



کانون نشر علوم

سازار اس ۳۳

# مرجع کاربردی ابزارهای تکمیلی هک برای کالی لینوکس

مؤلف:

مهندس مجید داوری دانات آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

ناشر:

کانون نشر علوم



ناشر علوم

www.nashreloom.com

پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

سرشناسه: داوری دولت‌آبادی، مجید، ۱۳۵۹ -

عنوان و نام پدیدآور: مرجع کاربردی ابزارهای تکمیلی هک برای کالی لینوکس / مولف مجید داوری دولت‌آبادی.

مشخصات نشر: تهران: کانون نشر علوم: کاتوزی، ۱۳۹۵.

مشخصات ظاهری: ۳۶۰ص: مصور، جدول، نمودار.

شابک: ۹۷۸۹۶۴۳۲۷۱۵۹۶

وضعیت فهرست‌نویسی: فیا

یادداشت: ۳۵۹.

موضوع: سیستم‌های عامل لینوکس

موضوع: UNIX

موضوع: سیستم‌های عامل (تر)

موضوع: (Computers) system, Opera

رده‌بندی کنگره: ۱۵۲ ۲۸۴۱ س/۱۶۱/۷۶/۱۰۵

رده‌بندی دیویی: ۰۰۵/۴۳۲

شماره کتابشناسی ملی: ۳۷۷۸

نام کتاب: مرجع کاربردی ابزارهای تکمیلی هک برای کالی لینوکس

ناشر: کانون نشر علوم

ناشر همکار: کاتوزی

مؤلف: مهندس مجید داوری دولت‌آبادی

صفحه‌آرا: فاطمه آدیگوزل‌پور اردبیلی

طرح جلد: زهرا سلطان‌آبادی

چاپ اول: پاییز ۱۳۹۵

تیراژ: ۱۰۰۰

چاپ و صحافی: کانون نشر علوم

قیمت: ۳۵۰۰ تومان

شابک: ۹۷۸۹۶۴۳۲۷۱۵۹۶

دفتر مرکزی پخش: خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد ۱

تلفن: ۶۶۹۶۱۵۶۸-۶۶۴۹۴۹۱۱



## سخن ناشر

به نام خداوند بخشنده و مهربان

نستره دانش بشری در برابر علم بی‌پایان و نامتناهی حضرت حق (جلّ جلاله) بسیار ناچیز است؛ هرچنان که کریمه «و ما عطا نکردیم به شما علم را جز اندکی» شاهدی است بر ضعف معرفت انسان نسبت به حکمت صمدانی. با این حال چه نیکو سفارش فرموده است خاتم انبیاء، حضرت محمد طه (ص)، که «بجوید علم را اگر چه به سرزمین چین». این توصیه، تمامی پیروان راستین دین سیف السلام را به فراگیری و اکتساب علوم و فنون مختلف در همه زمان‌ها و همه مکان‌ها فرا می‌خواند.

تلاش کانون نشر علوم، همواره مصوف به تولید آثار شایسته و بایسته در زمینه فنی و مهندسی بوده است؛ اگرچه که در این راه مشکلات دشواری‌های فراوانی حادث شده و خواهد شد. این امر تا حدی بسیار، تابعی از ماهیت رشته‌های فنی و مهندسی و معارف مربوط به آنهاست؛ چرا که این رشته‌ها به سرعت و بی‌وقفه در حال نو به نو شدن می‌باشند. این امر رسالت کانون نشر علوم را در نشر آثار مربوطه، اعم از تألیف یا ترجمه، صابریز کرده و می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از قافله علمی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجهت علمی و پژوهشی، رتور شأن مخاطبین اندیشمند و فاضل نیز باشد. امید است که خداوند متان در این مهم مساعدت نماید.

