

بسم الله الرحمن الرحيم

راهنمای متاسیلویت

ویژه : متخصصین امنیت فناوری اطلاعات و تست نفوذ

اولین مرجع فارسی متاسیلویت

نویسندگان :

مهندس رضا مقدم

مهندس میلاد کهساری الهادی

شابک	۹۷۸-۶۰۰-۷۰۲۶-۶۲-۵
شماره کتابشناسی ملی	۳۲۳۴۶۷۸
عنوان و نام پدیدآور	راهنمای متاسپلویت/ مولفین رضا مقدم، میلاد کهساری الهادی.
مشخصات نشر	تهران: آرنا، ۱۳۹۲.
مشخصات ظاهری	۳۶۰ ص.
موضوع	متاسپلویت (منبع الکترونیکی)
موضوع	کامپیوترها -- کنترل دستیابی
موضوع	آزمایش نفوذ (ایمن سازی کامپیوتر)
موضوع	شبکه های کامپیوتری -- تدابیر ایمنی
موضوع	نرم افزار متن باز
رده بندی دیویی	۰۰۵/۸
رده بندی کنگره	۷۷۱۳۹۲/م۲۹/۷۶QA
میشناسه	مقدم، رضا، ۱۳۶۹ -
شناسه داده	کهساری الهادی، میلاد، ۱۳۷۳ -
وضعیت فهرست	فیا
نویسی	



نشر آرنا

عنوان : راهنمای متاسپلویت

نویسنده : رضا مقدم، میلاد کهساری الهادی

ناشر : آرنا

طرح جلد : رضا مقدم

چاپ : اول ۱۳۹۲

شمارگان : ۱۰۰۰ نسخه

قیمت: ۱۳۰۰۰ تومان

شابک : ۹۷۸-۶۰۰-۷۰۲۶-۶۲-۵

www.arnapub.com

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

لَهُ عَجَلٌ لَوْلِيكَ الْفَرَجَ وَالْعَافِيَهُ وَالنَّصْرَ وَاجْعَلْنَا
مِنْ خَيْرِ أَنْصَارِهِ وَاعْوَانِهِ وَالْمُسْتَشْهِدِينَ بَيْنَ يَدَيْهِ

پادشاه، ولیّات حضرت محمد بن الحسن که دروذهای تو بر او و بر پدراناش باد.

در این لحظه و در تمام لحظات سیرت و نگاهدار و راهبر و یاری گر و راهنما

دیدباناش باش، تا او را به صورتی که خواهد بود اوست ساکن زمین گردانی ، و

تو زمان طولانی در آن بهره‌مند سازی.

پیشگفتار^۱

سپاس خداوند یکتا را که فرصت دوباره ای را فراهم آورد تا بتوانیم کتاب راهنمای چهارچوب متاسپلویت را به زبان پارسی برگردانده و یک مرجع کامل برای آن تعریف نماییم. همواره در عرض امنیت و اطلاعات کشورمان جای خالی یک کتاب مرجع و راهنما برای این برنامه آزمایش صحه امنیت به زبان پارسی حس می شد، به همین دلیل با استناد به نیازمندی ها در این زمینه ، دست به قلم برده شد و نهایتا موجب تالیف این کتاب گردید .

این کتاب راهنمای استفاده از چهارچوب متاسپلویت میباشد که در زمینه امنیت و نفوذگری برای متخصصین فناوری اطلاعات یک برنامه فوق العاده کاربردی به شمار می رود، این برنامه امنیتی می توان فروشگاه ، انبارز و های نفوذگری فرض نمود زیرا هر درخواستی که یک شخص متخصص امنیت اطلاعات طلب نماید می تواند در آن به دست آورد. متاسفانه درحال حاضر اکثریت متخصصین در کشور عزیزمان ، این برنامه را مختص به هک و نفوذ کلاینت می دانند و با دید قابلیت های این برنامه آشنایی کامل ندارند .

