نفوذ و ضد نفوذ

تکنیک‌های کاربردی برای نفوذگران و متخصصان امنیت شبکه

به زبان پایتون

تالیف

[illegible] زاجس

مترجمان

محمد حسین مهری خوانساری دکتر ابراهیم مهدی پور

سرشناسه	: زایتس ، جاستین Seitz,Justin
عنوان و نام پدیدآور	: نفوذ و ضد نفوذ تکنیک های کاربردی برای نفوذگران و متخصصان امنیت شبکه به زبان پا یتون/نویسنده جاستین سایتز[مترجمین]محمد حسین مهری خوانساری،ابراهیم مهدی پور
مشخصات نشر	: تهران: ناقوس،۱۳۹۷.
مشخصات ظاهری	: ۲۱۶ص. : مصور.
شابک	: 978-600-473-150-8 ۳۵۰۰۰۰ریال
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: عنوان اصلی: Black hat Python:Python Programming For Hackers and pentesters,[2018]
عنوان دیگر	: تکنیک های کاربردی برای نفوذگران و متخصصان امنیت شبکه به زبان پایتون
موضوع	: کامپیوترها—ایمنی اطلاعات
موضوع	: Computer Security
موضوع	: پایتون(زبان برنامه نویسی کامپیوتر)
موضوع	: Python(Computer Program Language)
شناسه افزوده	: مهری خوانساری،محمد حسین،۱۳۶۸- ، مترجم
شناسه افزوده	: مهدی پور،ابراهیم،۱۳۵۹- ، مترجم
رده بندی کنگره	: ۱۳۹۷ ۱۷ز۹ ک /QA۷۶
رده بندی دیویی	: ۰۰۵/
شمارهٔ کتابشناسی ملی	: ۱۰۷

NAGHOOS PUBLICATION

انتشارات ناقوس

نام کتاب	: نفوذ و ضد نفوذ تکنیک های کاربردی برای نفوذگران و متخصصان امنیت شبکه به زبان پایتون
ناشر	: انتشارات ناقوس
نویسنده	: Justin Seitz
مترجمین	: محمد حسین مهری خوانساری،ابراهیم مهدی پور
چاپ اول	: پاییز۱۳۹۷
تیراژ	: ۱۰۰۰نسخه
قیمت	: ۳۵۰۰۰۰ریال
ناظر چاپ	: یاسمن تجلی محدث
چاپ و صحافی	: نارنجستان
شابک	:۹۷۸-۶۰۰-۴۷۳-۱۵۰-۸
ISBN	: 978-600-473-150-8

مرکز پخش: انتشارات ناقوس
۱-خیابان انقلاب- بلوار کشاورز- خیابان ۱۶آذر-کوچه پارسی-پلاک ۱۰
تلفن و فاکس : ۶۶۴۷۸۹۵۷ - ۶۶۴۷۸۹۵۸
۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

پیش گفتار مولف

به طور خلاصه نویسنده این کتاب را در یک جمله می‌توان توصیف کرد: نفوذگر به زبان پایتون. در پروژه *Immunity* شانس این را داشتم که با افراد حرفه‌ای در برنامه نویسی پایتون کار کنم. شخصا یکی از این افراد نیستم و بیشتر زمان خود را صرف انجام آزمون نفوذ کرده‌ام که لازمه آن توسعه سریع ابزارهای مبتنی بر پایتون است و تاکید بر اجرای هرچه سریع‌تر و بدست آوردن نتایج دارد (نه ساختار مهندسی کدها یا بهینه سازی یا حتی استحکام کدهای نوشته شده). البته این مساله را (عدم تمرکز بر جزییات مهندسی نرم‌افزار) به عنوان یک آزمون‌گر نفوذ نقطه قوت خود می‌دانم. به مرور در خلال مطالعه کتاب با شیوه کدنویسی من آشنا خواهید شد. امیدوارم که این شیوه کدنویسی برای شما نیز مفید باشد.