پایان سخن اینکه، کانون نشر علوم دست یاری و همت تمامی مؤلفین و مترجمین علاقه‌مند در زمینه علوم فنی و مهندسی را به گرمی می‌فشارد و تمامی ایشان را خاضعانه و خاشعانه به همکاری فرا می‌خواند. همچنین این مجموعه از تمامی مخاطبین استدعا دارد که با نظرات صائب و راهگشای خود، در بهبود شکلی و محتوایی آثار منتشر شده مساعدت فرمایند؛ و صد البته که تمامی کاستی‌ها از این رهگذر تنها و تنها متوجه این مجموعه بوده و هست.

سید محمدحسین منوری

کانون نشر علوم



## مقدمه مؤلف

توزیع لینوکس Kali، یکی از توزیع‌های قدرتمندی است که امروزه به دلیل پشتیبانی مستمر و دقیق بسیار مورد توجه نفوذگران، متخصصان آزمایش نفوذ و حتی کاربران حوزه شبکه و امنیت قرار دارد. در واقع این توزیع لینوکس به نوعی عصای دست متخصصان حوزه امنیت و شبکه به حساب می‌آید که در آن تمامی ابزارهای مورد نیاز یک آزمایش‌کننده نفوذ و یا نفوذگر برای رسیدن به اهدافشان به‌صورت پیش‌فرض وجود دارد. هر کدام از این ابزارها به نوبه خود، جزء اجزای مهمی از حوزه‌های مختلف هستند و در روند انجام عملیات نفوذ و یا آزمایش کمک آزمایش‌کننده و یا نفوذگر می‌آیند و کار را برای آن‌ها ساده‌تر و سریع‌تر می‌کنند. البته برخی از ابزارهای تکمیلی، در صورت نیاز جهت پیاده‌سازی حملات حرفه‌ای‌تر هک و آزمایش نفوذ به‌صورت پیش‌فرض بر روی این توزیع موجود نمی‌باشند. این ابزارها و Frameworkها می‌توانند توسط فرد و یا گروه‌های خاصی طراحی و ارائه شده باشند. لازم به‌ذکر است که توزیع لینوکس Kali در زمینه نصب و اضافه کردن ابزارها به مجموعه ابزارهای خود از انعطاف‌پذیری بالایی برخوردار است و به‌راستی می‌توان آن‌ها را بر روی هر نسخه‌ای از این توزیع نصب کرد. همچنین توسعه‌دهندگان این ابزارها نیز، نرم‌افزارها و Frameworkهای خود را مخصوص توزیع لینوکس Kali طراحی و پیاده‌سازی کرده‌اند، در نتیجه به‌راحتی بر روی این توزیع قابل نصب و راه‌اندازی می‌باشند.

در این کتاب سعی شده است تا به بررسی و تحلیل ابزارها و Frameworkهای تکمیلی و حرفه‌ای توسعه داده شده برای توزیع لینوکس Kali پرداخته شود. این کتاب در جهت پیاده‌سازی یک حمله و خط‌مشی حملات هکری استفاده گردد. در این کتاب با کمک این ابزارهای تکمیلی قدرتمند، انواع حملات مطرح در حوزه نفوذگری مورد بررسی و پیاده‌سازی قرار گرفته است. البته لازم به‌ذکر است که در کنار این ابزارها در روند پیاده‌سازی حملات از ابزارهای پیش‌فرض توزیع Kali نیز بهره گرفته شده است. در این کتاب از تمامی منابع معتبر و پایه‌ای مربوط به توزیع لینوکس Kali و علم هک استفاده شده است که البته با تجزیات ناچیز اینجانب آمیخته گردیده است تا کتابی جامع و مفید ایجاد شود.

اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی مرجع به‌منظور افزایش آگاهی متخصصین، دانشجویان و مدیران شبکه در زمینه نحوه



استفاده از ابزارهای توسعه داده شده برای توزیع لینوکس Kali که به صورت پیش فرض بر روی این توزیع نصب نمی باشند، اما توسط نفوذگران حرفه ای برای این نوع توزیع نوشته شده اند. بوم تا آن ها را با اصول فنی آزمایشات نفوذ با کمک این ابزارها آشنا و آگاه سازم و بتوانند از آن ها در فرآیندها و پروژه های آزمایش نفوذ استفاده کنند (گرچه مدیران و متخصصین امنیت شبکه حکم اساتید اینجانب را دارند، اما به حکم وظیفه بر خود لازم دانستم که این آگاه سازی را انجام دهم). همان طور که گفته شد، شیرازه اصلی کتاب حاضر برگرفته از کتاب ها و منابع معتبر در حوزه توزیع لینوکس Kali می باشد که با تجربیات اینجانب در این خصوص سیخته شده است، که به فرم کاملاً آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن ها صورت گرفته است. پیشاپیش تمام کاستی های آن را می پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی های دلسوزانه آن ها را به دیده منت پذیرا هستم.

( m\_Davari@TOP-co.ir )

( m\_Davary@Parshack.zzn.com )

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می کنم. بخیر و خرد لازم می دانم از زحمات بی دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی کنیم. زحمات خاضعانه ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است.

در پایان از مدیریت فرزانه انتشارات کانون نشر علوم جناب آقای منوری و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده اند، صمیمانه قدردانی می نمایم.

**خدایا نام تو در دل عیان است کنار محفلم یادت نهان است**

**به راه راست بر دل را، که تنها تو را دارم، چه حاجت بر بیان است**

(مجید داوری دولت آبادی - پاییز ۱۳۹۵)



## فهرست مطالب

مقدمه مؤلف ..... ۵

فصل ۱: مروری بر مفاهیم پایه‌ای و استانداردهای عملی در آزمایش نفوذ ..... ۱۳

۱-۱- استانداردها در آزمایشات نفوذ ..... ۱۴

فصل ۲: راه‌اندازی یک آزمایشگاه تست نفوذ برای اقدامات آینده ..... ۱۹

۲-۱- طراحی و ایجاد یک آزمایشگاه برای آزمایش نفوذ ..... ۲۰

۲-۲- ایجاد یک شبکه تستی بر دامنه ..... ۲۰

۲-۳- ایجاد سرورهای تستی اضافی ..... ۲۱

۲-۳-۱- ماشین‌های تستی آلوده Metasploitable2 ..... ۲۱

۲-۳-۲- ماشین‌های تستی آلوده OWASP/BWA ..... ۲۱

۲-۴- ایجاد جعبه ابزار آزمایش نفوذ ..... ۲۲

۲-۴-۱- سخت‌افزار مورد نیاز ..... ۲۲

۲-۴-۲- نرم‌افزارهای تجاری در مقابل کدپار ..... ۲۳

۲-۴-۳- راه‌اندازی جعبه ابزار ..... ۲۴

۲-۴-۴- راه‌اندازی توزیع لینوکس Kali ..... ۲۵

۲-۵- بهره‌برداری‌های باینری ..... ۲۷

فصل ۳: پویش شبکه پیش از حمله ..... ۳۵

۳-۱- ابزار Recon-NG ..... ۳۶

۳-۲- ابزار Discover ..... ۴۱

۳-۳- ابزار Spiderfoot ..... ۴۳

۳-۴- ابزارهای مخصوص ایجاد لیستی از کلمات عبور ..... ۴۵

۳-۴-۱- Wordhound ..... ۴۵

۳-۵- ابزار Brutescrape ..... ۴۸

۳-۶- استفاده از لیست‌های کشف شده برای یافتن آدرس‌های پست‌الکترونیکی و اعتبارنامه‌ها ..... ۵۰

