

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 ناچرا-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 (ایمن سازی کامپیوتر)
موضوع	: Penetration testing (Computer security)
رده بندی دیوبی	: ۰۰۵/۴۳۲
رده بندی کنگره	: QA۷۶/۷۶ ۱۳۹۵ ۲ن۹۴س/
سرشناسه	: ناخرا-گوتییرز، خیلبرتو Nájera-Gutiérrez, Gilberto
شناسه افزوده	: تاجبخش، مهران، ۱۳۴۷ - مترجم
وضعیت فهرست نویسی	: فیپا

انتشارات پندار پارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴

info@pendarepars.com

www.pendarepars.com

نام کتاب : راهنمای تست نفوذ وب با Kali Linux 2

ناشر : انتشارات پندار پارس

تالیف : گیلبرتو ناچرا-گوتییرز

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 : ۹۷۸-۶۰۰-۸۲۰۱-۲۵-۰

هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد

تقدیرم به مادرم

به خاطر زحمات بی دریغش

و پسرم

که مایه امید و انرژی من است

فهرست

۱	فصل ۱؛ نصب و آماده‌سازی سیستم‌عامل
۱	به‌روزرسانی و ارتقای سیستم‌عامل Kali Linux
۴	نصب و راه‌اندازی نرم‌افزار "OWASP Mantra"
۹	نصب و راه‌اندازی نرم‌افزار ماشین مجازی VirtualBox
۱۰	نصب و راه‌اندازی ماشین مجازی قابل نفوذ (طعمه/هدف)
۱۳	نصب و راه‌اندازی ماشین مهاجم (حمله‌کننده)
۱۵	تنظیم ماشین‌های ماشین‌های مجازی برای برقراری ارتباط مناسب
۱۹	بررسی نرم‌افزارهای موجود در ماشین مجازی قابل نفوذ (سرویس دهنده)
۲۳	فصل ۲؛ بررسی و شناسایی
۲۴	بررسی و شناسایی سرویس‌های هدف با استفاده از Nmap
۲۷	تعیین فایروال مورد استفاده در نرم‌افزار کاربردی تحت وب
۲۹	مشاهده و بررسی کد برنامه‌های سمت کاربر
۳۱	استفاده از افزونه "Firebug" برای بررسی و تغییر عملکرد صفحه تارنما
۳۳	جمع‌آوری و تغییر در محتویات کوکی‌ها
۳۵	استفاده از قابلیت‌های فایل "robots.txt"
۳۷	پیدا کردن فایل‌ها و پوشه‌ها با استفاده از نرم‌افزار "DirBuster"
۴۰	فهرست برداری از واژگان مناسب برای حدس رمز عبور با استفاده از CeWL
۴۲	استفاده از فناوری "John the Ripper" برای تولید فهرست واژگان (Dictionary)
۴۴	پیدا کردن فایل‌ها و فهرست‌ها با استفاده از "ZAP"
۴۹	فصل ۳؛ فهرست‌کننده‌ها و ابزارهای رهگیری زنجیره‌های ارتباطی تارنماها
۵۱	دریافت محتویات صفحه تارنما برای بررسی و آنالیز غیربرخط با استفاده از "Wget"
۵۳	دریافت محتویات صفحه تارنما برای بررسی و آنالیز غیربرخط با استفاده از "HTTrack"
۵۵	استفاده از نرم‌افزار "ZAP's spider"

۵۸	جست‌وجو و جمع‌آوری اطلاعات از تارنما (Crawling) با استفاده از نرم‌افزار "BurpSuite"
۶۱	تکرار درخواست‌ها با استفاده از نرم‌افزار "BurpSuite"
۶۴	استفاده از نرم‌افزار "WebScarab"
۶۷	مشخص کردن فایل‌ها و پوشه‌های مرتبط از اطلاعات نسخه‌برداری شده در فناوری "Crawling"
۷۱	فصل ۴؛ یافتن نقاط ضعف
۷۲	استفاده از افزونه "Hackbar" برای دسترسی و تغییر در متغیرهای صفحه تارنما
۷۴	استفاده از افزونه "Tamper Data" برای نسخه‌برداری از درخواست‌ها و تغییر در آنها
۷۶	استفاده از نرم‌افزار "ZAP" برای تغییر در درخواست‌ها
۸۰	استفاده از نرم‌افزار BurpSuite برای مشاهده و تغییردرخواست‌ها
۸۲	مشخص کردن نفوذپذیری بر اساس انتقال کد میان تارنماها (XSS)
۸۶	تشخیص آسیب‌پذیری تزریق "SQL" بر اساس بروز خطا
۸۹	شناسایی آسیب‌پذیری تزریق "SQL" کورکورانه (Blind SQL Injection)
۹۱	تشخیص آسیب‌پذیری در فایل‌های کوکی
۹۳	جمع‌آوری اطلاعات در ارتباط با پروتکل‌های "SSL/TLS" با استفاده از نرم‌افزار "SSLScan"
۹۶	بررسی امکان افزودن فایل به محتوای تارنما (File Inclusion)
۹۹	تشخیص آسیب‌پذیری "Poodle"
۱۰۱	فصل ۵؛ اسکنرهای خودکار
۱۰۲	اسکن آسیب‌پذیری با استفاده از نرم‌افزار "Nikto"
۱۰۴	شناسایی آسیب‌پذیری‌ها با استفاده از نرم‌افزار "Wapiti"
۱۰۸	استفاده از نرم‌افزار "OWASP ZAP" برای کنترل آسیب‌پذیری
۱۱۲	بررسی آسیب‌پذیری با استفاده از نرم‌افزار "w3af"
۱۱۶	استفاده از نرم‌افزار "Vega" برای بررسی آسیب‌پذیری
۱۱۹	بررسی و شناسایی آسیب‌پذیری نرم‌افزارهای تحت وب با استفاده از "Metasploit's Wmap"
۱۲۳	فصل ۶؛ استفاده از آسیب‌پذیری‌ها برای نفوذ - مقدماتی

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

۲۰۵	حمله مردمیانی با استفاده از نرم‌افزار "Wireshark" و نسخه‌برداری از ترافیک
۲۰۸	تغییر در محتوای ترافیک بین سرویس‌دهنده و سرویس‌گیرنده
۲۱۲	حمله مردمیانی در ترافیک "SSL"
۲۱۴	دست یابی به اطلاعات ترافیک "SSL" با استفاده از نرم‌افزار "SSLsplit"
۲۱۷	حمله گون زدن سرویس‌دهنده "DNS" و تغییر مسیر در ترافیک
۲۲۱	فصل ۹؛ حملات سمت کاربر و مهندسی اجتماعی
۲۲۲	ایجاد ابزاری برای جمع‌آوری گذرواژه‌ها با استفاده از "SET"
۲۲۹	ایجاد پوسته (خط فرمان) معکوس با استفاده از "Metasploit" و نسخه‌برداری از ترافیک
۲۳۲	استفاده از ابزار "browser_autpwn2" در نرم‌افزار "Metasploit" برای حمله به کاربر
۲۳۵	حمله با استفاده از "BeEF"
۲۳۸	وادارکردن کاربر برای ورود به تارنمای آلوده
۲۴۱	فصل ۱۰؛ مقابله با ده مورد از بیشترین آسیب‌پذیری‌های وب (OWASP - TOP 10)
۲۴۲	A1- مقابله با حمله تزریق
۲۴۵	A2- ایجاد سیستم تأیید هویت و مدیریت ارتباط مناسب
۲۴۸	A3- مقابله با حمله انتقال کد بین تارنما (XSS)
۲۵۰	A4- مقابله با ارجاع مستقیم به محتواها به صورت غیر امن
۲۵۱	A5- راهنمای تنظیمات اولیه امنیتی
۲۵۴	A6- محافظت از داده‌های مهم و حساس
۲۵۶	A7- اطمینان از سطح دسترسی مناسب بر حسب عملکرد
۲۵۷	A8- مقابله با حمله "CSRF"
۲۵۹	A9- کجا در مورد آخرین نفوذپذیری‌ها جست‌وجو کنیم
۲۶۱	A10- اعتبارسنجی غیر مستقیم

پیش‌گفتار

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 بی‌سابقه‌ای پیدا کرده است.

