ادله الکترونیک با

Kali Linux

Digital Forensics with Kali Linux

Shiva V.N. Parasram

ترجمه: مهندس مهران تاجبخش

انتشارات پندار پارس

سرشناسه	:	پاراسرام، شیوا وی. ان. Parasram, Shiva V.N.
عنوان و نام پدیدآور	:	ادله الکترونیک با Kali Linux/ [شیوا وی.ان پاراسرام] ؛ ترجمه مهران تاجبخش.
مشخصات نشر	:	تهران : پندار پارس ، ۱۳۹۷.
مشخصات ظاهری	:	۲۰۲ ص.: مصور.
شابک	:	۲۵۰۰۰ ریال978-600-8201-64-9:
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	عنوان اصلی: DIGITAL FORENSICS WITH KALI LINUX, 2017.
موضوع	:	سیستم عامل لینوکس
موضوع	:	Linux
موضوع	:	نرم‌افزار کاربردی -- طراحی و توسعه
موضوع	:	Application software -- Development
شناسه افزوده	:	تاجبخش، مهران، ۱۳۴۷ -، مترجم
رده بندی کنگره	:	۱۳۹۷ ۷۶/۷۶QA ۲پ۹۴س/
رده بندی دیویی	:	۰۰۵/۴۳۲
شماره کتابشناسی ملی	:	۵۲۲۷۱۲۸

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ www.pendarepars.com

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸همراه: ۰۹۱۲۲۴۵۱۰۰۸ info@pendarepars.com

نام کتاب	:	ادله الکترونیک با Kali Linux
ناشر	:	انتشارات پندار پارس
تألیف	:	Shiva V.N. Parasram
ترجمه	:	مهران تاجبخش
چاپ نخست	:	تیرماه ۹۷
شمارگان	:	۵۰۰ نسخه
طرح جلد	:	سارا یعسوبی
چاپ، صحافی	:	روز
قیمت	:	۲۵۰۰۰ تومان شابک : ۹-۶۴-۸۲۰۱-۶۰۰-۹۷۸

فهرست

فصل نخست؛ مقدمه‌ای بر ادله الکترونیک ۳

ادله الکترونیک چیست؟ ۵

تاریخچه مختصری از ادله الکترونیک ۶

نیاز به علم ادله الکترونیک با پیشرفت فناوری ۷

ابزارهای تجاری در زمینه ادله الکترونیک ۹

سیستم‌های عامل و ابزارهای متن باز ادله الکترونیک ۱۰

توزیع DEFT ۱۱

توزیع لینوکس CAINE ۱۲

توزیع کالی لینوکس ۱۴

استفاده از چند توزیع برای بررسی ادله الکترونیک ۱۸

ضد ادله الکترونیک و تهدید برای ادله الکترونیک ۱۹

رمزنگاری ۲۰

گمنامی آنلاین و آفلاین ۲۱

فصل دوم؛ نصب کالی لینوکس ۲۳

ویرایش‌های سیستم‌عامل ۲۳

دانلود سیستم‌عامل کالی لینوکس ۲۴

نصب سیستم‌عامل کالی ۲۵

نصب کالی لینوکس بر روی VirtualBox ۲۶

آماده سازی ماشین مجازی حاوی سیستم‌عامل کالی لینوکس ۲۷

نصب سیستم‌عامل کالی لینوکس بر روی ماشین مجازی ۲۹

پارتیشن بندی دیسک ۳۳

مروری بر سیستم‌عامل لینوکس ۳۷

خلاصه ۴۰

فصل سوم؛ آشنایی با سیستم فایل و رسانه‌های ذخیره‌سازی ۴۱

رسانه ذخیره‌سازی ۴۱

IBM و تاریخچه رسانه ذخیره‌سازی ۴۲

رسانه‌های ذخیره‌سازی قابل حمل ۴۳
نوارهای مغناطیسی ۴۳
فلاپی دیسک‌ها ۴۳
تحول فلاپی دیسک‌ها ۴۳
رسانه ذخیره‌سازی نوری ۴۴
دیسک‌های فشرده (CD) ۴۴
DVD (Digital Versatile Disk) ۴۵
دیسک بلو-ری (Blu-ray) ۴۶
فلش دیسک ۴۶
دیسک فلش USB ۴۷
کارت‌های حافظه فلش ۴۸
دیسک‌های سخت ۵۰
دیسک‌های سخت با واسطه ارتباطی IDE ۵۱
دیسک‌های سخت SATA ۵۲
دیسک‌های SSD ۵۳
سیستم‌های فایل و سیستم‌های عامل ۵۴
داده چیست؟ ۵۶
وضعیت‌های داده ۵۶
داده توصیفی ۵۶
فضای اضافی ۵۷
داده فرآ ۵۸
حافظه مجازی و اهمیت آنها در بررسی ادله الکترونیک ۶۰

فصل چهارم: مقابله با رخدادها و جمع‌آوری شواهد ۶۳

رویه‌های جمع‌آوری شواهد و ادله الکترونیک ۶۴
برخورد با حوادث و نخستین اقدامات در صحنه جرم ۶۴
مستندسازی و جمع‌آوری شواهد ۶۵
جمع‌آوری و نگهداری شواهد فیزیکی ۶۶
ابزارهای جمع‌آوری فیزیکی ۶۷