۳-۷- ابزار مخصوص تجزیه و تحلیل Github (ابزار Gitrob) ..... ۵۲

۳-۸- کشف و شناسایی فعال داخلی و خارجی ..... ۵۴

۳-۹- ابزار Masscan ..... ۵۴

۳-۱۰- ابزار Sparta ..... ۵۷

۳-۱۱- ابزار Http Screenshot و EyeWitness ..... ۶۱

۳-۱۲- ابزارهای پویش آسیب‌پذیری‌ها ..... ۶۷

۳-۱۳- ابزار Open VAS ..... ۶۷

۳-۱۴- پویش برنامه‌های کاربردی تحت وب ..... ۷۰



|     |                                                  |
|-----|--------------------------------------------------|
| ۷۱  | ۳-۱۵- ابزارهای پویش برنامه‌های کاربردی تحت وب    |
| ۸۰  | ۳-۱۶- ابزار OWASP Zap Proxy                      |
| ۸۲  | ۳-۱۷- انجام عملیات Parsing با کمک ابزار Discover |
| ۸۵  | ۳-۱۸- ابزارهای تکمیلی دیگر در حوزه پویش و بازرسی |
| ۸۵  | ۳-۱۸-۱- Firewall                                 |
| ۸۹  | ۳-۱۸-۲- lazagne                                  |
| ۹۱  | ۳-۱۸-۳- ParanoicScan                             |
| ۹۳  | ۳-۱۸-۴- PenBox                                   |
| ۹۴  | ۳-۱۸-۵- ابزار                                    |
| ۱۰۲ | ۳-۱۸-۶- SinovEmail                               |

#### فصل ۴: بهره‌برداری از سیستم‌های نام شده

|     |                                                       |
|-----|-------------------------------------------------------|
| ۱۰۶ | ۴-۱- ابزار Metasploit                                 |
| ۱۱۱ | ۴-۲- اسکریپت‌ها                                       |
| ۱۱۳ | ۴-۳- تحلیل و سوءاستفاده از چاپگرها                    |
| ۱۱۶ | ۴-۴- ابزار Heartbleed                                 |
| ۱۲۱ | ۴-۵- آسیب‌پذیری Shellshock                            |
| ۱۲۱ | ۴-۶- آزمایشگاه آسیب‌پذیری Shellshock                  |
| ۱۲۵ | ۴-۷- آزادسازی مجموعه اطلاعات Git                      |
| ۱۲۷ | ۴-۸- ابزار NoSQLmap                                   |
| ۱۳۱ | ۴-۹- ابزار Elastic_shell                              |
| ۱۳۴ | ۴-۱۰- ابزارهای تکمیلی دیگر در حوزه بهره‌برداری و نفوذ |
| ۱۳۴ | ۴-۱۰-۱- Airededdon                                    |
| ۱۳۵ | ۴-۱۰-۲- BetterCap                                     |
| ۱۳۷ | ۴-۱۰-۳- ExploitPack                                   |
| ۱۳۸ | ۴-۱۰-۴- GoldenEye                                     |
| ۱۳۹ | ۴-۱۰-۵- HT-WPS BREAKER                                |
| ۱۴۲ | ۴-۱۰-۶- IISlap                                        |
| ۱۴۴ | ۴-۱۰-۷- Katana                                        |
| ۱۴۶ | ۴-۱۰-۸- Kill Chain                                    |
| ۱۴۷ | ۴-۱۰-۹- LazyKali                                      |
| ۱۵۰ | ۴-۱۰-۱۰- Litesploits                                  |
| ۱۵۱ | ۴-۱۰-۱۱- MITMf                                        |
| ۱۵۳ | ۴-۱۰-۱۲- Mole                                         |
| ۱۵۶ | ۴-۱۰-۱۳- RouterSploit                                 |



- ۱۶۲..... ۴-۱۰-۱۴- ابزار (SPF (SpeedPhish Framework
- ۱۶۲..... ۴-۱۰-۱۵- ابزار Viper
- ۱۶۳..... ۴-۱۰-۱۶- ابزار zarp