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

تحقیق توسط کمپانی جونپیر - 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 دائماً 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 و ابزارها و روش‌های موجود در حوزه تست نفوذ وب با استفاده از یکی از بهترین سیستم‌عامل‌های 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 عبارت‌اند 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 حاوی 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 عمدتاً 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

فصل ۱

نصب و آماده‌سازی سیستم‌عامل

مطالبی که در این فصل فرا خواهید گرفت:

- به‌روزرسانی و ارتقای سیستم‌عامل کالی لینوکس
- نصب و راه‌اندازی نرم‌افزار OWASP Mantra-
- راه‌اندازی مرورگر وب Iceweasel
- نصب نرم‌افزار ماشین مجازی VirtualBox
- ایجاد ماشین مجازی نفوذپذیر (طعمه/هدف)
- ایجاد ماشین مجازی تست کننده (مهاجم/هکر)
- تنظیم‌های مورد نیاز برای برقراری ارتباط مناسب میان سیستم‌های مهاجم و هدف
- تشخیص نرم‌افزارهای تحت وب موجود در ماشین مجازی نفوذپذیر (طعمه/هدف)

در این فصل به نصب و راه‌اندازی آزمایشگاه مورد نیاز برای تست نفوذ نرم‌افزارهای تحت وب با استفاده از سیستم‌عامل Kali Linux می‌پردازیم.

به‌روزرسانی و ارتقای سیستم‌عامل Kali Linux

پیش از بررسی امنیت نرم‌افزارهای تحت وب باید از به‌روز بودن تمامی ابزارهای مورد استفاده در آن مطمئن شویم. زیرا همه‌ی بررسی‌ها و آزمایش‌هایی که در ادامه به آن‌ها اشاره خواهیم کرد، بر اساس آخرین ویرایش نرم‌افزارها و ابزارهای موجود در سیستم‌عامل کالی می‌باشند.

در آغاز، فرض بر این است که لینوکس کالی به عنوان سیستم‌عامل اصلی بر روی کامپیوتر نصب شده است و سیستم مورد نظر به اینترنت دسترسی دارد. از سیستم‌عامل کالی نسخه 2.0 برای انجام آزمایش‌های تست نفوذ استفاده خواهیم کرد. می‌توانید نسخه‌های قابل نصب و یا اجرای زنده (Live) این سیستم‌عامل را از مسیر زیر دانلود کنید:

<https://www.kali.org/downloads>

چون فرض بر این است که پیش‌تر نسخه‌ای از سیستم‌عامل کالی را بر روی سیستم خود نصب کرده‌اید، آن را همانند شکل زیر فعال کرده و در پنجره خط فرمان، مراحل زیر را انجام دهید:

۱. به عنوان کاربر اصلی وارد شوید (Login as root). برای این کار می‌بایست فرمان زیر را وارد کنید (به طور پیش‌فرض، نام کاربری و رمز عبور کاربر ارشد در سیستم‌عامل کالی "root/toor" می‌باشد).

```
sudo su
```

۲. با استفاده از فرمان "apt-get update" همه نرم‌افزارها و ابزارهای موجود در کالی به‌روزرسانی خواهند شد. (با توجه به حجم به‌روزرسانی، انجام آن تا یک ساعت نیز در این مرحله به طول خواهد کشید.) بخشی از مراحل به‌روزرسانی در شکل زیر نشان داده شده است.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get update
Get:1 http://security.kali.org kali/updates Release.gpg [819 B]
Get:2 http://http.kali.org kali Release.gpg [819 B]
Get:3 http://security.kali.org kali/updates Release [11.0 kB]
Get:4 http://http.kali.org kali Release [21.1 kB]
Get:5 http://security.kali.org kali/updates/main Sources [159 kB]
Get:6 http://http.kali.org kali/main Sources [7,571 kB]
Get:7 http://security.kali.org kali/updates/contrib Sources [20 B]
Get:8 http://http.kali.org kali/non-free Sources [119 kB]
Get:9 http://security.kali.org kali/updates/non-free Sources [20 B]
Get:10 http://http.kali.org kali/contrib Sources [56.9 kB]
Get:11 http://security.kali.org kali/updates/main amd64 Packages [347 kB]
Get:12 http://http.kali.org kali/main amd64 Packages [8,475 kB]
Ign http://security.kali.org kali/updates/contrib Translation-en_US
Ign http://http.kali.org kali/contrib Translation-en_US
Ign http://security.kali.org kali/updates/contrib Translation-en
Ign http://http.kali.org kali/contrib Translation-en
Ign http://security.kali.org kali/updates/main Translation-en_US
Ign http://security.kali.org kali/updates/main Translation-en
Ign http://http.kali.org kali/main Translation-en_US
Ign http://security.kali.org kali/updates/non-free Translation-en_US
Ign http://http.kali.org kali/main Translation-en
Ign http://security.kali.org kali/updates/non-free Translation-en
Ign http://http.kali.org kali/non-free Translation-en_US

```

۳. پس از اینکه عملیات به‌روزرسانی ابزارها و نرم‌افزارهای اصلی به اتمام رسید، با استفاده از فرمان "apt-get upgrade" می‌توانیم برنامه‌های غیر سیستمی موجود در کالی را به جدیدترین نسخه آن‌ها ارتقا دهیم. نحوه انجام آن در شکل زیر نشان داده شده است.

```

root@kali: ~
File Edit View Search Terminal Help
Reading package lists... Done
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  aircrack-ng greenbone-security-assistant openvas openvas-cli openvas-manager openvas-scanner
  reaver w3af w3af-console
The following packages will be upgraded:
  arj automater burpsuite curl dnsmasq-base dpkg dpkg-dev exploitdb fern-wifi-cracker file fimap
  gnupg gpgv gstreamer0.10-plugins-bad hexinject icedtea-6-jre-cacao icedtea-6-jre-jamvm icoweasel
  javawsnoop keimpx laudanum libapache2-mod-php5 libavcodec53 libavdevice53 libavformat53
  libavutil51 libcurl3 libcurl3-gnutls libdpkg-perl libfreetype6 libfreetype6-dev libgcrpyt11
  libgd2-xpm libgnutls26 libgstreamer-plugins-bad0.10-0 libicu48 libldap-2.4-2 libmagic-dev
  libmagic1 libmysqlclient18 libnss3 libpostproc52 libruby1.8 libruby1.9.1 libssl-dev libssl-doc
  libssl1.0.0 libsvn1 libwvscale2 libtasn1-3 libx11-6 libx11-data libx11-dev libx11-doc
  libx11-xcbl libxfont1 libxal-libxal-perl libxal2 libxal2-dev libxal2-utils libxrender-dev
  libxrender1 mercurial mercurial-common metasploit metasploit-common metasploit-framework
  mysql-client-5.5 mysql-common mysql-server mysql-server-5.5 mysql-server-core-5.5 ntp
  openjdk-6-jdk openjdk-6-jre openjdk-6-jre-headless openjdk-6-jre-lib openjdk-7-jdk openjdk-7-jre
  openjdk-7-jre-headless openssl php5 php5-cli php5-common php5-mysql pipal ppp python-impacket
  python-libxal2 python-magic recon-ng responder ruby-ethon ruby-ffi ruby-typhoeus ruby1.8
  ruby1.8-dev ruby1.9.1 ruby1.9.1-dev set sqlite3 subversion tcpdump wpscan zapoxy
185 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
Need to get 640 MB of archives.
After this operation, 26.5 MB of additional disk space will be used.
Do you want to continue [Y/n]? Y

```

ارتقای نرم افزارهای غیر سیستمی

۴. در حین انجام آن ممکن است که برای ادامه عملیات به‌روزرسانی در بخش‌های گوناگون سوال شود که در پاسخ گزینه "y" را انتخاب می‌کنیم تا مراحل ارتقای نرم‌افزارها ادامه یابد. پس از پایان ارتقای نرم‌افزارهای غیر سیستمی، آخرین مرحله نوبت به به‌روزرسانی سیستم‌عامل کالی می‌رسد که برای انجام آن از فرمان "apt-get dist-upgrade" استفاده می‌کنیم. روش انجام آن را در شکل زیر مشاهده می‌کنید.

```

root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages will be REMOVED:
  libopenvas7
The following NEW packages will be installed:
  ieee-data libhiredis0.10 libjemalloc1 libopenvas8 pixiewps python-markdown python-vulndb
  redis-server
The following packages will be upgraded:
  aircrack-ng greenbone-security-assistant openvas openvas-cli openvas-manager openvas-scanner
  reaver w3af w3af-console
9 upgraded, 8 newly installed, 1 to remove and 0 not upgraded.
Need to get 29.2 MB of archives.
After this operation, 7,996 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://http.kali.org/kali/ kali/main libhiredis0.10 amd64 0.10.1-7 [23.7 kB]
Get:2 http://http.kali.org/kali/ kali/main greenbone-security-assistant amd64 6.0.1-0kali1 [

```

ارتقای قابل‌های اصلی سیستم‌عامل

اکنون سیستم‌عامل کالی به همراه ابزارهای موجود در آن آماده برای انجام عملیات تست نفوذ خواهند بود.

نکته: در سیستم‌عامل کالی، ابزارهای ویژه‌ای همچون "Metasploit" وجود دارند که برای به‌روزرسانی آنها باید از فرمان‌های ویژه استفاده شود (msfupdate).

نصب و راه‌اندازی نرم‌افزار "OWASP Mantra"

در پروژه امنیت نرم‌افزارهای متن باز تحت وب (OWASP - Open Web Application Security Project) از افزونه‌های موجود در نرم‌افزار Mozilla Firefox برای کمک به عملیات تست نفوذ و تولید نرم‌افزارهای تحت وب استفاده شده است. در این بخش می‌خواهیم به نحوه نصب و راه‌اندازی و همچنین آشنایی با برخی از ویژگی‌های نرم‌افزار "OWASP-Mantra" بپردازیم. (<http://www.getmatra.com>)

اغلب نرم‌افزارهای تحت وب از طریق مرورگر وب اجرا می‌شوند، به همین دلیل نرم‌افزارهای مورد نظر نیاز به یک مرورگر به همراه ابزارهای مناسب موجود در آن برای اجرا دارند. نرم‌افزار "OWASP Mantra" دارای افزونه‌های فراوانی است که با استفاده از آنها می‌توانیم عملیات زیر را انجام دهیم:

- رصد و نسخه‌برداری از ترافیک‌های درخواست "HTTP"
- اشکال‌یابی از کدهای نرم‌افزار سمت کاربر
- مشاهده و تغییر در کوکی‌ها
- جمع‌آوری اطلاعات در مورد تارنماها و نرم‌افزارهای تحت وب

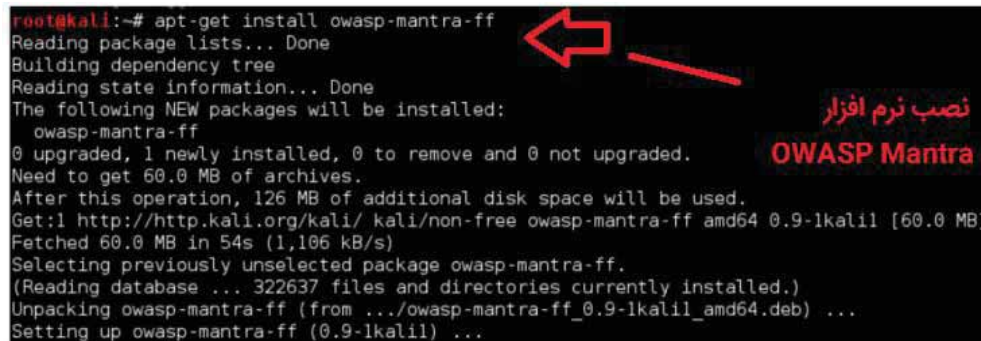
با توجه به اینکه نرم‌افزار "OWASP Mantra" از جمله ابزارهایی است که همراه سیستم‌عامل کالی ارائه شده است، تنها کافی است برای اینکه مطمئن شوید از آخرین نسخه آن استفاده می‌کنید از فرمان زیر برای به‌روزرسانی آن استفاده کنید:

```
apt-get update
```

اگر بخواهید به هر دلیلی نرم‌افزار "OWASP Mantra" را از نو نصب کنید می‌بایست از فرمان زیر استفاده کنید:

```
apt-get install owasp-mantra-ff
```

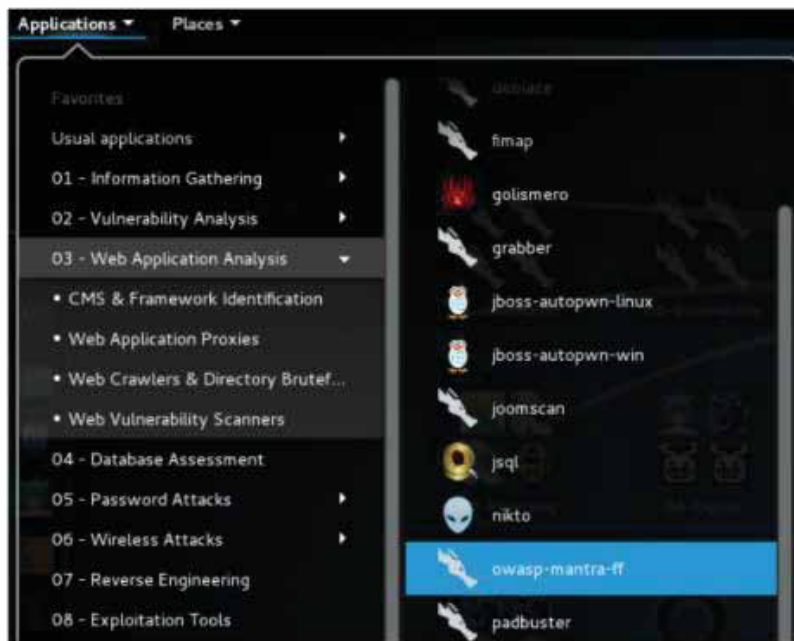
مراحل نصب در شکل زیر نشان داده شده است:



