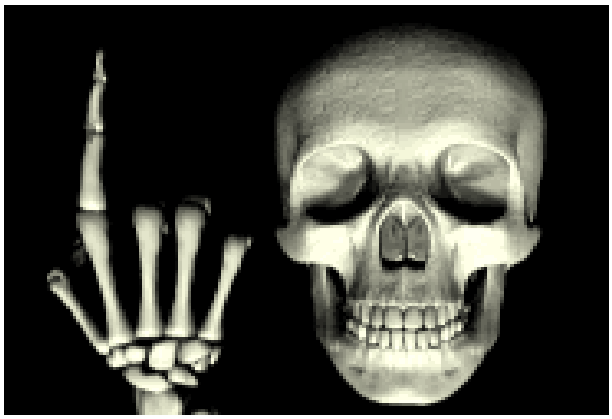
آموزش هک

به نام خدا



من می خواهم یک آیدی یاهو را هک کنم ! چه طور می تونم که پسورد دوستمو داشته باشم !!! من می خوام یک وبلاگ یا سایت رو هک کنم !! با چه برنامه ای می تونم اکنت دوستم رو هک کنم ؟ چه جور می تونم به ایمیل دوستانم دسترسی داشته باشم ؟ من یک برنامه لازم دارم که ID بگیرد و Password بدهد !

روزی هزاران (منظورم اینه که زیاد !) سوال در این رابطه از من پرسیده می شه و روزی نیست که در نظرات وبلاگم یک همچنین سوالاتی و یا مشابه شان وجود نداشته باشد . پس اجازه بدهید با جواب هایی کلی تر پاسخ تان را بدهم ، به دست آوردن پسورد غیر ممکن نیست ولی ۱۰۰ درصد امکان هم ندارد ! در دنیای اینترنت همه چیز همین طور است ، یعنی هیچ چیز به طور کامل ممکن و یا غیر ممکن نیست ... ! ! !
و باید انتظار هر چیزی را داشت (حتی هک شدن سایت های بزرگی مانند گوگل !!!) چون هر برنامه نویسی هر چه قدر هم که باهوش باشد ، باز هم باهوش تر از او پیدا می شود ...

در مورد سوالاتتون که در مورد هک سایت بود بگم که : یعنی واقعاً انتظار دارید چنین سایت های بزرگی قابل هک باشند ، آن هم به همین سادگی ؟ یعنی فکر می کنید این همه مسئولان امنیتی سایت ها نفهمیده اند و برنامه نویس می تواند اسم بدهد و پسورد بگیرد ! نخیر دوستان عزیز امنیت بعضی سایت ها به یافتن یک پسورد یا Username و Password کفایت نمی کند ! ! !
ببینید ، اشتباه نشه ، همیشه هر سیستمی اشتباهات و مشکلاتی دارد ، ولی از زمانی که آن مشکل هویدا می شود تا زمانی که مشکل حل می شود به ندرت یک روز هم طول می کشد و این مشکلات هم به هیچ وجه در حدی نیستند که با استفاده از آنها بشود چنین و چنان کارهایی کرد . فقط کافی است که کمی با منطق فکر کنید .
چنین سیستم هایی بسیار خوب محافظت می شوند ، ولی حال امکان دارد بگویید : " من یک دوست دارم که یک دوست داره که می تونه هر ID رو هک کنه و می گه یک برنامه داره که آیدی می گیره و رمزش رو می ده . "
این رو که دوستتون خیلی ساده و به راحتی بتونه پسورد خیلی ها رو پیدا کنه نشان از ضعف یاهو نیست ، بلکه نشان دهنده ی ضعف آن آدم هاست ! یعنی همون افراد هستند که رمزشون رو به دوستتون هدیه می کنند .