#### فصل ۵: به کارگیری یافته‌ها در خصوص برنامه‌های کاربردی تحت وب به فرم دستی ۱۶۷

- ۱۶۸..... ۵-۱- آزمایش نفوذ در حوزه برنامه‌های کاربردی تحت وب
- ۱۶۹..... ۵-۲- تست SQL
- ۱۶۹..... ۵-۱- Burp با SQLMap
- ۱۷۵..... ۵-۲- ریف SQL به صورت دستی
- ۱۷۵..... ۵-۳-۱- ابزار SQLmap
- ۱۷۸..... ۵-۳-۲- ابزار sqlninja
- ۱۸۳..... ۵-۳-۳- تزریق‌های پایگاه داده SQL NoSQL
- ۱۸۵..... ۵-۳-۴- حمله به MongoDB
- ۱۸۸..... ۵-۳-۵- سیستم‌های مدیریت محتوا (CMS)
- ۱۹۱..... ۵-۴- مکانیزم XSS (Cross-Site Scripting)
- ۱۹۲..... ۵-۴-۱- ابزار EF Exploitation Framework
- ۱۹۸..... ۵-۴-۲- حملات XSS (Cross-Site Scripting) برنامه ریزی شده
- ۱۹۸..... ۵-۴-۳- مفهوم Crowd Sourcing
- ۱۹۹..... ۵-۵- حملات براساس CSRF (Cross-Site Request Forgery)
- ۲۰۰..... ۵-۵-۱- استفاده از ابزار Burp برای حملات CSRF Replay
- ۲۰۲..... ۵-۶- توکن‌های نشست
- ۲۰۶..... ۵-۶-۱- Fuzzing های اضافی / اعتبارسنجی ورودی
- ۲۱۱..... ۵-۷- ده آسیب‌پذیری برتر در OWASP
- ۲۱۳..... ۵-۸- آزمایش‌های منطقی و کاربردی

#### فصل ۶: سیری در اعماق شبکه ۲۱۵

- ۲۱۶..... ۶-۱- شبکه بدون مجوز و اعتبارسنجی
- ۲۱۶..... ۶-۱-۱- ابزار Responder.py
- ۲۲۰..... ۶-۲- مسموم سازی ARP
- ۲۲۱..... ۶-۲-۱- ابزار Ettercap
- ۲۲۳..... ۶-۲-۲- ابزار Backdoor Factory Proxy
- ۲۲۵..... ۶-۲-۳- مراحل پس از مسموم سازی ARP
- ۲۳۴..... ۶-۳- استفاده از هر اعتبارنامه دامنه (غیر مدیریتی)
- ۲۳۴..... ۶-۳-۱- شناسایی اولیه سیستم
- ۲۳۸..... ۶-۳-۲- تنظیمات Group Policy



|     |                                                                  |
|-----|------------------------------------------------------------------|
| ۲۴۰ | ۶-۳-۳- افزایش امتیازات و دسترسی‌ها                               |
| ۲۴۵ | ۶-۳-۴- صفر تا صد لینوکس                                          |
| ۲۴۶ | ۶-۴- استفاده از هر مدیر محلی و یا حساب مدیر دامنه                |
| ۲۴۶ | ۶-۴-۱- داشتن شبکه با گواهی‌نامه‌ها و Psexec                      |
| ۲۴۹ | ۶-۴-۲- دستورات Psexec برای عبور از سیستم‌های تشخیص نفوذ (Kali)   |
| ۲۵۱ | ۶-۴-۳- حرکت‌های جانبی با WMI (ویندوز)                            |
| ۲۵۳ | ۶-۴-۴- Kerberos - MS14-0۰۸                                       |
| ۲۵۵ | ۶-۴-۵- مفهوم Pass-The-Ticket                                     |
| ۲۵۷ | ۶-۴-۶- حرکت‌های SQL با Postgres                                  |
| ۲۵۹ | ۶-۴-۷- اعتبارنامه‌های تیره شده                                   |
| ۲۶۰ | ۶-۵- حمله به کنترل‌کننده‌ها                                      |
| ۲۶۱ | ۶-۵-۱- ابزار BExec                                               |
| ۲۶۳ | ۶-۵-۲- ابزار PSExec - NTDSgrab                                   |
| ۲۶۶ | ۶-۶- ماندگاری و نگهداری دسترسی                                   |
| ۲۶۶ | ۶-۶-۱- ابزار Veil و Powerhell                                    |
| ۲۶۸ | ۶-۶-۲- ماندگاری و تداوم با مکانیزم برنامه‌ریزی و زمان‌بندی وظایف |
| ۲۷۰ | ۶-۶-۳- مفهوم Golden Ticket                                       |
| ۲۷۷ | ۶-۶-۴- مفهوم Skeleton Key                                        |
| ۲۷۹ | ۶-۶-۵- مفهوم Sticky Keys                                         |