```
root@kali:~# apt-get install owasp-mantra-ff
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  owasp-mantra-ff
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 60.0 MB of archives.
After this operation, 126 MB of additional disk space will be used.
Get:1 http://http.kali.org/kali/ kali/non-free owasp-mantra-ff amd64 0.9-1kalil [60.0 MB]
Fetched 60.0 MB in 54s (1,106 kB/s)
Selecting previously unselected package owasp-mantra-ff.
(Reading database ... 322637 files and directories currently installed.)
Unpacking owasp-mantra-ff (from ../owasp-mantra-ff_0.9-1kalil_amd64.deb) ...
Setting up owasp-mantra-ff (0.9-1kalil) ...
```

پس از اینکه مراحل نصب به پایان رسید، می‌توانید از طریق مسیر زیر از منوی سیستم‌عامل کالی آن را اجرا کنید:

Applications | 03 – Web Application Analysis | Web Vulnerability Scanners | owasp-mantra-ff

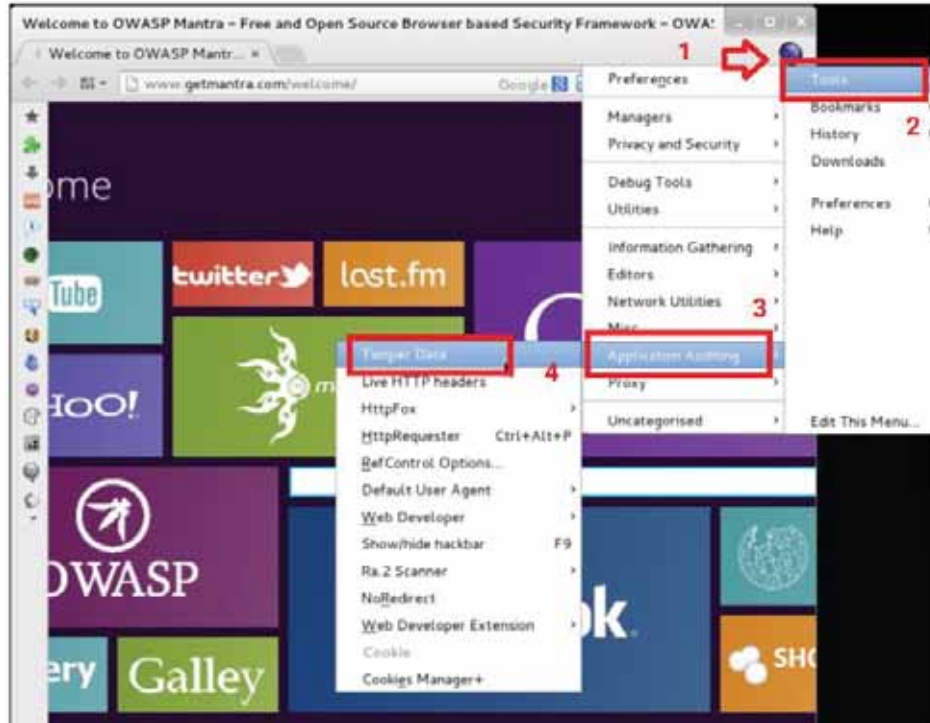


و یا اینکه از طریق پنجره ترمینال، فرمان زیر را برای اجرای نرم‌افزار "OWASP Mantra" وارد کنید:

```
owasp-mantra-ff
```

پس از اینکه نرم‌افزار "Mantra" اجرا شد، آنگاه می‌توانید همانند شکل زیر از طریق مرورگر وب آن را مورد استفاده قرار دهید.

نخست همانند شکل زیر بر روی لوگوی موجود در گوشه سمت راست مرورگر، کلیک کرده و سپس از منوی ظاهر شده بر روی صفحه، گزینه "Tools" را انتخاب کنید. آن گاه به تمامی ابزارها و نرم‌افزارهای موجود در آن دسترسی خواهید داشت.

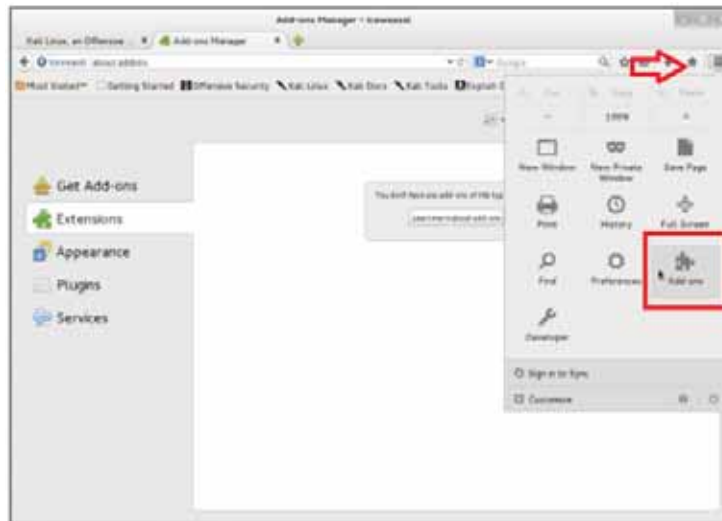


نسخه دیگری از نرم افزار "OWASP Mantra" که برای مرورگر "Chromium" آماده شده است، "MoC - Mantra" نام دارد. این نرم افزار را می توانید از مسیر زیر دانلود و نصب کنید. این نرم افزار هم اکنون تنها می تواند در سیستم عامل ویندوز نصب و اجرا شود.

<http://www.getmantra.com/mantra-on-chromium.html>

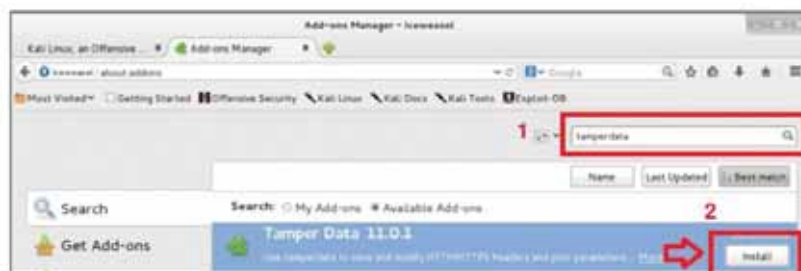
اگر از مرورگر پیش فرضی که همراه نرم افزار "OWASP Mantra" ارائه می شود خوشتان نمی آید و می خواهید از مرورگر دیگری استفاده کنید، می توانید مراحل زیر را انجام دهید که در آنها بر روی آخرین ویرایش مرورگر Firefox و نسخه ای از آن که به نام "Icweasel" در سیستم عامل کالی وجود دارند، نصب و نحوه استفاده از ابزارهای "Mantra" نشان داده شده اند.

مرورگر "Icweasel" را باز کنید و سپس از منوی "Tools" گزینه "Add-ons" را انتخاب کنید، همان گونه که در شکل زیر نشان داده شده است.



در بخش جست‌وجو عبارت "Tamper data" را وارد کنید و سپس بر روی کلید "Enter" کلیک کنید.

برای نصب افزونه مورد نظر، بر روی گزینه "Install" کلیک کنید. پنجره‌ای بر روی صفحه نمایش باز می‌شود که با پذیرفتن حقوق مولف و شرایط استفاده (EULA) نصب افزونه انجام خواهد شد.



توجه: پس از نصب و برای فعال شدن افزونه مورد نظر، می‌بایست مرورگر را از نو راه‌اندازی کنید.

در بخش جست‌وجو عبارت "cookies Manager+" را وارد کنید و سپس گزینه "Install" را کلیک کنید.

در ادامه، افزونه "Firebug" را جست‌وجو و نصب کنید.

سپس افزونه "Hackbar" را همانند موارد بالا، جست‌وجو و نصب کنید.

پس از آن افزونه "HTTP Request" را نصب کنید.

در پایان، افزونه "Passive Recon" را جست‌وجو و سپس نصب کنید.

تا این مرحله، تعدادی از افزونه‌های مورد نظر را در مرورگر نصب کرده‌ایم، این افزونه‌ها در پروژه تست نفوذ برای انجام کارهای زیر می‌توانند مورد استفاده قرار گیرند.

“Cookie Manager” افزونه‌ای است که برای مشاهده کوکی‌های نرم‌افزارهای تحت وب و در برخی مواقع ویرایش آن‌ها مورد استفاده قرار می‌گیرد.

“Firebug” این افزونه برای هر برنامه‌نویس تحت وب مورد نیاز است. وظیفه اصلی این افزونه، اشکال‌یابی صفحه‌های وب به صورت برخط می‌باشد. این ابزار برای انجام برخی تغییرات در صفحه وب سمت کاربر نیز مورد استفاده قرار می‌گیرد.

“Hackbar” افزونه‌ای خیلی ساده می‌باشد که امکان ارسال ورودی‌های گوناگون به صفحه تارنمای مورد نظر را بدون تغییر در آدرس “URL” آن می‌دهد. از این افزونه برای تست نفوذپذیری در حملات “XSS” و تزریق^۲ استفاده می‌شود.

“Http Requester” با استفاده از این افزونه می‌توان بسته‌های درخواست همانند آنچه که در پروتکل “HTTP” وجود دارد نظیر “Get” و “Post” و “Put” را شبیه‌سازی نموده تا پیامی که از جانب سرویس‌دهنده برای آن‌ها تولید می‌شود را به صورت خام مشاهده کرد.

“Passive Recon” این افزونه با جست‌وجو و جمع‌آوری اطلاعات از منابعی که از پیش تنظیم شده‌اند، اطلاعات کاملی از تارنمایی که در مرورگر آن را مشاهده می‌کنیم را جمع‌آوری می‌کند. برخی از منابع تارنما که توسط این افزونه مورد استفاده قرار می‌گیرند، عبارتند از استخراج رکوردهای مربوط به آن از سرویس‌دهنده “DNS” و تارنمای “Whois” و جست‌وجو در موتور جست‌وجوگر “Google” و آدرس‌های رایانامه مورد استفاده در آن و ...

“Tamper Data” این افزونه امکان نسخه‌برداری و تغییر درخواست‌هایی که از سمت کاربر به سرویس‌دهنده در تارنمای مورد نظر ارسال می‌شود، را دارد. با این افزونه می‌توان شکل و قالب ارسال درخواست به سرویس‌دهنده را تشخیص داده و درخواست مورد نظر را با همان شکل و قالب به سرویس‌دهنده مورد نظر ارسال نمود.

نکته: افزون بر افزونه‌هایی که در بالا به آن‌ها اشاره شد، از افزونه‌های دیگری که در زیر فهرست آن‌ها را مشاهده خواهید کرد نیز می‌توانید در مرورگر وب استفاده کنید.

XSS Me, SQL Inject Me, FoxyProxy, iMacros, FirePHP, RESTClient, Wappalyzer

¹Cross Site Scripting

²Injection

نصب و راه‌اندازی نرم‌افزار ماشین مجازی VirtualBox

در این بخش یکی از چهار مرحله آماده‌سازی لابراتوار مجازی برای انجام آزمایش‌های تست نفوذ را با یکدیگر انجام خواهیم داد. در این قسمت با نحوه نصب و راه‌اندازی ماشین‌های مجازی مورد نیاز در آزمایشگاه با استفاده از نرم‌افزار "VirtualBox" آشنا خواهیم شد.

پیش از شروع نصب نرم‌افزارها در سیستم‌عامل کالی باید مطمئن شویم که همه نرم‌افزارهای موجود در آن به‌روز باشند، به همین منظور از فرمان "apt-get update" استفاده می‌کنیم.

نخست نرم‌افزار "VirtualBox" را دانلود و نصب می‌کنیم. برای این کار، همانند شکل زیر از فرمان "apt-get install virtualbox" استفاده می‌کنیم.

