



سازدو اس ۴۸۶۳۴

برترین ابزارها و چهارچوب‌های هک در کالی لینوکس

مؤلف:

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

ناشر:

کانون نشر علوم

[illegible]

شماره: ۹۷۸۹۶۴۳۲۷۱۵۷۲

تلفن: ۶۶۹۶۱۵۶۸-۶۶۴۹۴۹۱۱



www.nashreloom.com

www.nashreloom.com

پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

سخن ناشر

به نام خداوند بخشنده و مهربان

گستره دانش بشر در ابر علم بی‌پایان و نامتناهی حضرت حق (جلّ جلاله) بسیار ناچیز است؛ همچنان که کلمه «و ما عطا نکردیم به شما علم را جز اندکی» شاهدهی است بر ضعف معرفت انسانی نسبت به رحمت صمدانی. با این حال چه نیکو سفارش فرموده است خاتم انبیاء، حضرت محمد مصطفی (ص)، که «جوید علم را اگر چه به سرزمین چین». این توصیه، تمامی پیروان راستین دین حبیب اسلام را به فراگیری و اکتساب علوم و فنون مختلف در همه زمان‌ها و همه مکان‌ها فرا می‌خواند.

تلاش کانون نشر علوم، همواره معطوف به تولید آثار ساینسی و بایسته در زمینه فنی و مهندسی بوده است؛ اگرچه که در این راه مشکلات و 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، خنجر بر کمر می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از قافله علم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجاهت علمی، در خواست‌های مخاطبین اندیشمند و قاضل نیز باشد. امید است که خداوند متعال در این مهم مساعدت فرماید.

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

در حال حاضر یکی از توزیع‌های قدرتمندی که مورد توجه نفوذگران، متخصصان آزمایش نفوذ و حتی کاربران حوزه شبکه و امنیت قرار دارد، توزیع لینوکس Kali می‌باشد که پشتیبان کامل و دقیقی از آن به‌عمل می‌آید. در واقع این توزیع لینوکس به نوعی نمای دست به‌خصوص حوزه امنیت و شبکه به‌حساب 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 به‌ویژه خود جزو برترین‌های حوزه هک می‌باشند و در روند انجام عملیات نفوذ و یا آزمایش کمک آزمایش‌کننده و یا نفوذگر می‌آیند و کار را برای آن‌ها ساده‌تر و سریع‌تر می‌کنند. از این به‌پای ابزارهای حرفه‌ای‌تری نیز وجود دارند که در قالب Frameworkها تحت توزیع ارائه شده‌اند که از قابلیت‌ها و امکانات فوق‌العاده‌ای برخوردار هستند.

در این کتاب سعی شده است تا به بررسی و تحلیل ابزارها و Frameworkهای حرفه‌ای و برتر موجود در توزیع لینوکس Kali پرداخته شود و از آن‌ها در جهت پیاده‌سازی یک حمله و خط‌مشی حملات هکری استفاده گردد. در واقع در این کتاب با کمک این ابزارهای قدرتمند انواع حملات مطرح در حوزه نفوذگری مورد بررسی و سنجش قرار گرفته است. لازم به‌ذکر است که تمامی حملات و مدل‌های حمله‌ای که در این کتاب ارائه شده است با کمک ابزارهای موجود در توزیع لینوکس Kali انجام گرفته است. البته برخی حملات حرفه‌ای هک نیز نیازمند ابزارها و Frameworkهای تکمیلی هک می‌باشند که به‌صورت پیش‌فرض بر روی توزیع لینوکس Kali نصب نمی‌باشند و باید بر روی این توزیع نصب گردند. نحوه استفاده و خط‌مشی پیاده‌سازی حملات نفوذگری با کمک ابزارهای تکمیلی در توزیع لینوکس Kali در قالب کتاب دیگری ارائه شده است که می‌توان از آن برای پیاده‌سازی آزمایشات نفوذ و انجام حملات هکری با کمک ابزارهای تکمیلی استفاده کرد. در این کتاب از تمامی منابع معتبر و پایه‌ای مربوط به توزیع لینوکس Kali و علم هک استفاده شده است که البته با تجزیهات 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 ابزارها و Framework های برتر پیش فرض در توزیع لینوکس Kali به منظور پیاده سازی آزمایش نفوذ بودم تا آن ها را با اصول فنی آزمایشات نفوذ با کمک این ابزارها آشنا و آگاه سازم و بتوان از آن ها در فرآیندها و پروژه های آزمایش نفوذ استفاده نمود (گرچه مدیران و متخصصین امنیت شبکه حکم اساتید اینجانب را دارند، اما به حکم وظیفه برخورد لازم دانستم که این آگاه سازی را انجام دهم.) همان طور که گفته شد، شیرازه اصلی کتاب عسر بر گرفته از کتاب ها و منابع معتبر در حوزه توزیع لینوکس Kali می باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به فرم کاملاً آزاد از مطالب و تجربیات گردآوری، دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام کاستی های آن را می پذیرم و ممنونم از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی های دلسوزانه آن ها را دیده متذکر هستم.

