reading and Resources

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

D.1 Foundational Books

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

D.2 Advanced Exploitation & Reverse Engineering Books

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

D.3 Online Resources & Communities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

D.4 Essential Tools (Recap & Beyond)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

D.5 Practice Platforms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.

D.6 Final Advice

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/buffer-overflow-exploit-defense.