

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

راهنمای تجزیه و تحلیل کاربردی وب تاریک

در وب تاریک چه می‌گذرد و چگونه می‌توان از آن استفاده کرد؟

ساین رترکین

مهندس سیدنوآب موسوی - مهندس فاطمه خداپرست

تابستان ۱۴۰۰

سرشناسه	رتزکین، ساین
عنوان و نام پدیدآور	Retzkin, Sion راهنمای تجزیه و تحلیل کاربردی وب تاریک: در وب تاریک چه میگذرد و چگونه میتوان از آن استفاده کرد؟/ سایون رتزکین؛ مترجمان: سیدنواب موسوی، فاطمه خداپرست، ویراستار علمی جمشید نصرت آبادی، محسن آقایی.
مشخصات نشر	تهران: دانشکده علوم و فنون فارابی، انتشارات، ۱۴۰۰.
مشخصات ظاهری	۲۳۳ ص: مصور (رنگی).
شابک	978-600-6028-21-7
وضعیت فهرست نویسی	فیپا
یادداشت	عنوان اصلی: Hands-on Dark Web analysis : learn what goes on in the Dark Web, and how to work with it, 2018.
عنوان دیگر	در وب تاریک چه میگذرد و چگونه می‌توان از آن استفاده کرد؟.
موضوع	وب تاریک
شناسه افزوده	نصرت آبادی، جمشید، ۱۳۵۳ - ویراستار
شناسه افزوده	آقایی، محسن، ویراستار
رده بندی کنگره	QA۷۶/۹
رده بندی دیویی	۰۰۵/۷۴
شماره کتابشناسی ملی	۸۵۲۷۰۲۹
اطلاعات رکورد کتابشناسی	فیپا



انتشارات دانشکده علوم و فنون فارابی

نویسنده: سایون رتزکین

مترجمان: سیدنواب موسوی - فاطمه خداپرست

ویراستار علمی: جمشید نصرت آبادی - محسن آقایی

طراحی جلد: سیدنواب موسوی

صفحه آرایی: سیدنواب موسوی

ویراستاری: صابر زارع آغداش

ناشر: انتشارات دانشکده فارابی

نوبت چاپ: اول

تاریخ انتشار: ۱۴۰۰

شمارگان: ۱۰۰۰ نسخه

قیمت: ۶۵۰۰۰ تومان

تلفن: ۲۹۹۴۲۶۵۸؛ کد پستی: ۱۷۶۵۳۴۲۴

حق چاپ و نشر برای ناشر محفوظ است.

فهرست اجمالی

فصل ۱: شناخت وب عمیق و وب تاریک	۱۹
فصل ۲: کار با وب تاریک	۴۲
فصل ۳: آینده وب تاریک	۶۰
فصل ۴: نصب ماشین مجازی (VM) لینوکس	۷۹
فصل ۵: دسترسی به وب تاریک با TOR	۹۹
فصل ۶: نصب سیستم عامل تیلز	۱۱۷
فصل ۷: نصب سیستم عامل کیوبس	۱۳۸
فصل ۸: نصب سیستم عامل هونیکس	۱۵۱
فصل ۹: در وب تاریک چه می گذرد؟	۱۶۵
فصل ۱۰: خطرهای وب تاریک	۱۹۰
فصل ۱۱: استفاده از وب تاریک برای امور شغلی	۲۱۰
فصل ۱۲: پاسخنامه	۲۲۶

فهرست تفصیلی

۱۳	 مقدمه
۱۷	 سخن مترجمان
۱۹	 فصل ۱: شناخت وب عمیق و وب تاریک
۲۰	 منشأ اینترنت
۲۶	 وب عمیق
۲۸	 وب تاریک
۳۱	 اعمال قانون
۳۲	 روزنامه‌نگاری
۳۳	 حریم خصوصی
۳۵	 مجرمان
۳۵	 مواد مخدر و غیرقانونی
۳۶	 کالاهای تقلبی
۳۸	 اطلاعات سرقتی
۳۸	 هکرها
۳۹	 آنچه آموختیم
۴۰	 سؤال‌ها
۴۱	 منابعی برای مطالعه بیشتر
۴۲	 فصل ۲: کار با وب تاریک
۴۲	 ناشناسی و حفظ حریم خصوصی در وب تاریک
۴۵	 تراکنش و معامله در وب تاریک
۴۶	 روش‌های معامله مطمئن
۵۴	 ایمیل‌های وب عمیق (ایمیل آنیون)
۵۷	 آنچه آموختیم