با پیشروی در مطالعه کتاب متوجه خواهید شد که وارد جزئیات عمیق مباحث نمی‌شوم. این یک تصمیم تعمدی است. چرا که هدف اصلی ارائه دانش پایه در مورد هر مبحث است. با توجه به این نکته ایده‌ها و تمرینات اضافی را در انتهای گنجانده‌ام تا خواننده را در مسیر صحیح خود قرار دهم. خواننده را تشویق می‌کنم که در مورد این ایده‌ها کاوش کرده و ابزارهایی که توسعه می‌دهند را با من نیز به اشتراک بگذارند.

مشابه هر کتاب تخصصی دیگری، خوانندگان با سطوح مهارت‌های مختلف در زبان پایتون (یا به طور عمومی در زمینه امنیت اطلاعات) تجربه متفاوتی از مطالعه این کتاب خواهند داشت. برخی ممکن است مستقیما به فصلی مراجعه کنند که موضوع حرفه‌ای و مورد نیاز آنهاست در حالی که برخی دیگر کتاب را فصل به فصل و از ابتدا مطالعه می‌کنند. پیشنهاد می‌کنم که اگر یک برنامه نویس مبتدی یا متوسط زبان پایتون هستید مطالعه کتاب را از ابتدا و به ترتیب تعیین شده فصول آغاز کنید. مفاهیم پایه مفیدی در حوزه برنامه نویسی در خلال مطالعه فصول فرا خواهید گرفت.

در شروع کار مقدمات برنامه نویسی شبکه در فصل ۲ مطرح می‌شود و کار خود را با برنامه

نویسی سوکت‌های خام در فصل ۳ و ساخت یک اسنیفر ساده ادامه می‌دهیم. در فصل ۴ با استفاده از ابزار *Scapy* ابزارهای جالبی در حوزه شبکه توسعه می‌دهیم. در فصل ۵ کتاب به مبحث نفوذ به وب‌سایت‌ها پرداخته می‌شود. فصل ۶ روش‌های افزونه نویسی برای نرم‌افزار امنیتی معروف *Burp* را بررسی می‌کند. از اینجا به بعد عمده مطالب به نحوی مربوط به توسعه تروجان‌هاست. در فصل ۷ به نحوه فرماندهی و کنترل تروجان‌ها توسط سرویس *Github* پرداخته می‌شود و تا رسیدن به فصل ۱۰ که مربوط به تاکتیک‌های ارتقای سطح دسترسی در ویندوز است، مباحث تکمیل می‌شوند. فصل پایانی روش استفاده از ابزار *Volatility* برای خودکار سازی عملیات تحقیق و تفحص حافظه کامپیوتر پس از وقوع حمله را بیان می‌کند.

تلاش می‌کنم که کدها و همچنین توضیحات تا حد امکان کوتاه و مفید باشند. اگر در برنامه نویسی پایتون مبتدی هستید، شما را تشویق می‌کنم هر خط از کدها را با دقت مورد بررسی و موشکافی قرار دهید.

تمامی کدهای کتاب در سایت *http://nostarch.com/blackhatpython/* قابل دریافت هستند. کار را آغاز می‌کنیم.

