به نام خدا

کوله پشتی یک هکر

THE HACKER'S BACKPACK

حسین احمدی

https://mrpython.blog.ir

فهرست مطالب

مقدمه

هک ، کلمه ای هیجانی و پر طرفدار است به طوری که افراد زیادی را میتوانید پیدا کنید که با شنیدن و دیدن فعالیت های هکرها هیجان زده میشوند . شاید شما هم از دسته افرادی باشید که حداقل در یک دوره ای از زندگی خود دوست داشته اید تا یک هکر باشید و سعی کرده اید علوم هکینگ را فرا بگیرید . ولی باید بگویم که هک و هکینگ همیشه آن چیزی نیست که به نظر میرسد و مردم راجع به آن صحبت میکنند . وقتی صحبت از هکر ها میکنیم شاید تصویری که در ذهن خیلی از ما پدید می آید یک شخصیت شبیه الیوت آلدرسون (یکی از نقش های اصلی سریال مستررربات) است . اگر این سریال را دیده باشید الیوت آلدرسون که نقش هکر داستان را بازی میکرد ، یک نخبه در شبکه های کامپیوتری بود و بسیاری از سیستم های امنیتی را میتوانست دور بزند و در نتیجه در اکثر مواقع به سیستم های مختلف نفوذ میکرد . خب این تصویر اشتباهی نیست ولی تصویر کاملی از یک هکر نیز نیست . مشکل اینجاست که ما در ذهنمان فقط به نتیجه ی کارهای یک هکر فکر میکنیم . برای مثال اگر یک هکر بخواهد به یک شبکه ی مخابراتی نفوذ کند ، یک فرد عادی فقط به نتیجه ی کار این هکر فکر میکند . برای مثال یکی از نتیجه های کار این هکر این است که شاید میتواند بعضی مکالمات را شنود کند یا ...

همه ی این تصور ها در مورد نتایج کار های هکر درست است ولی نکته ای که فقط افراد متخصص در این زمینه یا عده ای کم به آن فکر میکنند این است که این هکر چه مراحلی را طی کرد تا به این نتیجه برسد !؟ از چه الگوریتمی برای این نفوذ استفاده کرد !؟

یکی از مشکل های سریال مستربات این بود که هیچوقت دردسر ها و سختی هایی که الیوت (یک هکر) برای یادگیری هکینگ تحمل میکند را به نمایش نگذاشت . البته شاید این یک مشکل نباشد چون این موضوع بستگی به مخاطبین سریال دارد . همه ی مخاطبین سریال هکر ها نیستند بنابراین طبیعی است که به این موضوعات در سریال توجه نشود .

در بخش بعدی کلمه ی هک را تعریف میکنیم و انواع هکر ها را شرح میدهیم و در کل در این مقاله کوتاه شما را با ابزارهای سخت افزاری که هکر ها برای هدف های مختلف از آن استفاده میکنند آشنا میکنیم .

هکر کیست و علم HACKING چیست ؟

در بخش قبلی راجع به یک سری از تصور های غلط مربوط به هک و هکر ها صحبت کردیم . در این بخش میخواهیم تعریف صحیح هک و هکر را داشته باشیم .

خب به احتمال زیاد خیلی از ما تعریف هک را نفوذ کردن به یک سیستم میدانیم ولی باید بگویم این تعریف کاملی از هک نیست ! . هک کردن همیشه یا حتی در اکثر مواقع نفوذ و کنترل یک سیستم الکترونیکی نیست .

به قول جادی هک کردن یعنی یک استفاده ای از یک ابزار بکنیم که سازنده ی اون ابزار فکر نمیکرده بشه چنین استفاده ای از این ابزار کرد !!!

بگذارید تا به درک بهتری نسبت به جمله ی بالا برسیم . در بیشتر مواقع مراحل نفوذ به یک سیستم به این صورت است که توضیح میدهم . در ابتدا برای نفوذ به سیستمی ما نیاز داریم تا یک آسیب پذیری از آن سیستم سراغ داشته باشیم . وقتی از سیستم هدف آسیب پذیری سراغ داشته باشیم با استفاده از آن آسیب پذیری میتوانیم عمل نفوذ به آن سیستم را انجام دهیم . فرض کنید شخصی میخواهد وارد یک اتاق شود . در اتاق قفل است و کلید در را ندارد . ولی قفل در خراب است و با چند ضربه ی محکم به در میتوان آن قفل را باز کرد . بنابراین شخص با دانستن همین موضوع که قفل در مشکل دارد و با ضربه باز میشود ، میتواند وارد اتاق شود . در اینجا قفل در نقطه ی آسیب پذیر ماجرا است که یک شخص از این آسیب پذیری استفاده کرد و بدون داشتن کلید وارد اتاق شد . وقتی شخصی میخواهد به یک سیستم

نفوذ کند نیز موضوع به همین شکل است و همانطور که گفته شد در بیشتر مواقع باید یک آسیب پذیری (bug) از سیستم هدف سراغ داشته باشد .