۵۸	سؤال‌ها
۶۰	فصل ۳: آینده وب تاریک
۶۰	آینده وب تاریک چه چیزی را برای ما حفظ می‌کند؟
۶۱	ارز وب تاریک
۶۲	معاملات
۶۴	بازارهای وب تاریک
۶۹	پروژه TOR
۷۳	علاقه عمومی به وب تاریک
۷۶	آنچه آموختیم
۷۷	سؤال‌ها
۷۹	فصل ۴: نصب ماشین مجازی (VM) لینوکس
۷۹	توزیع‌های لینوکس
۸۵	نصب و استفاده از ماشین مجازی (VM) لینوکس
۹۵	چه کارهای دیگری با لینوکس می‌توانیم انجام دهیم؟
۹۶	اجرای لینوکس از روی فلش‌مموری
۹۷	آنچه آموختیم
۹۸	سؤال‌ها
۹۸	منابع برای مطالعه بیشتر
۹۹	فصل ۵: دسترسی به وب تاریک با TOR
۹۹	مرورگر TOR چیست؟
۱۰۱	نصب TOR روی لینوکس
۱۰۹	نصب مرورگر TOR از طریق ترمینال، با بسته دانلودشده
۱۰۹	نصب مرورگر TOR تنها از طریق ترمینال
۱۱۰	توصیه‌های پروژه TOR درباره استفاده امن از TOR
۱۱۵	آنچه آموختیم
۱۱۶	سؤال‌ها

مقدمه

شبکه جهانی وب به سه حوزه وب سطحی، وب عمیق و وب تاریک تقسیم می‌شود. وب تاریک و وب عمیق مزیت‌های متعددی مانند گمنامی و حفظ حریم خصوصی را فراهم می‌کنند اما این مزیت‌ها برای مجرمین، قانون‌شکن‌ها و جنایتکاران نیز ایجاد می‌گردد. متخصصان امنیت و فناوری اطلاعات نیز با دسترسی به این حوزه‌ها از مزیت‌های آن برخوردار می‌شوند. این کتاب در ابتدا شما را با مفاهیم وب عمیق و وب تاریک و اهمیت آن‌ها آشنا و با استفاده از سیستم‌عامل‌ها و ابزارهای مختلفی مانند مرورگر Tor، روش‌های تقریباً بسیار امنی برای اتصال به وب تاریک معرفی می‌کند. کتاب همچنین در مورد اینکه چه داده‌هایی را می‌توان در وب عمیق و وب تاریک به‌دست آورد، بهترین روش‌ها برای دستیابی به نتیجه مدنظر با استفاده از آن ابزارها کدام است و اینکه چه کسانی از وب عمیق و وب تاریک بهره می‌برند، بحث می‌کند. رویکرد کتاب به شکلی است که در پایان آن شما تجربه عملی کار با وب عمیق و وب تاریک را خواهید داشت. جامعه هدف این کتاب متخصصان امنیت و فناوری اطلاعات، تحلیلگران امنیتی و تمامی علاقه‌مندان به یادگیری مفاهیم وب عمیق و وب تاریک است. برای بخش‌های عملی این کتاب مهارت‌های فنی‌ای مانند مرورگری در اینترنت، مفهوم و استفاده از ماشین‌های مجازی و نصب سیستم‌عامل لازم است. این کتاب شامل دستورالعمل‌های گام‌به‌گام، همراه با تصویرهایی از همه بخش‌های عملی است.

فصل ۱ شناخت وب عمیق و وب تاریک نام دارد. اما برای درک کامل آن‌ها، باید ابتدا منشأ اینترنت و چگونگی کار آن را درک کنیم چون این مفاهیم ذاتاً مرتبط هستند. به همین دلیل در این فصل به موضوع‌های منشأ اینترنت، وب عمیق و وب تاریک پرداخته می‌شود. عنوان فصل ۲ کار با وب تاریک است. در این فصل ارزش دیجیتال، بازارها و وب‌گردی در وب تاریک، حفظ حریم خصوصی، تراکنش و معامله در آن محیط و خدمات ایمیل موجود در وب تاریک (ایمیل آنیون) بررسی می‌گردند.