```
root@kali:~# apt-get install virtualbox
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  dkms libgsoap4 libvncserver0 linux-headers-3.18.0-kali3-amd64
  linux-headers-3.18.0-kali3-common linux-headers-amd64 linux-kbuild-3.18
  virtualbox-dkms virtualbox-qt
Suggested packages:
  libvncserver0-dbg vde2 virtualbox-guest-additions-iso
Recommended packages:
  linux-image
The following NEW packages will be installed:
  dkms libgsoap4 libvncserver0 linux-headers-3.18.0-kali3-amd64
  linux-headers-3.18.0-kali3-common linux-headers-amd64 linux-kbuild-3.18
  virtualbox virtualbox-dkms virtualbox-qt
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 27.2 MB of archives.
After this operation, 124 MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
```

نصب نرم‌افزار ماشین مجازی
VirtualBox

پس از اینکه نصب نرم‌افزار به اتمام رسید از طریق مسیر زیر در منوی سیستم‌عامل کالی آن را فعال می‌کنیم.

Applications | Usual Applications | Accessories | VirtualBox

و یا اینکه در پنجره ترمینال خط فرمان از عبارت "virtualbox" استفاده می‌کنیم.

با این کار پنجره نرم‌افزار "VirtualBox" همانند شکل بعدی بر روی صفحه نمایش باز خواهد شد.

با مشاهده صفحه آن در شکل زیر معلوم می‌شود که نرم‌افزار "VirtualBox" نصب شده است و آماده است تا در آن ماشین‌های مجازی مورد نیاز را تعریف کنیم.



با استفاده از نرم‌افزار "VirtualBox" و با کمک فناوری مجازی‌سازی می‌توانیم به طور همزمان چندین ماشین مجازی بر حسب نیاز تعریف کنیم. بدین ترتیب، به طور همزمان در آزمایشگاه مجازی مورد نظر چندین ماشین مجازی با سیستم‌عامل‌های گوناگون به طور همزمان مورد استفاده قرار خواهند گرفت.

نکته: برای نرم‌افزار "VirtualBox" بسته تکمیلی (Extension Pack) وجود دارد که امکان پشتیبانی از درگاه‌های "USB2.0/30" و همچنین ارتباط با میز کار از راه دور (Remote Desktop) را فراهم می‌سازد. برای دریافت و نصب آن کافی است که آن را از آدرس زیر دانلود کرده و سپس دوبار بر روی آن کلیک کنید. آنگاه نرم‌افزار "VirtualBox" بقیه مراحل مربوط به نصب و راه‌اندازی آن را انجام خواهد داد.

<https://virtualbox.org/wiki/Downloads>

نکته: گزینه‌های دیگری برای ایجاد و استفاده از فناوری مجازی‌سازی در کالی نیز وجود دارند که می‌توانید از آن‌ها استفاده کنید: KVM، Xen، Qemu، VMWare Player/Workstation

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

اکنون نوبت به نصب و راه‌اندازی نخستین ماشین مجازی در آزمایشگاه تست نفوذ می‌رسد. این ماشین مجازی سرویس‌دهنده‌ای خواهد بود که نرم‌افزارهای تحت وب بر روی آن نصب شده و به عنوان هدف در آزمایش‌های تست نفوذ قرار خواهد گرفت. برای این کار در ماشین مجازی از نرم‌افزار OWASP-bwa¹ استفاده

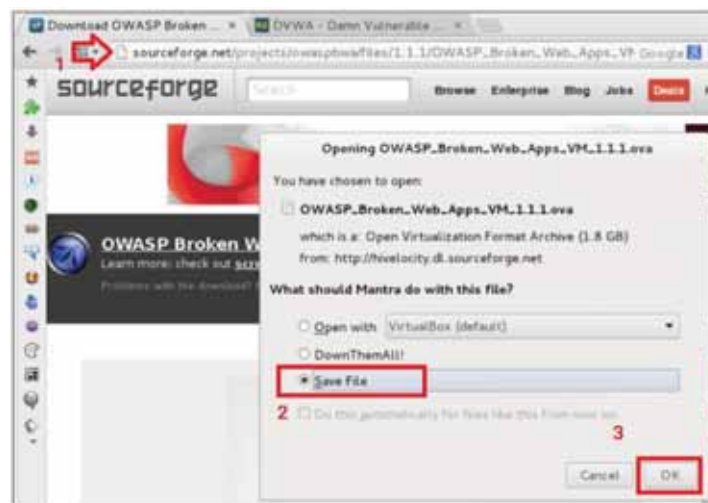
¹OWASP-Broken Web Apps

می‌کنیم. این نرم‌افزار مجموعه‌ای از تارنماهای تحت وب و قابل نفوذ برای انجام تست‌های نفوذ مورد نظر می‌باشد.

از مسیر زیر آخرین ویرایش نرم افزار مورد نظر را دانلود می‌کنیم. این نرم‌افزار با قالب "ova" ارائه شده است و در زمانی که این مستند آماده می‌شد، آخرین ویرایش آن با نام "OWASP_Broken_Web_Apps_VM_1.1.1.ova" در دسترس بوده است.

<http://sourceforge.net/projects/owaspbwa/files/>

نحوه انجام عملیات در شکل زیر نشان داده شده است:

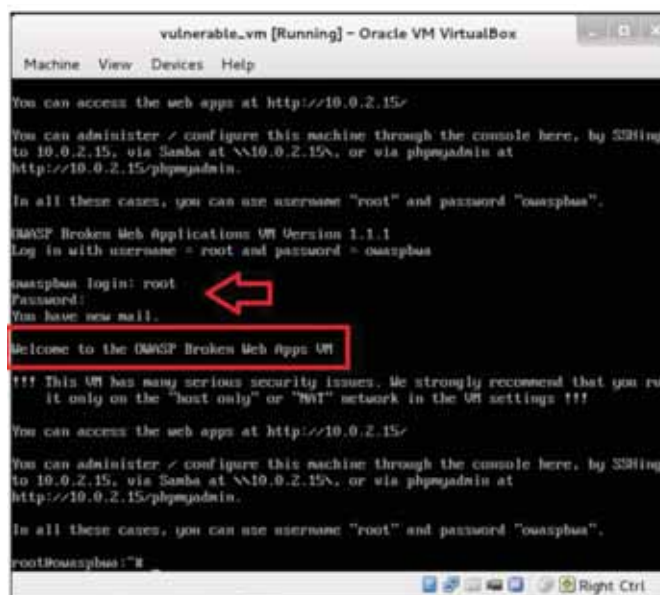


پس از اینکه دانلود نرم‌افزار مورد نظر به اتمام رسید، بر روی آن دوبار کلیک کنید تا محتویات آن که پیش‌تر تنظیم شده است در ماشین مجازی "VirtualBox" نصب شود. در هنگام نصب می‌توانید تنظیم‌های پیش‌فرض مربوط به آن را نیز تغییر دهید.

همانند شکل زیر نام ماشین مجازی را "vulnerable_vm" انتخاب می‌کنیم و بقیه موارد را به صورت پیش‌فرض در نظر گرفته و با استفاده از کلید "Import" ماشین مجازی مورد نظر را نصب می‌کنیم.



نصب ماشین مجازی مورد نظر می‌تواند حدود یک دقیقه به طول انجامد و پس از اتمام آن نام ماشین مجازی ایجاد شده را در فهرست نرم‌افزار "VirtualBox" مشاهده خواهیم کرد. نخست آن را انتخاب کرده و پس از آن برای فعال‌سازی آن بر روی کلید "Start" کلیک می‌کنیم.



پس از راه‌اندازی ماشین مجازی مورد نظر همانند شکل بالا نام کاربری و گذرواژه، پرسش خواهد شد که با استفاده از اطلاعات زیر وارد نرم‌افزار می‌شویم. اکنون نرم‌افزار مورد نظر برای انجام آزمایش‌های تست نفوذ آماده است.

User name: root

Password: owaspbwa

بسته نرم‌افزاری "OWASP-bwa" ابزاری برای ایجاد فضایی امن و مناسب برای متخصصان امنیت ایجاد می‌کند تا با انجام حملات تست نفوذ هم نفوذپذیری‌های موجود در نرم‌افزارهای تحت وب را مورد بررسی قرار دهند و هم مهارت انجام عملیات تست نفوذ را در خود ارتقا دهند. در ضمن به برنامه‌نویسان و راهبران نرم‌افزارهای تحت وب برای محافظت و ایمن‌سازی این نرم‌افزارها کمک می‌کند.

در بسته نرم‌افزاری مذکور انواع نرم‌افزارها در بستر ".NET" و "PHP" و "Java" و حتی سیستم‌های مدیریت محتوا نظیر "Worpress" و "Joomla" پیش‌بینی شده‌اند.

نکته: در ماشین‌های مجازی، امکان استفاده از گزینه‌های گوناگونی برای نرم‌افزارهای قابل نفوذ وجود دارد. در آدرس زیر می‌توانید مجموعه‌ای کامل از این نوع نرم‌افزارها را مشاهده کنید.

<https://www.vulnhub.com/>

در تارنمای بالا می‌توانید نمونه‌ای از آموزش‌های گام به گام در مورد آن‌ها را نیز مشاهده کنید.

