

نفوذ و ضد نفوذ

تکنیک‌های کاربردی برای نفوذ گران و متخصصان امنیت شبکه

به زبان پایتون

تالیف

مستیس زابنس

مترجمان

دکتر ابراهیم مهدی پور

محمد حسین مهری خوانساری

سرشناسه	زایتس، جاستین
عنوان و نام پدیدآور	Seitz, Justin
مشخصات نشر	تقوّد و ضد تقوّد تکنیک های کاربردی برای نفوذگران و متخصصان امنیت شبکه به زبان پایتون/نویسنده جاستین سایتز [مترجمین] محمد حسین مهری خوانساری، ابراهیم مهدی پور
مشخصات ظاهری	تهران: ناقوس، ۱۳۹۷.
شابک	۲۱۶ص. : مصور.
وضعیت فهرست نویسی: فیا	۸-۱۵۰-۴۷۳-۶۰۰-۹۷۸-۳۵۰۰۰ ریال
یادداشت	عنوان اصلی: [2018] Python Programming For Hackers and pentesters: Python Black hat
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 رده	مهری خوانساری، محمد حسین، ۱۳۶۸-، مترجم
شماره افزوده	مهدی پور ابراهیم، ۱۳۵۹-، مترجم
رده بندی مکرر	۱۳۹۷: ۹۳۱۷ ی ۹۸۷۶/۹
رده بندی دیویی	۰۰۵/۱
شماره کتابشناسی ملی: ۱۰۷۰۶	



برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.com

انتشارات ناقوس

نام کتاب	: تقوّد و ضد تقوّد 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	: پلیمز ۱۳۹۷
تیراژ	: ۱۰۰۰ نسخه
قیمت	: ۳۵۰۰۰ ریال
ناظر چاپ	: یاسمن تجلی محدث
چاپ و صحافی	: تارنجستان
شابک	: ۸-۱۵۰-۴۷۳-۶۰۰-۹۷۸
ISBN	: 978-600-473-150-8

کلیه حقوق برای ناشر محفوظ است. تکثیر تمامی یا قسمتی از این اثر بصورت حروفچینی یا چاپ مجدد، چاپ افست، پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مرکز پخش: انتشارات ناقوس

- ۱- خیابان انقلاب- بلوار کشاورز- خیابان ۱۶ آذر- کوچه پارسی- پلاک ۱۰
تلفن و فاکس: ۶۶۲۷۸۹۵۷-۶۶۲۷۸۹۵۸
- ۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۳

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 دا... (نه ساختار مهندسی کدها یا بهینه سازی یا حتی استحکام کدهای نوشته شده). البته این مساله را (عدم تمرکز بر جزئیات 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، خواهید دید 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 کتاب 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 مختلفی در زبان پایتون (یا به طور عمومی در زمینه امنیت اطلاعات) تجربه متفاوتی از مطالعه این کتاب خواهند داشت. برخی ممکن است مستقیماً 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 <http://nostarch.com/blackhatpython> در دسترس است. 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 صرفاً 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 احتمالاً 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، روزرسانی پیوسته سطح علمی و فنی مورد نیاز برای اقدامات مقابله‌ای متناسب با شدت تهدیدات می‌شوند. امروزه تقویت توان دفاع سایبری در میان ابرقدرت‌ها تبدیل به یک مسابقه تسلیحاتی بی‌پایان شده است که هر روز بر ابعاد و پیچیدگی‌های آن افزوده می‌شود. علیرغم وجود نیاز مبرم کشور به تربیت متخصصین ماهر در زمینه امنیت اطلاعات، در بسیاری موارد کمبود منابع آموزشی کافی، جابجایی و با دسترس نبودن عمومی در این حوزه به خصوص به زبان فارسی احساس شده است. در بسیاری از منابع و دوره‌های آموزش هک صرفاً به معرفی و نحوه کاربری چندین ابزار تجاری آماده برای عملیات تهاجمی، تدافعی نفوذ پرداخته می‌شود، بدون آنکه درک صحیحی از ماهیت و ساختار بنیادی اجرای کلاهبرداری نفوذ به مخاطب خود بدهد. در این حالت شما در بهترین حالت یک متخصص امنیتی مبتدی، مانند بازیابی‌های پیش پا افتاده محدود به نرم‌افزاری که از آن استفاده می‌کنید خواهید شد. از طرفی دیگر برخی منابع مسأله را به صورت کاملاً نظری با ارائه مفاهیم، تعاریف و تاکتیک‌ها بر روی کاغذ بدون پرداختن به جزئیات فنی و پیاده‌سازی 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 بعضاً خسته‌کننده که احتمالاً 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 اسنiffer 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" بارز دانده شده است. بدیهیست که تمامی مطالب عنوان شده در این کتاب صرفاً با اهداف آموزشی به مخاطب ارائه شده و مسئولیت هرگونه سوء استفاده از مطالب کتاب مستقیماً 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.

