

به نام ایزد یکتا

مرجع کامل
تست نفوذ و مهندسی معکوس نرم افزارها
با

OllyDbg



مهندس مجید زاده رستم

انتشارات پندار پارس

سرشناسه	: زاده رستم، مجید، ۱۳۶۸ -
عنوان و نام پدیدآور	: مرجع کامل تست نفوذ و مهندسی معکوس نرم افزارها با OllyDbg
مشخصات نشر	: تهران : پندار پارس، ۱۳۹۲.
مشخصات ظاهری	: ۳۸۲ ص.؛ مصور، جدول
شابک	: 978-600-6529-81-3
وضعیت فهرست نویسی	: فبیای مختصر
یادداشت	: فهرست نویسی کامل این اثر در نشانی: http://opac.nlai.ir قابل دسترسی است
یادداشت	: کتابنامه
شماره کتابشناسی ملی	: ۳۸۰۵۲۳۲

انتشارات پندار پارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ www.pendarepars.com
 تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴
info@pendarepars.com

نام کتاب	: مرجع کامل تست نفوذ و مهندسی معکوس نرم افزارها با OllyDbg
ناشر	: انتشارات پندار پارس
ترجمه و تالیف	: مجید زاده رستم
چاپ نخست	: اردیبهشت ۹۴
شمارگان	: ۵۰۰ نسخه
طرح جلد	: رامین شکرالهی
چاپ، صحافی	: روز

قیمت: ۲۸۰۰۰ تومان شابک: ۳-۸۱-۶۵۲۹-۶۰۰-۹۷۸

*هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

فهرست

فصل نخست: نرم افزار اشکال زدا چیست؟ ۲

۴	OllyDbg چیست؟
۵	مروری بر OllyDbg
۱۲	قالب پشته
۱۸	تفاوت های نسخه ۱.۱۰ و ۲.۰۱
۱۸	آشنایی مختصر با زبان اسمبلی
۱۹	ثبات های پایهای
۲۰	دستورالعمل های پایه ای
۲۶	ثبات های FPU
۲۷	ثبات های MMX
۲۸	۳DNow!
۲۸	دستورالعمل های FPU
۳۳	برخی Data Type ها
۳۳	قراردادهای فراخوانی (Calling Conventions)

فصل دوم: حریم خصوصی و امن شما ۳۵

۳۶	نسخه اصلی OllyDbg
۳۷	نصب
۳۸	اصول کلی
۴۳	اجزای OllyDbg
۴۳	Disassembler
۴۴	Assembler
۴۷	Analyzer (تحلیلگر)
۵۴	ردیابی به کمک ثبات - یک مثال
۵۴	تحلیلگر چگونه کار می کند - یک مثال
۵۷	Object Scanner (پویسگر شی)
۵۸	ImplibScanner (پویسگر کتابخانه وارداتی)
۵۸	برچسب ها (Labels)
۶۰	توضیحات کاربر
۶۱	اصول کار دیباگرها در ویندوز

فصل سوم: چگونگی آغاز یک نشست اشکال زدایی ۶۳

۶۸	اشکال زدایی در زمان اجرا
۶۹	نوار ابزار
۷۱	گشتی در پنجره های نرم افزار
۷۱	پنجره CPU
۷۲	Disassembler
۷۴	منوی Disassembler
۷۴	راهنمای API حساس به متن
۷۵	Decoding Hints (راه گشاها)
۷۷	Command History (دستورهای تازه دیده شده)
۷۷	Backup (پشتیبان)
۷۹	Information

