به‌نام خداوند جان و خرد

پیاده‌سازی آزمایشگاه تحلیل بدافزار در لینوکس و ویندوز

(REMnux Linux, Cuckoo Sandbox, Multi-AV, ...)

www.ketab.ir

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندارپارس

سرشناسه	:	داوری دولت‌آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور	:	پیاده‌سازی آزمایشگاه تحلیل بدافزار در لینوکس و ویندوز (REMnux Linux, Cuckoo Sandbox, Multi-AV, ...)/ مجید داوری‌دولت‌آبادی.
مشخصات نشر	:	تهران : پندارپارس، ۱۳۹۵.
مشخصات ظاهری	:	۲۴۴ ص.: مصور، جدول، نمودار.
شابک	:	978-600-8201-05-2: ۱۸۰۰۰۰ ریال
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه.
موضوع	:	نرم‌افزار بدافزار
موضوع	:	سیستم عامل لینوکس
موضوع	:	سیستم عامل یونیکس
موضوع	:	ویروس‌های کامپیوتر
موضوع	:	کامپیوترها -- ایمنی اطلاعات
رده بندی کنگره	:	۱۳۹۵۷۶/۷۶QA ۱۷۵د۹/
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۴۲۰۰۰۰۹

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی [illegible]پی، شماره ۴ واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹[illegible]۳۷۱۹۶۴ **info@pendarepars.com**

نام کتاب	:	پیاده‌سازی آزمایشگاه تحلیل بدافزار در لینوکس و ویندوز
ناشر	:	انتشارات پندار پارس
ترجمه و تالیف	:	مجید داوری دولت آبادی
چاپ نخست	:	اردیبهشت ۹۵
شمارگان	:	۵۰۰ نسخه
طرح جلد	:	مصطفی مصباحی
چاپ، صحافی	:	روز
قیمت	:	۱۸۰۰۰ تومان شابک : ۲-۰۵-۸۲۰۱-۶۰۰-۹۷۸

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

www.ketab.ir

فهرست

فصل نخست: آغاز کار با ابزار تحلیل‌بدافزار Cuckoo Sandbox ۳
روش‌های تجزیه و تحلیل بدافزار ۳
نظریه اساسی در ساختار Sandbox ٤
آزمایشگاه تحلیل بدافزار ٥
ابزار Cuckoo Sandbox ۷
نصب و راه‌اندازی ابزار Cuckoo Sandbox ۹
نیازمندی‌های سخت‌افزاری ۹
آماده‌سازی Host OS ۱۰
نصب و راه‌اندازی Python در Ubuntu ۱۰
پیکربندی و تنظیم ابزار Cuckoo Sandbox بر روی Host OS ۱۳
آماده‌سازی Guest OS ۱۴
پیکربندی شبکه ۱۶
تنظیم دایرکتوری اشتراکی میان Host OS و Guest OS ۱۸
ایجاد یک حساب کاربری ۲۲
نصب و پیکربندی ابزار Cuckoo Sandbox ۲۲
فایل cuckoo.conf ۲۳
فایل <machinemanager.conf> ۲۳
فایل processing.conf ۲۴
فایل reporting.conf ۲۴
فصل دوم: بهره‌گیری از ابزار Cuckoo Sandbox برای تحلیل یک بدافزار نمونه ۲۷
راه‌اندازی و اجرای ابزار Cuckoo Sandbox ۲۷
فرستادن نمونه‌های گوناگون بدافزار به ابزار Cuckoo Sandbox ۲۹
فرستادن یک بدافزار از نوع مستندات Word ۳۱
فرستادن یک بدافزار از نوع مستندات PDF ۳۷
فرستادن یک بدافزار در قالب مستندات نرم‌افزار Excel با پسوند xls ۳۹
فرستادن یک URL مُخرب به ابزار Cuckoo ٤۱
فرستادن یک صفحه از یک URL مُخرب به ابزار Cuckoo ٤۳
فرستادن یک فایل باینری به ابزار Cuckoo ٤٤
پزشکی قانونی حافظه با استفاده از Cuckoo Sandbox و dump حافظه ٤۹
پزشکی قانونی حافظه اضافی با استفاده از Volatility ٥۲
استفاده از ابزار Volatility ٥۲
فصل سوم: تجزیه و تحلیل خروجی ابزار Cuckoo Sandbox ٥٥
ماژول‌های پردازش ٥٦
تحلیل یک حمله APT با استفاده از ابزارهای Cuckoo، Volatility و Yara ٥۸
فصل چهارم: گزارش‌گیری با کمک ابزار Cuckoo Sandbox ۷۳
ایجاد یک گزارش ساخته شده در فرمت HTML ۷۳
ایجاد یک گزارش از نوع MAEC ۷٥
استخراج تحلیل گزارش داده از ابزار Cuckoo فرمت‌های دیگر ۸۱
فصل پنجم: نکات و ترفندها در ابزار Cuckoo Sandbox ۸۹
سخت‌گیری‌های ابزار Cuckoo Sandbox در مقابل تشخیص ماشین مجازی ۸۹