هدف از ارائه این کتاب ، ابتدا آشنایی با اصول برنامه متاسپلویت و سپس ارتقاء سطح علم مخاطب به یک کاربر نیمه حرفه ای در استفاده از برنامه متاسپلویت می باشد. در نهایت جای دار از آقایان پدرام امینی، سعید بیکی، محمد جرجندی و علی بیگی که ما را در نوشتن این کتاب یاری نموده اند تشکر فراوان نماییم.

مانطور که پیش تر گفته شد ، این کتاب طراحی شده تا اصول کار با فریمورک متاسپلویت و تکنیک های بهره برداری از ضعف های امنیتی^۱ را با استفاده از چهارچوب متاسپلویت به متخصصین امنیت اطلاعات آموزش دهد. هدف اصلی ارائه این کتاب که نسخه مرجع می باشد، آموزش به مبدیان و ایجاد یک منبع کامل برای علاقه مندان به علوم هکینگ و امنیت بوده است. مل ذکر است که مطالب این کتاب فقط بر روی متاسپلویت متمرکز نخواهد بود و در تشریح برخی ملاحظات به توضیح دادن برخی های دیگر خواهیم پرداخت.

پایین حال این کتاب ، کم کاستی هایی خواهد داشت و نمی توان گفت که تمام نیاز های خوانندگان را در بر می تواند بگیرد ، اما تلاش مکرر سعی در بروز رسانی و گسترش محتویات آن داریم .

اول از آنکه شروع به تشریح فصول کتاب نمودیم ، این موضوع دقت داشته باشید. برای انجام مایشات امنیت نیاز به دانش برنامه نویسی در حد کافی می باشید. مسلما پایه ترین مهارت یک مکر یا متخصص امنیت، مهارت آن در برنامه نویسی است، اگر تا به حال هیچ زبانه برنامه نویسی فرا نگرفتید، پیشنهاد می شود که با مفسر پایتون شروع کنید. پایتون به خوبی طراحی و مستند سازی شده و تقریبا ابتدایی است، اما با اینکه پایتون زبان اولیه خوبی برای شروع است، بسیاری آن را یک اسباب بازی فرض نکنید. بلکه زبان برنامه نویسی پایتون بسیار قدرتمند و انعطاف پذیر طراحی و سازماندهی شده است. اما علاوه بر پایتون خوانندگان این کتاب نیاز دارند با زبان برنامه نویسی روبي هم آشنا باشند، زیرا در استفاده از متاسپلویت و مزیف های که آن در دست کارسازی فرآیند های آزمایش نفوذ ارائه می دهد و تماما این چهارچوب و سایر ابزارها با روبي دست سازی شده است.

^۱ Exploitation Vulnerability

عموما هر شخصی که قصد دارد در زمینه نفوذگری فعالیت نماید لازم است از علم برنامه نویسی برخوردار باشد، با این حال همواره پیشنهاد می شود که در مرحله اول یک زبان برنامه نویسی فرا گرفته سپس بعد از فراگیری زبان برنامه نویسی (پایتون یا روبی) وارد دنیای آزمون امنیتی شوید، چرا که دانستن یک زبان برنامه نویسی کمک شایانی در درک مطالب این کتاب بهره داری پیشرفته از ضعف های امنیتی و سفارشی سازی حملات به شما می کند و در آیند این امکان را به شما خواهد داد که بتوانید حملات موفق تری را پیاده سازی و سازماندهی کنید.