پیش‌گفتار مترجم

یادگیری فنون هک شبکه‌های کامپیوتری همواره یکی از جذاب‌ترین و پر درخواست‌ترین حوزه‌های آموزشی در زمینه علوم کامپیوتر و شبکه بوده است. برخی شاید صرفا به دلیل کنجکاوی و حواشی و افسانه‌های متعدد پیرامون این حوزه و بدون داشتن تجربه و دانش قبلی در زمینه کامپیوتر به آن علاقمند شوند، در حالی که برخی دیگر که احتمالا پیشینه علمی و تجربی قوی در این زمینه دارند با نگاهی موشکافانه متوجه گسترش روز افزون و شدت خطرات موجود در دنیای سایبری و به تبع آن لزوم بروزرسانی پیوسته سطح علمی و فنی مورد نیاز برای اقدامات مقابله‌ای متناسب با شدت تهدیدات هستند. امروزه تقویت توان دفاع سایبری در میان ابرقدرت‌ها تبدیل به یک مسابقه تسلیحاتی بی پایان شده است که هرروز بر ابعاد و پیچیدگی‌های آن افزوده می‌شود. علیرغم وجود نیاز مبرم کشور به نیروی متخصصین ماهر در زمینه امنیت اطلاعات، در بسیاری موارد کمبود منابع آموزشی کافی، جامع و با دسترسی عمومی در این حوزه به خصوص به زبان فارسی احساس شده است. در بسیاری از منابع و دوره‌های آموزش هک صرفا به معرفی و نحوه کاربری چندین ابزار تجاری آماده برای عملیات تهاجمی و تدافعی نفوذ پرداخته می‌شود، بدون آنکه درک صحیحی از ماهیت و ساختار بنیادی اجرای یک سناریوی نفوذ به مخاطب خود بدهد. در این حالت شما در بهترین حالت یک متخصص امنیتی ماتوسط با توانایی‌های پیش پا افتاده محدود به نرم‌افزاری که از آن استفاده می‌کنید خواهید شد. از طرفی دیگر برخی منابع مساله را به صورت کاملا نظری با ارائه مفاهیم، تعاریف و تاکتیک‌ها بر روی کاغذ بدون پرداختن به جزئیات فنی و پیاده سازی ارائه می‌کنند و در نهایت مخاطب خود را با این پرسش اساسی رها می‌کنند که حال برای اجرای یک حمله نفوذ در دنیای واقعی از کجا باید شروع کنم؟

آنچه مطالب این کتاب را نسبت به سایر منابع آموزشی موجود متمایز میکند این است که در هر فصل بدون ورود به مباحث تئوری طولانی و بعضا خسته کننده که احتمالا در بسیاری منابع

دیگر به تفصیل بیشتر یافت می‌شود می‌توانید از ابتدا بر روی نحوه اجرای یک سناریوی خاص نفوذ تمرکز کنید و تمام ابزارهای مورد نیاز برای اجرای آن سناریو را از ابتدا. به طور مثال در فصل سوم به تشریح نحوه ساخت یک اسنیفر ساده پرداخته می‌شود که ابزاری ضروری برای استراق سمع ترافیک شبکه است. گرچه ابزارهای آماده متعددی همچون ***Wireshark*** برای انجام این کار وجود دارد، اما یادگیری نحوه ساخت چنین ابزاری از ابتدا دانش بنیادی مخاطب را در مورد ساختارهای شبکه به طرز چشمگیری افزایش می‌دهد. زمانی که نفوذگر، خود توانایی توسعه ابزارهای مورد نیازش را داشته باشد قدرت عمل و ابتکار بیشتری در اجرای سناریوهای خود خواهد داشت. در خلال هر فصل ایده‌هایی برای بهبود و گسترش تکنیک استفاده مطرح می‌شود که انجام آن جهت تمرین بیشتر و تشویق به تفکر بیشتر در مورد مساله به خواننده واگذار می‌شود.

در پایان لازم به ذکر است که مترجمان اثر بر این باورند که بهترین شیوه دفاع در دنیای سایبری یادگیری شیوه عمل مهاجمین است. بر مبنای همین تفکر عنوان انگلیسی کتاب ***Black Hat Python*** به فارسی "نفوذ و ضد نفوذ با پایتون" ترجمه شده است. بدیهیست که تمامی مطالب عنوان شده در این کتاب صرفا با اهداف آموزشی به مخاطب ارائه شده و مسئولیت هرگونه سو استفاده از مطالب کتاب مستقیما بر عهده مخاطب است. امید می‌رود که ترجمه این اثر گامی موثر در ارتقا و پیش‌برد سطح دانش فنی متخصصین کشور عزیزمان در حوزه دفاع سایبری باشد.

محمد حسین مهری خوانساری

پاییز ۹۷

فهرست مطالب