

۱۱۱۱۲۹۹



آموزش گام به گام تست نفوذ با

سیستم عامل Kali Linux

تألیف:

مهندس امین کیانی



ویراستار علمی: مهندس رامین مولاناپور
طراحی جلد: همتا بیداریان

مدیر تولید و ناظر چاپ: حسین رعدشندی
حروفچینی و صفحه‌آرایی: همتا بیداریان

آموزش گام به گام تست نفوذ با سیستم عامل Kali Linux

مؤلف: مهندس امین کیانی

ناشر: انتشارات آتی‌نگر

چاپ اول، ۱۳۹۵

شمارگان: ۱۰۰۰ نسخه

قیمت: ۳۲۰,۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۷۶۳۱-۰۷-۲

ISBN: 978-600-7631-07-2

کلیه حقوق برای انتشارات آتی‌نگر محفوظ است.

نشانی دفتر فروش: خیابان جمالزاده جنوبی، رده بندی رتبه ششم، پلاک ۱۴۴، واحد ۲

نمابر: ۶۶۵۶۵۳۳۷

تلفن: ۸-۶۶۵۶۵۳۳۶

www.ati-negar.com * info@ati-negar.com



کیانی، امین، ۱۳۶۶-

آموزش گام به گام تست نفوذ با سیستم عامل Kali Linux / مؤلف: امین کیانی. - تهران: آتی‌نگر، ۱۳۹۵.

۵۵۲ ص: مصور.

ISBN: 978-600-7631-07-2

فیبا.

موضوع: سیستم عامل لینوکس -- سیستم‌های عامل (کامپیوتر) -- آزمایش نفوذ (ایمن‌سازی کامپیوتر) -- هکرها

