راهنمای

تست نفوذ وب با

Kali Linux 2

Web Penetration Testing Cookbook

گیلبرتو ناجرا- گوتی یرز

برگردان:

مهندس مهران تاجبخش

انتشارات پندار پارس

شابک : 978-600-8201-25-0 : ۲۴۰۰۰۰ ریال با لوح ویدیویی دیجیتال
شماره کتابشناسی ملی : ۴۴۹۸۰۳۹
عنوان و نام پدیدآور : راهنمای تست نفوذ وب با Kali Linux 2= Web penetration resting cookbook/ گیلبرتو ناجرا- گوتی‌یرز؛ برگردان مهران تاجبخش.
مشخصات نشر : تهران : پندار پارس، ۱۳۹۵.
مشخصات ظاهری : ۲۷۲ ص.: مصور، جدول + یک لوح ویدیویی دیجیتال.
یادداشت : عنوان اصلی: Kali Linux web penetration testing cookbook, 2016.
موضوع : سیستم عامل لینوکس
موضوع : Linux
موضوع : آزمایش نفوذ (ایمن‌سازی کامپیوتر)
موضوع : Penetration testing (Computer security)
رده بندی دیویی : ۰۰۵/۴۳۲
رده بندی کنگره : QA۷۶/۷۶ ۱۳۹۵ ۲ن۹۴س/
سرشناسه : ناخرا-گوتیرث، خیلبرتو
Nájera-Gutiérrez, Gi[illegible]
شناسه افزوده : [illegible]بخش، مهران، ۱۳۴۷ -، مترجم
وضعیت فهرست نویسی : فیپا

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کو[illegible]شی، شماره ۱۴، واحد ۱۶
تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹[illegible]
info@pendarepars.com
www.pendarepars.com

نام کتاب : راهنمای تست نفوذ وب با Kali Linux 2
ناشر : انتشارات پندار پارس
تالیف : گیلبرتو ناجرا- گوتی یرز
برگردان : مهران تاجبخش
چاپ نخست : دی ماه ۹۵
شمارگان : ۵۰۰ نسخه
طرح جلد : رامین شکرالهی
چاپ، صحافی : روز
قیمت : ۲۴۰۰۰ تومان به همراه DVD
شابک : ۰-۲۵-۸۲۰۱-۶۰۰-۹۷۸

فهرست

فصل ۱: نصب و آماده‌سازی سیستم‌عامل ۱

به‌روزرسانی و ارتقای سیستم‌عامل Kali Linux ۱

نصب و راه‌اندازی نرم‌افزار "OWASP Mantra" ۴

نصب و راه‌اندازی نرم‌افزار ماشین مجازی VirtualBox ۹

نصب و راه‌اندازی ماشین مجازی قابل نفوذ (طعمه/هدف) ۱۰

نصب و راه‌اندازی ماشین مهاجم (حمله کننده) ۱۳

تنظیم ماشین‌های مجازی برای برقراری ارتباط مناسب ۱۵

بررسی نرم‌افزارهای موجود در ماشین مجازی قابل نفوذ (سرویس دهنده) ۱۹

فصل ۲: بررسی و شناسایی ۲۳

بررسی و شناسایی سرویس‌های هدف با استفاده از Nmap ۲۴

تعیین فایروال مورد استفاده در نرم‌افزار کاربردی تحت وب ۲۷

مشاهده و بررسی کد برنامه‌های سمت کاربر ۲۹

استفاده از افزونه "Firebug" برای بررسی و تغییر عملکرد صفحه تارنما ۳۱

جمع آوری و تغییر در محتویات کوکی‌ها ۳۳

استفاده از قابلیت‌های فایل "robots.txt" ۳۵

پیدا کردن فایل‌ها و پوشه‌ها با استفاده از نرم‌افزار "DirBuster" ۳۷

فهرست برداری از واژگان مناسب برای حدس رمز عبور با استفاده از CeWL ۴۰

استفاده از فناوری "John the Ripper" برای تولید فهرست واژگان (Dictionary) ۴۲

پیدا کردن فایل‌ها و فهرست‌ها با استفاده از "ZAP" ۴۴

فصل ۳: فهرست کننده‌ها و ابزارهای رهگیری زنجیره‌های ارتباطی تارنماها ۴۹

دریافت محتویات صفحه تارنما برای بررسی و آنالیز غیر برخط با استفاده از "Wget" ۵۱

دریافت محتویات صفحه تارنما برای بررسی و آنالیز غیربرخط با استفاده از "HTTrack" ۵۳

