HACK

کپی برداری بدون ذکر نام منبع مجاز نیست

شاید تا به حال برای شما اتفاق افتاده باشد که مورد حمله هکرها (hackers)قرار بگیرید. شاید بارها account های اینترنت تان در عرض یک روز خالی شده باشد بدون آنکه خودتان استفاده کرده باشید. شاید متوجه شده باشید که در yahoo messenger شخص دیگری هم از ID شما استفاده می کند.

هک چیست و Hacker کیست ؟ hack به زبان ساده و شاید عامیانه ترین تعبیر آن...

parsi e-book
WWW.PARSIBOOK.4T.COM

دزدیده شدن کلمه عبور یک سیستم یا account می باشد.

به طور کلی نفوذ به هر سیستم امنیتی کامپیوتری را hack می گویند.

کپی برداری بدون ذکر نام منبع مجاز نیست

Hackerشخصی است باهوش، فرصت طلب ، دارای معلومات بالا با

parsi e-book

افکار سازنده و مطمئنا با وجدان.

لازم به ذکر است که از نظر من هکرها با دزدان اینترنتی و یا

الکترونیکی فرق دارند. هکرهای واقعی در میان خود مرام نامه ای

دارند که همه پایبند به آن می باشند.

هکر در موقع هک کردن یک سیستم امنیتی هدفش ضربه زدن (چه

مادی و چه معنوی) به شخص یا اشخاصی نیست.

او هک می کند تا معلوماتش را نشان دهد. هک می کند تا همگان

بدانند که سیستمهای امنیتی دارای مشکل هستند. هک می کنند تا

نواقص (حفره های امنیتی) این سیستمها نمایان شوند. اگر هکرها نمی

parsi e-book
WWW.PARSIBOOK.4T.COM

بودند مطمئنا سیستمهای امنیتی به کاملی سیستمهای امروزی نمی بود.

پس هکرها مفیدند.

در این میان افرادی هستند که با سوءِ استفاده از معلومات خود و یا

دیگران هدفشان از هک کردن ضربه زدن به اشخاص است یا به دنبال

پرکردن جیب خود می باشند. از نظر من این افراد دزدانی بیش

نیستند.

در این مقاله منظور من از هکر همان دزد اینترنتی یا الکترونیکی است.

به دلیل اینکه نمی خواهم وارد مباحث تخصصی شوم و حتی آنقدر

اطلاعاتش را ندارم و البته هیچکدام از ما بانک اینترنتی یا فروشگاه

مجازی نیز نداریم ، لذا منظور من از هک در اینجا دزدیدن کلمه عبور

حسابهای dialUp و yahoo messenger و Hotmail می باشد که

بسیاری از خوانندگان از آنها استفاده می کنند.

کپی برداری بدون ذکر نام منبع مجاز نیست
parsi e-book
WWW.PARSIBOOK.4T.COM

چگونه هک می شویم ؟!

کپی برداری بدون ذکر نام منبع مجاز نیست

روزی با هکری صحبت می کردم و از او پرسیدم رایج ترین و مطمئن ترین روش هک کردن چیست ؟ و او در جواب گفت :رایج ترین روش ، ساده ترین روش است. آنروز معنی سخنش را نفهمیدم. ولی وقتی کمی تحقیق کردم و در دنیای اینترنت هک شدم، متوجه منظورش شدم. یکی از متداول ترین روش های هک کردن، حدس زدن passwordاست.

روش رایج دیگر خواندن password از روی دست User به هنگام تایپ آن می باشد. یا فرستادن صفحه ای مانند صفحه ورودی Hotmail , Yahooبه صورت یک Email که در آن به ظاهر کارکنان شرکت سرویس دهنده از user خواسته اند به منظور اطمینان از

parsi e-book
WWW.PARSIBOOK.4T.COM

صحت سرویس دهی password خود را تایپ کند. که این password

در همان لحظه برای هکر mail می شود.

برنامه جالبی وجود دارد که LOG تمامی حرفهایی که وارد شده است

را ذخیره می کند. هکر برنامه را اجرا می کند و بعد از شما می خواهد

که رمز خود را بزنید. کلیدهای تایپ شده توسط شما درون یک فایل

متنی TXT ذخیره می شود و هکر بعدا به آن رجوع می کند و رمز

شما را کشف می نماید.

