

بمنام خداوند جان و خرد

آموزش تست نفوذ با

Metasploit Framework

www.ketab.ir

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندار پارس

سرشناسه	: داوری دولت آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور	: آموزش تست نفوذ با Metasploit Framework/مجد داوری دولت آبادی.
مشخصات نشر	: تهران: پندار پارس، ۱۳۹۲.
مشخصات ظاهری	: ۳۳۰ص.: مصور، جدول.
شابک	: 978-600-6529-86-8 : ۲۸۰۰۰۰ ریال
وضعیت فهرست نویسی	: فیبا
یادداشت	: کتابنامه: ص. ۳۲۵.
موضوع	: مناسپلویت (منبع الکترونیکی)
موضوع	: کامپیوترها -- کنترل دستیابی
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: آزمایش نفوذ (ایمن سازی کامپیوتر)
رده بندی کنگره	: ۹۷۴QA ۱۳۹۲ ۱۶د۲/م
رده بندی دیویی	: ۵/۸
شماره کتابشناسی ملی	: ۳۹۱۹۹۳۸

با ثبت بوک کد کتاب‌های پندارپارس در سایت، عضو باشگاه خوانندگان
پندارپارس شوید و از خدمات ویژه اعضا بهره‌مند شوید.

انتشارات پندارپارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ www.pendarepars.com
تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ ممراه: ۰۹۲۱۴۳۷۱۹۶۴
info@pendarepars.com

نام کتاب	: آموزش تست نفوذ با Metasploit Framework
ناشر	: انتشارات پندار پارس
تدوین	: مجید داوری دولت آبادی
چاپ نخست	: شهریور ماه ۹۴
شمارگان	: ۵۰۰ نسخه
طرح جلد و صفحه‌آرایی	: سارا یعسوبی
چاپ، صحافی	: روز

قیمت : ۲۸۰۰۰ تومان : شابک : ۹۷۸-۶۰۰-۶۵۲۹-۸۶-۸

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

فهرست مطالب

۹	 سخنی با خوانندگان
۱۱	 فصل نخست: مفاهیم پایه‌ای و نصب ابزار Metasploit در لینوکس
۱۲	 تاریخچه ابزار Metasploit
۱۲	 معماری ابزار Metasploit Framework
۱۷	 نصب و راه‌اندازی ابزار Metasploit بر روی لینوکس
۱۹	 فصل دوم: واسطه‌های کاربری ابزار Metasploit
۱۹	 واسط کاربری msfcli
۲۲	 واسط کاربری msfweb
۲۳	 واسط کاربری Armitage
۲۳	 واسط کاربری msfgui
۲۷	 واسط کاربری msfconsole
۴۵	 فصل سوم: پایگاه‌های داده در ابزار Metasploit
۴۵	 اتصال به پایگاه داده مخصوص ابزار Metasploit
۴۸	 اضافه کردن عناصر گوناگون به پایگاه داده و ابزار Metasploit
۵۱	 حذف و پاکسازی پایگاه داده و عناصر موجود در آن
۵۲	 لیست کردن عناصر ثبت شده در پایگاه داده
۵۴	 وارد کردن عناصر و مقادیر به پایگاه داده
۵۶	 پایگاه‌های داده پیش فرض دیگر در ابزار Metasploit
۵۹	 فصل چهارم: ماژول‌ها در ابزار Metasploit
۵۹	 ماژول‌های کمکی یا Auxiliary
۸۹	 ماژول Exploit و Payload
۱۰۱	 ماژول Encoder
۱۰۲	 ماژول NOPS

۱۰۴.....	مازول POST
۱۰۶.....	اضافه کردن یک مازول جدید به ابزار Metasploit
۱۰۹.....	فصل پنجم؛ پلاگین‌ها در ابزار Metasploit
۱۱۰.....	استفاده از پلاگین nessus
۱۱۱.....	استفاده از پلاگین NeXpose
۱۱۳.....	استفاده از پلاگین openvas
۱۱۵.....	استفاده از پلاگین pcap_log
۱۱۵.....	بهره‌گیری از پلاگین pentest
۱۱۸.....	استفاده از پلاگین wmap
۱۱۹.....	بهره‌گیری از پلاگین‌های دیگر در واسطه کاربری msfconsole
۱۲۵.....	اضافه کردن پلاگین به ابزار Metasploit
۱۲۷.....	فصل ششم؛ بهره‌گیری از ابزارهای جانبی Metasploit
۱۲۷.....	ابزار msfpayload
۱۳۱.....	ابزار msfencode
۱۳۵.....	ابزار msfvenom
۱۳۶.....	ابزار pattern_create , pattern_offset
۱۳۷.....	ابزار nasm_shell
۱۳۷.....	ابزار msfpescan
۱۳۸.....	ابزار msfupdate
۱۳۹.....	فصل هفتم؛ جمع‌آوری اطلاعات و پوشش با کمک ابزار Metasploit
۱۳۹.....	شناسایی و جمع‌آوری اطلاعات غیرفعال
۱۴۰.....	شناسایی و جمع‌آوری اطلاعات فعال
۱۴۰.....	بهره‌گیری از ابزار Whois, nslookup و dig در حالت غیرفعال
۱۴۲.....	بهره‌گیری از دستور db_nmap برای پیاده‌سازی پوشش پورت
۱۴۵.....	استفاده از مازول‌ها برای جمع‌آوری اطلاعات در حالت فعال
۱۵۷.....	فصل هشتم؛ پوشش آسیب‌پذیری‌ها با کمک ابزار Metasploit

