به‌نام خداوند جان و خرد

آموزش تست نفوذ با
Metasploit Framework

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندار پارس

سرشناسه : داوری دولت‌آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور : آموزش تست نفوذ با Metasploit Framework/مجید داوری‌دولت‌آبادی.
مشخصات نشر : تهران: پندار پارس، ۱۳۹۴.
مشخصات ظاهری : ۳۳۰ص.: مصور، جدول.
شابک : 978-600-6529-86-8: ۲۸۰۰۰۰ریال
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه: ص. ۳۲۵.
موضوع : متاسپلویت (منبع الکترونیکی)
موضوع : کامپیوترها -- کنترل دستیابی
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : آزمایش نفوذ (ایمن‌سازی کامپیوتر)
رده بندی کنگره : ۹/۷۶QA ۱۳۹۲ ۱۶د۳م/
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۳۹۱۹۹۳۸

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸همراه: 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 : ۸-۸۶-۶۵۲۹-۶۰۰-۹۷۸

فهرست مطالب

سخنی با خوانندگان

امروزه در دنیای هک و آزمایش نفوذ، ابزارهای گوناگونی به‌صورت آماده پیاده‌سازی و ارائه شده است که معمولا در قالب توزیع‌های حرفه‌ای و مخصوص نفوذ لینوکس (Kali ،BackTrack و ...) و یا به‌صورت فایل اجرایی قابل نصب در محیط سیستم‌عامل ویندوز منتشر می‌شوند. بیشتر این ابزارها کمک شایانی به آزمایش‌کننده نفوذ و هکر می‌کنند و نفوذگران از آن‌ها استفاده‌های فراوانی می‌برند. یکی از این نوع ابزارها که پشتیبانی بسیار مناسبی از آن نیز به عمل می‌آید، ابزار قدرتمند Metasploit Framework است که به‌عنوان سکوی نرم‌افزاری در زمینه آزمایش‌نفوذ و هک مورد استفاده قرار می‌گیرد. در واقع با کمک این ابزار می‌توان همه‌ی مراحل یک حمله کامل را با همه‌ی جزئیات پیاده‌سازی کرد. به نوعی می‌توان گفت آزمایش‌کننده نفوذ یا نفوذگر چنانچه به این ابزار دسترسی داشته باشد و وارد محیط کنسول اصلی آن شود، به‌سادگی می‌تواند همه‌ی اقدامات نفوذی خود را انجام دهد و در بیشتر موارد نیازی به مراجعه به محیط ابزارهای دیگر برای پیشبرد اهداف خود ندارد.

هم‌اینک این ابزار در همه‌ی توزیع‌های حرفه‌ای و ویژه نفوذ لینوکس به‌صورت آماده و نصب شده موجود می‌باشد و نیازی به نصب آن در این نوع توزیع‌ها نیست، اما در سیستم‌عامل ویندوز باید آن‌را نصب کرد تا بتوان با کنسول خط‌فرمان و وب از امکانات آن استفاده کرد. هرچند، گفتنی است که توانایی‌ها و قابلیت‌هایی که در نسخه‌های لینوکسی این ابزار وجود دارد دست نفوذگر یا آزمایش‌کننده نفوذ را برای پیاده‌سازی انواع حملات هکری باز می‌گذارد و ویژگی‌های بسیاری به آن می‌افزاید؛ پس پیشنهاد می‌شود برای استفاده بهتر از این ابزار از نسخه‌های نصب شده بر روی توزیع‌های حرفه‌ای و ویژه‌ی هک لینوکس استفاده شود تا بتوان به آسانی از همه‌ی امکانات موجود در آن بهره برد. در این کتاب نیز مبنای اصلی آموزش، نسخه‌های موجود در توزیع‌های حرفه‌ای و ویژه هک لینوکس می‌باشد. این کتاب تلاش دارد تا متخصصان امنیت یا دانشجویان علم امنیت و هک را هر چه بیشتر به‌صورت عملی با انواع پیاده‌سازی حملات هکری آشنا سازد تا آن‌ها بتوانند در قالب یک محیط عملی این نوع حملات را اجرا کنند و به دنبال راه‌کارهای امنیتی و مقابله‌ای با انواع حملات باشند، زیرا این ابزار به آن‌ها نشان می‌دهد که چگونه به‌سادگی می‌توان با داشتن علم کافی در دنیای امنیت و هک و با کمک ابزارهای موجود می‌توان به سیستم مقصد نفوذ کرد.

در این کتاب از همه‌ی منابع معتبر و پایه‌ای علم هک استفاده شده است که البته با تجربیات ناچیز اینجانب آمیخته شده است تا کتابی جامع و مفید ایجاد شود. اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تالیف کتابی آموزشی به‌صورت گام به گام به‌منظور افزایش کارایی عملی متخصصان، دانشجویان و مدیران شبکه در زمینه استفاده از یکی از ابزارهای اساسی آزمایش‌های نفوذ و هک بودم تا آن‌ها 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 برخود لازم دانستم که این آگاه‌سازی را انجام دهم.)

همان‌گونه که گفته شد، شیرازه‌ی اصلی این کتاب برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه‌ی امنیت داده، اصول آزمایش‌های نفوذ و علم هک، توزیع‌های استاندارد آزمایش نفوذ و هک و همچنین منابع معتبر آموزش ابزار Metasploit Framework می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به‌فرم کاملا 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 دیده 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 تالیف شده است. درنتیجه عواقب ناشی از هرگونه سوء استفاده از مطالب این کتاب برعهده شخص خاطی 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. برخود 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 خاصم 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)