درجه فرآر بودن ۷۰
حفظ پیوستگی روند تحقیق و تفحص (Chain of Custody) ۷۱
مقایسه جمع‌آوری شواهد و ادله در سیستم‌های خاموش و روشن ۷۲
مسدود کردن نوشتن ۷۳
نسخه برداری از داده‌ها و رمزنگاری hash ۷۴
کد رمزنگار MD5 hash ۷۵
الگوریتم رمزنگار SHA ۷۶
ستم‌العمل و توصیه‌های کاربردی برای جمع‌آوری تجهیزات و داده‌ها ۷۷

فصل پنجم: جمع‌آوری و نگهداری شواهد با استفاده از DC3DD و GUYMAGER . ۷۹

ویژگی‌های دیسک و پارتیشن در لینوکس ۷۹
شناسایی دیسک با استفاده از دستور fdisk ۸۰
حفظ مشمولیت شواهد ۸۲
استفاده از دستور DC3DD در لینوکس ۸۳
تقسیم فایل با استفاده از ابزار DC3DD ۸۷
مقایسه کد اعتبارسنجی فایل‌های نسخه‌برداری شده ۸۹
پاک کردن محتویات دیسک با استفاده از ابزار DC3DD ۸۹
نسخه‌برداری از شواهد و ادله با استفاده از ابزار Guymager ۹۱
اجرای ابزار Guymager ۹۱
جمع‌آوری شواهد با استفاده از Guymager ۹۳
مقایسه کد رمز Hash ۹۷

فصل ششم: بازیابی فایل‌ها و کاوش در داده‌ها با استفاده از FOREMOST، SCALPEL و BULK EXTRACTOR ۱۰۱

بررسی ادله الکترونیک در شواهد نسخه‌برداری شده با استفاده از Foremost & Scalpel ۱۰۲
استفاده از Foremost برای بازیابی فایل و داده‌کاوی ۱۰۲
استفاده از ابزار Scalpel برای داده‌کاوی ۱۰۵
انتخاب انواع فایل در ابزار Scalpel ۱۰۵

استفاده از ابزار scalpel برای داده‌کاوی ۱۰۷
مقایسه ابزارهای Foremost و Scalpel ۱۰۸
ابزار Bulk_extractor ۱۰۹
فایل نمونه نسخه‌برداری شده از شواهد برای استفاده در ابزار Bulk_extractor ۱۱۰
استفاده از ابزار Bulk_extractor ۱۱۰
مشاهده نتایج بدست آمده توسط Bulk_extractor ۱۱۲
فصل هفتم؛ بررسی ادله الکترونیک در حافظه با استفاده از VOLATILITY ۱۱۷
دریافت ابزار Volatility Framework ۱۱۷
دانلود نمونه شواهد و ادله الکترونیک نسخه‌برداری شده برای استفاده در ابزار Volatility ... ۱۱۸
محل فایل نسخه‌برداری شده از شواهد ۱۱۹
استفاده از ابزار Volatility در کالی لینوکس ۱۲۰
انتخاب پروفایل در ابزار Volatility ۱۲۲
افزونه imageinfo ۱۲۲
شناسایی پردازش‌ها و بررسی آن‌ها ۱۲۳
دستور pslist ۱۲۳
دستور pstree ۱۲۵
دستور psscan ۱۲۵
افزونه psxview ۱۲۶
بررسی سرویس‌های شبکه و ارتباط‌ها ۱۲۷
دستور connections ۱۲۷
دستور connscan ۱۲۷
افزونه sockets ۱۲۹
آنالیز فایل‌های DLL ۱۲۹
دستور verinfo ۱۳۰
افزونه dlllist ۱۳۰
دستور getsids ۱۳۱
آنالیز رجیستری ۱۳۳

افزونه hivescan ۱۳۳
افزونه hivelist ۱۳۴
نسخه‌برداری از اطلاعات رمزعبور ۱۳۴
بازه زمانی رخدادها ۱۳۵
افزونه timeliner ۱۳۵
آنالیز بدافزار ۱۳۶
فصل هفتم؛ AUTOPSY – THE SLEUTH KIT ۱۳۹
معرفی ابزارهای Autopsy – The Sleuth Kit ۱۴۰
فاد نسخه‌برداری شده نمونه برای استفاده در ابزار Autopsy ۱۴۱
ادله الکترونیک با استفاده از Autopsy ۱۴۲
راه اندازی Autopsy ۱۴۲
ایجاد پرونده جدید ۱۴۴
آنالیز و بررسی با استفاده از Autopsy ۱۵۱
مرتب سازی فایل‌ها ۱۵۵
باز کردن مجدد یک پرونده در Autopsy ۱۵۷
فصل نهم؛ آنالیز ترافیک شبکه و اینترنت با استفاده از XPLICO ۱۵۹
نرم‌افزارهای مورد نیاز ۱۶۰
اجرای Xplico در سیستم‌عامل کالی لینوکس ۱۶۰
اجرای Xplico در سیستم‌عامل Linux DEFT 8.2 ..... ۱۶۳
آنالیز بسته‌های ترافیکی نسخه‌برداری شده با استفاده از Xplico ۱۶۶
آنالیز ترافیک وب و پروتکل HTTP با استفاده از Xplico ۱۶۶
آنالیز ایمیل با استفاده از ابزار Xplico ۱۷۲
تمرین بر روی پروتکل SMTP با استفاده از فایل نسخه‌برداری شده با Wireshark ۱۷۸
فصل دهم؛ آشکار کردن شواهد و ادله الکترونیک با استفاده از DFF ۱۸۱
نصب DFF ۱۸۲
آنالیز فایل با استفاده از DFF ۱۸۵