۱۵۸.....	بهره‌گیری از ماژول‌های Auxiliary برای یافتن آسیب‌پذیری‌ها
۱۵۹.....	پوشش آسیب‌پذیری‌ها با کمک پلاگین nessus
۱۶۲.....	پوشش آسیب‌پذیری‌ها با کمک پلاگین openvas
۱۶۶.....	پوشش آسیب‌پذیری‌ها با کمک پلاگین nexpose
۱۶۹.....	پوشش آسیب‌پذیری‌ها با کمک پلاگین wmap
۱۷۳.....	فصل نهم: فرآیند Exploitation
۱۷۳.....	آزمایش نفوذ بر روی سیستم‌عامل ویندوز XP SP2
۱۷۴.....	آزمایش نفوذ بر روی سیستم‌عامل ویندوز XP SP3
۱۷۷.....	آزمایش نفوذ بر روی سیستم‌عامل ویندوز Server 2003
۱۷۸.....	آزمایش نفوذ بر روی سیستم‌عامل ویندوز 7
۱۸۰.....	آزمایش نفوذ بر روی سیستم‌عامل ویندوز Server 2008
۱۸۲.....	آزمایش نفوذ بر روی سیستم‌عامل لینوکس Ubuntu
۱۸۴.....	آزمایش نفوذ بر روی سرویس VOIP
۱۸۴.....	آزمایش نفوذ خودکار بر روی سیستم‌های عامل مختلف
۱۸۹.....	فصل دهم: پیاده‌سازی فرآیند Exploitation غیرفعال (سمت مشتری)
۱۸۹.....	بهره‌برداری مبتنی بر آسیب‌پذیری‌های موجود در مرورگرها
۱۹۷.....	بهره‌برداری مبتنی بر فرمت فایل‌ها
۲۰۴.....	استفاده از ماژول Exploit نوع handler
۲۰۷.....	فصل یازدهم: بهره‌گیری از مکانیزم Meterpreter
۲۰۸.....	دستورات هسته ماژول Meterpreter
۲۱۴.....	دستورات سیستم‌فایل مبتنی بر ماژول Stdapi Meterpreter
۲۱۸.....	دستورات شبکه‌ای مبتنی بر ماژول Stdapi Meterpreter
۲۲۰.....	دستورات سیستمی مبتنی بر ماژول Stdapi Meterpreter
۲۲۷.....	دستورات واسط کاربری مبتنی بر ماژول Stdapi Meterpreter
۲۳۰.....	دستورات Webcam مبتنی بر ماژول Stdapi Meterpreter
۲۳۱.....	دستورات حرفه‌ای و عالی مبتنی بر ماژول Priv Meterpreter

۲۳۲.....	دستورات پایگاه داده کلمه عبور مبتنی بر Priv مازول Meterpreter
۲۳۲.....	دستور Timestamp مبتنی بر Priv مازول Meterpreter
۲۳۴.....	اسکرپت های مازول Meterpreter
۲۵۸.....	استفاده از مازول های Post در قالب مازول Meterpreter
۲۶۹.....	استفاده از الحاقیات در قالب مازول Meterpreter
۲۷۴.....	پیاده سازی مفهوم Pivoting
۲۷۵.....	حفظ و نگهداری دسترسی به سیستم هدف
۲۸۳.....	فصل دوازدهم: ابزارهای SET و Fast-Track
۲۸۵.....	پیکربندی ابزار SET
۲۹۱.....	بردار حمله Spear-Phishing
۲۹۵.....	بردار حملات وب (Web Attack)
۳۰۲.....	بردار حمله براساس تولیدکننده رسانه های ذخیره سازی الوده
۳۰۲.....	ایجاد Payload و Listener
۳۰۲.....	حملات سامانه ارسال نامه الکترونیکی انبوه
۳۰۲.....	بردار حملات Teensy USB HID
۳۰۴.....	بردار حملات جعل SMS
۳۰۴.....	بردار حملات نقطه دسترسی بی سیم
۳۰۴.....	ابزار مازول های Third Party
۳۰۷.....	ابزار Fast-Track
۳۲۵.....	مراجع کتاب