ضمناً هر چقدر تجربه کار با متاسپلویت بیشتر گردد ، متوجه خواهید شد که این فریمورک به طور مرتب با ویژگی های جدید، اکسپلویت ها و حملات به روز می شود. از همین روی ما در این کتاب بر روی اصول متاسپلویت تمرکز خواهیم کرد تا بتوانید با یک بار فراگیری اینکه چهارچوب متاسپلویت چگونه کار می کند، با تغییراتی که در طول توسعه آن حاصل می شود به راحتی کنار بیایید و خود را با آن هماهنگ سازید. در حالت کلی در این کتاب می آموزید که چگونه کار با متاسپلویت را شروع کنید و سپس خداتان را از یک کاربر معمولی یا آماتور به یک کار نیمه حرفه ای بالا ببرید، و نکته قابل ذکر دیگر اینست که، تمامی فصل های این کتاب به ه دیگر مرتبط هستند و برای اینکه بتوانید مهارت خود را در آزمایش نفوذپذیری و آزمایش امنیتی بالا ببرید، باید تمامی دروس را فرا بگیرید. ♦

فهرست مطالب

۱۹	 فصل اول: مبانی مطلق در آزمون نفوذ
۲۰	 متاسپلویت چیست؟
۲۰	 تاریخچه مختصری از متاسپلویت
۲۲	 مبانی مطالبی در آزمون نفوذ
۲۳	 فاز های آزمایش امنیت استاندارد
۲۳	 فاز اول: توافق ای قبل از قرارداد
۲۴	 فاز دوم : جمع آوری اطلاعات
۲۵	 فاز سوم : مدل سازی یک سیستم
۲۶	 فاز چهارم : تحلیل آسیب پذیری ها
۲۶	 فاز پنجم : اکسپلویت کردن آسیب پذیری ها
۲۷	 فاز ششم : پس از اکسپلویت کردن سیستم
۲۷	 فاز هفتم : گزارش نویسی
۲۸	 انواع آزمون های نفوذ
۲۸	 آزمایش امنیت آشکارا
۲۹	 آزمایش امنیت پنهان
۳۰	 واژگان
۳۰	 اکسپلویت
۳۰	 پایلود
۳۱	 شلکد
۳۱	 ماژول

۱		شنونده
۲		بویشرهای آسیب پذیری (حفره های امنیتی)
۶		فصل دوم: اصول استفاده از متاسپلویت
۶		واسط های کاربری متاسپلویت
۷		منسول متاسپلویت
۷		واسط کسور متاسپلویت
۹		واسط خط فرمان
۳		واسط گرافیک متاسپلویت
۴		واسط آرمیتج
۵		کار با پایگاه داده در متاسپلویت
۵		نصب PostgreSQL
۶		متصل شدن به بانک اطلاعاتی
۸		وارد کردن نتایج پویش namp به داخل متاسپلویت
۹		آنالیز داده های ذخیره شده
۰		برنامه های کاربردی متاسپلویت
۱		MSFPayload
۲		قسمت ششم: رمز نگاری شلکد
۳		پوسته ی اسمبلر NASM
۳		نسخه های تجاری متاسپلویت
۶		فصل دوم : جمع آوری اطلاعات

۵۸	جمع آوری غیرمستقیم اطلاعات
۵۸	جمع آوری اطلاعات مستقیم
۵۹	جمع آوری اطلاعات از طریق مهندسی اجتماعی
۵۹	WHOIS
۶۱	Netcraft
۶۲	کارگزار نام دامنه
۶۲	کارگزار نام دامنه چیست؟
۶۲	NSLookup
۶۳	اجرای برنامه NSLookup
۶۵	جمع آوری مستقیم اطلاعات
۶۵	نحوه عملکرد برنامه های پویشر درگاه ها
۶۶	Nmap چیست؟
۶۷	پویش درگاه به وسیله Nmap
۶۸	اجرا کردن Nmap در متاسیلویت
۶۸	پویش TCP Connect :
۶۹	پویش TCP SYN :
۷۰	پویش UDP :
۷۱	پویش ACK :
۷۲	استفاده از Nmap برای شناسایی سیستم عامل و نسخه آن
۷۳	گزینه های دیگر Nmap:

۴	پوش مخفیانه (Decoy Scan)
۵	بررسی ماژول های کمکی متاسپلویت برای پوشگری
۹	مدیریت تردها
۰	پوشگری سرویس های هدف با ماژول های کمکی متاسپلویت
۳	پوشگری ضعف های امنیتی با Nessus
۸	کار کردن با Nessus در مرورگر
۹	پوشگری با استفاده از NeXpose
۱	وارد کردن نتایج پوش به متاسپلویت
۱	به اشتراک گذاری اطلاعات با استفاده از Dradis
۸	فصل چهارم: بهره برداری و ارزیابی امنیت، مبتنی بر سیستم عامل
۹	راهنما سریع استفاده از اکسپلویت ها
۰۰	show exploits و show payloads
۰۰	: search
۰۱	: use exploit
۰۱	: show options
۰۲	: Set
۰۳	: Unset
۰۴	: show targets
۰۴	: Info
۰۵	آزمایش امنیت ویندوز XP سرویس پک دو

فعال سازی دسترسی از راه دور	۱۱۰
دسترسی از راه دور به هدف	۱۱۳
آزمودن امنیت سرور های ویندوز سرور ۲۰۰۳	۱۱۶
حلقه های نهایی در سرویس SMB سمت کاربر	۱۲۰
اکسپلورر کردن سیستم عامل لینوکس	۱۲۳
درک خطای ترمینال DEL در ویندوز هفت	۱۲۷
ابزار HijaackAudit	۱۳۱
صل پنجم: بهره برداری سمت کاربر و دور زدن آنتی ویروس ها	۱۳۴
یک مرور کلی	۱۳۶
آسیب پذیری پیکربندی اشتباه به صورت اسکریپت نویسی غیر ایمن در مرورگر اینترنت اکسپلورر	۱۳۸
تخریب حافظه به وسیله Aurora	۱۴۵
تخریب حافظه بواسطه ی فراخوانی بازگشتی یک فایل CSS	۱۴۵
گم شدن NET CLR	۱۴۹
آسیب پذیری سر ریز پشته Word RTF مایکروسافت	۱۵۰
سرریز بافر تابع util.printf() در ادوبی ریدر	۱۵۴
تولید فایل باینری و شلکد از msfpayload	۱۶۰
دور زدن آنتی ویروس سمت کاربر با استفاده از msfencode	۱۶۷
آزمایش کردن فایل ها توسط VirusTotal	۱۷۷
غیر فعال کردن آنتی ویروس با استفاده از اسکریپت killerav.rb	۱۷۸

۷۹	مفسر متاسپلویت
۸۳	غیر فعال کردن آنتی ویروس
۸۴	نگاهی عمیق تر به اسکریپت <code>killerav.rb</code>
۸۹	از بین بردن سرویس آنتی ویروس از طریق خط فرمان
۹۳	<code>msfvenom</code> چیست؟! ..
۹۸	فصل ششم: استفاده کردن از مفسر متاسپلویت برای کاوش قربانی مورد نفوذ قرار گرفته
۰۱	تحلیل سیستم فرماندهی مفسرم متاسپلویت
۰۲	: Background
۰۲	: Getuid
۰۳	: Getpid
۰۳	: Ps
۰۴	: Sysinfo
۰۴	: Shell
۰۵	: Exit
۰۶	اما مفسر متاسپلویت چگونه کار می کند؟
۰۶	بالا بردن سطح دسترسی و کوچ دادن پروسه
۰۸	روش جعل مسیر ارتباطی پروسه ها (Namedpipe)
۰۸	روش تکرار توکن
۰۹	اکسپلویت <code>KiTrapOD</code>
۱۱	راه اندازی چندین کانال ارتباطی با قربانی

