

هو القهار

آزمایش تست نفوذ

برنامه‌های وب با متاسیلویت

(هنر ظریف استفاده از متاسیلویت ۵ برای تست نفوذ برنامه‌های وب)

ویرایش سال ۲۰۲۰

با تشکر از زحمات همسر مهربانم

ترجمه و تألیف:

حسام محمدی ده‌چشمه

تابستان ۱۴۰۰

سرشناسه	محمدي ده‌چشمه، حسام، ۱۳۶۴-
عنوان و نام پديدآور	آزمایش تست نفوذ برنامه‌های وب با متاسپلویت ۵ / ترجمه و تالیف حسام محمدی ده‌چشمه.
مشخصات نشر	تهران: موسسه آموزشی تالیفی ارشدان، ۱۴۰۰.
مشخصات ظاهری	۵۲۶ ص: مصور.
شابک	۹۷۸-۶۲۲-۰۸-۱۴۳۱-۳
وضعیت فهرست نویسی	فیا
موضوع	متاسپلویت (منبع الکترونیکی)
موضوع	کامپیوترها -- کنترل دستیابی
موضوع	آزمایش نفوذ (ایمن سازی کامپیوتر)
موضوع	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	ترم افزار متن باز
رده بندی کنگره	QAV۶/۹ :
رده بندی دیویی	۰۰۵/۸ :
شماره کتابشناسی ملی	۸۴۸۶۳۵۹
اطلاعات رکورد کتابشناسی فیا	فیا

www.ketab.ir

ارشدان

مؤسسه آموزشی تالیفی ارشدان

آزمایش تست نفوذ برنامه‌های وب با متاسپلویت ۵

حسام محمدی ده‌چشمه

آمورشی تالیفی ارشدان

اول

اول ۱۴۰۰

قادر انصاری

۹۷۸-۶۲۲-۰۸-۱۴۳۱-۳

۱۰۰۰

www.arshadan.com

www.arshadan.net

۰۲۱۴۷۶۲۵۵

۱۳۰۰۰۰ تومان

■ نام کتاب:

■ ترجمه و تالیف:

■ ناشر:

■ ویرایش:

■ نوبت چاپ:

■ طراح جلد:

■ شابک:

■ شمارگان:

■ مرکز خرید آنلاین:

■ مرکز بخش و توزیع:

■ قیمت:

۲۳	مقدمه‌ای بر کاربرد تست نفوذ وب
۲۴	تست نفوذ چیست؟
۲۴	انواع تست نفوذ
۲۴	تست نفوذ جعبه سفید
۲۵	تست نفوذ جعبه سیاه
۲۵	تست نفوذ جعبه خاکستری
۲۵	مراحل تست نفوذ
۲۶	شناسایی و جمع‌آوری اطلاعات
۲۷	سرشماری (Enumeration)
۲۸	ارزیابی و تحلیل آسیب‌پذیری
۲۸	بهربرداری (Exploitation)
۲۹	گزارش‌نویسی
۳۰	اصطلاحات مهم
۳۱	روش‌های تست نفوذ
۳۲	کپیچه راهنمای روش‌های تست امنیت منبع آزاد (OSSTMM)
۳۶	چارچوب ارزیابی امنیت سیستم‌های اطلاعاتی (ISSAF)
۳۷	استاندارد اجرای تست نفوذ (PTES)
۴۱	شناسایی ضعف مشترک (CWE)
۴۱	۱۰ مورد برتر لیست OWASP
۴۲	۲۵ مورد برتر لیست SANS
۴۳	خلاصه

سؤالات	۴۳
خواندن بیشتر	۴۴
ملزومات متاسیلویت	۴۵
الزامات فنی	۴۶
مقدمه‌ای درباره متاسیلویت فریم‌ورک	۴۶
اصطلاحات متاسیلویت فریم‌ورک	۴۷
نصب و راه‌اندازی متاسیلویت	۴۹
نصب متاسیلویت فریم‌ورک در لینوکس	۵۰
نصب متاسیلویت فریم‌ورک در ویندوز	۵۲
شروع کار با متاسیلویت فریم‌ورک	۵۶
تعامل با متاسیلویت فریم‌ورک با استفاده از msfconsole	۵۶
دستورات کنسول MSF	۵۸
تولید پیلود در MSF	۸۱
خلاصه	۸۳
سؤالات	۸۳
خواندن بیشتر	۸۴
رابط وب متاسیلویت	۸۵
الزامات فنی	۸۵
مقدمه‌ای بر رابط وب متاسیلویت	۸۵
نصب و راه‌اندازی رابط وب	۸۶
نصب متاسیلویت نسخه (CF) در ویندوز	۸۷
نصب متاسیلویت CF بر روی لینوکس / دیبیا	۹۱
شروع کار با رابط وب متاسیلویت	۹۴