استفاده از نرم‌افزار "ZAP's spider" ۵۵

جست‌وجو و جمع‌آوری اطلاعات از تارنما (Crawling) با استفاده از نرم‌افزار "BurpSuite" ۵۸
تکرار درخواست‌ها با استفاده از نرم‌افزار "BurpSuite" ۶۱
استفاده از نرم‌افزار "WebScarab" ۶۴
مشخص کردن فایل‌ها و پوشه‌های مرتبط از اطلاعات نسخه‌برداری شده در فناوری "Crawling" ۶۷
فصل ٤؛ یافتن نقاط ضعف ۷۱
استفاده از افزونه "Hackbar" برای دسترسی و تغییر در متغیرهای صفحه تارنما ۷۲
استفاده از افزونه "Tamper Data" برای نسخه‌برداری از درخواست‌ها و تغییر در آنها ۷۴
استفاده از نرم‌افزار "ZAP" برای تغییر در درخواست‌ها ۷۶
استفاده از نرم‌افزار "BurpSuite" برای مشاهده و تغییردرخواست‌ها ۸۰
مشخص کردن نفوذپذیری بر اساس انتقال کد میان تارنماها (XSS) ۸۲
تشخیص آسیب‌پذیری تزریق "SQL" بر اساس بروز خطا ۸۶
شناسایی آسیب‌پذیری تزریق "SQL" کور (Blind SQL Injection) ۸۹
تشخیص آسیب‌پذیری در فایل‌های کوکی ۹۱
جمع‌آوری اطلاعات در ارتباط با پروتکل‌های "SSL/TLS" با استفاده از نرم‌افزار "SSLScan" ۹۳
بررسی امکان افزودن فایل به محتوای تارنما (File Inclusion) ۹۶
تشخیص آسیب‌پذیری "Poodle" ۹۹
فصل ٥؛ اسکنرهای خودکار ۱۰۱
اسکن آسیب‌پذیری با استفاده از نرم‌افزار "Nikto" ۱۰۲
شناسایی آسیب‌پذیری‌ها با استفاده از نرم‌افزار "Wapiti" ۱۰۴
استفاده از نرم‌افزار "OWASP ZAP" برای کنترل آسیب‌پذیری ۱۰۸
بررسی آسیب‌پذیری با استفاده از نرم‌افزار "w3af" ۱۱۲
استفاده از نرم‌افزار "Vega" برای بررسی آسیب‌پذیری ۱۱۶
بررسی و شناسایی آسیب‌پذیری نرم‌افزارهای تحت وب با استفاده از "Metasploit's Wmap" ۱۱۹
فصل ٦؛ استفاده از آسیب‌پذیری‌ها برای نفوذ - مقدماتی ۱۲۳

استفاده مخرب از افزودن و بارگذاری فایل ۱۲۴
استفاده از آسیب‌پذیری تزریق فرمان‌های سیستم‌عامل ۱۲۸
استفاده از آسیب‌پذیری به تزریق متغیر از خارج در "XML" ۱۳۲
کشف گذرواژه با استفاده از فناوری "Brute Force" و نرم‌افزار "HTC-Hydra" ۱۳۵
کشف رمز با استفاده از فناوری "Dictionary" و نرم‌افزار "BurpSuite" ۱۳۹
جمع آوری اطلاعات از کوکی‌های جلسات با استفاده از آسیب‌پذیری "XSS" ۱۴۵
گام به گام حمله تزریق "SQL" مقدماتی ۱۴۹
یافتن آسیب‌پذیری تزریق "SQL" و استفاده از نرم‌افزار "SQLMap" ۱۵۳
حمله کشف رمز سرویس هدف و "Tomcat" با استفاده از "Metasploit" ۱۵۸
استفاده از نرم‌افزار مدیریت "Tomcat" برای اجرای کد مخرب ۱۶۱
فصل ۷؛ استفاده از آسیب‌پذیری‌ها برای نفوذ - پیشرفته ۱۶۵
جست‌وجو در "Exploit-DB" برای یافتن اکسپلویت‌های موجود در سرویس‌دهنده‌های وب ۱۶۶
استفاده از آسیب‌پذیری "Heartbleed" برای نفوذ ۱۶۸
استفاده از آسیب‌پذیری "XSS" و نرم‌افزار "BeFF" برای نفوذ ۱۷۲
استفاده از آسیب‌پذیری تزریق "SQL" کورکورانه برای نفوذ ۱۷۷
استفاده از ابزار "SQLMap" برای دریافت اطلاعات از بانک اطلاعاتی ۱۸۲
حمله بر اساس دست‌کاری و گول زدن در درخواست بین تارنما ۱۸۵
اجرای فرمان با استفاده از ابزار "Shellshock" 191
باز گشایی رمز در هم ریخته شده (Hash) با استفاده از فناوری "John the Ripper" و فهرست واژگان کاندید (Dictionary) ۱۹۵
بازگشایی رمز درهم ریخته شده (Hash) با استفاده از فناوری "Brute Force" و "oclHashcat/cudaHashcat" ۱۹۷
فصل ۸؛ حملات مرد میانی (MITM) ۲۰۱
حمله گول زدن با استفاده از نرم‌افزار "Ethercap" ۲۰۲