#### فصل ۷: ظاهرسازی با کمک مکانیزم‌های مهندسی اجتماعی

|     |                            |
|-----|----------------------------|
| ۲۸۲ | ۷-۱- حملات مبتنی بر SSH    |
| ۲۸۳ | ۷-۲- حملات Phishing        |
| ۲۸۴ | ۷-۲-۱- کدهای Phishing دستی |
| ۲۹۰ | ۷-۲-۲- ابزار SEF           |

#### فصل ۸: انجام اقدامات مخفیانه و عبور از نرم‌افزارهای ضدویروس

|     |                                                     |
|-----|-----------------------------------------------------|
| ۲۹۴ | ۸-۱- عبور از ضدویروس                                |
| ۲۹۴ | ۸-۱-۱- ابزار Backdoor Factory                       |
| ۲۹۹ | ۸-۱-۲- ابزار Veil                                   |
| ۳۰۲ | ۸-۱-۳- ابزار SMBExec                                |
| ۳۰۳ | ۸-۲- پیاده‌سازی Keylogger با استفاده از Nishang     |
| ۳۰۴ | ۸-۳- پیاده‌سازی Keylogger با استفاده از Powersploit |



## فصل ۹: درهم شکستن، بهره‌برداری و استفاده از ترفندها ۳۰۵

- ۳۰۶ ..... ۹-۱- درهم شکستن کلمات عبور
- ۳۰۷ ..... ۹-۱-۱- ابزار John The Ripper
- ۳۰۹ ..... ۹-۲- جستجوی آسیب‌پذیری‌ها
- ۳۰۹ ..... ۹-۲-۱- ابزار Searchsploit
- ۳۱۰ ..... ۹-۲-۲- پرس‌وجو از Metasploit
- ۳۱۱ ..... ۹-۲-۳- ترفندها و ترفندها
- ۳۱۱ ..... ۹-۲-۳-۱- اسکریپت‌های RC در داخل Metasploit
- ۳۱۲ ..... ۹-۲-۳-۲- Sniffer-ها: بدوز
- ۳۱۴ ..... ۹-۳-۳- عبور UAC
- ۳۱۵ ..... ۹-۳-۴- NetHunter- لینوکس Kali
- ۳۲۰ ..... ۹-۳-۵- ساخت یک پست‌مستفاد
- ۳۲۵ ..... ۹-۳-۶- عبور از دیوارهای امنیتی: برنامه‌های کاربردی
- ۳۲۷ ..... ۹-۳-۷- ابزارهای PowerShell
- ۳۳۵ ..... ۹-۳-۸- ارسال فایل‌ها به میزبان و بدوز: نسخه
- ۳۳۶ ..... ۹-۳-۹- مفهوم Pivoting

## فصل ۱۰: شمایی از صفر تا صد حمله ۳۴۵

- ۳۴۶ ..... ۱۰-۱- فاز اول حمله
- ۳۴۷ ..... ۱۰-۲- فاز دوم حمله
- ۳۴۸ ..... ۱۰-۳- فاز سوم حمله
- ۳۴۹ ..... ۱۰-۴- فاز چهارم حمله
- ۳۵۱ ..... ۱۰-۵- فاز پنجم حمله
- ۳۵۳ ..... ۱۰-۶- فاز ششم حمله
- ۳۵۵ ..... ۱۰-۷- فاز نهایی حمله