۹۴	رابط
۹۷	ایجاد پروژه (Project creation)
۹۹	سرشماری هدف (Target Enumeration)
۱۰۶	انتخاب ماژول (Module selection)
۱۱۹	خلاصه
۱۱۹	سوالات
۱۱۹	خواندن بیشتر
۱۲۳	استفاده از متاسپلویت برای شناسایی
۱۲۳	الزامات فنی
۱۲۳	مقدمه شناسایی
۱۲۴	شناسایی فعال
۱۲۴	ربودن بنر (Banner Grabbing)
۱۲۶	تشخیص هدر HTTP (HTTP Header Detection)
۱۲۸	ربات اسکن صفحه وب (Web Robot Page Enumeration)
۱۳۱	یافتن مخزن‌های پنهان گیت‌هاب
۱۳۴	تشخیص پراکسی باز (Open Proxy Detection)
۱۳۵	شناسایی غیرفعال
۱۳۵	لینک‌های دامنه بایگانی‌شده (Archived Domain URL.s)
۱۴۰	شناسایی SSL (SSL Recon)
۱۴۲	خلاصه
۱۴۲	سوالات
۱۴۲	خواندن بیشتر
۱۴۳	بررسی برنامه‌های وب با استفاده از متاسپلویت

۱۴۳	الزامات فنی
۱۴۳	مقدمه سرشماری
۱۴۴	سرشماری DNS
۱۴۶	وقت بیشتری صرف کنید - ویرایش کد منبع
۱۵۲	سرشماری فایل‌ها
۱۵۵	جستجو و کنکاش در وب با متاسیلویت
۱۵۸	اسکن میزبان‌های مجازی
۱۵۹	خلاصه
۱۶۰	سؤالات
۱۶۰	خواندن بیشتر
۱۶۱	اسکن آسیب‌پذیری با استفاده از WMAP
۱۶۱	الزامات فنی
۱۶۲	درک WMAP
۱۶۳	فرآیند اسکن WMAP
۱۶۳	شناسایی داده‌ها
۱۶۹	بارگیری اسکنر
۱۷۱	بیکربندی WMAP
۱۷۵	راه‌اندازی WMAP
۱۷۷	ترتیب اجرای مازول WMAP
۱۸۱	افزودن مازول به WMAP
۱۸۸	اسکن خوشه‌ای با استفاده از WMAP
۱۹۶	خلاصه
۱۹۷	سؤالات

۱۹۷	خواندن بیشتر
۱۹۹	ارزیابی آسیب‌پذیری با استفاده از Nessus
۱۹۹	الزامات فنی
۲۰۰	معرفی نیسوس
۲۰۱	استفاده از نیسوس با متاسیلویت
۲۰۲	احراز هویت نیسوس از طریق متاسیلویت
۲۰۴	دستورات اساسی نیسوس
۲۰۹	وصله کتابخانه متاسیلویت
۲۱۰	انجام اسکن نیسوس از طریق متاسیلویت
۲۱۵	استفاده از دینایس متاسیلویت برای اسکن نیسوس
۲۱۸	وارد کردن اسکن نیسوس در دینایس متاسیلویت
۲۱۹	خلاصه
۲۲۰	سؤالات
۲۲۰	خواندن بیشتر
۲۲۳	تست نفوذ به سیستم‌های مدیریت محتوا - وردپرس
۲۲۳	الزامات فنی
۲۲۴	معرفی وردپرس
۲۲۴	معماری وردپرس
۲۲۵	ساختار قابل پوشه
۲۲۷	شناسایی و سرشماری وردپرس
۲۲۷	تشخیص نسخه
۲۳۲	شناسایی وردپرس با استفاده از متاسیلویت
۲۳۲	سرشماری وردپرس با استفاده از متاسیلویت

ارزیابی آسیب پذیری برای وردپرس.....	۲۳۵
بهره برداری از وردپرس قسمت ۱ - حذف خودسرانه فایل وردپرس	۲۴۷
جریان آسیب پذیری و تجزیه و تحلیل	۲۴۸
بهره برداری از آسیب پذیری با استفاده از متاسپلویت	۲۴۹
قسمت ۲ بهره برداری از وردپرس - تزریق SQL بدون احراز هویت	۲۵۹
جریان آسیب پذیری و تجزیه و تحلیل	۲۵۹
بهره برداری از آسیب پذیری با استفاده از متاسپلویت	۲۶۱
بهره برداری از وردپرس قسمت ۳- وردپرس ۵ اجرای کد از راه دور	۲۶۱
جریان آسیب پذیری و تجزیه و تحلیل	۲۶۱
بهره برداری از آسیب پذیری با استفاده از متاسپلویت	۲۶۴
پیشروی کنید - سفارشی کردن بهره برداری با متاسپلویت	۲۷۴
خلاصه	۲۷۷
سؤالات	۲۷۷
خواندن بیشتر	۲۷۷
نست نفوذ به سیستم های مدیریت محتوا - جوملا	۲۷۹
الزامات فنی	۲۷۹
مقدمه ای برای جوملا	۲۸۰
معماری جوملا	۲۸۰
ساختار فایل و پوشه	۲۸۱
شناسایی و سرشماری	۲۸۳
تشخیص نسخه	۲۸۳
سرشماری پلاگین ها و ماژول های جوملا با استفاده از متاسپلویت	۲۸۹
سرشماری صفحه	۲۸۹