(m_Davari@TOP-co.ir)

(m_Davary@Parshack.zzn.com)

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

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

وز قول بد و فعل بد خود خجلم

یارب ز گناه زشت خود منفعلم

تا محو شود خیال باطل ز دلم

فیضی به دلم ز عالم قدس رسان

(مجید داوری دولت آبادی - پاییز ۱۳۹۵)



فهرست مطالب

فصل ۱: مفاهیم پایه‌ای در خصوص کالی لینوکس ۱۵

۱۶	 کالی لینوکس
۱۷	 خصوصیات و ویژگی‌های لینوکس Kali
۱۸	 تفاوت لینوکس و ویندوز
۱۹	 لینوکس Kali مخصوص نفوذگران و متخصصان امنیت
۱۹	 پیش‌نیازهای نصب لینوکس Kali
۱۹	 نحوه نصب لینوکس Kali

فصل ۲: ابزارهای ضروری در کالی لینوکس ۳۱

۳۲	 ابزار NetCat (nc)
۳۷	 ابزار Ncat
۳۸	 ابزار Wireshark
۴۲	 ابزار Tcpdump

فصل ۳: ابزارها و Frameworkهای جمع‌آوری اطلاعات ۴۵

۴۶	 خط‌مشی و روال عملی پیاده‌سازی مکانیزم جمع‌آوری اطلاعات
۴۶	 ابزارهای بررسی و شناسایی DNS
۵۰	 ابزارهای تعیین محدوده آدرس‌های IP
۵۳	 ابزارهای شناسایی سیستم‌های فعال در شبکه
۵۹	 ابزارهای پوشش پورت
۶۸	 ابزارهای بررسی و شناسایی SMB
۷۰	 ابزارهای بررسی و شناسایی SMTP
۷۲	 ابزارهای بررسی و شناسایی SNMP

فصل ۴: ابزارهای مخصوص استراق‌سمع و جعل ۸۱

۸۲	 خط‌مشی و روال عملی پیاده‌سازی حملات استراق‌سمع و جعل
۸۲	 ابزار DNSChuf
۸۴	 ابزار mitmproxy
۸۶	 ابزار HexInject
۸۸	 ابزار hamster-sidejack (hamster)



۸۹	ابزار Ferret
۹۰	ابزار iSMTP
۹۰	ابزار Yersinia
۹۲	ابزار macchanger
۹۳	ابزار netsniff-ng
۹۴	ابزار responder
۹۵	ابزار respoc
۹۸	ابزار WebDav
۹۹	ابزار SSLStrip
۱۰۰	ابزار SSLsplit
۱۰۵	ابزار Ettercap
۱۱۵	ابزار dsniff

فصل ۵: ابزارها و Frameworkهای تجزیه و تحلیل آسیب پذیری‌ها ۱۱۷

۱۱۸	خطمشی و روال عملی پیاده‌سازی مکانیزم‌های آسیب پذیری‌ها
۱۱۹	ابزار NMap
۱۲۰	ابزار Nessus
۱۲۵	ابزار OpenVAS
۱۳۷	ابزار MSF auxiliary modules
۱۳۸	ابزار BBQSQL
۱۳۹	ابزار BED
۱۴۰	ابزار DBPwAudit
۱۴۱	ابزار DotDotPwn
۱۴۲	ابزار HexorBase
۱۴۳	ابزار Inguma
۱۴۴	ابزار JSQZ
۱۴۶	ابزار Oscanner
۱۴۶	ابزار Powerfuzzer
۱۴۸	ابزار sqlmap
۱۵۵	ابزار Sqlninja
۱۶۵	ابزار sqlsus
۱۶۸	ابزار nikto