سخنی با خوانندگان

امروزه در دنیای هک و آزمایش نفوذ، ابزارهای گوناگونی به صورت آماده پیاده سازی و ارائه شده است که معمولاً در قالب توزیع های حرفه ای و مخصوص نفوذ لینوکس (Kali, BackTrack و...) و یا به صورت فایل اجرایی قابل نصب در محیط سیستم عامل ویندوز منتشر می شوند. بیشتر این ابزارها کمک شایانی به آزمایش کننده نفوذ و هکر می کنند و نفوذگران از آن ها استفاده های فراوانی می برند. یکی از این نوع ابزارها که پشتیبانی بسیار مناسبی از آن نیز به عمل می آید، ابزار قدرتمند Metasploit Framework است که به عنوان سکوی نرم افزاری در زمینه آزمایش نفوذ و هک مورد استفاده قرار می گیرد. در واقع با کمک این ابزار می توان تمامی مراحل یک حمله کامل را با تمامی جزئیات پیاده سازی کرد. به نوعی می توان گفت آزمایش کننده نفوذ یا نفوذگر چنانچه به این ابزار دسترسی داشته باشد و وارد محیط کنسول اصلی آن شود، به سادگی می تواند تمامی اقدامات نفوذی خود را انجام دهد و در بیشتر موارد نیازی به مراجعه به محیط ابزارهای دیگر برای پیشبرد اهداف خود ندارد.

همانک این ابزار در تمامی توزیع های حرفه ای و ویژه نفوذ لینوکس به صورت آماده و نصب شده موجود می باشد و نیازی به نصب آن در این نوع توزیع ها نیست، اما در سیستم عامل ویندوز باید آن را نصب کرد تا بتوان با کنسول خط فرمان و وب از امکانات آن استفاده کرد. هرچند، گفتنی است که توانایی ها و قابلیت هایی که در نسخه های لینوکسی این ابزار وجود دارد دست نفوذگر یا آزمایش کننده نفوذ را برای پیاده سازی انواع حملات هکری باز می گذارد و ویژگی های بسیاری به آن می افزاید؛ پس پیشنهاد می شود برای استفاده بهتر از این ابزار از نسخه های نصب شده بر روی توزیع های حرفه ای و ویژه ای هک لینوکس استفاده شود تا بتوان به آسانی از تمامی امکانات موجود در آن بهره برد. در این کتاب نیز مبنای اصلی آموزش، نسخه های موجود در توزیع های حرفه ای و ویژه هک لینوکس می باشد. این کتاب تلاش دارد تا متخصصان امنیت یا دانشجویان علم امنیت و هک را هر چه بیشتر به صورت عملی با انواع پیاده سازی حملات هکری آشنا سازد تا آن ها بتوانند در قالب یک محیط عملی این نوع حملات را اجرا کنند و به دنبال راه کارهای امنیتی و مقابله ای با انواع حملات باشند، زیرا این ابزار به آن ها نشان می دهد که چگونه به سادگی می توان با داشتن علم کافی در دنیای امنیت و هک و با کمک ابزارهای موجود می توان به سیستم مقصد نفوذ کرد.

در این کتاب از تمامی منابع معتبر و پایه ای علم هک استفاده شده است که البته با تجربیات ناچیز اینجانب آمیخته شده است تا کتابی جامع و مفید ایجاد شود. اینجانب به عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تالیف کتابی آموزشی به صورت گام به گام به منظور افزایش کارایی عملی متخصصان، دانشجویان و مدیران شبکه در زمینه استفاده از یکی از ابزارهای اساسی آزمایش های نفوذ و هک بودم تا آن ها را با اصول فنی استفاده از این ابزار آشنا و آگاه سازم (گرچه مدیران و متخصصان امنیت شبکه حکم اساتید اینجانب را دارند، اما به حکم وظیفه برخورد لازم دانستم که این آگاه سازی را انجام دهم).

همان گونه که گفته شد، شیرازه ای اصلی این کتاب برگرفته از کتاب ها و منابع معتبر و استاندارد شاخه ای امنیت داده، اصول آزمایش های نفوذ و علم هک، توزیع های استاندارد آزمایش نفوذ و هک و همچنین منابع معتبر آموزش ابزار Metasploit Framework می باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به فرم کاملاً آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام

کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آن‌ها را به دینه منت پذیرا هستم.

(m_Davari@TOP-co.ir)

(m_Davary@Parshack.zzn.com)

هشدار

این کتاب تنها برای افزایش آگاهی و رشد علمی متخصصان علم امنیت و کامپیوتر تألیف شده است. در نتیجه عواقب ناشی از هرگونه سوء استفاده از مطالب این کتاب برعهده شخص خاالی بوده و مؤلف و انتشارات هیچ‌گونه مسئولیتی در این مورد برعهده نخواهند گرفت.

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام این کار ناچیز فشردند، تشکر می‌کنم. برخورد لازم می‌دانم از زحمات بی دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی کنم. زحمات خاضعانه‌ی ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است. در پایان از مدیریت فرزانه‌ی انتشارات پندار پارس جناب آقای مهندس حسین یعسوبی و همهی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یارب ز کمال لطف خالصم گردان

واقف به حقایق خواصم گردان

ز عقل جفا کار دل افگار شدم

دیوانه خود کن و خلاصم گردان

(مجید داوری دولت آبادی - بهار ۱۳۹۴)