QA ۷۶/۷۶/س۹۴ک۹ ۱۳۹۵

رده‌بندی کنگره

۰۰۵/۴۳۲

رده‌بندی دیویی

۴۲۲۱۵۴۶

شماره کتابشناسی ملی

فهرست مطالب

بخش اول: اصول پایه‌ای | ۹

فصل اول: راه‌اندازی آزمایشگاه مجازی | ۱۱

نصب نرم‌افزار VMware | ۱۱

راه‌اندازی سیستم‌عامل Kali | ۱۱

راه‌اندازی ماشین‌های مجازی هدف | ۳۴

راه‌اندازی ماشین هدف Windows XP SP3 | ۲۳

راه‌اندازی ماشین هدف Ubuntu 8.10 | ۴۸

راه‌اندازی ماشین هدف Windows 7 SP1 | ۴۸

فصل دوم: استفاده از سیستم عامل Kali Linux | ۶۳

ساختار فایل‌ها و دایرکتوری‌ها | ۶۳

آشنایی با خط فرمان Linux | ۶۸

آشنایی با دستورات Linux | ۶۸

کنترل دسترسی به فایل‌ها در Kali Linux | ۷۸

ویرایش فایل‌ها در سیستم عامل Kali | ۸۰

دستکاری داده | ۸۳

مدیریت پکیج‌های نصب‌شده | ۸۵

پردازش‌ها و سرویس‌ها | ۸۷

مدیریت شبکه | ۸۷

ابزار Netcat (چاقوی ارتش سوئیس برای اتصالات TCP/IP) | ۹۱

آشنایی با زمان‌بندی خودکار در سیستم عامل Kali | ۹۶

فصل سوم: برنامه‌نویسی | ۹۹

مقدمه | ۹۹

آشنایی با دو اصطلاح مهم | ۹۹

نسخه‌های مختلف شل | ۱۰۰

اسکرپت‌نویسی Bash | ۱۰۰

اسکرپت‌نویسی به‌وسیله زبان برنامه‌نویسی Python | ۱۰۹

برنامه‌نویسی و کامپایل زبان C | ۱۱۱

فصل چهارم: استفاده از Metasploit Framework | ۱۱۵

آشنایی با متاسپلویت | ۱۱۵

اجرای متاسپلویت در سیستم عامل Kali | ۱۱۸

پیدا کردن ماژول‌های متاسپلویت | ۱۲۰

رابط کاربری Msfconsole | ۱۲۱

تنظیم گزینه‌های ماژول | ۱۲۳

شل‌کد یا پیلود | ۱۲۵

انواع شل | ۱۲۸

تنظیم پیلود به‌صورت دستی | ۱۲۹

رابط کاربری Msfcli | ۱۳۱

ساخت پیلودهای مستقل با استفاده از رابط کاربری Msfvenom | ۱۳۵

استفاده از ماژول‌های Multi/Handler | ۱۳۹

استفاده از ماژول‌های کمکی | ۱۴۱

به‌نگام‌رسانی متاسپلویت | ۱۴۳

بخش دوم: ارزیابی و تشخیص | ۱۴۵

فصل پنجم: جمع‌آوری اطلاعات | ۱۴۷

جمع‌آوری اطلاعات متن باز (OSINT) | ۱۴۷

پیش‌پورت | ۱۶۰

فصل ششم: کشف آسیب پذیری ها | ۱۷۳

از پویش Nmap Version تا آسیب پذیری های بالقوه | ۱۷۳

ابزار Nessus | ۱۷۴

موتور اسکرپت نویسی Nmap | ۱۸۱

اجرای یک اسکرپت منفرد NSE | ۱۸۳

ماژول های پویشگر در متاسپلویت | ۱۸۵

تابع Check در اکسپلویت متاسپلویت | ۱۸۶

پویش برنامه کاربردی وب | ۱۸۷

تحلیل به صورت سنت | ۱۹۱

فصل هفتم: ضبط ترافیک | ۱۹۵

شبکه کردن برای ضبط ترافیک | ۱۹۵

استفاده از ابزار Wireshark | ۱۹۵

مسمومیت مخزن ARP | ۲۰۲

مسمومیت مخزن DNS | ۲۰۹

حملات SSL | ۲۱۲

برداشتن SSL | ۲۱۶

بخش سوم: حملات | ۲۱۹**فصل هشتم: اکسپلویت | ۲۲۱**

ملاقات مجدد MS08-067 | ۲۲۱

اکسپلویت کردن اعتبارنامه پیش فرض WebDAV | ۲۲۵

اکسپلویت کردن phpMyadmin باز | ۲۲۹

دانلود فایل های حساس | ۲۳۲

اکسپلویت نرم افزار شخص ثالث به وسیله تکنیک سرریز بافر | ۲۳۴

اکسپلویت کردن برنامه های کاربردی وب شخص ثالث | ۲۳۶

اکسپلویت کردن یک سرویس به خطر افتاده | ۲۳۹

