بسم الله الرحمن الرحیم

تست نفوذ در وب
با اژدهای لینوکس

جوناید احمد انصاری

ترجمه و تالیف:

مهندس ارسطو مدیری

سرشناسه	: انصاری، جونید احمد	Ansari, Juned Ahmed
عنوان و پدیدآور	: تست نفوذ در وب با اژدهای لینوکس/[جونیداحمد انصاری]؛ مترجم ارسطو مدیری.	
مشخصات نشر	: اهواز: ترآوا، ۱۳۹۶.	
مشخصات ظاهری	: ۳۱۲ ص.: مصور، جدول، نمودار.	
شابک	: ۹۷۸-۶۰۰-۳۴۷-۲۲۷-۳	
وضعیت فهرستنویسی	: فیپا	
یادداشت	: عنوان اصلی:	Web Penetration Testing with Kali Linux,2nd ed,2015
موضوع	: سیستم عامل لینوکس Linux	
موضوع	: وبگاه‌ها –ارزشیابی	Web sites -- Evaluatio
موضوع	: وبگاه‌ها – آزمایش	Web sites-- Testing
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی	Computer networks -- Security measures
موضوع	: آزمایش نفوذ (ایمن‌سازی کامپیوتر)	Penetration testing (Computer security)
شناسه افزوده	: مدیری ، ارسطو ، ۱۳۵۶ -	
رده بندی کنگره	: QA /۷۶/۷۶/س۹۴الف۸ ۱۳۹۶	
رده بندی دیویی	: ۰۰۵/۴۳۲	
شماره کتابشناسی ملی	۴۶۷۵۸۶۶	

تست نفوذ در وب با اژدهای لینوکس

نویسنده: جونید احمد انصاری

ترجمه و تألیف: ارسطو مدیری

ایده‌ی طرح روی جلد و صفحه‌آرایی: مریم بخیت

اجرای طرح روی جلد: محمد محمدعلی پورویس

ناشر: ترآوا

شماره‌ی نشر: ۴۷۵

نوبت چاپ: اوّل/ ۱۳۹۶

تیراژ: ۱۰۰۰ نسخه

شابک: ۳-۲۲۷-۳۴۷-۶۰۰-۹۷۸

قیمت: ۲۴۰۰۰ تومان

نشر ترآوا: اهواز- کیانپارس- خیابان نهم غربی- پلاک ۱۲۸

نمابر: ۰۶۱۳۳۹۰۳۷۱۴ همراه: ۰۹۱۶۱۱۳۶۷۸۵

Taravapublication@yahoo.com

فروشگاه اینترنتی: www.tarava.com

taravapub

فهرست مطالب

مقدمه

توزیع لینوکس کالی بطور وسیعی در زمینه‌های حرفه ایی امنیت بکار می‌رود که مجموعه ایی از ابزارهای موثر در خصوص ارزیابی امنیت را در خود جا دارد و در مراحل مختلف تست نفوذ مانند جمع آوری اطلاعات، آسیب پذیری‌ها و مرحله بهره‌برداری از آسیب پذیری (*exploitation*) کاربرد دارند.

Web App ها در قسمت‌های مختلف شبکه قرار دارند و هنگام اجرای ارزیابی‌های امنیت باید به آنها اهمیت داده شود.

تست نفوذ با کالی برای تست کننده نفوذ شبکه که می‌خواهد *web App* را هک کند بخوبی طراحی شده است.

هدف، در این کتاب بدست آوردن دریک در خصوص حفره‌های امنیتی مختلف که در *web app*ها وجود داشته و استفاده از ابزارهای لینوکس کالی برای شناسایی آسیب پذیری هایشان ودر نهایت بهره‌برداری آن هاست فصول این کتاب بر اساس مراحلی که لازم است برای تست نفوذ در دنیای واقعی بکار روند طراحی شده اند کتاب با تشریح ایجاد بلوک‌های تست نفوذ سپس برپایی آزمایشگاهی با لینوکس کالی ۲ در فصل‌های بعدی ما را مرحله به مرحله تا رسیدن به یک تست کننده حرفه ایی نفوذ با استفاده از ابزارهای کالی هدایت می‌کند.