۸۱	 Appearance	منوی
۸۲	 Dump	
۸۵	 Dump	منوی
۹۱	 Registers	
۹۳	 Stack	
۹۶	 Log	پنجره
۹۷	 Handles	پنجره
۹۷	 File/Drive	پنجره
۹۹	 Executable Modules	پنجره
۱۰۰	 Profile	
۱۰۱	 Heap	لیست
۱۰۱	 Patch	ها (اصلاحات)
۱۰۱	 Memory Map	پنجره
۱۰۶	 References	(مراجع)
۱۰۸	 Names	پنجره
۱۱۰	 Windows	پنجره
۱۱۱	 SEH	پنجره
۱۱۳		کنترل و بررسی
۱۱۴	 Threads	(نخ‌ها)
۱۱۷	 Call stack	(پشته فراخوانی)
۱۱۸	 Call tree	(درخت فراخوانی)
۱۲۰	 Breakpoints	(نقاط توقف)
۱۲۸	 Disassembler	منوی
۱۴۱	 Hi.exe	برنامه
۱۴۵	فصل چهارم: اجرای گام به گام و حرکتی	
۱۴۷	 Execute till return	(اجرا تا بازگشت)
۱۴۸	 Execute till user code	(اجرا تا کد کاربر)
۱۴۸	 Hit trace	
۱۵۳	 Run trace	
۱۶۴	 Minesweeper	یک مثال
۱۷۸	 Buffer Overflow	یک مثال
۱۸۳		فایل‌های خود استخراج شونده
۲۱۱	فصل پنجم: ارزیابی عبارات	
۲۱۲		اجزای اولیه
۲۱۳		محتویات حافظه
۲۱۳		داده‌های علامت‌دار و بی علامت
۲۱۴		عملگرها
۲۱۴		عبارت‌های چندگانه
۲۱۵		عملگرهای رشته‌ای
۲۱۷		جست‌وجو
۲۱۷		دستورهای غیرصریح
۲۱۸		چند مثال:
۲۲۱		جست‌وجو به دنبال رشته‌های دودویی
۲۲۳		جست‌وجو به دنبال ارجاع‌ها

۲۲۵	جست‌وجو به دنبال رشته‌های متنی مورد ارجاع قرار گرفته
۲۲۶	جست‌وجو به دنبال یک ثابت
۲۲۶	جست‌وجو به دنبال مجموعه‌ای از دستورها
۲۲۷	جست‌وجو به دنبال فراخوانی‌های درون‌مازولی
۲۲۸	جست‌وجو به دنبال دستورها یا داده‌های تغییر داده شده
۲۲۹	توضیحات توابع
۲۲۹	مقدمه
۲۳۲	قواعد کلی
۲۳۶	نوع‌های از پیش تعریف شده
۲۳۹	فصل ششم: تنظیمات
۲۴۰	General (کلی)
۲۴۲	Defaults (پیش‌فرض‌ها)
۲۴۴	Dialogs (تظیمات)
۲۴۵	Directories (فهرست)
۲۴۵	Fonts (قلم)
۲۴۶	Colours (رنگ)
۲۴۷	Code highlighting (برجسته‌سازی کد)
۲۴۹	Security (ایمنی)
۲۵۱	Debug (اشکال‌زدایی)
۲۵۲	Events (رویدادها)
۲۵۴	Exception (خطاها)
۲۵۴	Trace (ردیابی)
۲۵۶	SFX
۲۵۷	Strings (رشته‌ها)
۲۵۹	Addresses
۲۶۱	Commands (دستورها)
۲۶۲	(Disassembly) Disasm
۲۶۴	CPU
۲۶۷	Registers (ثبات‌ها)
۲۶۷	Analysis - بخش نخست
۲۶۹	Analysis - بخش دوم
۲۷۰	Analysis - بخش سوم
۲۷۲	Stack
۲۷۳	فایل ini
۲۷۵	فصل هفتم: اشکال‌زدایی DLL‌های مستقل
۲۸۶	LOADDLL.EXE برنامه
۲۸۷	محدودیت‌ها و مشکلات OllyDbg
۲۹۱	فصل هشتم: پلاگین‌ها
۲۹۲	Plugin‌ها چگونه کار می‌کنند
۲۹۷	منوها و میانبرها
۳۰۰	میانبرها
۳۰۰	جایدهی منوها
۳۰۲	توابع خدماتی
۳۰۴	پلاگین Bookmark

۳۰۵		Command line	پلاگین
۳۰۸		توضیح چند مثال	
۳۰۹		(OllyScript) ODbgScript	پلاگین
۳۰۹		متغیرهای رزرو شده	
۳۱۰		مجموعه دستورها	
۳۳۱		GOTO label	
۳۳۵		INIR key, def	
۳۳۵		INIW key, val	
۳۳۵		"iniw "key", "x	
۳۳۵		iniw "key", ۱۰	
۳۵۰		برچسبها	
۳۵۰		توضیحات	
۳۵۷		پیوست	
۳۵۷		میانبرهای سرتاسری	
۳۶۰		پیغامهای پنجره	
۳۶۳		(Jump)	دستورهای پرش
۳۶۶		ASCII	جدول کاراکترهای
۳۶۸		APIهای پرکاربرد	لیستی از
۳۷۰		روشهای آدرس دهی	