متاسفانه اکثر دوستانی که ادعای هک و هکری می کنند (که جزو جوجه هکر ها هم به حساب نمیایند !) روششان آن قدر مسخره است که باید خیلی مراقب این باشند که آن لو نرود ، پس همین است که امکان دارد بگویند روش دیگری دارند یا یک موضوع خیلی محرمانه است یا چرت و پرت دیگری .... حال لطفاً سوال زیر را بخوانید :

((من می خواهم رمز یک نفر رو دربیارم ، چی کار کنم ؟))

خوب در این مورد هر کس روش خودشو داره ، و من هم به روش خودم عمل می کنم و این واضحه که هیچ کس روش خودشو بروز نمی ده !
اگر فرد مورد نظر در یک سایت کوچک که تمام آن هم نوشته شده توسط برنامه نویسان است باشد ، امکان Hack کردن آن وجود دارد ، من در اینجا صرفاً به ذکر روشی اکتفا می کنم که از بقیه روش ها بیشتر لو رفته است و آن این است که در قسمت رمز عبور (یا در صورت نیاز هم در قسمت نام کاربری و هم در قسمت رمز عبور) بنویسید :

-- or 1=1 '

این یکی از ساده ترین حالت های روش موسوم به SQL Injection است که روشی بسیار قوی است ، اما این حالت ساده آن در حدود 90% سایت ها از جمله سایت های Yahoo و HotMail و سایت های معروف دیگر (معروف همون با امنیته دیگه !) کار نخواهد کرد . یعنی اگر بدشانس نباشید باید حداقل این را در ۱۰ سایت امتحان کنید تا در یکی از آن ها کار کند .

اما در ادامه پاسخ به سوال شما : حال اگر فرض کنیم سایتی مانند یاهو مد نظرتان باشد (چه بلند پرواز !) در اینجا ابتدا خیال خودمان را از این بابت راحت می کنیم که نمی توانیم رمز رو از روی سرور یاهو دربیاریم (مگه شهر هرته ؟) پس باید رمز امتحان کنیم (Broute Force) یا رمز را از صاحب رمز بگیریم (Social Engineering) یا رمز را از صاحب آن بدزدیم (Trojans) !

در حالت اول به تخصص نیاز دارد و حتی گاهی غیر ممکن است زیرا سیستم ها بعد از چند بار امتحان رمز اشتباه از سوی شما دیگر رمزی قبول نمی کنند . مثلاً یاهو شما را مجبور می کند که کلمه ای که هر بار تغییر می کند را نیز همراهش وارد کنید . می توانید در صفحه ایمیل Yahoo چندین بار رمز اشتباه

بزنید تا نتیجه را ببینید و اگر چه می توان مشکل بستن IP را با استفاده از Proxy Server های رایگان تا حدی برطرف کرد ، باز هم این روش بیشتر مناسب سیستم های ساده تر است (کاربرد این روش در صفحاتی که برالی کسانی که رمز خود را فراموش کرده اند طراحی شده است را فراموش نکنید ! اگر تاریخ تولد وارد شده و کد پستی کسی را بدانید شاید حدس زدن بقیه اطلاعات عملی باشد !)
بنابراین استفاده از نرم افزار های امتحان کننده رمز هم برای این سرور های معروف نتیجه ای نخواهد داشت . راه دیگر Trojan Horse است ، اگر تقاضا برایش زیاد باشد ، درموردش جداگانه توضیح داده خواهد شد . می توانید از تروجان ها استفاده کرده و پس از ساخت آن را برای قربانی فرستاده و منتظر بمانید تا پسورد برای شما ارسال شود ، این یکی از ساده ترین راههای هک بود (به همین دلیل هرگز فال های مشکوک را از دیگران دریافت نکنید !) مثلاً می توانید از تروجان های مشهوری مانند مجیک پی اس استفاده کنید ، فکر نمی کنم پیدا کردن آنها در اینترنت هم مشکلی داشته باشد (به راحتی !) اما از آن جایی که اولاً نرم افزار های ضد ویروس ممکن است آن را (تروجان) بیابند و ثانیاً سیستم عامل ویندوز XP با داشتن یک فایروال (Firewall) به نسبت خوب می تواند جلوی اکثر اینها را بگیرد ، عملاً قابل استفاده نخواهد بود ، مگر کسانی که یا به کامپیوترشان دسترسی داشته باشید و یا اطمینان داشته باشید که از یک سیستم عامل قدیمی (باورتون می شه کسی از ویندوز ۵ سال پیش استفاده کنه ؟!!! از ویندوز ۹۸ ؟؟؟ واقعاً که آدم متاسف می شه !!! ۵ سال ؟؟ اونم توی کامپیوتر ؟) استفاده می کند و ضد ویروس (Anti Virus) ندارد یا زیاد آن را به روز نمی کند .