حمله مردمیانی با استفاده از نرم‌افزار"Wireshark" و نسخه‌برداری از ترافیک..... ۲۰۵
تغییر در محتوای ترافیک بین سرویس‌دهنده و سرویس گیرنده..... ۲۰۸
حمله مردمیانی در ترافیک "SSL"..... ۲۱۲
دست یابی به اطلاعات ترافیک "SSL" با استفاده از نرم‌افزار "SSLsplit"..... ۲۱۴
حمله گون زدن سرویس‌دهنده "DNS" و تغییر مسیر در ترافیک..... ۲۱۷
فصل ۹: حملات سمت کاربر و مهندسی اجتماعی..... ۲۲۱
ایجاد ابزاری برای جمع آوری گذرواژه‌ها با استفاده از "SET"..... ۲۲۲
ایجاد پوسته رخط فرمان معکوس با استفاده از "Metasploit" و نسخه برداری از ترافیک..... ۲۲۹
استفاده از ابزار "browser_autopwn2" در نرم‌افزار "Metasploit" برای حمله به کاربر..... ۲۳۲
حمله با استفاده از "BeEF"..... ۲۳۵
وادارکردن کاربر برای ورود به تارنما..... ۲۳۸
فصل ۱۰: مقابله با ده مورد از بیشترین آسیب‌پذیری‌های وب (OWASP - TOP 10)..... ۲۴۱
A1- مقابله با حمله تزریق..... ۲۴۲
A2- ایجاد سیستم تأیید هویت و مدیریت ارتباط مناسب..... ۲۴۵
A3-مقابله با حمله انتقال کد بین تارنما (XSS)..... ۲۴۸
A4- مقابله با ارجاع مستقیم به محتواها به صورت غیر امن..... ۲۵۰
A5- راهنمای تنظیمات اولیه امنیتی..... ۲۵۱
A6- محافظت از داده‌های مهم و حساس..... ۲۵۴
A7- اطمینان از سطح دسترسی مناسب بر حسب عملکرد..... ۲۵۶
A8- مقابله با حمله "CSRF"..... ۲۵۷
A9- کجا در مورد آخرین نفوذپذیری‌ها جست‌وجو کنیم..... ۲۵۹
A10- اعتبارسنجی غیر مستقیم..... ۲۶۱

پیش گفتار

سادگی دسترسی به اینترنت از طریق انواع رایانه‌های رومیزی و سیستم‌های هوشمند همراه، همچون نوت‌بوک‌ها و تلفن‌های همراه و تبلت‌ها، باعث شده است که استفاده از شبکه وب و نرم‌افزارهای کاربردی تحت وب در خانه، محل کار و مکان‌های عمومی روز به روز گسترش یابد. در این میان حملات و نفوذ به این شبکه و نرم‌افزارها و فناوری‌های موجود در آن نیز هم به لحاظ کمی و هم کیفی رشد بی سابقه‌ای پیدا کرده است.

هزینه جرائم فضای مجازی ناشی از سرقت و دست کاری داده‌های سازمان، موسسات و افراد تا سال ۲۰۱۹ به بیش از ۲,۱ تریلیون دلار بالغ خواهد شد

تحقیق توسط کمپانی جونیپر - منتشر شده توسط موسسه تحقیقاتی گارتنر

در این میان وظیفه متخصصان امنیت و تست نفوذ برای شناسایی و پیشگیری از حملات و نفوذپذیری‌های موجود در این شبکه و نرم‌افزارهای مورد استفاده در آن بسیار مهم و حائز اهمیت می‌باشد.

با توجه به اینکه شکل و نوع تهدیدها و نفوذپذیری‌ها دائما در حال تغییر است، بنابراین یک متخصص تست نفوذ می‌بایست به صورت روزآمد با ابزارها و فناوری‌های موجود در حوزه تست نفوذ در این بخش آشنایی داشته باشد.