www.ketab.ir

بررسی ساختار Cuckooforcanari، تجمیع ابزار Cuckoo Sandbox با پروژه Maltego ۹۶
نصب ابزار Maltego ۹۷
ضمیمه‌های نامه الکترونیکی خودکار با Cuckoo MX ۱۰۳
فصل ششم؛ بهره‌گیری از ابزار Multi-AV، Pyew و VirusTotal Scanner برای تحلیل بدافزار ۱۰۹
راه‌اندازی ابزار Multi-AV ۱۰۹
ماژول‌های Sophos، Trend، Avira، Emsisoft و Kaspersky ۱۱۰
ماژول Trend Micro ۱۱۲
ماژول Avira ۱۱۳
ماژول Kaspersky ۱۱۴
منوی موتور ضد بدافزار Emsisoft ۱۱۵
اطلاعات تکمیلی برای استفاده از ابزار Multi-AV ۱۱۷
استفاده از سرور پراکسی با Multi-AV ۱۱۸
استفاده از یک کامپیوتر جایگزین برای دریافت فایل‌های ماژول‌ها ۱۱۹
متوقف کردن آیندهای در حال اجرا توسط ابزار Multi-AV ۱۲۰
بررسی اطلاعات تکمیلی در مورد ابزار Multi-AV ۱۲۱
تحلیل بدافزار با کمک ابزار Pyew ۱۲۲
ابزار پویشگر VirusTotal ۱۲۶
فصل هفتم؛ بهره‌گیری از ابزار Malcom، Hook Analyser برای تحلیل اتصالات بدافزار در ترافیک شبکه ۱۲۹
نصب ابزار Malcom ۱۳۰
پیکربندی گزینه‌های ابزار Malcom ۱۳۱
بررسی رهگیری TLS ۱۳۳
محیط مناسب برای اجرای ابزار Malcom ۱۳۳
بهره‌گیری از ابزار Hook Analyser ۱۳۵
فصل هشتم؛ توزیع REMnux و ابزارهای متداول برای تحلیل بدافزار ۱۳۹
توزیع لینوکس REMnux ۱۳۹
نصب ماشین مجازی REMnux در نرم‌افزار VMware ۱۴۰
نصب ماشین مجازی REMnux در نرم‌افزار VirtualBox ۱۴۱
بررسی ابزارهای موجود در توزیع REMnux ۱۴۲
ابزارهای مخصوص بررسی بدافزارهای مرسوم ۱۴۲
ابزارهای بررسی فایل‌های مستندات ۱۵۶
ابزارهای ویژه‌ی استخراج و رمزگشایی کدها و داده‌ها ۱۷۰
ابزارهای ویژه‌ی رسیدگی به تعاملات شبکه ۱۸۵
ابزارهای ویژه‌ی نمونه‌های متعدد فرآیند و پردازش ۱۸۹
ابزارهای ویژه‌ی بررسی محتواها و ویژه‌گی‌های فایل‌ها ۱۹۵
ابزارهای ویژه‌ی بررسی بدافزارهای لینوکسی ۲۰۶
ابزارهای ویژه‌ی ویرایش و نمایش فایل‌ها ۲۱۴
ابزارهای بررسی گزارش‌های ویژه و فوری از حافظه ۲۱۷
ابزارهای بررسی ایستای فایل‌های PE ۲۱۹
ابزارهای بررسی بدافزارهای موبایل ۲۲۵
برخی از ابزارهای مورد نیاز دیگر ۲۲۶
نصب ابزارهای اضافی ۲۳۱