اکسپلویت کردن اشتراک های باز NFS | ۲۴۱

فصل نهم: حملات رمز عبور | ۲۴۵

مدیریت رمز عبور | ۲۴۵

حملات رمز عبور به صورت آنلاین | ۲۴۶

حملات رمز عبور به صورت آفلاین | ۲۵۳

نسخه‌برداری از متن ساده رمز عبور از حافظه به وسیله WCE | ۲۶۵

فصل دهم: اکسپلویت سمت کلاینت | ۲۶۷

دور زدن فایرها به وسیله پیلودهای متاسیلویت | ۲۶۸

حملات سمت کلاینت | ۲۷۱

فصل یازدهم: مهندسی اجتماعی | ۳۰۱

آشنایی با مهندسی اجتماعی | ۳۰۱

ابزار مهندسی اجتماعی SET | ۳۰۳

حملات Spear-Phishing | ۳۰۴

حملات وب | ۳۱۰

حملات توده‌ای ایمیل | ۳۱۴

حملات چند جانبه | ۳۱۶

فصل دوازدهم: دور زدن برنامه‌های کاربردی آنتی‌ویروس | ۳۱۷

اسب‌های تروا | ۳۱۷

برنامه‌های کاربردی آنتی‌ویروس چگونه کار می‌کنند؟ | ۳۱۹

Microsoft Security Essentials | ۳۲۲

آشنایی با VirusTotal | ۳۲۳

به‌دست آوردن سابقه یک برنامه کاربردی آنتی‌ویروس | ۳۲۵

پنهان شدن در معرض دید | ۳۳۹

فصل سیزدهم: بعد از اکسپلویت کردن | ۳۴۱

مترپرتر | ۳۴۱

اسکرپت‌های مترپرتر | ۳۴۴

ماژول‌های پس از اکسپلویت متاسپلویت | ۳۴۶

Railgun | ۳۴۸

بالا بردن سطح دسترسی محلی | ۳۴۹

جمع‌آوری اطلاعات محلی | ۳۶۱

حرکت جانبی | ۳۶۸

چرخیدن | ۳۸۰

ماندگاری | ۳۸۷

فصل چهاردهم: تست برنامه‌های کاربردی وب | ۳۹۳

استفاده از Burp Proxy | ۳۹۳

تزریق SQL | ۳۹۸

تزریق XPath | ۴۰۳

گنجاندن فایل محلی یا FFI | ۴۰۵

گنجاندن فایل‌ها از راه دور یا RFI | ۴۰۷

اجرای دستورات | ۴۰۹

اسکرپت‌نویسی فراسایت یا XSS | ۴۱۰

جعل درخواست XSS | ۴۱۷

پویش برنامه‌های کاربردی وب با استفاده از ابزار w3af | ۴۱۱

فصل پانزدهم: حملات بی‌سیم | ۴۲۱

راه‌اندازی | ۴۲۱

حالت پایش | ۴۲۳

ضبط بسته‌ها | ۴۲۵

بی‌سیم باز | ۴۲۶

حريم خصوصی معادل شبکه سیمی یا WEP | ۴۲۶

دسترسی حفاظت‌شده وای‌فای یا WPA | ۴۳۵

دسترسی حفاظت‌شده وای‌فای یا WPA2 | ۴۳۶

تنظیم حفاظت‌شده وای‌فای یا WPS | ۴۴۳

بخش چهارم: توسعه اکسیلویت | ۴۴۵

فصل شانزدهم: سرریز بافر مبتنی بر پشته در Linux | ۴۴۷

تنوری حافظه | ۴۴۷

سرریز بافر در Linux | ۴۵۲

فصل هفدهم: سرریز بافر مبتنی بر پشته در Windows | ۴۷۳

در جستجوی شیء گونه آسیب‌پذیری شناخته‌شده در نرم‌افزار War-FTP | ۴۷۴

از کار انداختن | ۴۷۷

مکان‌یابی EIP | ۴۷۹

سرقت اجرا | ۴۸۵

به دست آوردن یک شیء | ۴۸۷

فصل هیجدهم: بازنویسی ساختار یافته S.D. ننده استشنا | ۴۹۹

SEH اکسیلویت‌ها را بازنویسی می‌کند | ۵۰۰

انتقال کنترل به SEH | ۵۰۵

یافتن یک رشته حمله در حافظه | ۵۰۶

تکنیک POP POP RET | ۵۰۹

SafeSEH | ۵۱۰

استفاده از یک پرش کوتاه | ۵۱۴

انتخاب یک پیلود | ۵۱۶

فصل نوزدهم: تکنیک Fussing، انتقال اکسیلویت و ماژول‌های متااسپلویت | ۵۲۱

برنامه‌های Fuzzing | ۵۲۱

انتقال اکسیلویت‌های عمومی برای تامین نیازهای شما | ۵۲۸

نوشتن ماژول‌های متااسپلویت | ۵۳۶

تکنیک‌های کاهش اکسیلویت | ۵۴۹