اما راه اصلی یعنی Social Engineering (یا مهندسی اجتماعی بخش دوم) خوب این راه اصلیه و به راحتی می تونید ازش استفاده کنید ، پس از اینجا به بعد به خوبی توجه کنید :

Social Engineering تاریخی طولانی دارد و معمولاً نازی های آلمان را از جمله استفاده کنندگان موفق آن می دانند . این روش یعنی کاری کنید که خودش به ما رمز را بگوید ! من فقط چند روش ممکن را برای شما می نویسم :

۱ – ساختن صفحه ای شبیه صفحه یاهو . به عنوان مثال یک ایمیل به شکل کارت پستال برایتان ارسال می شود که ممکن است به نظر بیاید از طرف دوستان نزدیکتان آمده است و وقتی روی لینک کارت پستال کلیک می کنید پیغامی مانند Your Session has been Expired و یا Relogin می گیرید اما در صفحه ای به جز Yahoo هستید ! یعنی اگر رمزتان را بنویسید عملاً خودتان آن را به نفوذ گر هدیه کرده اید . حالت دیگر ساختن صفحاتی است که جلب توجه کند مثل صفحه ای که می گوید با یاهو قرارداد دارد و می توانید با اکانت یاهو خود وارد آن شوید !!! (دروغ محض !) به عنوان مثال صفحه ای با عکس های مستهجن از دختران ایرانی و ... که جلب توجه می کنند . خیالتان راحت باشد که رمز و اسم یاهو فقط در یاهو کار می کند و هرجای دیگر که پسوردتان را بزنید دو دستی آن را تقدیم کرده اید . ! !!
همیشه باید مواظب باشید که هرگز در صفحه ای به جز صفحه ی واقعی خود یاهو اسم و رمز خود را وارد نکنید !

این روز ها مد شده است که بسیاری از دوستان با ساختن صفحاتی مشابه یاهو (معمولاً Save کردن خود صفحه Sign In یاهو و سپس تغییر مسیر فرمی که باید رمز را به میزبان یاهو انتقال دهد ، به صورتی که پسورد شما را به سازنده صفحه ایمیل کند یا در یک فایل ذخیره کند .

برای این کار کافی است که یک Host رایگان بگیرید و فایل های خود را در آن قرار دهد ، فقط باید مواظب باشید که حتماً از Coffee Net استفاده کند !) اقدام به دزدی رمز عبور می کنند . حالا سوال اینجاست که از کجا بفهمیم که صفحه ای که داخل آن هستیم واقعاً از طرف خود یاهو است یا خیر ؟ به عنوان یک قاعده کلی ، ابتدا F6 و سپس کلید Home را بزنید . با این کار شما ابتدا نوار آدرسی را که آدرس صفحه وب را نشان می دهد می بینید . (راه دیگر : کافی است ، با کلیک موس روی نوار آدرس آن را فعال کنید و با فلش سمت چپ به سراغ اول آن بروید .) اگر آغاز آن به شکل زیر نبود ، صفحه را ببندید (پیشنهاد می شود قبل از بستن صفحه تعداد زیادی کلمات بی معنی به عنوان اسم و رمز جهت سرگرم کردن دزد یاد شده وارد فرمایید) و اگر مانند زیر بود و پس از آن هم فقط حروف و اعداد و علامت / و ? آمده بود ، با خیال راحت اسم و رمز خود را وارد فرمایید :

http://login.yahoo.comهرچیزی/

البته اگر به جای کلمه Login هر چیز دیگری باشد با دقت به این که به yahoo.com ختم شده باشد ، باز هم از صفحات خود یاهو خواهد بود .
مهم : بهتر است علاوه بر آن ، با کلیک روی "Secure" منتظر شوید تا عکس یک قفل را در Internet Explorer خود مشاهده کنید . (باز هم ۱۰۰% نیست !)