www.ketab.ir

سخنی با خوانندگان

دنیای بدافزارها و نرم‌افزارهای مُخرب امروزه وسعت بسیاری پیدا کرده است و همه‌ی تجهیزات و منابع اطلاعاتی و ارتباطی را تحت تأثیر خود قرار داده است. این نوع نرم‌افزارها همیشه در علم کامپیوتر و شبکه مطرح بوده و می‌باشند و در همه‌ی دوران‌ها یکی از دقدقه‌های اصلی مدیران سیستم و امنیت شبکه بوده است و هم اینک و در آینده نیز روز به‌روز بر اهمیت آن افزوده می‌شود. اکنون بدافزارها بسیار فعال‌تر از گذشته شده‌اند و از هوشمندی بالایی برخوردار هستند. از این‌رو ممکن است برخی از نرم‌افزارهای ضدویروس نتوانند به سرعت بدافزارها را شناسایی و پاکسازی کنند. در این حوزه همیشه کمبود ابزارهایی افزون بر نرم‌افزارهای ضدویروس، به‌منظور تجزیه و تحلیل بدافزارها و شناسایی رفتار و عملکرد آن‌ها احساس می‌شد، که خوشبختانه چند سالی است محققان و طراحان نرم‌افزارهای امنیتی در این حوزه نیز وارد شده‌اند و ابزارهای متنوعی برای کمک به امر تجزیه و تحلیل بدافزارها، طراحی و پیاده‌سازی نموده‌اند. این ابزارها به‌صورت ساخت‌یافته‌ای و براساس مکانیزم‌های گوناگون تحلیل رفتاری به بررسی و تحلیل انواع نرم‌افزارها و کدهای مُخرب می‌پردازند و در این خصوص کمک شایانی به تحلیلگران در این زمینه می‌کنند. وجود چنین ابزارهایی در آزمایشگاه‌های بررسی بدافزارها و شرکت‌های تولیدکننده ضدویروس، بسیار حیاتی می‌باشند و می‌توانند در امر شناسایی رفتار و تولید پادزهر بدافزارها کمک فراوانی به متخصصان تحلیل و تولید نرم‌افزارهای ضدویروس نمایند.

امروزه در این حوزه، آزمایشگاه‌هایی برپایه تحلیل بدافزار در کنار آزمایشگاه‌های شناسایی بدافزارهای موجود در فضای اینترنت و طراحی نرم‌افزارهای ضدویروس ایجاد شده‌اند که نقش اساسی در تولید ابزارهای ضدویروس برای یک بدافزار خاص و در حالت کلی برای یک نسخه کامل ضدویروس بازی می‌کنند. این نوع آزمایشگاه‌ها نیازمند تجهیزات و امکانات متنوع و صرف هزینه‌های بالا نمی‌باشند و به‌راحتی با کمک نرم‌افزارهای مجازی‌سازی مانند VirtualBox ،VMware و غیره می‌توان آن‌ها را بر روی سیستم‌های‌عامل لینوکس و ویندوز پیاده‌سازی کرد که در این‌کار سهم سیستم‌عامل لینوکس به‌واسطه انبوه ابزارهای طراحی شده برای آن در این مقوله، نسبت به ویندوز بیشتر می‌باشد و از کارآیی بیشتری برخوردار است. در این حوزه ابزارهای خاص و قدرتمندی درقالب Sandboxها برای تحلیل بدافزارها طراحی شده‌اند که می‌توان از آن‌ها برای شناسایی رفتار بدافزارهای گوناگون و حتی جدید استفاده کرد. همچنین توزیع‌های لینوکس قدرتمندی نیز براساس این ساختار طراحی و منتشر شده‌اند که به‌صورت پیش‌فرض همه‌ی نرم‌افزارهای مورد نیاز برای تجزیه و تحلیل بدافزارها و پیاده‌سازی یک آزمایشگاه کامل در این