این کتاب تلاش دارد تا با ارائه آخرین فناوری‌ها، ابزارها و روش‌های موجود در حوزه تست نفوذ وب با استفاده از یکی از بهترین سیستم عامل‌های موجود در این بخش یعنی سیستم عامل کالی لینوکس، اطلاعات کاملی را به صورت عملی و کاربردی ارائه نماید.

چه مطالبی را در این کتاب خواهید آموخت

در این کتاب مطالب در ۱۰ فصل ارائه شده است که به طور خلاصه عبارتند از:

فصل نخست به چگونگی ایجاد و تست و راه‌اندازی آزمایشگاه تست نفوذ به همراه ابزارها و نرم‌افزارهای مورد نیاز با آخرین ویرایش سیستم عامل کالی (نسخه ۲) و سیستم هدف حرفه‌ای سیستم عامل ویندوز می‌پردازد.

فصل‌های دوم و سوم به یکی از مهم‌ترین مراحل در اجرای یک پروژه تست نفوذ که جمع‌آوری اطلاعات اولیه از هدف موردنظر می‌باشد، پرداخته است.

فصل‌های چهارم و پنجم به بررسی و آنالیز اطلاعات به‌دست آمده و دست‌یابی و شناسایی نقاط ضعف موجود در آنها می‌پردازد. این مرحله در پروژه تست نفوذ نخستین قدم عملیاتی برای تعیین و انتخاب استراتژی حمله و نفوذ به سیستم هدف می‌باشد.

فصل‌های ششم و هفتم نیز به معرفی ابزارها و روش‌های حمله و نفوذ با استفاده از نقاط ضعف شناسایی شده در سیستم هدف پرداخته شده است. فناوری‌های ارائه شده در این مرحله در دو بخش مقدماتی و پیشرفته طبقه‌بندی شده‌اند.

با توجه به اینکه حملات مرد میانی (MiTM) و همچنین مهندسی اجتماعی به منظور جمع‌آوری اطلاعات و پیدا کردن نقاط ضعف سیستم‌های هدف، بسیار متداول و معمول می‌باشند و همچنین این حملات عمدتا در سمت کاربر و یا به دلیل ضعف در تنظیم و پیکربندی فناوری‌های مورد استفاده رخ می‌دهد، سعی کرده‌ایم تا این موارد را در فصل‌های هشتم و نهم با جزئیات بیشتر ارائه نماییم تا متخصصان تست نفوذ به طور دقیق‌تر و کامل‌تر با روش‌های حمله و نفوذ در این بخش آشنا شوند تا آن را در سیستم هدف مورد نظر خود به کار ببرند.

و سرانجام در فصل پایانی ده مورد از بیشترین آسیب‌پذیری‌هایی که شبکه و نرم‌افزارهای تحت وب را تهدید می‌کنند را معرفی کرده و برای کمینه کردن ضعف‌ها و حملات ناشی از آنها، راه‌کارهایی را ارائه داده‌ایم . این آسیب‌پذیری‌ها به طور سالیانه بر اساس تحقیقات انجام شده توسط موسسه Offensive Security انجام می‌گیرد و با نام OWASP Top 10 ارائه می‌شود.

این کتاب برای چه کسانی است

با توجه به اینکه آشنایی با روش‌های جمع‌آوری اطلاعات و شناسایی نقاط ضعف و آسیب‌پذیری‌ها و همچنین ابزارها و فناوری‌هایی که برای نفوذ استفاده می‌شوند، برای همه متخصصان امنیت و تست نفوذ و ادله الکترونیک لازم و ضروری است، بنابراین مطالعه این کتاب به همه این گروه‌ها توصیه می‌شود. هرچند، این کتاب می‌تواند برای همه کسانی که در حوزه پیاده‌سازی نرم‌افزارهای تحت وب و یا افرادی که در حوزه امنیت فضای مجازی به‌ویژه اینترنت و شبکه وب وارد شده‌اند نیز مفید باشد.

برای استفاده مناسب از مطالب ارائه شده در این کتاب، آشنایی با مفاهیم و ساختار و پروتکل‌های اینترنت و وب و همچنین سیستم عامل‌های لینوکس و ویندوز لازم و ضروری می‌باشد.

درباره مترجم

با بیش از ۲۶ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه، در حدود ۱۰ سال است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و فضای مجازی و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت دارد و دارای مدارک بین المللی فراوانی در حوزه شبکه، امنیت شبکه و تست نفوذ است که عبارت‌اند از:

Network+, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW security Professional, ISO27001 Lead Auditor.

برای برقراری ارتباط با ایشان می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com