۲ – فرد نفوذ گر یک ID مانند : auto-password-sender@yahooc.com ثبت می کند و به شما می گوید که اگر ایمیلی به فرم خاص و عجیبی با آن آدرس بفرستید و در جاهای خاصی از آن آدرس ایمیل خود و رمز عبور خود و در جایی دیگر ایمیل کسی که رمز او را می خواهید بنویسید و به آنجا ارسال کنید تا رمز برای شما اتوماتیک ایمیل شود . زمانی که ما به نیت آزمایش همین سیستم را پیاده کردیم متاسفانه تعداد خیلی زیادی ایمیل دریافت کردیم که عملاً رمز خود را به ما هدیه کرده بودند و یک پاسخ هم ارسال می کردیم که ظرف یک هفته دیگر عملاً رمز را می گیرید و ظاهر آن را با تبلیغات و طراحی زیبا واقعی کرده بودیم . برای کسانی هم که می فهمیدند و ایمیل مسخره می فرستادند ایمیل با پیغام های خطا می فرستادیم ، به صورتی که آنها نیز وسوسه می شدند !!! پس مواظب باشید رمز عبور خور را به هیچ شکلی به کسی هدیه نکنید و خود را مسخره ی دست آن هکر نکنید ... ! خیالتان راحت باشد که هرگز هیچ سیستمی از طریق ایمیل یا تلفن رمز عبور شما را نخواهد پرسید و هرگز یاهو به شما ایمیل نمی زند که در آن رمز خود را بنویسید ! اگر روزی آنها نیاز داشته باشند ، رمز عبور شما را عوض می کنند و آن را به شما اطلاع می دهند نه اینکه رمز شما را بپرسند !

Social Engineering به اینجا ختم نمی شود و داستان های زیادی از آن باقی است . در پایان اشاره ای به یک داستان واقعی می کنیم :
فردی که قصد نفوذ به یک ساختمان دارای اتاق های سرور کاملاً حفاظت شده با انواع دوربین ها و دزدگیر ها را داشت ، به راحتی خود را مسوول بازبینی سرور ها برای سازگاری با سال ۲۰۰۰ معرفی می کند و از تک تک افراد رمزشان را می پرسد و یادداشت می کند ! حتی با گفتن اینکه بگویید فایل های مهمتان کجاست تا از آنها پشتیبانی تهیه کنیم که مبادا در حین آزمایش سیستم ها به آنها صدمه ای برسد ، زحمتی برای جستجو به دنبال فایل های مهم هم متحمل نشد ! شما هرگز و تحت هیچ شرایطی نه حضوری ، نه پای تلفن و نه در ایمیل نباید رمز خود را به کسی بگویید ! حتی رمز اکانت اینترنت خود را به مدیر شرکتی که از آن اینترنت گرفته اید هم ندهید ! (البته من این قدر ها هم بدبین نیستم !) چون اگر او وقعاً نیاز داشته باشد به راحتی آن را تغییر می دهد .

من به دلیل محدودیت زمانی به همین روش های فوق اکتفا می کنم و امیدوارم که هیچ وقت گول هیچ آدم متقلب (به اسم هکر) را نخورید و در کارتان موفق باشید .
امیدوارم این مقاله که در وقت محدودی نوشتم به اندازه ی کافی جامع بوده باشد و شما از آن نهایت استفاده را برده باشید .
روش های هک در دنیای اینترنت فراوانند و هیچ کس (هکر) نمی تواند ادعا کند که همه چیز را بلد است ، چون روزی ممکن است این شتر (هک شدن) بر در خانه ی او نیز بخوابد !

نویسنده مقاله : **R.M.R Hacker**
وبلاگ تخصصی آموزش هک و کرک (www.ct.sub.ir)