پیش‌گفتار

امنیت در حوزه فناوری اطلاعات و فضای مجازی، گستره وسیعی را در بر می‌گیرد. استانداردها، روش‌ها و ابزارهای مورد استفاده در این حوزه را می‌توان به سه بخش، پیشگیری، عملیاتی و مقابله و برخورد تقسیم کرد. در بخش پیشگیری، از فناوری‌های مربوط به تست نفوذ استفاده می‌شود. در این بخش، هدف تست آسیب‌پذیری و قابلیت نفوذ به سیستم‌ها، ابزارها و نرم‌افزارهای مورد استفاده می‌باشد تا با شناسایی نقاط ضعف و آسیب‌پذیر، تا حدامکان آنها را برطرف کرده و یا کاهش دهیم. در بخش عملیاتی، به طور معمول ابزارها و فناوری‌های رصد و کنترل برخط سیستم و رخدادهای مربوط به آن مد نظر قرار دارند. هدف استفاده از این فناوری‌ها، محافظت سیستم در برابر حملات شناخته نشده و روز صفر می‌باشد و سرانجام در بخش مقابله با رخدادها و حملات، فناوری‌ها و ابزارهایی مورد استفاده قرار می‌گیرند که با استفاده از آنها، داده‌ها و اطلاعات باقی مانده از حمله و نفوذ و یا رخداد مورد نظر، جمع آوری، آنالیز و بررسی می‌شوند تا منشا و هدف حمله، عامل و میزان خسارات وارد شده مشخص شوند. این بخش همان فناوری ادله الکترونیک (Digital Forensics) می‌باشد.

فناوری ادله الکترونیک و مباحث مربوط به آن چندان جدید نمی‌باشند و از دهه ۱۹۹۰ این فناوری برای نخستین بار مطرح شد، اما از سال ۲۰۰۰ میلادی به بعد، ایجاد انجمن‌ها و مؤسسات تخصصی در این حوزه و ورود سازمان‌ها و ارگان‌های انتظامی و قضایی به موضوع ادله الکترونیک، نشانه اهمیت و لزوم توجه به این بخش از امنیت فناوری اطلاعات و فضای مجازی است.

از آن زمان تاکنون، استانداردهای مختلفی در حوزه ادله الکترونیک و قانونی و بخش‌های مختلف آن، اعم از جمع آوری داده‌ها و اطلاعات، نگهداری آنها و بررسی و آنالیز و در نهایت تهیه گزارش ارائه شده‌اند.

مهمترین بخش در حوزه ادله الکترونیک، مربوط به آنالیز و بررسی تخصصی داده‌ها و شواهد جمع آوری شده از صحنه جرم است. این بخش، از پیچیدگی‌های مخصوص به خود برخوردار می‌باشد. مهمترین چالش پیش روی متخصص ادله الکترونیک در بخش آنالیز و بررسی شواهد و ادله به‌جای مانده، مربوط به شمار زیاد ابزارها، فناوری‌ها و نرم‌افزارهای مورد استفاده توسط کاربران، سیستم‌ها و شبکه‌های سازمان‌ها و همچنین عدم مستندسازی کامل و دقیق آنها می‌باشد.

هم اینک بسیاری از نرم افزارها و ابزارهای مورد استفاده، متن باز نبوده و مستندات دقیق و کاملی از ساختار داخلی و فرمت و قالب داده‌های مورد استفاده و چگونگی ارتباط بین بخش‌های مختلف آن، در دسترس نمی‌باشند، به‌همین دلیل متخصص ادله الکترونیک باید با استفاده از تجربه و ابزارهای تخصصی بررسی و آنالیز ادله الکترونیک، داده‌ها و شواهد مورد نیاز خود را از آنها استخراج کرده و نتیجه‌گیری‌های لازم از آنها را در قالب گزارش ارائه کند.

در کتاب سعی کرده‌ایم تا علاوه بر معرفی این فناوری، استانداردها، روش‌ها و ابزارهای مورد استفاده در این حوزه را معرفی کرده و به صورت عملی مراحل اجرای پرونده ادله الکترونیک را ارائه کنیم.

مطالعه این کتاب را به همه متخصصان حوزه امنیت اطلاعات و فضای مجازی و راهبران سیستم و امنیت شبکه سازمان‌ها توصیه می‌کنیم.