

ردگیری هکرها

7291179

Hackers Trace (Forensic)

مؤلفان:

سید سعید حسینی

احسان نیکانر



NAGHOOS
PUBLICATION

سرشناسه	حسینی، سید سعید، ۱۳۶۰-
عنوان و نام پدیدآور	ردگیری هکرها-(Hackers Trace(Forensic)/مولف سید سعید حسینی احسان نیک آور
مشخصات نشر	تهران: انتشارات ناقوس، ۱۳۹۷
مشخصات ظاهری	۱۵۲ ص: مصور
شابک	978-600-473-097-6
وضعیت فهرست نویسی	فیفا
موضوع	هکرها
موضوع	Hackers:
موضوع	شبکه های کامپیوتری—تدابیر ایمنی
موضوع	Computer networks—Security measures:
موضوع	کامپیوترها ایمنی اطلاعات
موضوع	Computer Security:
موضوع	آزمایش نفوذ(ایمن سازی کامپیوتر)
موضوع	Penetration testing (Computer Security):
شناخت افزایی	نیک آور، احسان، ۱۳۶۶-
رده بندی خنکره	TK ۵۱۰۵/۵۹/ح ۵ ر ۳ ۱۳۹۷
رده بندی دیویی	۰۰۵/۸:
شماره کتابشناس ملی	۵۰۸۰۵۱۰



برای سید Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناقوس

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۳

کتاب حق برای سرمایه گذار محفوظ است. کتب علمی یا قسمتی از این اثر به صورت رونق یا چاپ مجدد، چاپ افست، پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی

نام کتاب	ردگیری هکرها
ناشر	انتشارات ناقوس
مولف	سید سعید حسینی-احسان نیک آور
چاپ اول	۱۳۹۷:
تیراژ	۱۰۰۰ جلد
چاپ و صحافی	نارنجستان
ناظر چاپ	یاسمن تجملی محدث
قیمت	۱۷۰۰۰۰ ریال
شابک	۹۷۸-۶۰۰-۴۷۳-۰۹۷-۶
ISBN	978-600-473-097-6

مرکز پخش: انتشارات ناقوس

۱- خیابان بلوار کشاورز-خیابان ۱۶ آذر-کوچه پارسی-پلاک ۱۰

تلفاکس-۶۶۴۷۸۹۵۷-۶۶۴۷۸۹۵۸

۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

۳- کتابفروشی گلریزان: ضلع جنوب شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

فهرست مطالب

فصل اول : مقدمات علم جرم‌یابی

۳.....	مقدمه
۳.....	فارنزیك بدافزارها
۴.....	مفاهيم علم فارنزيك
۴.....	پيش از بررسي (Before the investigation)
۵.....	چالش‌های مربوط به شواهد
۶.....	متدلوژی بازرس فارنزيکی
۸.....	چند راهنمایی برای توسعه يك استراتژی تحقیقاتی:
۸.....	Collect Evidence
۹.....	نکاتی در خصوص گردآوری شواهد

فصل دوم: ویندوز سیستم عامل کاملاً ناشناخته

۱۳.....	فایل سیستم ویندوز
۱۴.....	بوت
۱۴.....	اتفاقات کامپیوتر پس از روشن شدن
۱۵.....	مراحل بوت در ویندوز
۱۷.....	سرانجام، هسته ویندوز
۱۸.....	کانکشن و شبکه
۲۱.....	فرایندها در ویندوز
۲۲.....	انواع فرایندها
۲۶.....	حافظه
۲۸.....	بخش‌های مخفی ویندوز
۲۹.....	ریجستری
۳۰.....	مدل‌های مرجع
۳۰.....	OSI Reference Model
۳۵.....	مدل TCP/IP
۳۷.....	پروتکل‌های مدل TCP/IP

فصل سوم: هک و آزمایشگاه

۴۳	چرخه هک و نفوذ
۴۵	چهار نوع آسیب‌پذیری
۴۵	آزمایشگاه نخست- حملات
۵۰	آنالیز حمله
۵۱	آزمایشگاه دوم- حملات
۵۶	آنالیز حمله

فصل چهارم: متدهای ردگیری هکر

۶۱	جرم‌یابی قانون شبکه
۶۱	انگیزه‌های جرم‌یابی قانونی شبکه
۶۲	منابع کسب مدارک مبتنی بر شبکه
۶۹	ابزارهای جرم‌یابی قانونی شبکه
۷۱	ابزار Network Miner
۷۱	ابزار آنالیز OmniPeek Network Analyzer
۷۸	ابزار Microsoft Network Monitor
۷۸	روش استفاده از برنامه Microsoft Network Monitor
۸۰	ابزار FayeTracker
۸۱	ابزارهای ردگیری پروسه‌ها و سرویس‌ها
۸۲	ابزار WhatsRunning
۸۴	ابزار Process Hacker
۸۴	ابزار Proce Net Monitor
۸۵	حافظه
۸۵	رونوشت گرفتن از حافظه‌ی فیزیکی
۸۵	Memoryze
۸۷	FTK Imager
۸۷	ابزار DumpIt
۸۸	ویژگی‌های کلی ابزارهای نرم‌افزاری رونوشت‌گیری حافظه
۸۸	رونوشت گرفتن از حافظه‌ی فیزیکی: مجازی‌سازی
۸۸	ابزار جرم‌یابی قانونی حافظه‌ی volatility

۸۹.....	volatility
۹۰.....	تشخیص پردازه‌های مخفی شده با تکنیک DKOM
۹۲.....	بازرسی DLLها در رونوشت حافظه
۹۵.....	ابزار Responder PRO
۹۷.....	Handle.exe
۹۸.....	Listdll.exe
۱۰۱.....	نحوه کار با ابزار
۱۰۸.....	ابزار OSForensics
۱۱۰.....	رجیستری ویندوز
۱۱۰.....	چرا رجیستری ریختن حساس است؟
۱۱۲.....	سازمان و ساختار رجیستری
۱۱۲.....	Registry Forensic
۱۱۲.....	ابزارها
۱۱۳.....	ابزار AutoStart and ProcessView
۱۱۳.....	ابزار Reg Scanner
۱۱۵.....	ابزار Regshot
۱۱۵.....	Registry Forensics: General Forensic Information
۱۱۶.....	مسیرهای Registry و بدافزارها
۱۱۷.....	Shellbag Microsoft
۱۱۷.....	ساختار shellbag رجیستری در ویندوز
۱۱۸.....	ساختار ShellBag در ویندوز xp
۱۱۹.....	معرفی ابزار
۱۱۹.....	Sbag.exe
۱۲۰.....	Shellbag Analyzer
۱۲۱.....	تشخیص و آنالیز بدافزار
۱۲۲.....	شاخص شناسایی بدافزار
۱۲۲.....	روش تجزیه و تحلیل بدافزار
۱۲۲.....	دسته‌بندی براساس اهداف
۱۲۳.....	معرفی ابزارها براساس آنالیز رفتار
۱۲۳.....	ابزار Security Task Manager
۱۲۶.....	ابزار Freefixer

۱۲۸.....	ابزار PCHunter
۱۲۹.....	یک سناریو
۱۳۰.....	ابزار PEid
۱۳۱.....	ابزار Dependency Walker
۱۳۱.....	نرم افزار Resource Hacker
۱۳۲.....	ابزار PEView
۱۳۳.....	ابزار FileAlyzer
۱۳۴.....	ابزار VoodooShield
۱۳۷.....	ابزار byShelter

منابع

۱۴۱.....	منابع
----------	-------