آنچه این کتاب پوشش می‌دهد:

فصل ۱، به معرفی تست نفوذ و *web App*ها، انواع روشها و روالهای حرفه ای امنیتی برای ارزیابی *web App*ها می‌پردازد و مروری بر ساختار بلوک‌های *web App* و پروتکل *http* انجام می‌دهد.

فصل ۲، برپایی آزمایشگاه کالی لینوکس، در این فصل روشهای نصب کالی و همچنین برپایی یک آزمایشگاه فراگرفته می‌شود و ابزارهای مهم و برپایی *Tor* برای ارتباط تزریح داده می‌شود.

فصل ۳، شناسایی و پروفایل کردن *web server*، این فصل روی مرحله جمع آوری اطلاعات تاکید دارد و از ابزارهای کالی برای تشخیص فعال (*Active*) و غیرفعال (*Passive*) استفاده می‌کند و شناسایی سیستم عامل، نسخه *App*ها و اطلاعات اضافی که برای مراحل بعدی تست نفوذ موردنیاز است می‌پردازد.

فصل ٤، حفره‌های مهم در *web App*، حفره‌های امنیتی در سطوح مختلف برای *web App*ها توضیح داده می‌شود. در این فصل حفره‌ها امنیتی با اهمیت کمتر مانند نشت اطلاعات شروع و به اهمیت بالاتر مانند حفره‌های تزریق (*Injection*) می‌رسیم.

فصل ٥، حمله به سرور با استفاده از حفره‌های تزریق مبنا، در خصوص تقریبا تمام فرمان‌های تزریق، حفره‌های تزریق *SQL* بحث می‌شود و یک درک عمیق از حفره تزریق و نحوه استفاده از آن توسط *Metasploit* فراگیری می‌شود و نیز در خصوص حملات بالقوه حفره تزریق *SQL* و استفاده از ابزارهای کالی برای بهره‌برداری از آن پرداخته می‌شود.

فصل ٦، بهره‌برداری از *Client*ها با استفاده از حفره‌های *XSS* و *CSRF*، در این فصل تاکید بر حمله *XSS* است و از ابزارهای کالی برای پویش خودکار *web App*ها برای *XSS* استفاده می‌شود و در بخش *CSRF* روش حمله و استفاده از ابزارها برای بهره‌برداری از آن تشریح می‌شود.

فصل ۷، حمله به وب سایتهای *SSL* ـ مبنا، در خصوص شناسایی پیاده سازی‌های ضعیف *SSL* و استفاده از حمله مردمیانی (*Man – in – the – Middle*) در ارتباطات *SSL* توضیحاتی داده می‌شود.

فصل ۸، بهره‌برداری از *Client* با استفاده از فریم ورک‌های حمله، تکنیک‌ها و حیله‌های مختلفی برای تحت کنترل گرفتن کامپیوترهای *Client* توضیح داده می‌شود و از مهندسی اجتماعی (*Social Engineering Toolkit*) برای حمله *Phishing* با ابزارهای کالی استفاده می‌کنیم و در بخش دیگر از *Browser exploitation Framework (BeEF)* برای تحت کنترل گرفتن *Browser* کاربر با استفاده از حفره *XSS* استفاده خواهیم کرد و نیز ماژول‌های مختلف *BeEF* را توضیح می‌دهیم.

فصل ۹، *AJAX* و وب سرویس‌ها ـ موضوعات امنیتی، حفره‌های امنیتی اپلیکشن‌های *AJAX* و ارزیابی آنها توضیح داده خواهد شد و سرویس‌های وب بهمراه موضوعات امنیتی آنها در این فصل تشریح می‌شوند.

فصل ۱۰، *Fuzzing web App*، انواع تکنیک‌های *Fuzzing* معرفی می‌شود و با متدهای مختلف شناسایی حفره‌های وب *App*ها با استفاده از *Fuzzing* آشنا می‌شویم و در مرحله بعد *Fuzzer* که در لینوکس کالی است بنام *Burp Intruder*، برای *Fuzz* کردن یک *Web App* بکار برده می‌شود.

آنچه برای این کتاب لازم است:

این کتاب برای کسانیکه تست کننده نفوذ هستند و قصد دارند دانش خود را برای نفوذ در *Web APP* توسعه دهند بسیار مناسب است و کسانیکه علاقه مند به یادگیری ابزارهای لینوکس کالی و کاربرد آنها در تست *Web App* هستند نیز می‌توان مورداستفاده قرار گیرد.