**فصل ۶: ابزارها و Framework های مخصوص بهره‌برداری ۱۷۱**

۱۷۲	خط‌مشی و روال عملی پیاده‌سازی مکانیزم‌های بهره‌برداری
۱۷۲	ابزار Backdoor Factory
۱۷۵	ابزار Metasploit
۱۸۱	ابزار Armitage
۱۸۳	ابزار BeEF
۱۹۲	ابزار mmix
۱۹۸	ابزار S.T
۲۰۷	ابزار searchsploit

فصل ۷: ابزارها و Framework ها- بهره‌داری دسترسی یا Post Exploitation ۲۰۹

۲۱۰	خط‌مشی و روال عملی پیاده‌سازی مکانیزم Post Exploitation
۲۱۰	ابزار CryptCat
۲۱۱	ابزار dbd
۲۱۱	ابزار Intersect
۲۱۴	ابزارهای PowerSploit
۲۲۷	ابزار pwnat
۲۲۸	ابزار sbd
۲۲۸	ابزار Weevely
۲۳۰	ابزار Mimikatz
۲۳۴	ابزار nishang

فصل ۸: ابزارهای مخصوص درهم شکستن کلمات عبور ۲۳۹

۲۴۰	خط‌مشی و روال عملی مکانیزم‌های درهم شکستن کلمات عبور
۲۴۰	ابزار chntpw
۲۴۲	ابزار CmosPwd
۲۴۵	ابزار crunch
۲۴۷	ابزار findmyhash
۲۴۸	ابزار hash-identifier
۲۴۹	ابزار Unshadow و john the ripper
۲۵۱	ابزار Hydra
۲۵۳	ابزار medusa



۲۵۵	ابزار keimpx
۲۵۶	ابزار Ncrack
۲۵۷	ابزار patator
۲۵۸	ابزار acccheck
۲۵۹	ابزار CeWL
۲۶۰	مجموعه ابزارهای RainbowCrack
۲۶۲	ابزار RSFang
۲۶۲	ابزار SQLmap
۲۶۳	ابزار sqlmap
۲۶۳	ابزار hashcat

فصل ۹: ابزارها و Framework، ابزار علی، سامه‌های کاربردی تحت وب

۲۶۶	ختمشی و روال عملی حمله علیه سامه‌های کاربردی تحت وب
۲۶۶	ابزار Arachni
۲۶۸	ابزار BlindElephant
۲۶۹	ابزار Burp Suite
۲۷۷	ابزار DAVTest
۲۷۸	ابزار DIRB
۲۷۸	ابزار DirBuster
۲۸۱	ابزار fimap
۲۸۲	ابزار Grabber
۲۸۳	ابزار joomscan
۲۸۵	ابزار Paros
۲۸۹	ابزار Parsero
۲۹۰	ابزار plecost
۲۹۱	ابزار ProxyStrike
۲۹۴	ابزار Recon-ng
۲۹۹	ابزار Skipfish
۳۰۰	ابزار ua-tester
۳۰۰	ابزار Uniscan
۳۰۱	ابزار Vega
۳۰۷	ابزار w3af
۳۱۰	ابزار WebScarab



www.nashreloom.com

www.nashreloom.com

پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

۳۱۲	ابزار Webshag
۳۱۴	ابزار WebSploit
۳۱۸	ابزار Wfuzz
۳۱۹	ابزار WPScan
۳۲۲	ابزار XSSer
۳۲۳	ابزار owasp-zap یا Burp Proxy