فصل ۳ آینده وب تاریک است. وقتی از یک فناوری استفاده می‌نماییم، باید به این فکر کنیم که آن فناوری و استفاده از آن در آینده چگونه خواهد بود، چگونه توسعه می‌یابد و چه کسی از آن استفاده خواهد کرد. در این فصل سعی می‌شود به این سؤال‌ها پاسخ داده شود. البته کمتر در مورد شایعه‌هایی که درباره وب تاریک می‌شنوید (فعالیت‌های غیرقانونی

در وب تاریک و ... صحبت می‌کنیم و بیشتر به جنبه‌های مثبت و عملی آینده وب تاریک مانند بازارهای آنلاین و مهم‌تر از همه حریم خصوصی می‌پردازیم. به همین دلیل آینده وب تاریک ذاتاً با آینده حریم خصوصی همه ما عجین شده است. مهم‌ترین مطالب این فصل بررسی آینده وب تاریک، بازارهای وب تاریک، پروژه TOR و علاقه عمومی به وب تاریک است.

فصل ۴ با عنوان نصب ماشین مجازی (VM) در لینوکس، با نصب لینوکس، مرورگر Tor و دسترسی به وب تاریک شروع می‌شود و توزیع‌های لینوکس، نصب و استفاده از ماشین مجازی لینوکس و اینکه چه کارهایی می‌توان با آن انجام داد بررسی می‌گردد.

نام فصل ۵ دسترسی به وب تاریک با Tor است. در فصل ۵ با استفاده از یک توزیع استاندارد لینوکس، با چند روش مختلف مرورگر Tor را در لینوکس نصب می‌کنیم. منظور از توزیع استاندارد، توزیعی است که در رایانه‌های رومیزی معمولی کاربرد دارد و فقط امنیت‌محور نیست (بر خلاف توزیع‌هایی که در فصل‌های بعدی به آن‌ها خواهیم پرداخت و بر ویژگی امنیت متمرکز هستند). به‌طور خلاصه مهم‌ترین عنوان‌های مورد بحث فصل ۵ را می‌توان آشنایی با مرورگر Tor، نصب Tor روی لینوکس و توصیه‌های پروژه Tor در مورد استفاده ایمن از مرورگر Tor دانست.

فصل ۶ با عنوان نصب سیستم‌عامل تیلز^۱ به استفاده از این سیستم‌عامل برای دسترسی به وب تاریک می‌پردازد. این سیستم‌عامل زنده^۲ را می‌توان با استفاده از یک فلش‌مموری یا دی‌وی‌دی تقریباً روی همه رایانه‌ها راه‌اندازی کرد. فصل ۶ روی آشنایی، پیش‌نیازها، دانلود و در نهایت نصب سیستم‌عامل تیلز و نیز دسترسی به وب تاریک با استفاده از این سیستم‌عامل متمرکز است.

فصل ۷ با عنوان نصب سیستم‌عامل کیوبس، در مورد یک سیستم‌عامل مبتنی بر Xen و بسیار ایمن به نام کیوبس است. سیستم‌عامل کیوبس با این فرض که از قبل امنیت آن

^۱ Tails

^۲ Live Operating System

نقض شده است عمل می‌کند و هر برنامه‌ای در محیط مجازی خاص خود اجرا می‌شود. در این فصل چگونگی نصب و استفاده از سیستم‌عامل کیوبس برای دسترسی به وب تاریک را یاد خواهیم گرفت. مهم‌ترین موضوع‌های این فصل آشنایی با سیستم‌عامل کیوبس، چگونگی نصب آن و دسترسی به وب تاریک با آن است.