خب شاید سازنده ی آن سیستم از این آسیب پذیری خبر نداشته و نمیدانسته است که با استفاده از این آسیب پذیری میتوان به این سیستم نفوذ کردو این یعنی هک کردن با توجه به تعریفی که در ابتدا از هک کردیم .

حال با توجه به توضیحات بالا به راحتی میتوان هکر را تعریف کرد . البته باید گفت که درک کردن یک هکر به طور کامل فقط برای یک متخصص واقعی امکان پذیر است . هکر کسی است که توانایی هک کردن را دارد . یعنی میتواند به نحوی نقاط آسیب پذیر را پیدا کند و از آن ها استفاده کند که دیگران از آن خبر نداشته اند . به طور کلی هکر ها را به سه دسته تقسیم میکنند : هکر های کلاه سفید ، کلاه سیاه و کلاه خاکستری .

هکر های کلاه سفید آن دسته هکر هایی هستند که علم زیادی در این زمینه دارند و روز به روز تلاش میکنند تا نقاط آسیب پذیر را در سیستم های کامپیوتری پیدا کنند و به صاحبان آن ها خبر بدهند تا آن ها را برطرف سازند .

اما هکر های کلاه سیاه دقیقا برعکس هکر های کلاه سفید هستند . هکر های کلاه سیاه همان هکر های مخرب هستند که نقاط آسیب پذیر را پیدا میکنند و از آن ها برای نفوذ به سیستم های مختلف استفاده میکنند یا به عبارتی از آن ها سوء استفاده میکنند .

هکر های کلاه خاکستری میان هکر های کلاه سفید و هکر های کلاه سیاه هستند یعنی گاهی اوقات به عنوان هکر کلاه سفید و گاهی اوقات به عنوان هکر کلاه سیاه عمل میکنند .

در اینجا خوب است تا شما را با بزرگ ترین هک هایی که در تاریخ کامپیوتر ها تا به الان اتفاق افتاده آشنا کنیم .

1 – هک 37 میلیون اکانت کاربری در سال 2015

در سال 2015 گروه هکری به نام Impact Team به سرور های سایت Avide Life Media حمله کردند و اطلاعات شخصی 37 میلیون کاربر را به سرقت بردند . پس از اتمام هک و سرقت اطلاعات ، هکر ها اطلاعات هک شده را در اینترنت منتشر کردند .

2 – ویروس STUXNET

ویروس استاکس حجمی کمتر از 1 مگابایت داشت و یکی از معروف ترین و خطرناک ترین ویروس های تاریخ شناخته میشود . این ویروس برای سیستم های هسته ای طراحی شده بود و میتوانست کنترل سانتریفیوژ های یک پایگاه هسته ای را تحت کنترل بگیرد و نمونه های اورانیوم را نابود کند .

این ویروس در یک دوره ای به سانتریفیوژ های نطنز نیز وارد شد و آسیب هایی به آن ها وارد کرد. پس از مدتی ایران موفق به تشخیص این ویروس شد و مشخص شد که این ویروس به دستور باراک اوباما ، توسط آمریکا با همکاری اسرائیل ساخته شده بود .

3 – هک بیش از 50 میلیون کارت اعتباری در سال 2014

هکر ها با استفاده از رمز عبور یکی از فروشگاه ها توانستند به بزرگترین ذخیره کارت های اعتباری تاریخ بشریت دست پیدا کنند . این هکر ها توانستند با نفوذ به سیستم عامل ویندوز پیش از اینکه مایکروسافت جلوی آسیب پذیری را بگیرد ، به سرور ها حمله کنند . هکر ها پس از نفوذ به سرور اطلاعات بانکی کاربران زیادی را شنود و به سرقت بردند .

4 – بزرگترین حمله ی DDOS تاریخ در سال 2013

حمله ی DDOS حمله ای است که طی آن هکر یا هکر ها تعداد زیادی اطلاعات را به یک سرویس دهنده (برای مثال سرور) ارسال میکنند و این موضوع باعث کندی فعالیت سرور یا حتی ازکار افتادن سرور میشود .

در ماه مارس سال 2013 حمله ی DDOS انجام شد و به اندازه ای بزرگ بود که موجب کندی اینترنت در آمریکای شمالی و کانادا شد . در این حمله ، 300 گیگابیت داده در هر ثانیه به سرور ها ارسال میشد و در نتیجه شرکت های سرویس دهنده توانایی پاسخگویی به درخواست ها را نداشتند .

