

目录

第 1 章 CTF 简介	1
1.1 赛事介绍	1
1.1.1 赛事起源	1
1.1.2 竞赛模式	1
1.1.3 竞赛内容	2
1.2 知名赛事及会议	3
1.2.1 网络安全竞赛	3
1.2.2 网络安全会议	5
1.2.3 网络安全学术会议	6
1.3 学习经验	6
1.3.1 二进制安全入门	6
1.3.2 CTF 经验	8
1.3.3 对安全从业者的建议	8
参考文献	10
第 2 章 二进制文件	11
2.1 从源代码到可执行文件	11
2.1.1 编译原理	11
2.1.2 GCC 编译过程	12
2.1.3 预处理阶段	13
2.1.4 编译阶段	14
2.1.5 汇编阶段	15
2.1.6 链接阶段	15
2.2 ELF 文件格式	16
2.2.1 ELF 文件的类型	16
2.2.2 ELF 文件的结构	18

2.2.3 可执行文件的装载.....	24
2.3 静态链接.....	26
2.3.1 地址空间分配.....	26
2.3.2 静态链接的详细过程.....	27
2.3.3 静态链接库.....	29
2.4 动态链接.....	30
2.4.1 什么是动态链接.....	30
2.4.2 位置无关代码.....	31
2.4.3 延迟绑定.....	32
参考文献.....	33
第 3 章 汇编基础.....	34
3.1 CPU 架构与指令集.....	34
3.1.1 指令集架构.....	34
3.1.2 CISC 与 RISC 对比.....	35
3.2 x86/x64 汇编基础.....	36
3.2.1 CPU 操作模式.....	36
3.2.2 语法风格.....	36
3.2.3 寄存器与数据类型.....	37
3.2.4 数据传送与访问.....	38
3.2.5 算术运算与逻辑运算.....	39
3.2.6 跳转指令与循环指令.....	40
3.2.7 栈与函数调用.....	41
参考文献.....	44
第 4 章 Linux 安全机制.....	45
4.1 Linux 基础.....	45
4.1.1 常用命令.....	45
4.1.2 流、管道和重定向.....	46
4.1.3 根目录结构.....	47
4.1.4 用户组及文件权限.....	47
4.1.5 环境变量.....	49
4.1.6 procfs 文件系统.....	51
4.1.7 字节序.....	52
4.1.8 调用约定.....	53
4.1.9 核心转储.....	54
4.1.10 系统调用.....	55
4.2 Stack Canaries.....	58
4.2.1 简介.....	58

4.2.2	实现.....	61
4.2.3	NJCTF 2017: messenger	63
4.2.4	sixstars CTF 2018: babystack.....	65
4.3	No-eXecute.....	69
4.3.1	简介.....	69
4.3.2	实现.....	70
4.3.3	示例.....	73
4.4	ASLR 和 PIE.....	75
4.4.1	ASLR	75
4.4.2	PIE.....	76
4.4.3	实现.....	77
4.4.4	示例.....	79
4.5	FORTIFY_SOURCE.....	83
4.5.1	简介.....	83
4.5.2	实现.....	84
4.5.3	示例.....	86
4.5.4	安全性.....	89
4.6	RELRO.....	90
4.6.1	简介.....	90
4.6.2	示例.....	90
4.6.3	实现.....	93
	参考文献.....	94
第 5 章	分析环境搭建	96
5.1	虚拟机环境.....	96
5.1.1	虚拟化与虚拟机管理程序.....	96
5.1.2	安装虚拟机.....	97
5.1.3	编译 debug 版本的 glibc	98
5.2	Docker 环境.....	100
5.2.1	容器与 Docker.....	100
5.2.2	Docker 安装及使用	101
5.2.3	Pwn 题目部署.....	102
	参考文献.....	103
第 6 章	分析工具.....	104
6.1	IDA Pro	104
6.1.1	简介.....	104
6.1.2	基本操作.....	105
6.1.3	远程调试.....	108

6.1.4	IDAPython	110
6.1.5	常用插件.....	114
6.2	Radare2	115
6.2.1	简介及安装.....	115
6.2.2	框架组成及交互方式.....	115
6.2.3	命令行工具.....	118
6.2.4	r2 命令	122
6.3	GDB	125
6.3.1	组成架构.....	125
6.3.2	工作原理.....	125
6.3.3	基本操作.....	127
6.3.4	增强工具.....	130
6.4	其他常用工具.....	132
6.4.1	dd.....	133
6.4.2	file	133
6.4.3	ldd.....	134
6.4.4	objdump	134
6.4.5	readelf.....	135
6.4.6	socat	136
6.4.7	strace<race	136
6.4.8	strip.....	137
6.4.9	strings.....	138
6.4.10	xxd.....	138
	参考文献.....	139
第 7 章	漏洞利用开发	141
7.1	shellcode 开发.....	141
7.1.1	shellcode 的基本原理.....	141
7.1.2	编写简单的 shellcode.....	141
7.1.3	shellcode 变形.....	143
7.2	Pwntools.....	145
7.2.1	简介及安装.....	145
7.2.2	常用模块和函数	145
7.3	zio.....	152
7.3.1	简介及安装.....	152
7.3.2	使用方法.....	153
	参考文献.....	155

