بسم الله الرحمن الرحیم

راهنمای متاسپلویت

ویژهٔ : متخصصین امنیت فناوری اطلاعات و تست نفوذ

اولین مرجع فارسی متاسپلویت

نویسندگان :

مهندس رضا مقدم

مهندس میلاد کهساری الهادی

شابک	:	۹۷۸-۶۰۰-۷۰۲۶-۶۲-۵
شماره کتابشناسی ملی	:	۳۲۳۳۶۷۸
عنوان و نام پدیدآور	:	راهنمای متاسپلویت/ مولفین رضا مقدم، میلاد کهساری‌الهادی.
مشخصات نشر	:	تهران: آرنا، ۱۳۹۲.
مشخصات ظاهری	:	۳۶۰ ص.
موضوع	:	متاسپلویت (منبع الکترونیکی)
موضوع	:	کامپیوترها -- کنترل دسترسی
موضوع	:	آزمایش نفوذ (ایمن‌سازی کامپیوتر)
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	:	نرم‌افزار متن‌باز
رده بندی دیویی	:	۰۰۵/۸
رده بندی کنگره	:	QA۷۶/۹م/ ۱۳۹۲ ۷م
شناسه	:	مقدم، رضا، ۱۳۶۹ -
شناسه افزوده	:	کهساری الهادی، میلاد، ۱۳۷۳ -
وضعیت فهرست نویسی	:	فیپا

عنوان : راهنمای متاسپلویت

نویسندگان : رضا مقدم، میلاد کهساری‌الهادی

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 اللّهِ الرَّحْمنِ الرَّحيمِ

ـلّـهـ عـجّـل لـولـيـک الـفَـرَج و العـافـيـهٔ و الـنَـصـر و اجـعـلـنـا
من خَيرَ اَنـصاره و اعوانه و المُستشهَدين بَـينَ يَـدَيـه

دايا، ولیّ ات حضرت حجت بن الحسن که درودهای تو بر او و بر پدرانش باد.

ر این لحظه و در تمام لحظات سرپرست و نگاهدار و راهبر و یاری گر و راهنما

دیدبانش باش، تا او را به صورتی که خشنود اوست ساکن زمین گردانی ، و

ت زمان طولانی در آن بهره‌مند سازی.

پیشگفتار[1]

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 عرصه امنیت و اطلاعات کشورمان جای خالی یک کتاب مرجع و راهنما برای این برنامه آزمایش صحت 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 را می توان فروشگاهی از ابزارها و 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 دیگر قابلیت های این برنامه آشنایی کامل ندارند .

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

---

[1] cknowledgments

قدمه

مانطور که پیش تر گفته شد ، این کتاب طراحی شده تا اصول کار با فریمورک متاسپلویت و تنیک های بهره برداری از ضعف های امنیتی[1] را با استفاده از چهارچوب متاسپلویت به خصصی امنیت اطلاعات آموزش دهد. هدف اصلی ارائه این کتاب که نسخه مرجع می باشد، وزش به مبتدیان و ایجاد یک منبع کامل برای علاقه مندان به علوم هکینگ و امنیت بوده است. ل ذکرست که مطالب این کتاب فقط بر روی متاسپلویت متمرکز نخواهد بود و در تشریح برخی ملات به توضیح دادن برنامه های دیگر خواهیم پرداخت.

این حال این کتاب کمی پیشرفته هایی خواهد داشت و نمی توان گفت که تمام نیاز های وانندگان را در بر می تواند بگیرد، اما تلاش مکرر سعی در بروز رسانی و گسترش محتویات آن ردیم .

ل از آنکه شروع به تشریح فصول کتاب نمایم ، به این موضوع دقت داشته باشید، برای انجام مایشات امنیت نیاز به دانش برنامه نویسی در حد کافی می باشید. مسلما پایه ترین مهارت یک کر 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 نمایید، زیرا پایتون به خوبی طراحی و ستند سازی شده و تقریبا ابتدایی است، اما با اینکه پایتون زبان برنامه نویسی خوبی برای شروع است، ی آن را یک اسباب بازی فرض نکنید. بلکه زبان برنامه نویسی پایتون بسیار قدرتمند و انعطاف یر طراحی و سازماندهی شده است. اما علاوه بر پایتون خوانندگان این کتاب نیاز دارند با زبان امه نویسی روبی هم آشنا باشند، زیرا در استفاده از متاسپلویت و مزیت هایی که آن در ودکارسازی فرآیند های آزمایش نفوذ ارائه می دهد و تماما این چهارچوب و سکو را با روبی ده سازی شده است.

[1] Exploition 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 امنیت
شوید، چرا که دانستن یک زبان برنامه نویسی کمک شایانی در درک مطالب این کتاب
بهره برداری پیشرفته از ضعف های امنیتی و سفارشی سازی حملات به شما می کند و در آینده
این امکان را به شما خواهد داد که بتوانید حملات موفق تری را پیاده سازی و سازماندهی کنید.

ضمنا 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 سطح خودتان را از یک کاربر معمولی یا آماتور به یک کاربر
نیمه حرفه ای بالا ببرید، و نکته قابل ذکر دیگر اینست که، تمامی فصل های این کتاب به هم
دیگر مرتبط هستند و برای اینکه بتوانید مهارت خود را در آزمایش نفوذپذیری و آزمایش امنیت
بالا ببرید، باید تمامی دروس را فرا بگیرید.

فهرست مطالب