این ها نمونه هایی از هک های بزرگ تاریخ بودند که ذکر کردیم . با تحقیق بیشتر میتوانید هک های بزرگ تاریخ که در اینجا ذکر نشد را مطالعه کنید .

ابزار های داخل کوله پشتی

در این بخش بالاخره به بحث اصلی میرسیم . در بخش های قبلی با برخی مفاهیم اولیه آشنا شدیم . در این بخش بررسی میکنیم یک هکر از چه سخت افزار هایی و برای چه هدف هایی استفاده میکند یا به عبارتی چه وسایلی را میتوان داخل کوله پشتی یک هکر پیدا کرد !

1 – LAPTOP

خب قطعا در اکثر اوقات مهمترین و حیاتی ترین وسیله ای که هکر باید همراه خود داشته باشد یک لپ تاپ است . هکر ها در لپ تاپ خود طیف وسیعی از ابزار های نرم افزاری را دارند که بعضی از آن ها توسط خودشان ساخته شده و بعضی دیگر توسط هکر های دیگر که هرکدام از این ابزار ها کار خاصی را انجام میدهد . چون در این مقاله ما بر روی ابزار های سخت افزاری تمرکز میکنیم بنابراین ابزار های نرم افزاری را مورد بحث قرار نخواهیم داد .

2 – USB Memory

یکی دیگر از ابزار هایی که دنبال یک هکر است فلش مموری است .
این فلش مموری ها حافظه هایی هستند که هکر ها در حالت عادی از آن ها برای انتقال اطلاعات استفاده میکنند .

3 – Live Operation System

یکی از مواردی که هکر ها حداقل یکی از آن ها را همیشه دنبال خود دارند سیستم عامل های لایو (Live Operation Systems) است . اما سیستم عامل لایو چیست ؟

اگر شما یک کامپیوتر یا لپ تاپ شخصی داشته باشید ، قطعا یک سیستم عامل (ویندوز ، لینوکس یا ...) روی آن نصب کرده اید تا بتوانید از آن ها استفاده کنید . ولی این سیستم عاملی که روی سیستم شما نصب است یک سیستم عامل لایو نیست . از نظر فنی این سیستم عامل روی هارد شما نصب شده است . حال مشکل این کار برای هکر این است که این

سیستم عامل همیشه و همه جا برای او در دسترس نیست زیرا ممکن است سیستم خود یا هارد خود را همراه خود نداشته باشد .

اینجاست که سیستم عامل لایو به کار می آید . سیستم عامل لایو میتواند روی یک حافظه نوری مثل CD / DVD یا فلش مموری بوت شود . حال این فلش مموری یا CD / DVD همیشه دنبال هکر است . هرگاه بخواهد از این سیستم عامل استفاده کند کافی است این فلش مموری یا حافظه ای که سیستم عامل روی آن بوت شده است را به یک کامپیوتر یا لپ تاپ دلخواه وصل کند و با این کار بدونه نیاز به نصب سیستم عامل میتواند از آن سیستم عامل استفاده کند .

4 – Rubber Ducky

رابر داکی ها سخت افزار هایی هستند که وقتی آن ها به یک سیستم عامل وصل میشوند دستور های مخربی را که مد نظر هکر بوده است را به صورت خودکار روی آن سیستم اجرا میکنند . مثال این ابزار ها را شاید در بعضی فیلم ها دیده باشیم که هکر یک فلش مموری آلوده همراه خود دارد و با وصل کردن این فلش مموری به سیستم طرف باعث آلوده شدن آن سیستم میشود .