برخی از آزمایش‌های تست نفوذ از یک نرم‌افزار کاربردی دیگری با نام "bwAPP Bee-box" نیز استفاده می‌کنند و می‌توانیم آن را از آدرس زیر دانلود کنیم:

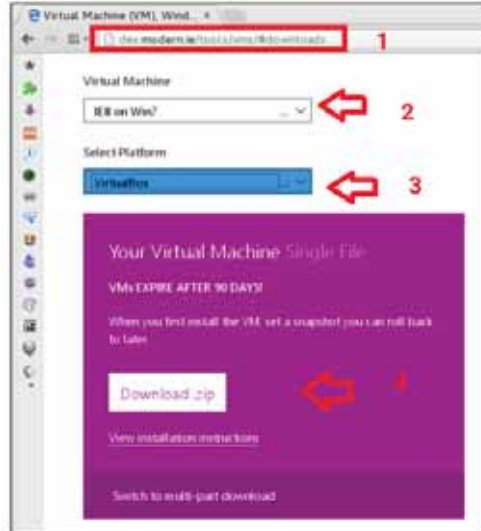
<https://www.vulnhub.com/entry/bwapp-bee-box-v16,53/>

نصب و راه‌اندازی ماشین مهاجم (حمله کننده)

در مواردی که حملات مردمیانی^۱ را انجام می‌دهیم، می‌بایست سیستمی برای ارسال درخواست به سرویس‌دهنده دستکاری شده در اختیار داشته باشیم. برای این کار از یک ماشین مجازی با سیستم‌عامل ویندوز استفاده می‌کنیم، مراحل دانلود و نصب و راه‌اندازی آن در زیر نشان داده شده است.

برای دانلود نرم‌افزار مورد نظر به آدرس زیر مراجعه می‌کنیم. سپس همانند آنچه که در شکل زیر نشان داده شده است، اقدام به دانلود نرم‌افزار مورد نظر می‌کنیم. برای انجام آزمایش‌ها از نرم‌افزار IE8 در سیستم‌عامل ویندوز 7 استفاده خواهیم کرد.

^۱MiTM – Man In the Middle Attack



پس از دانلود باید فایل آن را از حالت فشرده خارج کنیم. (برای این کار به محلی که فایل مزبور دانلود شده است می‌رویم و بر روی آن کلیک راست می‌کنیم و سپس گزینه "Extract Here" را انتخاب می‌نماییم.) در فایل‌های باز شده، بر روی فایل‌هایی که با پسوند ".ova" مشخص شده است، دوبار کلیک می‌کنیم تا مراحل نصب آن در نرم‌افزار "VirtualBox" آغاز شود.



پس از اتمام مراحل نصب ماشین مجازی (نام آن را "IE8-Win7" تعیین می‌کنیم) سپس با انتخاب نام آن و کلیک بر روی کلید "Start" از بالای صفحه، آن را فعال کنیم. صفحه ورودی این نرم‌افزار در شکل زیر نشان داده شده است.



مایکروسافت این نرم‌افزارها را در قالب‌های آماده و از پیش تنظیم شده ارائه نموده است تا بدین ترتیب متخصصان امنیت و طراحان نرم‌افزارهای کاربردی تحت وب و راهبران سیستم بتوانند آزمایش‌های مورد نظر خود را بر روی آن‌ها انجام دهند. این نرم‌افزارها در یک دوره زمانی ۳۰ روزه فعال می‌باشند که برای انجام آزمایش‌های مورد نظر کافی خواهند بود.

توجه: برای یک متخصص امنیت، آماده‌سازی و استفاده از آزمایشگاهی که در آن نرم‌افزارهای گوناگون و سیستم‌عامل‌ها و مرورگرهای متنوعی وجود داشته باشد از اهمیت زیادی برخوردار است. چون در محیط‌های واقعی امکان استفاده از ایستگاه‌های کاری با سیستم‌عامل‌ها و مرورگرهای گوناگون وجود دارد و متخصص تست نفوذ می‌بایست پیش‌تر بر روی آن‌ها آزمایش‌های تست نفوذ مورد نظر را انجام داده باشد.

نکته: اگر بخواهید از ماشین‌های مجازی دیگر با تنظیم‌های مورد نظر خود استفاده کنید، می‌توانید این کار را در نرم‌افزار "VirtualBox" و با استفاده از راهنمایی که در آدرس زیر خواهید یافت، انجام دهید:

<https://www.virtualbox.org/manual>

تنظیم ماشین‌های ماشین‌های مجازی برای برقراری ارتباط مناسب

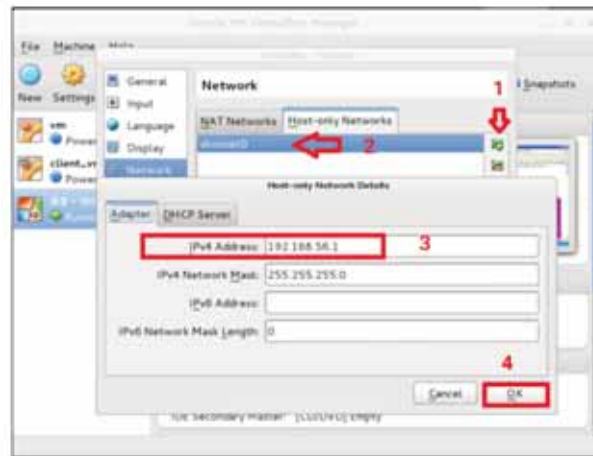
برای اینکه بتوانیم بین سرویس‌دهنده حاوی نرم‌افزارهای قابل نفوذ و سایر سیستم‌های موجود که برای تست نفوذ مورد استفاده قرار می‌گیرند، ارتباط برقرار کنیم، می‌بایست آن‌ها را در یک شبکه مشترک قرار دهیم. وجود سرویس‌دهنده نفوذپذیر در شبکه مورد استفاده می‌تواند ریسک امنیتی جدی برای آن ایجاد کند. به همین

منظور در نرم‌افزار "VirtualBox" ماشین‌های مجازی را به گونه‌ای تنظیم می‌کنیم تا سیستم‌هایی که در لابرتوار مجازی مورد نظر قرار دارند در یک شبکه جداگانه و مستقل با یکدیگر ارتباط داشته باشند.

پیش از انجام تنظیم‌ها، نخست از غیرفعال بودن همه ماشین‌های مجازی مطمئن شوید. سپس از مسیر زیر بخش مربوط به تنظیم‌های شبکه را در نرم‌افزار "VirtualBox" باز کنید:

File | Preferences... | Network

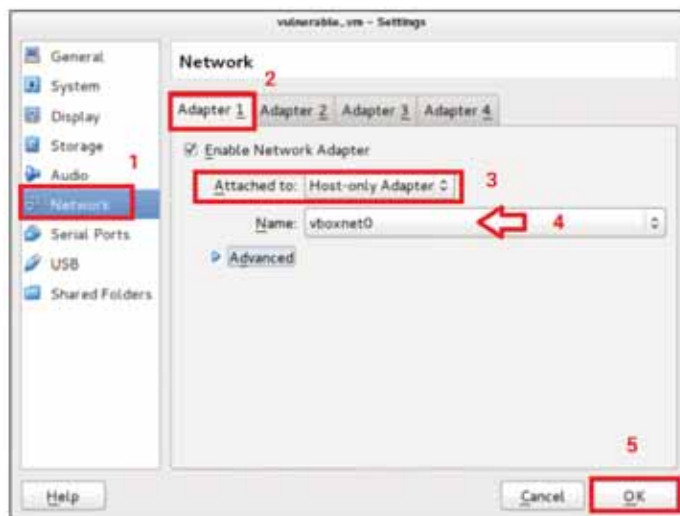
در پنجره تنظیمات شبکه، همانند شکل زیر بخش "Host-only Network" را انتخاب کنید و بر روی کلید "Add" کلیک کنید تا شبکه جدیدی ایجاد شود. برای شبکه جدید نام "vboxnet0" را در نظر بگیرید و با استفاده از کلید "Edit" همانند شکل زیر تنظیم‌های مربوط به آن را ویرایش کنید.



در این پنجره می‌توانید آدرس‌های مورد استفاده در شبکه جدید را تنظیم کنید. آدرس ارائه شده به طور پیش‌فرض به گونه‌ای انتخاب شده است که با دیگر شبکه‌های موجود تداخل ایجاد نشود. بنابراین بهتر است مقادیر پیش‌فرض را انتخاب کرده و آن‌ها را تغییر ندهید. اگر بخواهید از مجموعه‌ای از آدرس‌های دیگر در شبکه‌های داخلی استفاده کنید باید از آدرس‌های 10.0.0.0/8 یا 172.16.0.0/12 یا 192.168.0.0/16 استفاده کنید. پس از تنظیم آدرس شبکه با استفاده از کلید "OK" آن را ثبت می‌کنیم.

مرحله بعد تنظیم ماشین مجازی است که با نام "vulnerable_vm" مشخص شده است. نخست آن را انتخاب کرده و سپس با استفاده از کلید "Settings" در بالای صفحه، به بخش تنظیم‌های آن وارد می‌شویم.

همانند شکل زیر، نخست گزینه "Network" را انتخاب کرده و سپس در منویی که با نام "Attached to:" مشخص شده است گزینه "Host-Only Adapter" را انتخاب می‌کنیم. در آن نام شبکه مورد نظر را مشخص می‌کنیم (vboxnet0). سپس برای ثبت تنظیمات بر روی کلید "OK" کلیک می‌کنیم.



مراحل بالا را برای ماشین مجازی که با نام "IE8-Win7" مشخص شده است نیز تکرار می‌کنیم. اکنون که تنظیم دو ماشین مجازی مورد نظر به اتمام رسید، نوبت به آزمایش ارتباط میان آن‌ها می‌رسد. برای این کار، نخست ماشین‌های مجازی مورد نظر را در "VirtualBox" فعال می‌کنیم. همانند شکل زیر، پنجره سطر فرمان در سیستم اصلی (میزبان ماشین‌های مجازی که دارای سیستم‌عامل کالی است) را باز کرده و سپس با استفاده از دستور "ifconfig" مشخصات شبکه تعریف شده در آن را مشاهده می‌کنیم.