۲۱۱		راه اندازی کانال ارتباطی با فرمان execute
۲۱۶		دستورات سیستم فایل مفسر متاسپلویت
۲۱۹		تغییر دادن ویژگی فایل ها با استفاده از timestamp
۲۲۳		استفاده کردن از دستورات شبکه مفسر متاسپلویت
۲۲۴		Subnetmask
۲۲۴		Netmask
۲۲۴		Gateway
۲۲۹		دریافت صفحه نمایش و شناسایی کلیدهای فشرده شده
۲۲۹		Enumdesktops
۲۳۰		Getdesktop
۲۳۱		Setdesktop
۲۳۱		keyscan_start
۲۳۱		keyscan_dump
۲۳۵		استفاده از اسکریپت scraper مفسر متاسپلویت
۲۳۸		اسکریپت winenum.rb
۲۴۰		صل هفتم: مباحث پیشرفته مفسر متاسپلویت
۲۴۲		عبور هش
۲۴۵		رمزگشایی آنلاین کلمه های عبور
۲۴۷		راه اندازی یک ارتباط دائمی با بکدور
۲۴۸		اسکریپت Metsvc

.....	حمله محوری با استفاده از مفسر متاسپلویت	۵۴
.....	یک مثال عملی از حملات محوری	۵۸
.....	رابط های برنامه نویسی متاسپلویت	۷۰
.....	میکرین های مفسر متاسپلویت	۷۵
.....	Railgun تبدیل کننده مفسر روبی به یک صلاح قدرتمند	۷۸
.....	استندای Railgun	۸۲
.....	اضافه کردن کتابخانه پویا و تابع خود به Railgun	۸۲
.....	ساخت یک اسکریپت اسیر فعال کننده فایروال	۸۶
.....	استفاده مجدد از دستورات ها	۹۲
.....	تجزیه و تحلیل یک اسکریپت	۹۲
.....	فصل هشتم: کار با ماژول های اسکریپت متاسپلویت	۱۰۳
.....	تولید کلمه عبور با Crunch	۱۰۷
.....	کار با ماژول های کمکی مدیریت	۱۰۷
.....	ماژول های حملات تکذیب سرویس و تزریق	۱۱۰
.....	ماژول های پس از بهره برداری	۱۱۲
.....	اصول اسکریپت نویسی برای متاسپلویت	۱۱۵
.....	چگونه برای متاسپلویت اسکریپت بنویسم؟!	۱۱۶
.....	نوشتن یک اسکریپت ساده و فراخوانی آن از مفسر متاسپلویت	۱۱۶
.....	اصول ماژول نویسی برای متاسپلویت	۱۱۹
.....	فصل نهم: آرمیتج	۱۲۳

۳۲۵	نصب و راه اندازی آرمیتج در لینوکس
۳۲۷	پویشتگری و جمع آوری اطلاعات با آرمیتج
۳۲۹	پیدا کردن ضعف امنیتی و حمله به اهداف
۳۳۱	آرمیتج در فاز پس از بهره برداری
۳۳۳	آرمیتج در حملات سمت کاربر
۳۳۶	یوست اول - پیکربندی اماکن
۳۳۶	نصب و اعمال تنظیمات بر روی سیستم هدف
۳۳۶	VMWare چیست
۳۳۷	اما بک ترک چیست؟
۳۳۸	ابزارهای بک ترک
۳۳۹	دریافت بک ترک
۳۴۱	بررسی سلامت دانلود توسط MD5sum
۳۴۳	نصب و راه اندازی سیستم عامل
۳۵۰	نصب و راه اندازی ویندوز XP آسیب پذیر
۳۵۱	پیکربندی وب سرور بر روی ویندوز XP
۳۵۲	ساخت یک سرور SQL
۳۵۶	ساختن یک برنامه تحت وب آسیب پذیر
۳۶۰	یوست دوم : پویشتگر Nessus
۳۶۰	پویشتگر Nessus چیست؟!
۳۶۱	برخی از مزئیت های Nessus :

نصب و پیکربندی پوششگر Nessus ۶۲

نصب Nessus بر روی یک ترک: ۶۴

www.ketab.ir