第 8 章 整数安全.....	156
8.1 计算机中的整数.....	156
8.2 整数安全.....	157
8.2.1 整数溢出.....	157
8.2.2 漏洞多发函数.....	158
8.2.3 整数溢出示例.....	159
参考文献.....	161
第 9 章 格式化字符串.....	162
9.1 格式化输出函数.....	162
9.1.1 变参函数.....	162
9.1.2 格式化字符串.....	162
9.2 格式化字符串漏洞.....	164
9.2.1 基本原理.....	164
9.2.2 漏洞利用.....	166
9.2.3 fmtstr 模块.....	174
9.2.4 HITCON CMT 2017: pwn200.....	176
9.2.5 NJCTF 2017: pingme.....	178
参考文献.....	182
第 10 章 栈溢出与 ROP.....	183
10.1 栈溢出原理.....	183
10.1.1 函数调用栈.....	183
10.1.2 危险函数.....	186
10.1.3 ret2libc.....	186
10.2 返回导向编程.....	187
10.2.1 ROP 简介.....	187
10.2.2 ROP 的变种.....	189
10.2.3 示例.....	191
10.3 Blind ROP.....	192
10.3.1 BROP 原理.....	192
10.3.2 HCTF 2016: brop.....	193
10.4 SROP.....	200
10.4.1 SROP 原理.....	200
10.4.2 pwntools srop 模块.....	204
10.4.3 Backdoor CTF 2017: Fun Signals.....	204
10.5 stack pivoting.....	206
10.5.1 stack pivoting 原理.....	206
10.5.2 GreHack CTF 2017: beerfighter.....	209

10.6	ret2dl-resolve.....	213
10.6.1	ret2dl-resolve 原理.....	213
10.6.2	XDCTF 2015: pwn200.....	217
	参考文献.....	222
第 11 章	堆利用	224
11.1	glibc 堆概述.....	224
11.1.1	内存管理与堆.....	224
11.1.2	重要概念和结构体.....	226
11.1.3	各类 bin 介绍.....	229
11.1.4	chunk 相关源码.....	231
11.1.5	bin 相关源码.....	235
11.1.6	malloc_consolidate()函数.....	237
11.1.7	malloc()相关源码.....	239
11.1.8	free()相关源码.....	248
11.2	TCache 机制.....	251
11.2.1	数据结构.....	251
11.2.2	使用方法.....	252
11.2.3	安全性分析.....	255
11.2.4	HITB CTF 2018: gundam.....	257
11.2.5	BCTF 2018: House of Atum.....	263
11.3	fastbin dup.....	268
11.3.1	fastbin dup.....	268
11.3.2	fastbin dup consolidate.....	273
11.3.3	OCTF 2017: babyheap.....	275
11.4	house of spirit.....	283
11.4.1	示例程序.....	284
11.4.2	LCTF 2016: pwn200.....	287
11.5	不安全的 unlink.....	291
11.5.1	unsafe unlink.....	292
11.5.2	HITCON CTF 2016: Secret Holder.....	295
11.5.3	HITCON CTF 2016: Sleepy Holder.....	303
11.6	off-by-one.....	307
11.6.1	off-by-one.....	307
11.6.2	poison null byte.....	310
11.6.3	ASIS CTF 2016: b00ks.....	313
11.6.4	Plaid CTF 2015: PlaidDB.....	320
11.7	house of einherjar.....	325
11.7.1	house of einherjar.....	325

11.7.2	SECCON CTF 2016: tinypad	328
11.8	overlapping chunks.....	336
11.8.1	扩展被释放块	336
11.8.2	扩展已分配块	339
11.8.3	hack.lu CTF 2015: bookstore	342
11.8.4	0CTF 2018: babyheap	349
11.9	house of force	353
11.9.1	house of force	353
11.9.2	BCTF 2016: bcloud	356
11.10	unsorted bin 与 large bin 攻击	363
11.10.1	unsorted bin into stack.....	363
11.10.2	unsorted bin attack.....	367
11.10.3	large bin 攻击	370
11.10.4	0CTF 2018: heapstorm2	374
	参考文献.....	381
第 12 章	pwn 技巧	383
12.1	one-gadget	383
12.1.1	寻找 one-gadget	383
12.1.2	ASIS CTF Quals 2017: Start hard	385
12.2	通用 gadget 及 Return-to-csu	388
12.2.1	Linux 程序的启动过程	388
12.2.2	Return-to-csu.....	390
12.2.3	LCTF 2016: pwn100	392
12.3	劫持 hook 函数.....	395
12.3.1	内存分配 hook.....	396
12.3.2	0CTF 2017 - babyheap.....	397
12.4	利用 DynELF 泄露函数地址	401
12.4.1	DynELF 模块.....	401
12.4.2	DynELF 原理.....	402
12.4.3	XDCTF 2015: pwn200	403
12.4.4	其他泄露函数	406
12.5	SSP Leak	409
12.5.1	SSP.....	409
12.5.2	__stack_chk_fail().....	411
12.5.3	32C3 CTF 2015: readme	412
12.5.4	34C3 CTF 2017: readme_revenge.....	416
12.6	利用 environ 泄露栈地址.....	422
12.6.1	HITB CTF 2017: Sentosa.....	422

12.7 利用 <code>_IO_FILE</code> 结构	429
12.7.1 <code>FILE</code> 结构体	429
12.7.2 FSOP	431
12.7.3 FSOP (libc-2.24 版本)	433
12.7.4 HITCON CTF 2016: House of Orange	438
12.7.5 HCTF 2017: babyprintf	445
12.8 利用 <code>vsyscall</code>	449
12.8.1 <code>vsyscall</code> 和 <code>vDSO</code>	449
12.8.2 HITB CTF 2017: 1000levels	451
参考文献	456