```

root@kali: ~
└─$ ifconfig
eth0: Link encap:Ethernet HWaddr b8:ac:6f:ff:7c:60
      UP BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 teguawlen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo:   Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:65536  Metric:1
      RX packets:349 errors:0 dropped:0 overruns:0 frame:0
      TX packets:349 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 teguawlen:0
      RX bytes:99649 (97.3 KiB)  TX bytes:99649 (97.3 KiB)

vboxnet0: Link encap:Ethernet HWaddr 0a:00:27:00:00:00
      inet addr:192.168.56.1  Bcast:192.168.56.255  Mask:255.255.255.0
      inet6 addr: fe80::800:27ff:fe00:0/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:153 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 teguawlen:1000
  
```

تنظیمات شبکه و آدرس ایستگاه میزبان

همان گونه که در شکل بالا مشاهده می‌کنید، برای کارت رابط شبکه آدرس "192.168.56.1" و نام "vboxnet0" در نظر گرفته شده است. (با توجه به تنظیمات شبکه مورد استفاده می‌توانند این موارد تغییر کنند.)

در سطر فرمان ماشین مجازی "vulnerable_vm" با استفاده از دستور "ifconfig" تنظیم‌های مربوط به کارت شبکه "eth0" را در آن مشاهده می‌کنیم. اکنون به سیستم مهاجم (IE8-Win7) رفته و در پنجره سطر فرمان آن دستور "ipconfig" را وارد می‌کنیم.