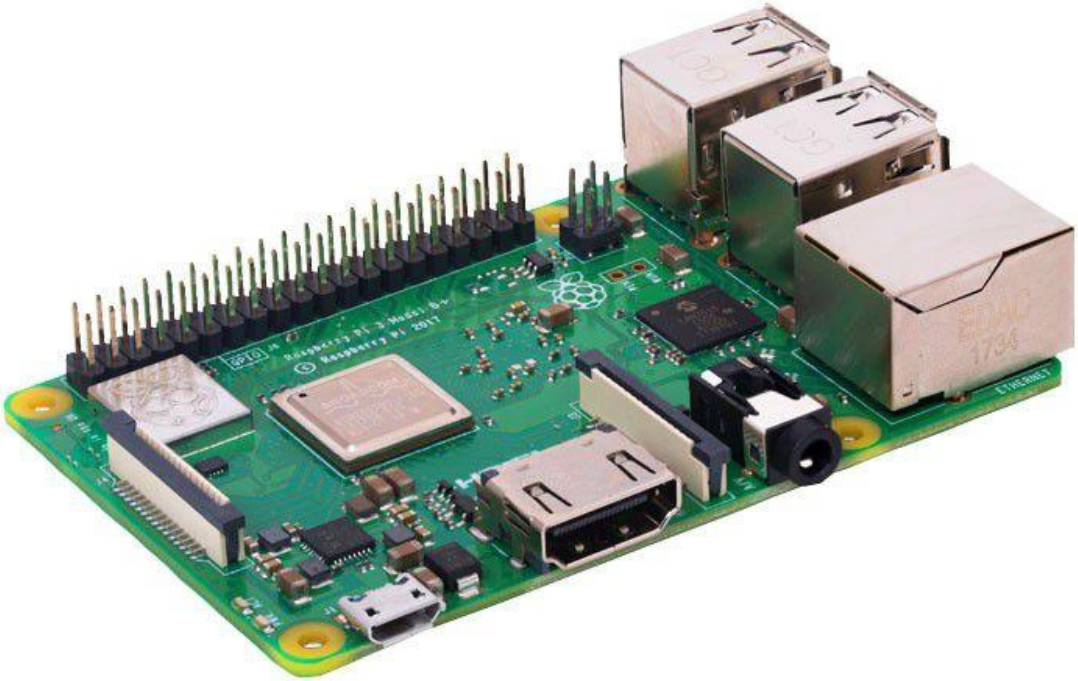
5 – Embedd Boards

برد های امبدد (Embedd Boards) یا سامانه های نهفته ، سخت افزار های نسبتا کوچکی هستند که برای هدف خاصی طراحی شده اند . این برد ها دارای CPU هستند و بعضی از این برد ها به عنوان مینی کامپیوتر شناخته میشوند . تصور کنید یک برد به اندازه ی کارت بانکی داشته باشید که میتوان روی آن سیستم عامل نصب کرد و صفحه به آن وصل کرد . دقیقا مثل یک کامپیوتر عادی .

یکی از معروف ترین برد های امبدد ، برد های رزبری پای (Raspberry pi) است .

این برد مدل های مختلفی دارد . برای مثال اندازه ی یکی از مدل های این برد در حد یک کارت بانکی است و میتوان روی آن سیستم عامل نصب کرد و صفحه مانیتور به آن وصل کرد تا درست مانند یک کیس کامپیوتر عمل کند .

این برد های مینی کامپیوتر که دارای قابلیت های فراوانی هستند در گاهی اوقات بسیار به کار هکر ها می آید .



6 – Wireless Cards

کارت شبکه های بیسیم سخت افزار هایی هستند که وقتی به یک سیستم متصل میشوند ، آن سیستم قابلیت ارسال و دریافت سیگنال های بیسیم را پیدا میکند .

کارت های شبکه بیسیم انواع مختلفی دارد . برای مثال کارت شبکه های وایفای (Wi-Fi) یا کارت شبکه های بلوتوث(Bluetooth) . خب شاید فکر کنید که چرا یک هکر باید اینگونه ابزار ها را دنبال خود داشته باشد ؟ مگر خود لپ تاپ قابلیت ارسال و دریافت سیگنال های وایفای و بلوتوث را ندارد یا به عبارتی مگر خود لپ تاپ ها کارت شبکه های بیسیم داخلی ندارند ؟

در جواب سوال بالا باید بگویم خیر همه ی لپ تاپ ها این کارت شبکه ها را به صورت داخلی ندارند . حتی اگر داشته باشند هم قابلیت های محدودی دارند و در بعضی حملات به کار هکر ها نمی آید . ولی کارت شبکه های بیسیم اکسترنال که هکر ها به صورت جداگانه تهیه میکنند قابلیت های زیادی دارد . هکر ها با استفاده از کارت شبکه های بیسیم میتوانند بسیاری از حملات را علیه شبکه های وایرلس پیاده سازی کنند . برای مثال حملات بدست آوردن رمز شبکه های وایفای (Wi-Fi).


EDUP

صحبت های پایانی

تا اینجا سعی کردیم در حد ابتدایی شما را با دیدگاه یک هکر و ابزار هایی که همراه خود دارد آشنا کنیم اما باید بگویم آنچه گفته شد همه ی آن چیزی نیست که باید بدانید . هکر ها از هزاران ابزار دیگر و هزاران روش خلاقانه دیگر برای کارهای خود استفاده میکنند و این مقاله صرفا جهت آشنایی ابتدایی بود

منابع استفاده شده :

Jadi.net

Mediasoft.ir

Plaza.ir