روش دیگر حدس زدن جواب سوالی است که شما انتخاب نموده اید تا

در صورت فراموش نمودن رمزتان از شما پرسیده شود. در yahoo

استفاده از این روش سخت است زیرا تاریخ دقیق تولد و آدرس و

حتی کد پستی را نیز می خواهد. ولی در سرویس hotmail به سادگی

می توانید جواب سوال را حدس بزنید و رمز را بدست آورید. و نیز

کپی برداری بدون ذکر منبع مجاز نیست
parsi e-book
WWW.PARSIBOOK.4T.COM

هکر می تواند به کارکنان hotmail نامه زده و در آن ابراز نماید که accountاش مورد هک قرار گرفته و درخواست رمز جدید کند که کارکنان Hotmail از او چند سوال در مورد سن و آخرین دسترسی به accountو آخرین رمزی که به خاطر دارد می کنند و سپس رمز جدید در اختیار او قرار می گیرد.

)چند بار از این روش توانسته ام به رمزها دست یابم) یا برای یافتن رمز account های اینترنت، به ISP شما زنگ می زند و با دادن مشخصات خواستار تغییر رمز می شود. جالب اینجاست که در بسیاری از موارد منشیان رمز قبلی را نمی پرسند.

اینها همه روشهای ساده ولی رایج و متداول بودند. روش دیگری که در اینجا در موردش صحبت می کنم کمی تخصصی است و هر شخصی نمی تواند از این روش استفاده کند بلکه باید معلوماتی در

کپی برداری بدون ذکر نام منبع مجاز نیست
parsi e-book
WWW.PARSIBOOK.4T.COM

خصوص اینترنت و IP و یک سری نرم افزارها داشته باشد.

در این روش شخص با فرستادن یک فایل آلوده به ویروس یا Trojan

سیستم شما را آلوده می کند. با اجرای این فایل ، فایل مورد نظر در

حافظه جای می گیرد و هر زمان که کامپیوتر روشن شود دوباره در

حافظه صدا می شود. پس با پاک نمودن فایل اولیه مشکل شما حل نمی

شود. این فایل کامپیوتر شما را به عنوان یک Server در می آورد و

یکی از پورت ها را برای استفاده هکر باز می گذارد. (برخی از این

trojanها پرتی را باز نمی گذارند بلکه از طریق یک email رمز ها را

برای هکر ارسال می نمایند.) حال هکر می تواند با پیدا کردن IP شما و

اتصال به پورت مورد نظر در زمانی که هم شما Online هستید هم

هکرتان هر کاری با کامپیوتر شما بکند حتی آنرا خاموش کند و

رمزهای موجود در کامپیوتر شما را بدزدد.

کپی برداری بدون ذکر منبع مجاز نیست
parsi e-book
WWW.PARSIBOOK.4T.COM

البته ارسال فایل گاهی به صورت online نمی باشد. هکر می تواند اگر با شما آشنایی داشته باشد به پشت کامپیوتر شما بی آید و فایل مورد نظر را روی آن اجرا کند.

کپی برداری بدون ذکر نام منبع مجاز نیست
parsi e-book

جالب اینجاست که اغلب ویروس کشها از شناسایی Trojan های جدید عاجزند. از همین رو من مدتها گرفتار یکی از آنان بودم.

چه باید کرد ؟!

چگونه هک نشویم ؟!

روشهای ساده را به سادگی و با کمی دقت می توان مسدود کرد. مثلا رمزی انتخاب کنید که حدس زدنش کار هر کسی نباشد. شماره تلفن ، اسم ، فامیل ، شماره شناسنامه یا تاریخ تولید و ترکیبی از اینها معمولا اولین چیزی است که به ذهن هر کسی می رسد. سعی کنید در رمز

parsi e-book
WWW.PARSIBOOK.4T.COM

انتخابی خود از پرانتز یا کروشه استفاده کنید یا حتی کاما که اینها به ذهن هیچ هکری نخواهد رسید. هنگامی که رمز خود را وارد می کنید مراقب باشید، کسی نزدیکتان نباشد. یا از کلید های منحرف کننده استفاده کنید. مثلا چند کلید الکی بزنید و بعد با Backspace پاکش کنید که اگر کسی هم دید ، متوجه رمز شما نشود.

کپی برداری بدون ذکر منبع مجاز نیست
parsi e-book

پشت کامپیوتر کسی که به او اطمینانی ندارید ، رمزی وارد نکنید. یا اگر مجبورید، با استفاده از کلید های Ctrl+Alt+Del و باز نمودن Task Manager کلیه برنامه های مشکوک را ببندید. معمولا اسامی آنها مانند Thief یا Keylogger یا keyl یا هر اسم مشکوک دیگری می تواند باشد. در موقع ثبت نام در سرویسهای Hotmail و Yahoo به شما تذکر داده می شود که کارکنان شرکت سرویس دهنده به هیچ عنوان از طریق Email از شما درخواست Password نمی کنند.

parsi e-book
WWW.PARSIBOOK.4T.COM

پس هیچ گاه از طریق هیچ Email ی رمز خود را وارد نکنید. از جایی اینترنت تهیه کنید که امنیت بیشتری دارد و تجربه کارشان بالاست.