```

root@kali:~# ping -c 4 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data:
64 bytes from 192.168.56.102: icmp_req=1 ttl=64 time=0.369 ms
64 bytes from 192.168.56.102: icmp_req=2 ttl=64 time=0.243 ms
64 bytes from 192.168.56.102: icmp_req=3 ttl=64 time=0.252 ms
64 bytes from 192.168.56.102: icmp_req=4 ttl=64 time=0.247 ms

--- 192.168.56.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.243/0.277/0.369/0.056 ms
root@kali:~# ping -c 4 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data:
From 192.168.56.1 icmp_seq=1 Destination Host Unreachable
From 192.168.56.1 icmp_seq=2 Destination Host Unreachable
From 192.168.56.1 icmp_seq=3 Destination Host Unreachable
From 192.168.56.1 icmp_seq=4 Destination Host Unreachable

--- 192.168.56.103 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3015ms

```

اکنون اطلاعات مربوط به شبکه ماشین میزبان و دو ماشین مجازی موجود در لابرتوار مجازی را به شرح زیر در اختیار خواهیم داشت:

192.168.56.1 -> Host

192.168.56.102 -> vulnerable_vm

192.168.56.103 -> IE8-Win7

برای آزمایش ارتباط بین آنها، همانند شکل زیر از پنجره سطر فرمان ماشین میزبان با استفاده از دستورهای زیر ارتباط آن را به دوماشین مجازی موجود در آن کنترل می‌کنیم.

```
ping -c 4 192.168.56.102
```

```
ping -c 4 192.168.56.103
```

می‌توانید همین آزمایش را از طریق سطر فرمان یکی از ماشین‌ها با آدرس ماشین مجازی دیگر نیز انجام دهید.

توجه: ممکن است به طور پیش‌فرض امکان استفاده از فرمان "ping" در ماشین مجازی که از سیستم‌عامل ویندوز استفاده می‌کند، غیرفعال شده باشد، به همین منظور برای تست ارتباط در آن می‌توانید از دستور زیر استفاده کنید:

```
arping -c 4 192.168.56.103
```

اکنون با توجه به تنظیم‌ها و تست ارتباط بین آنها، شبکه‌ای مجازی با آدرس‌های مخصوص به خود در اختیار داریم که از ایستگاه میزبان و دو ماشین مجازی دیگر تشکیل شده است که از آن‌ها به عنوان لابرتوار تست نفوذ استفاده می‌کنیم.

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

بسته نرم‌افزاری "OWASP-bwa" حاوی نرم‌افزارهای فراوانی است که نسبت به نفوذپذیری‌های شناخته شده، قابل نفوذ و حمله می‌باشند. برخی از آن‌ها برای تمرین تست نفوذ و استفاده از تکنیک‌های مشخص طراحی شده‌اند و برخی دیگر به عنوان الگویی از نرم‌افزارهای کاربردی موجود در دنیای واقعی در نظر گرفته شده‌اند که می‌بایست نفوذپذیری‌های موجود در آن‌ها را مشخص کنیم.

در این بخش به بررسی سرویس‌دهنده نفوذپذیری که در بخش‌های پیشین آن را نصب و راه‌اندازی کردیم می‌پردازیم تا نرم‌افزارهای موجود در آن را مشخص کنیم.

برای دسترسی به ماشین مجازی مورد نظر آدرسی را که در مراحل پیش برای آن در نظر گرفته‌ایم در اختیار داریم. (192.168.56.102)

در شرایطی که ماشین مجازی سرویس‌دهنده قابل نفوذ (vulnerable_vm) فعال است، پنجره مرورگر را در سیستم میزبان باز می‌کنیم و در سطر آدرس آن، آدرس مربوط به ماشین مجازی مورد نظر را وارد می‌کنیم (192.168.56.102) سپس همانند شکل زیر در صفحه مرورگر فهرستی از نرم‌افزارهای نصب شده بر روی آن را مشاهده خواهیم کرد.



اکنون نرم‌افزاری که با نام "Damn Vulnerable Web Application" مشخص شده است را انتخاب می‌کنیم.

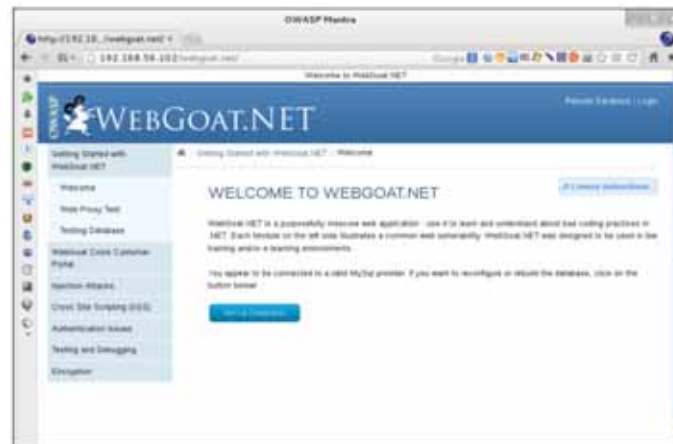
برای ورود به تارنمای مربوط به نرم‌افزار مذکور از نام عبور و گذرواژه "admin/admin" استفاده می‌کنیم. در این تارنما منویی در سمت چپ صفحه وجود دارد که در آن فهرستی از انواع نفوذپذیری‌هایی را که می‌توانید آن‌ها را در این تارنما آزمایش کنید، ارائه شده است. (Brute Force, Command Execution, SQL Injection, ...)

نکته: در این تارنما می‌توانید سطح امنیتی را برای آزمایش‌های خود در بخش "DVWA Security" تنظیم کنید.



از تارنمای مزبور خارج شده و به صفحه اصلی سرویس دهنده برمی‌گردیم.

از فهرست نرم‌افزارهای موجود در سرویس دهنده، نرم‌افزار "OWASP WebGoat.NET" را انتخاب می‌کنیم. در این نرم‌افزار می‌توانید حملات تزریق فایل و کد¹ و تبادل کد بین تارنما² و نقطه ضعف‌های ناشی از رمزنگاری را اجرا کنید. همچنین در این تارنما صفحه‌ای در نظر گرفته شده است که نرم‌افزار فروشگاهی را در تارنما شبیه‌سازی می‌کند و با استفاده از آن می‌توانید، برای تشخیص و استفاده از نفوذپذیری این گونه تارنماها تمرین و بررسی‌های مورد نظر را انجام دهید. صفحه اصلی این تارنما در شکل زیر نشان داده شده است.



از نرم‌افزار مذکور خارج شده و به صفحه اصلی سرویس دهنده برمی‌گردیم.

¹Code and File Injection Attack

²Cross Site Scripting