فصل ۱۰: ابزارهای مخصوص حملات شبکه‌های بی‌سیم ۳۲۵

۳۲۶	خط‌مشی و روش عملیات حمله به شبکه‌های بی‌سیم
۳۲۶	مجموعه ابزارهای بسته Aircrack-ng
۳۴۲	ابزار Asleap
۳۴۳	ابزار Crunch
۳۴۴	ابزار Bully
۳۴۵	ابزار coWPAtty
۳۴۷	ابزار Pyrit
۳۵۱	ابزار Fern WIFI Cracker
۳۵۸	ابزار Ghost Phisher
۳۵۸	ابزار Kismet
۳۶۱	ابزار mdk3
۳۶۴	ابزار PixieWPS
۳۶۵	ابزار Wifi Honey
۳۶۵	ماژول Wifi Jammer در ابزار Websploit
۳۶۷	مجموعه ابزارهای Wifitap
۳۶۸	ابزار Wifite
۳۷۱	ابزار Reaver
۳۷۵	ابزار macchanger
۳۷۵	ابزار Bluelog
۳۷۷	ابزار BlueMaho
۳۷۸	ابزار Bluepot
۳۷۸	ابزار redfang
۳۷۹	ابزار Spooftooth
۳۸۰	نفوذ به شبکه‌های بی‌سیم مبتنی بر WEP
۳۸۳	نفوذ به شبکه‌های بی‌سیم مبتنی بر رمزنگاری WPA و WPA2



فصل ۱۱: ابزارها و Frameworkهای پزشکی دیجیتال ۳۸۹

۳۹۰	ابزار Autopsy
۳۹۱	ابزار Binwalk
۳۹۲	ابزار bulk-extractor
۳۹۳	ابزار chkrootkit
۳۹۴	ابزار ddrescue
۳۹۴	ابزار DFF
۳۹۷	ابزار Dumpzill
۳۹۸	ابزار Foremost
۳۹۸	ابزار fashdeep
۳۹۹	ابزار Galleta
۳۹۹	ابزار Guymager
۴۰۰	ابزار peepdf
۴۰۱	ابزار RegRipper
۴۰۲	ابزار pdfid
۴۰۳	ابزار Volatility
۴۰۴	ابزار Xplico

فصل ۱۲: ابزارهای نفوذهای سخت افزاری ۴۰۵

۴۰۶	خطمشی و روال عملی حمله به تجهیزات موبایلی
۴۰۶	ابزار apktool
۴۰۷	ابزار Sakis3G
۴۰۷	ابزار smali
۴۰۷	ابزار SPF
۴۱۴	نفوذ به تجهیزات موبایل مبتنی بر سیستم عامل اندروید

فصل ۱۳: ابزارهای مخصوص آزمایش بار ۴۱۵

۴۱۶	ابزار DHCPig
۴۱۶	ابزار FunkLoad
۴۱۷	ابزار Inundator
۴۱۷	ابزار rtpflood
۴۱۸	ابزار SlowHTTPTest
۴۱۹	ابزار t50
۴۱۹	ابزار THC-SSL-DOS



فصل ۱۴: ابزارهای مخصوص مهندسی معکوس ۴۲۱

۴۲۲		ابزار dex2jar
۴۲۳		ابزار edb-debugger
۴۲۴		ابزار jad
۴۲۵		ابزار javasnoop
۴۲۶		ابزار JRegrind

فصل ۱۵: ابزارهای مخصوص گزارش گیری ۴۲۹

۴۳۰		ابزار cutycapt
۴۳۰		ابزار Dradis
۴۳۱		ابزار KeepNote
۴۳۲		ابزار MagicTree
۴۳۳		ابزار Metagoofil
۴۳۴		ابزار Nipper-ng
۴۳۴		ابزار papal

فصل ۱۶: بررسی کامل یک سناریوی حمله ۴۳۷

۴۳۸		فاز صفر حمله - تشریح سناریوی حمله
۴۳۹		فاز یک حمله - جمع آوری اطلاعات
۴۳۹		فاز دوم حمله - شناسایی آسیب پذیری و اولویت بندی ها
۴۴۲		فاز سوم حمله - تحقیق و توسعه
۴۴۲		فاز چهارم حمله - بهره برداری و سوء استفاده
۴۴۴		فاز پنجم حمله - نگهداری دسترسی با مکانیزم Post-Exploitation
۴۵۵		منابع و مراجع