حما حسین مهری خوانساری

فصل ۱: راه اندازی محیط برنامه نویسی	۱
۱.۱ نصب کالی	۱
۱.۲ ویرایشگر WingIDE	۴
فصل ۲: مقدمات برنامه نویسی شبکه	۱۱
۲.۱ ساخت TCP Client	۱۲
۲.۲ ساخت UDP Server	۱۳
۲.۳ ساخت TCP Server	۱۴
۲.۴ ساخت یک برار با یک Netcat	۱۶
۲.۵ ساخت TCP Proxy	۲۵
۲.۶ رمزنگاری ارتباطات با پروتکل SSL (Paramiko)	۳۲
۲.۷ تونل زدن با پروتکل SSH	۳۸
فصل ۳: ساخت یک استیفر ساده	۴۵
۳.۱ تولید یک ابزار کشف میزبان UDP	۴۶
۳.۲ اسنیف بسته‌های اطلاعاتی در ویندوز و لینوکس	۴۷
۳.۳ دیکد داده‌ها در لایه IP	۴۹
۳.۴ دیکد پیام‌های ICMP	۵۴
۳.۵ ماژول netaddr	۵۹
فصل ۴: تصاحب شبکه با ماژول Scapy	۶۱

۴.۱	سرقت اطلاعات هویتی ایمیل‌ها	۶۲
۴.۲	حمله <i>ARP Spoofing</i> با کتابخانه <i>Scapy</i>	۶۵
۴.۳	پردازش فایل‌های <i>PCAP</i>	۷۱
فصل ۵:	نفوذ به وب‌سایت‌ها	۷۹
۵.۱	کار با پروتکل <i>HTTP</i> (ماژول <i>urllib2</i>)	۷۹
۵.۲	وب‌سایت‌های مبتنی بر <i>CMS</i> های متن باز	۸۱
۵.۳	حمله <i>Bruteforce</i> بر روی پوشه‌ها و مسیر فایل‌ها	۸۴
۵.۴	حمله <i>Bruteforce</i> بر روی فرم‌های اعتبارسنجی <i>HTML</i>	۸۹
۵.۵	مقدمات <i>HTMLPower</i>	۹۶
فصل ۶:	افزونه نویسی در <i>Burp Suite</i>	۹۹
۶.۱	راه اندازی محیط توسعه	۱۰۰
۶.۲	آزمون فاز در <i>Burp</i>	۱۰۱
۶.۳	جستجوی اهداف با موتور جستجوی <i>Bin</i>	۱۱۳
۶.۴	تشخیص رمزهای عبور از محتوای وب سایت	۱۲۰
فصل ۷:	توسعه و کنترل تروجان‌ها با سرویس <i>GitHub</i>	۱۲۷
۷.۱	ایجاد یک حساب کاربری در <i>GitHub</i>	۱۲۸
۷.۲	ایجاد ماژول‌های تروجان	۱۲۹
۷.۳	پیکربندی تروجان	۱۳۰
۷.۴	ساخت تروجان مبتنی بر <i>GitHub</i>	۱۳۱
۷.۵	اصلاح عملکرد <i>import</i> در زبان پایتون	۱۳۴
فصل ۸:	عملیات متداول تروجان در ویندوز	۱۳۹

۸.۱ ساخت Keylogger ۱۳۹

۸.۲ گرفتن Screenshot از صفحه هدف ۱۴۴

۸.۳ اجرای فرامین پوسته با زبان پایتون ۱۴۶

۸.۴ تشخیص محیط سندباکس ۱۴۸

فصل ۹: هک مرورگر Internet Explorer ۱۵۵

۹.۱ حمله مهاجم در مرورگر ۱۵۶

۹.۲ ایجاد سرور HTTP ۱۶۰

۹.۳ درون کشیدن اطلاعات ۱۶۲

فصل ۱۰: ارتقاء سطح دسترسی در ویندوز ۱۷۳

۱۰.۱ نصب پیش‌بینی‌ها ۱۷۴

۱۰.۲ ایجاد یک ناظر آینده ۱۷۵

۱۰.۳ نظارت بر فرآیندها با Winlog ۱۷۶

۱۰.۴ سطوح دسترسی توکن در ویندوز ۱۷۹

۱۰.۵ پیروزی در مسابقه ۱۸۲

۱۰.۶ تزریق کد ۱۸۷

فصل ۱۱: فارتزیک تهاجمی ۱۹۱

۱۱.۱ نصب ابزار Volatility ۱۹۲

۱۱.۲ پروفایل‌ها ۱۹۲

۱۱.۳ ربودن مقدار هش رمزهای عبور ۱۹۳

۱۱.۴ تزریق کد مستقیم ۱۹۷