زیرا علاوه بر منشیان بی تجربه که بعضاً رمزها را برباد می دهند ، اگر شبکه (ISP) هک شده باشد ، دیگر از دست شما کاری بر نمی آید و رمز شما و دیگر کاربران در خطر می باشد.

کپی برداری بدون ذکر منبع مجاز نیست
parsi e-book

احتمال حمله با روش تخصصی که در بالا توضیح دادم به کاربرانی که از سیستمهای Instant messaging مانند Yahoo messenger یا MSN messengerیا ICQ و ... استفاده می کنند بیشتر است چون اینگونه برنامه ها به راحتی IP شما را در اختیار هکر قرار می دهند و همواره یک پورت آزاد را اشغال می کنند و معمولا به صورت مستقیم با کاربر مقابل در ارتباط هستند. مخصوصا در مواقع ارسال و دریافت فایل. پس اگر می خواهید در امان باشید از این برنامه ها استفاده

parsi e-book
WWW.PARSIBOOK.4T.COM

نکنید.

ولی امروزه در ایران اینترنت بدون اینگونه برنامه ها فایده ای ندارد !

پس هیچگونه فایلی را که از افراد ناشناس فرستاده می شود ، باز نکنید.

کپی برداری بدون ذکر نام منبع مجاز نیست
parsi e-book

حال اگر کامپیوتر شما از قبل آلوده شده باشد چه باید کرد ؟!

اگر مطئمن ترین راه را می خواهید. کامپیوتر خود را فرمت نموده و

دوباره ویندوز را نصب کنید. زیرا اغلب ویروس کشها قادر به

شناسایی یا پاک نمودن بسیاری از این نوع ویروسها نمی باشند. ولی

معمولا این روش به صرفه نیست. کاری که من برای مبارزه با این نوع

ویروس ها (که نمی دانم آیا به آن مبتلا هستم یا خیر) کردم این است

که یک ویروس کش جدید نصب نمودم که هر هفته آنرا Update می

کنم. من Norton Antivirus 2003 را پیشنهاد می کنم که خود به

parsi e-book
WWW.PARSIBOOK.MT.COM

صورت اتوماتیک هر ۱۰ روز یکبار به روز می شود.

حال اگر ویروسی پیدا شد که ویروس کش من نتوانست آنرا شناسایی کند چه ؟!

کپی برداری بدون ذکر نام منبع مجاز نیست
parsi e-book

همانطور که گفتم فایلی که در حافظه شما اجرا می شود و کامپیوتر شما را به عنوان Server آماده حمله هکر می کند برای اتصال به اینترنت و فرستادن اطلاعات احتیاج به یک پورت آزاد دارد. روشهای زیادی برای مسدود نمودن پورت های آزاد وجود دارد. همواره در ایران رسم است که می گویند اینترنت بدون Proxy بهتر است ولی باید بدانید که Proxy نه تنها سرعت کار شما در اینترنت را بالا می برد بلکه جلوی حمله هکرها را نیز می گیرد.

parsi e-book
WWW.PARSIBOOK.IT.COM

روش دیگر استفاده از Firewall می باشد. امروزه بسیاری برنامه های

کم حجم با عنوان Firewall خانگی وجود دارند.

شما با استفاده از یکی از این برنامه ها می توانید به راحتی هرگونه رد و بدل شدن اطلاعات بین کامپیوتر خود و اینترنت را ببینید و کنترل نمایید.برنامه ای که من پیشنهاد می کنم ZoneAlarm می باشد. با نصب این برنامه هرگاه ، برنامه ای بخواهد با اینترنت تبادل اطلاعات نماید ابتدا به شما تذکر می دهد و شما می توانید اگر برنامه مشکوکی بود اجازه فرستادن اطلاعات را از او صلب کنید. در ضمن هیچ شخص و برنامه ای هم نمی تواند بدون اطلاع شما از بیرون به کامپیوتر شما وصل شود. ویندوز XP از نظر امنیت در شبکه بسیار پیشرفته است و احتمال هک شدنش کمتر است ، پیشنهاد می کنم از این ویندوز استفاده کنید.

در آخر باید بگویم هیچ روشی به صورت ۱۰۰٪ شما را ایمن نمی کند. فقط سعی می کنیم احتمال هک شدنمان را پایین بیاوریم

کپی برداری بدون ذکر نام منبع مجاز نیست
parsi e-book
WWW.PARSIBOOK.41.COM