عنوان فصل ۸ نصب سیستم‌عامل هونیکس است. این فصل به هونیکس که توزیعی دیگر از لینوکس است می‌پردازد. هونیکس در واقع یک بازبینی و تغییر گسترده در پیکربندی لینوکس دبیان^۱ به منظور ارتقای امنیت و حریم خصوصی به سطحی پیشرفته است که درون چندین ماشین مجازی (VM) اجرا می‌شود و یک لایه قوی برای محافظت در برابر بدافزارها و نشت آدرس آی‌پی فراهم می‌کند. هونیکس تنها سیستم‌عاملی است که برای اجرا در داخل ماشین مجازی و هماهنگی با Tor طراحی شده است. این فصل به آشنایی با هونیکس، نصب و پیش‌نویس‌هایش و نیز استفاده از آن برای مرورگری در وب تاریک می‌پردازد.

همان‌طور که از عنوان در وب تاریک چه می‌گذرد پیدا است، فصل ۹ با ارایه مثال‌هایی به خطرها و مزیت‌های وب تاریک می‌پردازد که خواننده با توجه به آن‌ها می‌تواند برای ورود به وب تاریک تصمیم بگیرد. در این فصل افراد مختلفی که به وب تاریک وصل می‌شوند و دلیلشان برای این کار، بررسی می‌شود.

فصل ۱۰ خطرهای وب تاریک نام دارد و به چیزهایی که در وب تاریک در انتظار افراد است می‌پردازد. خطرهای وب تاریک چیست؟ چگونه می‌توان از آن‌ها پرهیز کرد؟ این‌ها سؤالاتی است که ممکن است در بررسی وب تاریک برای خواننده پیش بیاید. برخی به وب تاریک به شکل مکانی شیطانی می‌نگرند که در آن هرکس خرابکار در کمین ما نشسته‌اند. پس مهم‌ترین موضوع‌های این فصل خطرهای وب تاریک و چگونگی پرهیز از آن‌ها است.

عنوان فصل ۱۱ استفاده از وب تاریک برای امور شغلی است و به بررسی کاربران کنونی وب تاریک و دلیل استفاده‌شان از آن محیط می‌پردازد. این کار ممکن است بینشی در مورد چگونگی استفاده از وب تاریک برای سازمان‌های متبوع خوانندگان ایجاد کند. هدف این

^۱ Debian Linux

فصل آرایه ایده‌ها و استفاده کاربردی و عملی از مواردی است که بر اساس تجربه مشترک و شخصی می‌توانند به امور شغلی کمک کنند.

برای همگام شدن با رویکرد عملی این کتاب، باید یک فلش‌مموری و رایانه‌ای که مایل به قالب‌بندی آن هستید یا رایانه‌ای با منابع کافی برای ایجاد ماشین‌های مجازی داشته باشید. در متن کتاب در جاهایی از قالب‌های نوشتار ویژه‌ای بهره گرفته شده است. برخی از این قالب‌ها عبارت‌اند از:

- کدهای درون متن (CodeInText):

این نوع قالب نوشتاری در متن نشان‌دهنده نام جدول پایگاه داده، نام فولدرها، پسوند فایل‌ها، نام مسیرها در رایانه، URLها و ورودی کاربر است. به عنوان مثال: «برای راه‌اندازی مرورگر Tor روی فایل Start-tor-browser.desktop دو بار کلیک کنید». یک بلوک از برنامه‌نویسی با این قالب نوشتاری به صورت زیر نوشته می‌شود:

```
html, body, #map {
  height: 100%;
  margin: 0;
  padding: 0
}
```

هر ورودی یا خروجی خط فرمان به شکل زیر نوشته می‌شود:

sudo apt install gnupg

- **بولد:** یک اصطلاح جدید، یک کلمه مهم یا کلمه‌هایی را که روی صفحه مشاهده می‌کنید نشان می‌دهد. کلمات موجود در منوها یا جعبه‌های گفت‌وگو در متن به این شکل ظاهر می‌شوند. به عنوان مثال: «اکنون، فلش‌مموری دوم را وصل کنید و به مسیر زیر (در سیستم‌عامل تیلز) بروید و تیلز را روی آن نصب نمایید:

Applications | Tails | Tails Installer

❖ هشدارها یا یادداشتهای مهم با این نماد نمایش داده می‌شود.

✓ نکته‌ها و ترفندها با این نماد نشان داده شده‌اند.