www.ketab.ir

خصوص بر روی آن‌ها نصب و راه‌اندازی شده است و جز در مواردی خاص، به هیچ‌عنوان نیازمندی برای نصب ابزارها به‌منظور تحلیل بدافزارها وجود ندارد.

این کتاب تلاش دارد با بهره‌گیری از ابزارها و توزیع‌های موجود در زمینه تحلیل رفتاری بدافزارها، متخصصان امنیت و یا دانشجویان علم امنیت را با ابزارهای موجود در این حوزه و همچنین چگونگی پیاده‌سازی آزمایشگاه‌های شناسایی بدافزار آشنا سازد، زیرا هم‌اینک مقوله بدافزارها، تغییر مسیر و شیب تندی پیدا کرده است و به‌صورت تدریجی و هوشمند به سمتی هدایت می‌شود که وجود چنین آزمایشگاه‌هایی در هر سازمان و یا مجموعه‌ای که به هر نحوی با کامپیوتر و اینترنت سر و کار دارند، ضروری می‌باشد تا پیش از بُروز رخداد و اختلال در عملکرد شبکه توسط بدافزارها و ایجاد هزینه‌های گزاف برای سازمان مربوطه، متخصصان امنیت سازمان بتوانند پیش از به‌روزرسانی‌ها توسط شرکت‌های تولیدکننده ضدویروس، رفتارهای مشکوک در سطح شبکه خود را شناسایی کنند و در جهت محدودسازی فرآیند و پاکسازی موارد مشکوک، گام بر دارند.

شیرازه اصلی این کتاب برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه تجزیه و تحلیل رفتاری بدافزارها، اصول پیاده‌سازی آزمایشگاه تحلیل بدافزار، علم شناسایی نرم‌افزارهای مُخرب، ابزارها و توزیع‌های استاندارد پیاده‌سازی آزمایشگاه‌های تحلیل می‌باشد که البته با تجربیات ناچیز اینجانب در این‌باره آمیخته شده است، که به‌فرم کاملاً آزاد از مطالب و تجربیات گردآوری و دخل و تصرفی نیز با آن همراه بوده است. اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت درصدد گردآوری و تألیف کتابی آموزشی برپایه تحلیل بدافزارها به‌منظور افزایش کارایی عملی متخصصان، دانشجویان و مدیران شبکه در این زمینه بودم تا آن‌ها را با اصول فنی، چگونگی پیاده‌سازی یک آزمایشگاه تجزیه و تحلیل بدافزار در محل کار خود آشنا و آگاه سازم (گرچه مدیران و متخصصان امنیت شبکه حُکم اساتید اینجانب را دارند، اما به حُکم وظیفه برخود لازم دانستم که این آگاه‌سازی را انجام دهم). پیشاپیش همه‌ی کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آن‌ها را به دیده منّت پذیرا هستم.

(m_Davari@TOP-co.ir) (m_Davary@Parshack.zzn.com)

پس از سپاس و ستایش به درگاه پروردگار از همه‌ی دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می‌کنم. برخود لازم می‌دانم از زحمات بی‌دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانهٔ ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است. در پایان از مدیریت فرزانه انتشارات پندار پارس جناب آقای مهندس یعسوبی و همه‌ی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یارب غم آنچه غیر تو در دل ماست — بردار که بی‌حاصلی از حاصل ماست
الحمد که چون تو راهنمایی داریم — کز گمشدگانیم که غم، منزل ماست

(مجید داوری دولت آبادی – بهار ۱۳۹۵)

www.ketab.ir