آموزش Recon-NG : شناسایی اهداف هک و نفوذ در کالی لینوکس بخش ۱ (نسخه PDF)

ابزار زیادی در لینوکس کالی وجود دارنـد که در جمع آوری و شـناسایی اطلاعات بما کمک میکننـد. وقتی که یک هکر به یک هـدف حمله میکنـد، یکی از معمول ترین مراحلی را که پس از آن انجام میدهد، جمع آوری اطلاعات است؛ چرا که هکر میخواهد از شـبکه هدف بیشتر بداند تا بتواند بیشتر و اساسی تر حمله خود را انجام دهد.Maltego یکی از محبوبترین ابزار در این زمینه است که در بسیاری از کتاب های امنیتی و سمینارهای آموزشی از آن استفاده میکنند.

از آنجا که اسـتفاده از این ابزار کمی فراگیر است، بنابراین به نظر میرسـد بهتر باشـد در این بخش زمان را به آموزش دیگر ابزار موجود در کالی در این زمینه اختصاص دهیم. در این قسمت نگاهی به یکی از ابزارهای جدیدتر داریم؛ Recon-NG و دو ابزار دیگر که در کالی وجود دارند.فریم ورک Recon-NG ابزار قدرتمندی است که بشما این امکان را میدهد تا عملیات جمع آوری اطلاعات و شناسایی شبکه را بصورت خودکار انجام دهید. میتوانید به آن به دید Metasploit ای برای جمع آوری اطلاعات نگاه کنید. این ابزار بصورت خودکار بسـیاری از مراحل ابتدایی در انجام تست نفوذ را یک تنه انجام میدهد. این ابزار داری خصوصیات زیادی است که در ادامه به برخی از آن ها می پردازیم.

استفاده از Recon-NG

برای شروع استفاده از ابزار Recon-NG، محیط ترمینال را باز کرده و عبارت "recon-ng" را تایپ کنید:

عبارت help" را تایپ کنید تا لیستی از دستورات مرتبط برای شما نمایش داده شود:

حالا مانند محیط Metasploit، میتوانید با تایپ عبارت "show modules" لیستی از ماژول های موجود را مشاهده کنید:

برخی از ماژول های پسـیو هسـتند؛ به این معنی که آن ها هرگز در سیستم و شبکه مقصد تغییری ایجاد نمیکنند.یکی از تاکتیک هایی که در کاوش ساختار شـبکه بصورت پسـیو مورد استفاده قرار میگیرد، استفاده از موتور جستجوی گوگل برای محاسبه دومین های زیر مجموعه سایت است. شـما همیشه از دومین اصـلی هـدف مثل yahoo.com خبر داریـد امـا در مورد دومین هـای زیر مجموعه yahoo.com چیزی نمیدانید که باید به آن پی ببرید.

شما میتوانید با استفاده از سوئیچ های ":site" و ":inurl" دومین های زیر مجموعه را در گوگل جستجو کنید. سپس دومین های زیر مجموعه (inurl-) را که پیـدا کردیـد، پـاک کرده تا بقیه دومین های زیر مجموعه نیز نشان داده شونـد. این عمل اگر بصورت دستی و سـنتی انجام شود میتواند زمان زیادی را از شما بگیرد و در صورتی که دومین مورد نظر دارای زیر دومین های زیادی باشد، مستلزم تست و تایپ زیادی است.Recon-NG

تمـام این کارهـا را بصورت اتوماتیـک انجام داده و در صورت پیـدا کردن مواردی، آن را در دیتابیس خود ذخیره میکنـد. برای اینکار فقط کـافیست که ماژول "recon/hosts/gather/http/web/google_site" را برای اسـتفاده انتخاب کنیم. سـپس برای مشاهـده ملزومات این ماژول عبارت "show options" را تایپ میکنیم.

همـانطور کـه مشاهـده کردیـد، ایـن مـازول فقـط بـه تعییـن دومین مقصـد نیـاز دارد. اگر در Metasploit بودیـد، عبـارت "set domain] targetname.com]" را تایپ کرده و پس از اجرای آن با صدور فرمان "run"، ماژول اجرا خواهد شد. در زیر این مراحل را خواهیم دید:

پس از اجرای ماژول، با صفحه ای مشابه آن چه که ما در زیر برایتان شبیه سازی کرده ایم، روبرو میشوید:

همانطور که در شکل بالا مشاهده کردید، Recon-NG دومین های زیر مجموعه برای وب سایت SomeDomainName.com را محاسبه کرد. در عرض چند ثانیه چندین دومین زیر مجموعه بصورت لیست شده در اختیار شما قرار گرفتند که اگر شما اینکار را میخواستید بصورت دستی

انجام دهید، ممکن بود زمان زیادی را برای آن کنار میگذاشتید. تمام دیتایی که توسط Recon-NG گرداوری شده است در دیتابیس ذخیره میگردد. شـما میتوانید برای مشاهده دیتای گرداوری شده، یک گزارش ایجاد کنید. برای اینکار باید عبارت "back" را تایپ کرد تا از محیط مازول خارج شد:

مجددا عبارت "show modules" را تایپ کنید. به بخش "Notice" دقت کنید:

از یکی از فرمت های پیشنهاد شده استفاده کرده تا گزارشی از آنچه که بدست آورده اید در اختیارتان قرار گیرد:

تمامی فایل ها در آدرس "/usr/share/recon-ng/workspaces/default" ذخیره میشوند.

سربلند و مانا باشید.

پایان

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی