هک و روشهای مقابله با آن HACK AND THE WAYS OF DEFENCE

محمد رضا سلطانی MOHAMMAD REZA SOLTANY

بهار 1388

..: M R S :..
Email: mr.soltany66@gmail.com
Web: www.pnuni.ir

2009/4/23

دانشگاه پیام نور تهران واحد آبسرد

فهرست

..: M R S :.. Email: mr.soltany@yahoo.com

بسم الله الرحمن الرحیم

بنام خداوند آینه ها فروزنده مهردرسینه‌ها

چکیده مقاله :

با توجه به رشد و افزایش استفاده از اینترنت در جامعه و گره خوردن این فناوری با زندگی انسانها در قرن 21 اهمیت امنیت شبکه گسترده جهانی وب پررنگتر به نظر می رسد.

مقاله حاضر سعی دارد به صورت کاملا ساده و روان روشهای هک و جلوگیری از آن را آموزش دهد . تا با یادگیری مسائل امنیتی استفاده از اینترنت با خیالی آسوده از خدمات آن بهره ببرید.

هرچند با پیشرفت علوم فناوری اطلاعات و کامپیوتر همیشه درهای جدیدی پیش روی هکرها باز خواهد شد.

و امنیت به معنای مطلق آن تحقق پذیر نیست اما پیشگیری از آن عاقلانه ترین راه است.

نکته قابل تامل اینست که تاریخچه هک بسیار طولانیست و بدیهیست ادامه خواهد داشت.

ما همیشه باید از آخرین اخبار در مقوله فناوری اطلاعات مطلع باشیم .

مقدمه :

بیشتر به دلیل مبالغاتی که روزنامه ها و رسانه های عمومی درباره هک و هکرها انتشار داده و می دهند ، و همچنین عدم آگاهی کاربران با دانش کامپیوتر و فناوری اطلاعات باعث شده است که این عناوین برای آن ها مرموز و هکرها افرادی خارق العاده تصور شوند . حال آنکه هک در ساده ترین حالت می تواند ناشی از خطاهای برنامه نویسی و کاربرد باشد و یک جوان کنجکاو و کم اطلاع از دانش کامپیوتر می تواند یک هکر باشد .

امروزه هکرها طیف وسیعی از کاربران را تشکیل می دهند که بعضی از آن ها حتی در مقام مدیر سیستم و مشاوره مشغول به فعالیت می باشند .
مفهوم هک همپای پیشرفت کامپیوتر همواره تغییر کرده است . در ابتدا مفهوم هک استفاده از ابزارهای الکترونیکی و ارتباط نظیر تلفن جهت استفاده رایگان از آن ها بود که بعدها توسط کارشناسان نرم افزار جهت استفاده رایگان از آن ها بود که بعدها توسط کارشناسان نرم افزاری جهت بدست آوردن کد و اطلاعات برنامه ها تغییر نمود و در حال حاضر **هک به دستیابی غیر مجاز به اطلاعات یک کامپیوتر یا شبکه گفته می شود** . با توجه به اینکه این کار غیر قانونی و گاهاً مخرب است ، هکرها به عنوان کاربران خطرناک و حتی پس از حملات ۱۱ سپتامبر بعنوان تروریست کامپیوتری مشهور شده اند .
در گذشته ، تصور عمومی بر آن بود که هکرها بی آنکه قابل ردیابی باشند اطلاعات را به سرقت می بردند ، این در حالی است که اگر از کارشناسان امنیت کامپیوتر در این موارد استفاده شود ، می توانند نحوه هک شدن و نیز حتی فرد هکر را نیز شناسایی کنند .
هک میتواند ***جنبه شخصی یا حرفه ای*** داشته باشد ، به عبارت دیگر ، هکرها می توانند کلمات عبور یا اطلاعات شخصی یا شرکتی را به سرقت ببرند و یا در سطح بالاتری برای **امنیت ملی** خطراتی ایجاد کنند ، مانند دخالت در امور ارتباطی و مالی و ... .
برخلاف تصوری که مردم از هکرها به عنوان افراد منزوی و ناراحت دارند ، بسیاری از هکرها افراد باهوش و خلاق هستند و صرفاً بدلیل ارضاء حس کار گروهی یا **احساس قدرت** اقدام به این کار می نمایند .

هک چیست؟

هر نوع نفوذ که توسط هکر در یک سیستم امینتی شبکه و کامپیوتری انجام گیرید به نوعی هک گفته می شود البته نفوذ می تواند تنها وروردبه سیستم اطلاعاتی باشد و یا نفوذگر جلوتر رفته و بخشی از اطلاعات شما را تغییر داده و یا نابود نمایید حتی هکر می تواند با توجه به میزان نفوذ انجام شده کل مدیریت وبسایت یا سیستم شبکه کامپیوتری را در دست بگیرید و شما را دچار مشکل جدی کند .

هدف هک چیست هکرها چرا نفوذ می کنند؟

جواب این سوال قطعی نیست از لحاظ جامعه شناسی نفوذگر در تمام ادوار تاریخ وجود داشته است اما درسیستم های شبکه نفوذ می تواند چند علت اصلی داشته باشد .

1- اعلام سواد و تسلط بر فن آوری اطلاعات :
این نوع نفوذ کمتر با تخریب و تهدید نفوذگر همراه است فراموش نکنید برای نفوذ در سیستم های شبکه ؛ باید فرد دارای سواد پایه ای در حد کافی باشد .برخی از افراد برای به رخ کشیدن سواد و توانمندی خود در شبکه های نفوذ نموده و با به جا گذاشتن یک ردپایی خود برای اثبات نفوذ سعی می کنند که سواد خود را به همه اعلان کنند

2- اعلان ضعف امنیت شبکه کامپیوتری :
این نوع نفوذ هم با تخریب و تهدید کم انجام می شود تنها نفوذگر سعی می کند نقاط ضعف امنیت شبکه را به مدیریت اعلان نماید و در برخی موارد هم به مدیریت اعلام می شود که نفوذگر حاضر به همکاری در رفع نقص و تقویت امنیت شبکه است .

3- انتقام شخصی یا گروهی :
این نوع نفوذ به طور حتم بسیار خطرناک و دردسرساز است در اینگونه حمله ها نفوذگر سعی می کند سیستم را تا حد امکان نابود و خسارات جبران ناپذیری را انجام دهد ؛ برخورد سخت بارقبا یکی از این انگیزه نفوذگران با نیت انتقام است در برخی موارد هم برخی از وبسایتها و شبکه های منافع ملی ؛ گروهی یا فردی افراد را به مخاطره می اندازد و در مقابل نفوذ گر سعی در نابودی مورد اشاره دارد.

4- بدون دلیل:
حتمی نباید هر کاری دلیل داشته باشد ؛ برخی نیز برای خودنمایی یا سرگرمی و گاهی هم از سر بیکاری دست به نفوذ و تخریب شبکه می کنند این نوع نفوذ به دلیل اینکه کور و بدون دلیل است ممکن است خطرآفرین باشد امادر مواردی بیشتر به یک شوخی تمام می شود .

5- دلایل شخصی:
کمتر اتفاق می افتد که یک هکر انگیزه شخصی فراتر از انتقام داشته باشد ولی ممکن است این اتفاق بیافتد مانندا سید پاشی روی صورت معشوق و یا موارد دیگر البته این مورد کمتر اتفاق افتاده است

6- دستیابی به اموال مجازی افراد یا شرکتها

این امر ممکن است یکی از قویترین دلایل انجام هک باشد البته این نوع از نفوذ بیشتر از روش دزدی هویت یا فیشینگ صورت می گیرد فرد نفوذگر سعی می کنند با دستیابی به ای دی و شناسه کاربری قربانی و رمز عبور و پاسورد وی ؛ مدیریت بخشی از اموال مجازی فرد یا شرکت از قبیل وبلاگ ؛ صندوق پست الکترونیکی ؛ کارت اعتباری ؛ عضویت باشگاه ؛ عضویت وبسایت و یا هر مورد که می تواند وی را به اموال مجازی شخص قربانی نزدیک کند دست می زند در ایران و در بین هکرهای تازه کار که هدف هایی مانند انتقام ؛ اعلام سواد ؛ اعلان ضعف شبکه کمتر وجود دارد هکر سعی می کند تنها به دست دستیابی به مدیریت یک وبلاگ یا صندوق پست الکترونیکی نفوذ را انجام دهد این گونه نفوذهای ساده و با بهره گیری از ضعفهای امنیتی کاربران در ایران رایج است .

تاریخچه هک

هک کردن برخلاف انتظار مسئله ای تازه نیست و حتی به یک کشور هم محدود نمی شود . نوشتار پیش رو تاریخچه مختصری از این پدیده را در کشورهای مختلف بررسی می کند.

- ۱۹۷۱ در ویتنام دامپزشکی به نام «جان دراپر» از یک سوت ارزان قیمت در جعبه پاپ کورن و یک «جعبه آبی دست ساز» برای برقراری تماس تلفنی رایگان استفاده می کند . هم زمان با انتشار راهنمای شرکت «اسکوایر» در مورد چگونگی ساختن جعبه های آبی، آمار تقلب و کلاهبرداری در زمینه استفاده از تلفن در آمریکا به اوج خود می رسد .
- ۱۹۸۹ در آلمان غربی، تعدادی هکر به علت نفوذ غیرقانونی به سیستم های دولتی و شرکت ها و فروش کد منابع OS به KGB بازداشت شدند.
- ۱۹۹۱ شایعاتی درباره وجود ویروسی به نام «میکل آنژ» منتشر می شود مبنی بر این که این ویروس کامپیوترها را در ۶ مارس ۱۹۹۲ ؛ یعنی در پانصد و هفدهمین سالگرد تولد هنرمند، نابود می کند. هیچ اتفاقی در این روز نمی افتد .
- ۱۹۹۴ هکرهای روسی به رهبری «ولادیمیر لوین» ۱۰ میلیون دلار از بانک شهری، خارج و آن را به حساب های بانکی خود در سراسر دنیا منتقل کردند. پس از چندی «لوین» دستگیر و به جز ۴۰۰ هزار دلار مابقی پول ها پس گرفته شد .
- ۱۹۹۷ یک گروه هکر کانادایی به نام » انجمن وارز» به وب سایت یک شبکه تلویزیونی کانادایی نفوذ می کند .
- ۱۹۹۷ یک نوجوان ۱۵ ساله کراوات به کامپیوترهای نیروی هوایی آمریکا در «گوام» رخنه می کند.
- ۱۹۹۸ » اهود تنبوم» یک هکر ۱۹ ساله اسراییلی راه هایی برای ورود غیرقانونی به کامپیوترهای پنتاگون می یابد و برنامه های نرم افزاری آنجا را می دزدد. وی توسط FBI

بازداشت می گردد، اما بعدها از مقامات مهم شرکت مشاوره کامپیوتری می شود .

- ۱۹۹۸ دو هکر در چین به دلیل نفوذ به شبکه کامپیوتری یک بانک و دزدیدن مبلغی معادل ۳۱۳۲۵ دلار محکوم به اعدام می شوند .
- ۱۹۹۹ « کلینتون» اعلام می کند که دولت ۴۶/۱ میلیارد دلار در FYOO صرف بهبود سیستم امنیت کامپیوتری خواهد کرد .
- دسامبر ۱۹۹۹ یک هکر روسی سعی می کند از یک پخش کننده فروش سی دی در اینترنت مبلغ ۱۰۰ هزار دلار اخاذی می کند و برای رسیدن به خواسته اش موسسه را تهدید به افشای شماره کارت اعتباری مشتریانش می کند. او پس از ناکامی در گرفتن پول، این شماره ها را در یک وب سایت در معرض دید همگان می گذارد .
- مه ۲۰۰۰ ویروس «دوستت دارم» با قابلیت کپی کردن خود برای هرکس از طریق کتابچه آدرس به سرعت در تمام دنیا پخش می شود.
- فوریه ۲۰۰۱ یک هکر هلندی به منظور تنبیه بسیاری از کسانی که به دیدن عکس های غیراخلاقی یک قهرمان تنیس بسیار مشتاق بودند، ویروسی را به همین نام پخش می کند .
- سپتامبر ۲۰۰۱ در صبح یازدهم سپتامبر قوانین جدید ضد تروریسم تصویب شدند. در بسیاری از این قوانین از هکرها به عنوان تروریست یاد شده است.
- فوریه ۲۰۰۲ مایکروسافت در بخش «محاسبات قابل اطمینان ابتدایی»، ارتقای ویندوز را متوقف و هشت هزار برنامه نویس را تحت آموزش های امنیتی قرار می دهد .
- مه ۲۰۰۲ کرم «کلز- اچ» از تمام ویروس های شناخته شده از نظر تعداد کامپیوترهای ویروسی شده پیشی می گیرد .
- فوریه ۲۰۰۳ ایالات متحده یک هکر اهل قزاقستان را به علت نفوذ غیرقانونی به کامپیوترهای «بولومبرگ» و اقدام به اخاذی محکوم می کند .

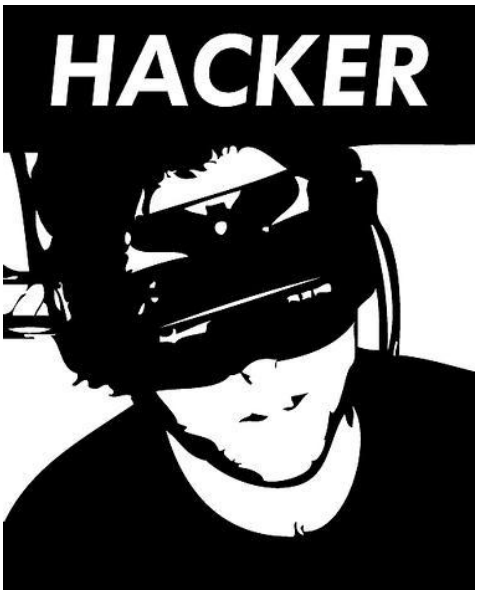
این مقوله ادامه داشت تا همین امروز

جالبترین اونها در بهمن 87 این خبر بود:

هکر ها نمره های دانشجویان پیام نور را تغییر دادند...

طبق اطلاعات رسیده چند دانشجو هفته گذشته با نفوذ به سایت داشنگاه پیام نور خودشان توانسته بودند که نمره های خود را تغییر دهند.این موضوع باعث واکنش وزارت علوم برای امن کردن سایت های دانشگاهی شد.

..: M R S :.. Email: mr.soltany@yahoo.com



انواع هکرها

هکرها را می توان بر اساس نوع فعالیت و دانش به پنج گروه طبقه بندی کرد که عبارتند از :

- **هکرهای کلاه سفید :**

که به آنها سامورایی یا هکرهای واقعی گفته می شود . هکرهای کلاه سفید متخصصان کامپیوتر و آشنا به فناوری اطلاعات می باشند و هدفشان از نفوذ به سیستم های کامپیوتری کشف عیوب امنیتی در سیستم و بر طرف نمودن آنها است ، نه سوء استفاده . به عبارت ساده تر ، کلاه سفید ها برای این کار باید مانند هکرهای کلاه سیاه عمل کنند تا بتوانند ضعف های سیستم را کشف کنند در حال حاضر بسیاری از شرکتها و مؤسسات از هکرهای کلاه سفید برای کنترل و محافظت از سیستم های کامپیوتری خود استفاده می کنند ، این موضوع پس از حملات گسترده سال گذشته به سایت های ایرانی وخسارت هایی که به این سایت ها و صاحبان آن ها و نیز خدمات دهندگان اینترنت وارد آمد ، تا مدتی مورد توجه قرار گرفته و مطبوعات در آن موقع در مورد لزوم امنیت سیستم های کامپیوتری بررسی های کامل انجام دادند . ولی با گذشت زمان متأسفانه بسیاری از شرکت ها و مؤسسات با علم به ضعف امنیتی سیستم های خود حاضر به قبول مشاوره و نیز بر طرف نمودن این عیوب که بعضاً به سادگی قابل بر طرف شدن می باشد ، نیستند .

- **هکرهای کلاه سیاه :**

به آنها واکر هم گفته می شود و از نظر کاری هکرهای کلاه سیاه دقیقاً برعکس هکر کلاه سفید عمل می نماید . به این معنی که هدف آن ها نفوذ به سیستم ها و سوء استفاده از اطلاعات می باشد .

این گروه از هکرها بیشترین صدمات را به سیستم های کامپیوتری وارد می نمایند که بی سابقه ترین و بزرگترین حمله توسط این گروه از هکرها در تاریخ ۲۱ اکتبر سال ۲۰۰۲ ساعت ۴ بعد از ظهر به وقت آمریکا رخ داد . این حمله که از نوع (DDOS) بود بر روی ۱۳ سرور اصلی اینترنت صورت گرفت ، در این حمله ۹ سرور به طور کامل از کار می افتد . اهمیت این واقعه آنقدر بود که حتی کاخ سفید و رئیس جمهور آمریکا وارد عمل می شوند و از آن بعنوان یک کار تروریستی مجازی اسم می برند ، و اگر تلاش به موقع کارشناسان امنیتی نبود و هکرها موفق می شدند عملیات خود را تکمیل کنند ، اکنون جهان درگیر یک فاجعه می شد .

- **قفل بازکن یا کراکر :**

از نظر ماهیت کار این گروه از هکرها جزو گروه هکرهای کلاه سیاه می باشند . فعالیت این گروه از هکرها بیشتر در مورد نرم افزارها و سیستمهای کامپیوتری می باشد که دارای قفل بوده و بصورت مجانی و یا اختصاصی مورد استفاده قرار می گیرد . فعالیت این گروه در حوزه نرم افزار بسیار فراگیر می باشد .

برخی از تولید کنندگان نرم افزار بر این باورند که کراکرها به سراغ محصولات آنها نمی روند . با وجودی که متخصصان امنیت کامپیوتر به روش های گوناگون در این مورد تولید کنندگان و کاربران این گونه محصولات هشدار می دهند ولی باز شاهد ضعف های این محصولات می باشیم . این ضعف ها می تواند بصورت نقص در کد یا منطق برنامه و یا حتی عدم سازگاری محصول نرم افزاری با سایر محصولات موجود بر روی سیسم بروز نماید .

این امر در بین محصولات نرم افزار ایرانی گستردگی بیشتری نسبت به سایر نرم افزار ها دارد، که جای تأمل و بررسی بیشتری دارد.

- **Preaker :**

از قدیمی ترین و در واقع هکرهای اولیه ای بودند که برای کارشناسان نیاز به کامپیوتر نداشتند و بیشتر کارشان نفوذ به خطوط تلفن برای تماس مجانی ، استراق سمع و ... بود .

- **هکرهای جوان (Script Kiddies)**

این گروه از هکرها با سایر گروه های هک تفاوت دارند و هکرهای جوان بر خلاف سایر هکرها که ابزار و برنامه های مورد نیاز را خودشان می نویسند و برای هک از معلومات خود استفاده می کنند ، با استفاده از برنامه های خدماتی ویژه هک که به وسیله دیگران نوشته شده است (مانند Sub۷) و به راحتی از طریق اینترنت و یا فروشگاه ها قابل تهیه می باشند ، به سیستم های کامپیوتری خسارت وارد می نمایند .

این گررروه از هکرها بیشتر با هدف سرگرمی و یا نمایش دانش خود به سایر دوستان و همکلاسی های خود اقدام به این کار می نمایند ولی گاهی مشاهده شده است که از این کار برای اهداف دیگری بهره گرفته اند ، بعنوان مثال می توان به هکی که توسط تعدادی دانش آموزان در یکی از مدارس آمریکا صورت گرفت اشاره نمود که در آن دانش آموزان با نفوذ به شبکه مدرسه نمرات امتحانی خود را تغییر داده اند .

بسیاری از کارشناسان معتقدند که ظهور رو به رشد هکرهای جوان ، مهمترین تهدید برای امنیت سیستم های کامپیوتری شده است . زیرا با وجود ابزارهای موجود و در اختیار این گروه و نیز وقتی که این گروه از هکرها برای این کار صرف می کنند ، از کار انداختن سایت های اینترنتی و یا نفوذ به یک شبکه ، نیاز به داشتن اطلاعات کامل در مورد کامپیوتر ندارد .

هکرها در همه جا حضور دارند ، اما شاید به اشتباه تصور کنید که سیستم شما به علت کوچک بودن و یا نداشتن اطلاعات مهم برای آن ها جالب توجه نیست ، باید به یاد داشته باشیم که هکرها همیشه کامپیوترهای خاص را هدف قرار نمی دهند ، آنها کامپیوتر های زیادی را کنترل می کنند تا حفره های امنیتی را در آن ها پیدا کنند . یک هکر ممکن است یک کارمند شرکت باشد که برای انتقال گرفتن به سیستم های شرکت صدمه می زند و یا فردی باشد که از سیستم شما برای حمله به سیستم دیگر استفاده می کند .

بهترین راه مقابله با هکرها بالا بردن امنیت سیستم های کامپیوتری می باشد . این کار ممکن است با تهیه سیستمهای نرم افزاری و سخت افزاری انجام شود . هیچ گاه به یک روش خاصی جهت حفظ امنیت اکتفا نکنید و نسخه جدید هر نرم افزار را تهیه کنید و دسترسی کاربران را به اطلاعات کنترل نمایید .
سعی کنید از هکران کلاه سفید بعنوان مشاوره امنیت سیستمهای کامپیوتری خود استفاده کنید و همیشه به خاطر داشته باشید که بر خلاف مدیران سیستم و شبکه که دارای وقت کمی برای جستجو و تحقیق و بررسی نقاط ضعف سیستم و بر طرف نمودن آنها می باشند ، هکرها دارای وقت کافی و منابع اطلاعاتی مناسب برای صدمه زدن به سیستمهای شما می باشند .

انواع هک

با بررسی مقالهای متعدد در زمینه هک به ان نتیجه رسیدم که هک در زمینه اینترنت به دو بخش کلی تقسیم میشود

1 -هک CLIENT
2 -هک SERVER

البته اگر هک را فقط در اینترنت بسط ندهیم مقوله هک گوشی های تلفن همره هک انواع سخت افزارها و نرم افزارها و برنامه های کاربردی مطرح میشود که از حوصله این مقاله خارج است.

کامپیوتر های client : کامپیوترهایی که استفاده کننده هستند مثل همین کامپیوتر خودتان که دارید ازش کار می کشید .
در ان نوع هک هکر به اطلاعات شخصی و پسوردهای کامپیوتر های خانگی نفوذ میکنند

کامپیوترهای server: به کامپیوتری که به کامپیوتر های دیگر جهت مشاهده صفحات وب سرویس می دهد , سرویس دهنده یا میزبان (server) می گوییم

در این نوع هک هکرها هدفشان حمله به سایتها و وبلاگهاست.

در هر دو نوع هک ما احتیاج به دانستن IP و port طرف مقابل و یا سایت مورد نظر داریم.

ip چیست؟

شماره ایست که به هر کامپیوتر متصل به اینترنت داده میشود تا بتوان به کمک آن شماره به آن کامپیوترها دسترسي داشت. اين عدد براي كامپيوترهايي كه حالت سرور دارند و نيز كامپيوترهاي كلاينتي كه معمولا به روشي غير از شمارهگيري (Dial Up) به اينترنت وصل هستند، عددي ثابت و براي ديگران عددي متغير است.و در هر بار وصل شدن به اينترنت اين شماره عوض ميشود يعني هر بار كه شما با شركت ISP خود تماس گرفته و به اينترنت وصل ميشويد، عددي

جدید به شما نسبت داده میشود.
این عدد یک عدد ۳۲ بیتي است و براي راحتي بهصورت زیر نوشته میشود:
xxx.xxx.xxx.xxx که منظور از xxx عددي بین ۰ تا ۲۵۵ است (البته بعضي شمارهها قابل استفاده نیست). مثلا ممکن است آدرس شما به صورت 195.219.176.69 باشد. حتي اسمهایي مثل http://www.yahoo.com که براي اتصال استفاده میکنید، در نهایت باید به یک IP تبدیل شود، تا شما سایت یاهو را ببینید.
در IP معمولا xxx اولي معناي خاصي دارد، که بعدا توضیح میدهم... فقط این را بگویم که اگر به روش Dial Up به اینترنت وصل شوید، معمولا عددي که به عنوان xxx اول میگیرید، مابین 192 تا 223 خواهد بود. این توضیح براي تشخیص کامپیوترهاي کلاینت از سرور (حداقل در ایران) بسیار میتواند مفید باشد.
برای دیدن ip خود کافیست به مسیر زیر برید

Start>RUN>

حالا تایپ کنید cmd در پنجره باز شده نایپ کنید IPCONFIG حالا ip شما مشخص میشود.

IP:راههای بدست آوردن

هر بار که یک کامپیوتر به کامپیوتر دیگري متصل مي شود، حداقل اطلاعاتي که باید به آن بدهد آدرس IP خود است؛ بنابراین یافتن IP کسي که به دلیلي قصد اتصال به رایانه شما را داشته است نه تنها غیر قانوني نیست بلکه یک موضوع کاملاً طبیعي است. تمامي روشهاي یافتن IP به نوعي به این اصل کلي برمي گردند. شاید به نظرتان بیاید که هنگامي که با کسي روي مسنجر صحبت مي کنید باید کامپیوترهاي شما به هم متصل باشند و بنابر این به سادگي بتوان IP فرد مقابل را به دست آورد، اما مسنجرهاي معتبر مانند Yahoo یا MSN در حقیقت میزبان خود را بین شما و فرد مقابل قرار مي دهند به این صورت که شما و دوستتان هر دو به سرور مسنجر متصل مي شوید و همه پیامها از آن عبور مي کنند. پس پیامي که شما مي نویسید وارد سرور مسنجر مي شود و سپس از طریق سرور مسنجر به فرد مقابلتان مي رسد و بالعکس. اما نگذارید این موضوع شما را ناامید کند! هنگامي که شما و دوستتان در یک بازي مسنجري شرکت کنید یا فایلي را به طور مستقیم براي او بفرستید دو کامپیوتر به طور مستقیم به هم متصل هستند! این روش یکي از مناسبترین روشهاست. در زیر چند روش مناسب یافتن IP را براي شما توضیح مي دهیم، اما قبل از آن، نکته مهمي را یادآوري مي کنیم: اگر کسي از اینترنت قطع شود، IP او عوض مي شود! پس اگر شما امروز IP کسي را به دست آورید که با خط تلفن و مودم به اینترنت وصل مي شود، ممکن است 30 ثانیه بعد او Disconnect کند و دوباره Connect شود که در این شرایط قاعدتاً IP دیگري خواهد داشت که این موضوع اطلاع قبلي شما را بي فایده مي کند! اما اگر کسي به هردلیل قصد حمله و آزار شما را داشت، بلافاصله IP او را به دست آورید که از طریق آن بتوانید به طور قانوني از وي شکایت کنید . از طرف دیگر اگر کسي از Proxy استفاده کند، به دست

آوردن IP او بسيار دشوار مي شود (اگر فرد Java Script را از كار نينداخته باشد با استفاده از آن مي توانيد IP را به دست آوريد!)

خواندن IP از طريق ايميل:

هنگامي كه شما يک ايميل از فردي مي گيريد، معمولاً آدرس IP وي در آن نامه وجود دارد. ابتدا بايد با رفتن به قسمت تنظيمات ايميل خود آن را در حالتي قرار دهيد كه تمامي Header نامه را به شما نشان دهد كه با كمي گردش در قسمت تنظيمات ايميل خود آن را پيدا خواهيد كرد. حال به بالاي ايميل دقت كنيد و به دنبال عبارت Received: from باشيد. شما معمولاً دو يا چند بار عبارت "Received: from" را در بالاي ايميل خواهيد ديد كه ما فقط با پاييني كار داريم كه معمولاً كمي با بالاييها فاصله دارد و بعد از Message ID قرار مي گيرد

به دست آوردن IP از طريق سايت خودتان:

اگر سايت يا وبلاگي داريد، راههاي بسياري براي به دست آوردن IP بازديدكنندگانتان داريد و با دادن آدرس سايت يا وبلاگتان به يكي از دوستان مي توانيد IP او را به دست آوريد. از آنجايي كه در يک لحظه ممكن است چندين بازديد كننده داشته باشيد، بهتر است صفحه زيبايي مخصوص اين كار بسازيد كه هيچ لينكي به آن نباشد و آن را براي به دست آوردن IP مورد استفاده قرار دهيد.

براي اين كار دو روش اصلي داريم:

1- برنامه نويسي: با كمي جستجو در اينترنت كدهاي بسيار كوتاهي را مي يابيد كه IP را به دست مي دهند و به سادگي مي توانيد آن را به همراه تاريخ و ساعت در يک فايل متني يا پايگاه داده ذخيره كنيد.

2- استفاده از سايتهاي ديگر: اكثر شمارنده ها اين امكان را به شما مي دهند كه IP بازديد كنندگان صفحات خود (حداقل چند بازديد كننده اخير) را ببينيد. پس با نصب يک شمارنده روي آن صفحه اي كه گفتيم، IP به دست آمده است.

به دست آوردن IP از طريق مسنجرها:

هنگام چت با فرد مورد نظر كافيست از برنامه های مانند mansor yasini استفاده كنيد كه براحتی ip طرف مقابل را بدست می آورد.

اما هر سايتی مانند هر شخص ip خاص خود را دارد كه از طريق زير ميتوانيد آن را بيابيد

1-در command prompt تايپ كنيد ping سپس نام سايت مورد نظر ip مشخص ميشود.

2-در هنگام باز شدن سايت مورد نظر در پايين مرورگرها ip آن سايت نمايان ميشود.

3-با رفتن به سایت www.samspade.org در جای خالی نام سایت مورد نظر را بزنید تا اطلاعات خوبی در مورد سایت مورد نظر دریافت کنید.

پورت (Port) چیست؟

محلي است كه دادهها وارد با خارج ميشوند. در مبحث هک معمولا با پورتهاي نرمافزاري سروكار داريم كه به هر كدام عددي نسبت ميدهيم. اين اعداد بين ۱ و ۶۵۵۳۵ هستند. معمولا به يک سري از پورتها كار خاصي را نسبت ميدهند و بقيه بهصورت پيشفرض براي استفاده شما هستند. پورتهاي كه فعال هستند، هركدام توسط يک نرمافزار خاص مديريت ميشوند. مثلا پورت ۲۵ براي ارسال Email است، بنابراين بايد توسط يک نرمافزار اين كار انجام شود و اين نرمافزار بر روي پورت ۲۵ منتظر (فالگوش) ميماند. اينجا ممكن است شخصي از فلان نرمافزار و ديگري از بهمان نرمافزار استفاده كند ولي بههر حال پورت ۲۵ هميشه براي ارسال Email است.

و پورتي كه ياهو مسنجر از آن استفاده ميكند ۵۰۵۰ هست. از پورت هاي مهم : ۷۹ ,۱۱۹,۲۳,۱۵,۷,۲۱,۱۳۹,۱۱۰و..

راه ارتباط هکر با کامپیوترهای قربانی همین پورتها هستند که با استفاده از برنامه های مانند telnet و nc با کامپیوتر مورد نظر مرتبط می شوند.

۱- استفاده از telnet :

اگر بخواهیم با ip ای به شماره194.225.184.13 از طریق پورت 25 صحبت کنیم باید بنویسیم:

```
telnet 194.225.184.13 25
```

و بعد اینکه ارتباط برقرار شد باید شروع کنیم و از طریق زبان پورت ۲۵ با آن صحبت کنیم.

۲- استفاده از nc :

اگر بخواهیم همان کار را با netcat انجام دهیم، باید بنویسیم:

```
nc -v 194.225.184.13 25
```

و بعد از برقراری ارتباط شروع به صحبت کنیم.

در پایین لیستی از مهمترین پورت‌ها و کاربردشون رو می‌بینین :

```
!Port Num Service Why it is phun
---------------------------------- ------- --------
type echo Host repearts what you 7
discard Dev/null 9
systat Lots of info on users 11
```

Time and date at computers location daytime 13
networks netstat Tremendous info on 15
.chargen Pours out a stream of ASCII characters 19
Transfers files ftp 21
.telnet Where you log in 23
smpt Forge email 25
Time time 37
rlp Resource location 39
whois Info on hosts and networks 43
domain Nameserver 53
gopher Out-of-date info hunter 70
on users finger Lots of info 79
http Web server 80
pop Incoming email 110
groups -- forge posts, cancels nntp Usenet news 119
shttp Another web server 443
notification biff Mail 512
rlogin Remote login 513
who Remote who and uptime
!shell Remote command, no password used 514
syslog Remote system logging
route Routing information protocol 520

و این مبحث ادامه دارد از دوستان علاقه مند خواهش میکنم این مقوله رو در اینترنت دنبال کنند من هم سعی میکنم در سایت خودمون قرار بدم به نشانی www.pnuni.ir

چون اصلی ترین راه هک سایت کار با پورتها و برنامه های مربوطه است که بحثی تخصصی و طولانیست و من از آن میگذرم.

به این سایت توجه کنید که توسط هکرها هک شده هکر ها بعد از نفوذ به سروری که سایت مورد نظر در آن قرار دارد صفحه اینترنتی را اضافه کردند و قصد خود را نشان دادن مشکل سایت و کمک برای حل و بستن راه نفوذ عنوان کرده اند . سایت مورد نظر سایت فضایی ایران است.

نکته:

اگر قصد هکر شدن دارید باید توجه کنید اولین کار یادگیری سواد برنامه نویسی مخصوصا زبان C و زبان هکری (مراجعه شود به پیوست مقاله)است ضمنا ممارست و پشت کار بسیار لازمه آن است باید بدانید که پیدا کردن فرد خاطی و هکرها آرزوی مدیران وب است و آنها هم به کمین هکرها نشسته اند و اینجاست که صحبت ظرف عسل به میان میاید

ظرف عسل چیست؟

با گذشت سال ها به تعداد هکر ها و نفوذ کنندگان به سرورها و شبکه های گسترده اینترنتی افزایش یافت و هر روز اطلاعات بسیار ارزشمندی از قبیل شماره های حساب بانکی شماره های کاربری پسورد ها و ... دزدیده می شدند و خسارتهای بسیار زیاد از نظر مالی و اعتباری به شرکتهای کوچک و بزرگ زده می شود حتی یک حمله کوچک گاهی بزرگ ترین خسارت ها رو وارد می کرد !

بنابراین دانشمندان و برنامه نویسان چیره دست سریع دست به کار شدند تا بتوانند جلوی این قبیل حملات رو بگیرند یا به نوعی هکرها رو منحرف کنند .

بهترین طعمه برای فریب دادن هکرها اطلاعات نادرست و گمراه کننده بود .

پس برنامه نویسان دانشمندان سخت افزار بعد چندی تالش توانستند قطعه و برنامه ای به نام ظرف عسل یا Honey Pot را تولید کنند وظیفه این ظرف عسل گمراه کردن و به دام انداختن هکرها است.

روش کار به این صورت است که با باز گذاشتن باگهای در سرور خود منتظر هکرها میمانند تا شاهد نفوذ آنها باشند اما در اصل آنها را به دام انداخته اند.

باگ چیست؟

به هر نقص يا ايراد يك نرم‌افزار يا برنامه كامپيوتري باگ مي‌گويند. باگ از نظر لغوي يعني خانمي كه در دانشگاه حشره كوچك و در تاريخ مهندسي نرم‌افزار گفته مي‌شود اين اصطلاح را هاروارد مشغول تحصيل و تحقيق در رشته كامپيوتر بود، به كار برده است. او كه در حال كار با يك‌بار با مشكل مواجه شد و تكنيسين‌هايي كه براي بررسي مشكل و تعمير كامپيوتر، آن را باز كرده بودند سوسكي را پيدا كردند كه وارد دستگاه شده بود و آن را از كار انداخته بود.

البته در حقيقت اين واژه را اولين بار همان تكنيسين‌هايي كه اين حشره را داخل دستگاه يافته بودند، طي يادداشتي (اولين دليل واقعي باگ / ايراد برنامه پيدا شد) به شوخي به توسط همين افراد ابداع شد.

Debugging

موضوع باگ يكي از سرفصل‌هاي مهم رشته مهندسي نرم‌افزار است. از اين رو متون و كتاب‌هاي مفصلي در زمينه يا اشكال‌زدايي از نرم‌افزار و متدهاي آن تأليف شده است و همچنان ادامه دارد. برنامه‌نويسان تازه‌كار معمولاً از اين شاخه مهندسي نرم‌افزار گريزانند و اميدوارند برنامه‌هايي بنويسند كه به قدري خوب باشد كه اصلاً كارش به اشكال زدايي نكشد، ولي پس از دو سه سال كار حرفه‌اي در اين زمينه سرانجام تسليم مي‌شوند و آشنايي با اصول علمي اشكال زدايي برايشان به يك ضرورت تبديل مي‌شود؛ مگر اين‌كه نخواهد به اصول اخلاقي و حرفه‌اي مهندسي نرم‌افزار متعهد باشند و از اين‌كه برنامه‌هاي ساخت آن‌ها پر از انواع باگ و ايراد باشد، باكي نداشته باشند، اما برطرف كردن باگ‌ها براي بسياري از برنامه‌نويسان غيرآماتور يكي از قسمت‌هاي چالش برانگيز و لذت بخش كار است و تقريباً مثل حل كردن معما است.
برنامه‌نويساني كه دائماً به فكر كاستن از باگ‌ها و ايرادهاي نرم‌افزارهاي خود هستند، در حقيقت به طور مداوم در حال انجام يك ورزش فكري هستند كه رشته‌اي تو در تو از حلقه‌هاي پرسش و پاسخ را در دل خود دارد

حافظه؛ شاه كليد باگ

منشأ پيدايش باگ‌ها، اتفاقات پيش‌بيني نشده‌اي است كه درون حافظه رخ مي‌دهند. آنجا محل زد و خورد داده‌هاي قد و نيم‌قدي است كه گاه بسيار كوچك‌تر از شرايط مرزي حافظه هستند و گاه با ديواره‌هاي آن برخورد مي‌كنند. گاهي كوچكند، اما سرشماري آن‌ها مثل شمارش كودكان در حال بازي در حياط يك دبستان شلوغ، كار سختي است.
دستورالعمل‌ها و متغيرها مي‌آيند و مي‌روند. بعضي پاك مي‌شوند و بعضي همچنان در گوشه‌اي از حافظه مي‌مانند و بايت‌هايي كه مي‌مانند، شرايط مرزي را براي دستورالعمل‌ها و ورودي‌هاي بعدي دشوارتر مي‌كنند. بامزه‌ترين نوع باگ‌ها در فرايندهاي مركب پديد مي‌آيند. مثلاً روتين را به حافظه مي‌فرستيد تا آنجا دنبال مقداري بگردد؛ غافل از اين‌كه يك روتين ديگر قبلاً به صورت اتفاقي آنجا آمده و آن مقدار را پاك كرده است و حالا روتين سرگردان اين سو و آن سوي حافظه دنبال گمشده‌اش مي‌گردد!

بنابراين به عنوان برنامه‌نويس اگر مايليد نرم‌افزارتان كمترين باگ را داشته باشد، بايد حافظه مورد استفاده نرم‌افزارتان را هنگام اجرا زير نظر بگيريد و ببينيد آنجا واقعاً چه خبر است.
مديريت حافظه بسيار مهم است؛ نه فقط از اين جهت كه حافظه را از وجود متغيرهاي بي‌استفاده و روتين‌هاي راكد پاك كنيد، بلكه از اين جهت كه نحوه تعامل ورودي‌ها، خروجي‌ها و فرايندهاي نرم‌افزار خود را به دقت مانيتور و تماشا كنيد. حافظه كامپيوتر مانند آزمايشگاهي است كه داده‌ها و دستورالعمل‌ها را در آن به جان هم مي‌اندازيد. پس خوب است همچون شيميدانان به ارلن و بِشِر خود نگاه كنيد و ببينيد مولكول‌ها چگونه به هم واكنش نشان مي‌دهند.

به اين مثال توجه كنيد

ترميم 26 حفره‌ي امنيتي محصولات مايكروسافت

در اين به‌روزرساني امنيتي، مايكروسافت دو حفره‌اي را كه پيش از اين براي انجام حملات اينترنتي عليه كاربران نسخه‌هاي 6 و 7 مرورگر اينترنت اكسپلورر، به‌كار گرفته شده را ترميم كرده و به‌علاوه با انتشار دو وصله‌ي امنيتي، پنج آسيب‌پذيري ديگر در اينترنت اكسپلورر را ترميم كرد كه طبق اعلام مايكروسافت در تمامي نسخه‌هاي اين مرورگر وجود دارند. اين باگها قابل ترميمند.

بر اساس اين گزارش نيمي از آسيب‌پذيري‌هاي ترميم شده به مجموعه نرم‌افزاري آفيس و برنامه‌هاي اكسل، پاورپوينت و ورد مربوط بودند؛

اين شركت نرم‌افزاري همچنين آسيب‌پذيري‌هاي ويندوز مسنجر، اوت لوك اكسپرس و ويندوز ميل را نيز ترميم كرد.

نکته:

همیشه سعی کنید از نسخه های بروز نرم افزارها استفاده کنید. از ویندوز اصل استفاده کنید تا قبلیت به روز رسانی داشته باشد.ضمننا از پتچ patch های ارئه شده توسط شرکت های نرم افزاری که مانند یک وصله عمل میکنند استفاده کنید.حتما از یک آنتی ویروس آپ دیت بهره ببرید.

ویروس چیست؟

ویروس های کامپیوتری برنامه هایی هستند که مشابه ویروس های بیولوژیک گسترش یافته و پس از وارد شدن به کامپیوتر اقدامات غیرمنتظره ای را انجام می دهند. با وجودی که همه ویروس ها خطرناک نیستند، ولی بسیاری از آنها با هدف تخریب انواع مشخصی از فایل ها، برنامه های کاربردی و یا سیستم های عامل نوشته شده اند.

ویروس ها هم مشابه همه برنامه های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده مرکزی و سایر منابع بهره می گیرند و می توانند اعمال خطرناکی را انجام دهند به عنوان مثال فایل های روی دیسک را پاک کرده و یا کل دیسک سخت را فرمت کنند. همچنین یک ویروس می تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احراز هویت فراهم آورد.

استفاده از آنتی ویروس

یک نرم افزار Anti Virus که به اختصار آنرا AV می نامیم، نرم افزارهای AV با مشاهده و بررسی محتوای فایل ها به دنبال الگوهای آشنای ویروسها یا کرم های اینترنتی می گردند. در صورت مشاهده این الگوها که به آن Virus Signature گفته می شود، از ورود آن به کامپیوتر شما و اجرا شدن جلوگیری می کنند و یا به شما هشدار لازم را می دهند و از شما دستور میگیرند که آیا فایل را حذف کنند و یا سعی در اصلاح آن نمایند .
شرکتهای سازنده آنتی ویروس با آمدن ویروسهای جدید، الگوهای نرم افزاری آنها را کشف و جمع آوری می کنند و به همین علت اغلب لازم است تا این نرم افزارها هر چندگاهی به روز (Update)شوند تا الگوهای جدید ویروسها را بشناسند.

ویروسها باهوش هستند

روشهای بسیاری وجود دارد که توسط آن برنامه های مختلفی که حامل ویروس هستند، نظاره گر رفتار کامپیوتر شما میشوند. شما در حال نگاه کردن به یک فیلم روی اینترنت هستنید، یا در حال خواندن یک نامه و بسیاری کارهای عادی دیگر ... و بدون آنکه بدانید در همان زمان شما به ویروسی اجازه دادید تا کامپیوتر شما را بررسی و تحلیل کند .

بسیاری از اوقات هنگامی که شما آنها را شناسایی می کنید و از بین می برید، خبر ندارید که ویروس برای ورود مجدد و فعال شدن در کامپیوتر شما قبلا" چاره لازم را اندیشیده است و راه های دیگری (Backdoors) برای حمله مجدد به کامپیوتر یا شبکه شما ایجاد کرده است .

ویروسها چگونه وارد کامپیوتر شما می شوند

راه های مختلفی برای رسیدن ویروس ها به کامپیوتر شما وجود دارد، مانند فلاپی دیسک، CD، مشاهده وب سایت، email، اجرای فایل های download شده و ... بنابراین لازم است که تمامی این موارد به هنگام استفاده مورد کنترل یک AV قرار گیرد. به بیان دیگر هنگامی که میخواهید برنامه ای را از روی یک CD را اجرا کنید و یا email ای را باز کنید باید آنها را توسط یک AV کنترل کنید.

تروجانها

تروجان یک فایل جاسوسی میباشد که توسط هکر با توجه به نیاز به اطلاعاته قربانی آماده میشود و برای قربانی فرستاده میشود

هکر با توجه به نیاز های خود به اطلاعات قربانی که میتواند این اطلاعات:پسورد ایمیل یا ایدی قربانی,اشتراک اینترنت(اکانت),نام و پسورد کامپیوتر قربانی و ... میباشد تنظیم میکند.

با توجه به تحقیقاتی که داشتم میتوانم بگویم هر هکری کار خود را با این نوع کارها شروع میکند.یعنی با تنظیم ترجان,فرستادن تروجان برای قربانی,هک کردن ایدی و اکانت اینترنت و....
در اوایل ورود این نوع جاسوسها به اینترنت فقط کارایی محدودی داشتند.همه کارایی آن نوع تروجانها به فرستادن پسورد یاهو ختم میشد.
با گذشت زمان و علاقه برنامه نویسان به این نوع جاسوس ها کم کم امکانات آن را افزایش دادند تا به امروز.

ولی امکانات یک تروجان امروزی چیست؟
تروجانهای امروزی میتوانم بگویم دیگر رشد کامل خود را تا حد زیادی طی نموده است امکان دارد با ورود یک تروجان به کامپیوتر شما:
1-فرستاده شدن پسورد ای دی مخصوصا ایدی و پسورد مسنجر شما برای هکر(به ایمیل هکر یا ایدی یا یک اف تی پی مشخص شده توسط هکر)
2-فرستاده شدن اکانت اینترنت شما برای هکر
3-فرستاده شدن نام کامپیوتر شما همراه با پسورد ویندوز برای هکر
4-محدود کردن کارهای شما با کامپیوتر(قفل شدن Task Manager یا Mscoing یا Rigistry و...) کامپیوتر شما توسط هکر
5-از کار انداختن ویروس کش و فایروال کامپیوتر شما
6-در اختیار داشتن هارد شما توسط هکر(پاک کردن فایل از کامپیوتر شما و یا اضافه کردن فایل توسط هکر)
بله همه اینها که خوندید امکان دارد.فقط کافیست یک تروجان روی کامپیوتر شما توسط هکر فعال شود.

ولی چگونه امکان دارد که تروجان وارد کامپیوتر ما شود:

1-در حال چت کردن هستید فرد مقابل برایتان میخواهد عکس خودش یا نرم افزاری را سند کند .شما آن را میگیرید ولی آیا این فایل سالم است.از کجا مطمئن هستید که حاوی تروجان نیست؟
2-در حال گشت در یک سایت آموزش هک هستید میخواهید یک نرم افزار دانلود کنید از کجا مطمئن هستید که این نرم افزار سالم است؟
3-برایتان یک ایمیل میاید.ایمیلی که فرستنده آن نامشخص است ایا ایمیل سالم است؟
و...
تروجان ها بر خلاف ویروس ها که فقط شامل چند شکل محدود میشوند دارای اشکال خیلی زیادی هستند.
یک تروجان میتواند خود را به شکلهای: عکس,یک فایل صوتی,یک فایل نقاشی,یک فایل Setup و....
پس میبینید تروجان یک شکل مخصوص ندارد .

چگونه متوجه شویم که در کامپیوتر ما تروجان فعال است:

1-در صورت از کار افتادن Task Managerو Msconfig
2-از کار افتادن ویروس کش
3-تغییر در شکل توپی پسورد در مسنجر ویا سیو نشدن آن
4-در صورت دیدن علائم مشکوک در مسنجر(باز و بسته شدن یک پنجره پی ام)
5-فعال بودن نرم افزار های مشکوک مثل Task Managerو Msconfig
6-خوانده شدن ایمیل های که ما آنها را قبلا نخوانده ایم در ایمیلمان

ولی ما برای مقابله با این نوع جاسوسها چه کارهایی باید انجام دهیم؟

1-داشتن یک ویروس کش قوی و به روز

2-داشتن یک فایروال خوب یا فعال کردن فایروال خود ویندوز
3-این را بدانید همیشه پسوند عکس (jpg,gif,..) میباشد و هیچ وقت یک عکس دارای پسوند exe نمیباشد و همیشه اگر فایل(عکس,نوشته و...) را گرفتید که داری پسوند مشکوک بود هرگز باز نکنید
4-همیشه Task Managerو Msconfigخود را چک کنید اگر چیزی مشکوک دیدید مثل sender.exeبروید و در درایو ویندوز پوشه windows/system32دنباله چنین فایلی باشید که مشکوک بود و آن را پاک کنید
5-هر گز از کسی که شناخت کافی ندارید فایلی دریافت نکنید
6-سعی کنید اگر میخواهید نرم افزار دانلود کنید از سایتهای معتبر دانلود کنید.
7-در صورت مشکوک شدن به وجود تروجان سریع اطلاعات خود را عوض کنید(پسورد ای دی,پسورد ویندوز و...)
8-سعی کنید ویندوز خود را عوض کنید و درایو ویندوز قبلی را فرمت کنید.
در مقالات بعدی به شما خواهیم گفت چگونه برای خود پسورد انتخاب نمایید که امکان هک شدنتان را تا حد امکان کم کند
9-وقتی کارتون با مسنجر یا mail box تموم میشه حتماً sign out کنید این موضوع خیلی مهمه در مبحث استفاده از ردپاها یا همون cookies ها روشی هست که هر چند تعداد خیلی کمی میتونن ازش استفاده کنن ولی میتونن از همین ردپا ها استفاده کنن و ایمیل های شما رو بخونن ولی با این روش نمی تونن پسورد بدست بیارن
10-یک تروجان به جای فونت مخصوص یک سایته که روشی که هنوز خیلی لو نرفته فرض کنید وارد یک صفحه میشید که اصلا نمیتونید فونتشو بخونید حالا یه لینک پایین گذاشته که گفته اقا جان این فایل رو دریافت کنید بعد از نصب میتونید متن صفحه رو بخونید حالا حساب کنید به جای فایل مربوط به فونت یک تروجان باشه

11-هیچ وقت cookies های اینترنت اکسپلور رو نگه ندارید و همیشه پاک کنید برای این کار در از منوهای بالایه صفحه گزینه Tools رو انتخاب کنید و بعد delete cookies رو بزنید یا کلا از settingگزینه never رو بزنید تا دیگه ردپایی از شما باقی نمونه

کرمها(worms)

کرمها اصولاً ويروس نيستند با اين وجود تفاوت بين آنها بسيار اندك است و معمولاً در اخبار روزمره آنها را با يكديگر اشتباه مي گيرند. ويروسها يك كامپيوتر منفرد را آلوده مي كنند وسعي نمي كنند به كامپيوتر ديگري راه پيدا كنند كرمها به كامپيوترهاي ديگر انتقال پيدا مي كنند با اعمال شما. (مثلاً با اشتراك گذاشتن فايلها بوسيله email يا بوسيله فلاپي ديسك ها كرمها به شدت علاقه مندند كه فقط خود را در ميان يك شبكه گسترش دهند. آنها به طور خود كار خودشان را به كامپيوترهاي ديگر انتقال مي دهند به علت اينكه انتقال آنها بين كامپيوترها به طور خودكار انجام مي پذيرد سرعت گسترش آنها بسيار سريعتر از ويروسها است.

معمولترين راه گسترش يك كرم اين است كه خود را به همه آدرسهاي email اي كه شما در address book خود ليست كرده ايد برساند يا outlook شركت مايكروسافت برنامه email اي است كه بيشترين آسيب پذيري را در برابر حمله كرمها دارد فقط به اين دليل كه عمومي ترين برنامه است براي كاهش دادن احتمال آلوده شدن به كرمها شما مي توانيد مراحل زير را اجرا كنيد

..: M R S :.. Email: mr.soltany@yahoo.com

- هيچ فايل الصاقي (attachment) غير منتظره اي را در email هاي خود باز نكنيد (بخصوص آنهايي را كه شامل پيغامهاي معمول مانند در اين جا فايلي كه شما درخواست كرده ايد وجود دارد.) هر چند آنها از منابع مطمئني براي شما ارسال شده باشند. براي فرستنده email اي بفرستيد (reply) و از او سئوال كنيد او واقعاً چنين فايلي براي شما فرستاده است يا نه؟
- يك آنتي ويروس نصب كنيد و آن را مرتباً up to date كنيد.
- اگر ممكن است از نرم افزار email اي به قير از Outlook Express استفاده كنيد.

كرمي كه به خوبي منتشر شده " Love Letter" نام دارد كه با فرستادن خود به آدرس email اي كه در address book نرم افزار Outlook Express وجود دارند منتشر مي شود به راحتي كپي كردن فايل در كامپيوتر قرباني خود را وارد مي كند و با يك عنوان به صورت " I LOVE YOU" وارد مي شود و پيغام آن به صورت زير است :

"Rindly chek the attached LOVE LETTER coming from me"

بدليل اينكه email از يك فرد شناخته شده براي گيرنده ارسال شده است بسياري از مردم گول مي خورند و كرم در حجم وسيع گسترش پيدا مي كند. اگر چه به كامپيوتر قرباني آسيب وارد مي شود ولي آسيب اصلي به كل شبكه وارد مي شود و همه آن را آلوده مي كند.

اسب تراوا چيز جالبي بنظر مي رسد اما چيزهاي آسيب رسان و كثيفي در بر دارد. و در لباس خدمات مفيد يا پيوستهاي (attachments) جذاب در email مثلاً يك screen saver پخش مي شود. آنها فايلهي الصاقي براي شما مي فرستند كه آنقدر براي شما جالب است كه آنها را براي دوستانتان مي فرستيد. در حاليكه آثار مخرب آن پنهان بوده با تأخير عمل مي كند بنابراين شما نمي دانيد چيزي كه در حال فرستادن آن هستيد يك فايل خطرناك است.

در مواقع ديگر اين كرمها تكثير مي شوند مانند يك كرم اينترنتي و خود را به صورت اتوماتيك به كامپيوترهاي ديگر مي رسانند و معمولاً از Outlook Express استفاده مي كنند.

چگونه یک پسورد مطمئن انتخاب کنیم؟

داشتن یک پسورد خوب و مطمئن میتواند احتمال هک شدن(لو رفتن پسورد)ایمیل یا ای دی خود را تا حد زیادی کاهش دهید.
ولی چه نوع پسوردی مطمئن میباشد.
همیشه برای انتخاب پسورد برای خود دو چیز را در نظر داشته باشید:
1-هیچ وقت پسورد خود را ساده انتخاب نکنید.
زیرا داشتن پسورد ساده کار هکر را راحت تر کرده و خیلی ساده میتواند پسورد آی دی شما را هک کند.
مثلا انتخاب پسورد123456 هیچ وقت نمیتواند پسوردی مناسب و خوب برای شما باشد.
2-هیچ گاه مشخصات فردی را برای پسورد خود انتخاب نکنید.

زیرا اگر کسی مشخصات شما را داشته باشد میتواند به ای دی شما نیز دست رسی داشته باشد.مثلا نام ,نام خانوادگی,شماره شناسنامه,نام همسر,شماره تلفن,تاریخ تولد و... نمیتواند پسورد مناسبی باشد.

چگونه پسورد مطمئنی داشته باشیم:

1-مد نظر گرفتن دو نکته بالا

2-همیشه سعی کنید از ترکیب اعداد و حروف برای پسورد خود انتخاب نمایید

3-استفاده از Space(فاصله) و Shift+123... (@#$%^&*) تا حد زیادی از لو رفتن پسورد جلوگیری میکند

4-سعی کنید پسورد خود را بین دوتگ <##>قرار دهید (یک پنجره پی ام باز کنید این نوشته را بفرستید <#PersianHack#>بعد آن را سند کنید ولی مشاهده میکنید که نوشته ای برای طرف مقابل فرستاده نشد)

5-استفاده از Alt مثلا استفاده ترکیبی کلیدهای Alt+0140 یا Alt+0256و...

استفاده از پیشنهادهای بالا برای انتخاب پسورد و خواندن مقالات قبلی تا حد زیادی از هک شدن شما جلوگیری میکند.

هکرها ایمیل و یا وبلاگ شمارا چگونه هک میکنند؟

هکرهای وبلاگها بخصوص بلاگفا بر این گونه است که آدرس ایمیل شما را از وبلاگ برداشته و ایمیل هشدار دهنده برای صاحب وبلاگ از طرف بلاگفا ارسال میشود و در متن ایمیل نوشته شده که عضویت شما در بلاگفا ایراد دارد به لینک زیر مراجعه کنید و مجددا آدرس وبلاگ و شناسه کاربری را وارد کنید این لینک لینکی مشابه با سایت خود بلاگفا است مثلا:

www.information.blogfa.com

و یا گونه های مختلف که کاربر را فریب دهد مثلا:

www.webmaster.blogfa.com

با این نوع آدرسها کاربر فکر میکند که مدیر سایت این میل را ارسال کرده و براحتی پسورد خود را در اختیار هکر قرار میدهند

کاربرها باید بدانند عضویت در هیچ سایتی به مشکل نمیخورد که مدیران سایت بخواهند برای شما ایمیلی که حاوی لینک باشد ارسال کنند اگر هم به مشکل بخورد برای شما لینکی ارسال نمیکنند فقط از شما امکان دارد درخواست کنند مجددا به سایت مراجعه کنید و عضو شوید که چنین چیزی تا حالا پیش نیامده است.

- استفاده از کافی نت هم بسیار در این امر خطرناک هست؟

کاربران باید توجه کنند که در کافی نت از چک کردن ایمیل و یا بروز کردن وبلاگ استفاده نکنند کافی نتها معمولا مرکز نرم افزارهای جاسوسی است و کسانی که به کافی نت ها مراجعه زیادی میکنند امکان دارد این برنامه ها را نصب کنند وبعد از استفاده شما امکان دارد هکر به کافی نت مراجعه کند و گزارش شناسه کاربری و کلمه عبور را در پایان هر روز از نرم افزار بگیرد.

امنیت خرید الکترونیکی:

هنگام انجام فعاليت هاي بسيار محرمانه مانند خريد و فروش آنلاين و يا انجام امور بانكي بايد نكات زير را هميشه به خاطر داشته باشيد:

1- از عدم حضور و فعاليت هر نوع كد مخرب در لحظه آغاز و در حين انجام فعاليت تجاري و دريافت هرگونه خدمات اينترنتي حساس، اطمينان حاصل كنيد.

در اين خصوص بايد گفت كه خطرناك ترين و در عين حال شايع ترين تهديد عليه فعاليت هاي مالي اعتباري در اينترنت، نوعي كد مخرب از خانواده تروژان هاي Banker مي باشد. اين تروژان پس از نفوذ در سيستم (اغلب به شكل نامحسوس)، بازديدهاي اينترنتي كاربر را كنترل مي كند و به محض ورود وي به پايگاه هاي مؤسسات مالي اعتبار، سيستم هاي پرداخت آنلاين، مراكز خريد وفروش اينترنتي و ... اطلاعات حساس مبادله شده را پس از سرقت، به مجرمان اينترنتي ارسال مي كنند.

2- تقريباً همه كارشناسان امنيتي عقيده دارند كه اكنون مؤثرترين ابزار دفاعي در رايانه ها، بهره گيري از روش هاي پيشگيرانه (Proactive) است. در اين روش رفتار خاص كدها و نرم افزارهاي فعال درموقعيت هاي مختلف، مهمترين عامل شناسايي و تفكيك كدهاي مخرب و مشكوك از كدهاي امن و مفيد است. در اين حالت نياز چنداني به استفاده از پايگاه هاي اطلاعات امنيتي ثبت شده و مشخصات ويروس هاي قديمي تر (البته تا حدي) نيست.

3- راهكار مؤثر ديگر استفاده از يك ابزار مكمل امنيتي در كنار نرم افزارهاي حفاظتي نصب شده در سيستم (يا به عبارتي در كنار همان راهكارهاي سنتي حفاظت از اطلاعات) براي ترميم نقاط ضعف آنهاست. يكي از اين سيستم هاي پيشرفته براي ردياب و كشف ويروس هاي ثبت نشده با نام TruPrevent™ ، ابزار قدرتمندي براي پيشگيري از نفوذهاي غيرمجاز و نيز افزايش توان بازدارندگي سيستم امنيتي نصب شده در رايانه است.

4- به هيچ وجه هرزنامه هاي موجود در صندوق پستي خود را جدي نگيريد و به آن ها اعتماد نكنيد؛ هرچند اگر بسيار جذاب و قابل توجه جلوه كنند.

5- قبل از انجام خريد از فروشگاه هاي آنلاين و يا از طريق پايگاه هاي الكترونيك، و نيز دريافت هرگونه خدمات اينترنتي، يكي از بهترين تدابير امنيتي، اطمينان از قانوني بودن، ميزان شهرت و سطح اعتبار اين مركز مالي تجاري ست. يك جستجوي ساده در اينترنت، شايد راهنماي خوبي در اين زمينه باشد.

6- سيستم هاي رايانه اي خود را همواره به روز نگاه داريد...

سيستم هاي عامل و نيز بسياري از برنامه هاي كاربردي نصب شده در رايانه شما يقيناً داراي نقص ها و حفره هاي امنيتي بي شماري هستند كه مي توانند توسط خرابكاران اينترنتي براي نفوذهاي نامحسوس و انجام فعاليت هاي غيرقانوني مورد استفاده قرار بگيرند. تنها يك اشكال كوچك امنيتي در برنامه هاي به ظاهر ساده و پركاربرد مانند Media Player، Yahoo Messenger و يا ACDSee، نقش خود را به نحو احسن ايفا مي كند.

7- هيچ گاه فايل ها و نرم افزارهاي نامطمئن را داونلود و اجرا نكنيد؛ به خصوص اگر آن ها در منابع و پايگاه هاي اينترنتي نامشخص و بي نام و نشان وجود داشته باشند. اين فايل ها مي توانند ضميمه نامه هاي الكترونيك و يا برگرفته از صفحات اينترنتي مشكوك باشند.. به خاطر داشته باشيد كه احتمال آلوده بودن اين فايل ها آنقدر زياد است كه با اجراي آن، بطور مستقيم كدهاي مخرب را در رايانه خود نصب مي كنيد.

8- هيچ گاه قبل از اطمينان كامل از شرايط امنيتي موجود، اقدام به پرداخت و يا نقل و انتقال پول نكنيد (درست به همان گونه كه معاملات حضوري و فيزيكي را انجام مي دهيد). به خاطر داشته باشيد كه احتمال كلاهبرداري و فعاليت غيرقانوني در اينترنت هميشه بيش از آن است كه فكر مي كنيد. شما نخستين فردي نيستيد كه شايد در ازاي سفارش آخرين و مدرن ترين نسل تلفن هاي همراه، جعبه اي پر از سنگ و ماسه دريافت كرده باشد!!

9- امروزه انجام مزايده هاي آنلاين در اينترنت به طور چشمگيري رواج يافته است. قبل از آغاز پيشنهاد قيمت و شروع مزايده، از شخصيت حقيقي و حقوقي مسئول مزايده اطلاع كامل پيدا كنيد و فريب تكنيك هاي حرفه اي فروش وي را نخوريد.

10- هيچ گاه اطلاعات حساس و محرمانه خود را از طريق نامه هاي الكترونيك ارسال نكنيد. كاربران عادي و حتي برخي از كاربران حرفه اي اينترنت گمان مي كنند كه اين روش بسيار امن تر از پركردن فرم هاي الكترونيكي ست. اما متآسفانه اين حقيقت ندارد. نامه هاي الكترونيك از لحاظ امنيتي بسيار آسيب پذيرند.

11- از تيزهوشي و حس شكاك خود بهره بگيريد. ظاهر و ساختار يك صفحه وب اغلب مي تواند نشان دهنده غيرواقعي بودن و يا امن نبودن آن باشد. به خاطر داشته باشيد كه در بسياري از موارد خرابكاران اينترنتي صفحات موقتي در اينترنت ايجاد مي كنند كه تنها كاربرد آن ها، كلاهبرداري از كاربران اينترنت است.

جرائم سایبری و رایانه در ایران

جرم رایانه ای شامل جرایمی است که با استفاده از رایانه درون فضای سایبر و علیه رایانه دیگر واقع می شوند. هرچه وابستگی انسان به رایانه بیشتر می شود زمینه توسعه جرائم رایانه ای نیز آماده تر می گردد .

- پول الکترونیک سرقت الکترونیک

مسئله اصلی در جرائم سایبر این است که اگر داده ها و اطلاعات دارایی و ثروت تلقی شود پس سرقت یا آسیب به آن نیز جرم تلقی می شود. از طرف دیگر جرم سایبر یک مسئله اجتماعی اغلب عاری از خشونت و بیشتر دارای ماهیت اقتصادی است. این جرم به اصطلاح تمیز مستلزم مهارت رایانه ای و برنامه ریزی دقیق است .

- مجرمان سایبر

مجرمان سایبر معمولا مرد، جوان، دارای تحصیلات لیسانس، کارمند سابق یا فعلی شرکت های رایانه ای، دارای وقت آزاد فراوان هستند و زمان غیر متعارفی را برای اتصال به شبکه صرف می کنند. پیشرفت فناوری، نیروی جوان تحصیل کرده، بیکاری تحصیل کردگان، بی ثباتی سیاسی و اقتصادی، فقدان قوانین و وجود خریداران ثروتمند برای خدمات مجرمان سایبری زمینه های اجتماعی گسترش جرایم سایبری را تشکیل می دهد .

- **نمونه هایی از جرائم سایبر**

۱)سرقت
- سرقت خط تماس تلفنی
- سرقت اطلاعات
- سرقت نرم افزار
- سرقت مشخصات تاشخصی ترین لایه ها

۲)تقلب
- تقلب مالیاتی
- پولشویی
- ناخنک زدن به حسابهای دیگران
- تقلب در بیمه نامه

۳)تروریسم سایبر
- نفوذ در زیر ساختهای ملی و تلاش برای کنترل آن مانند :
- تاسیسات دفاعی
- تاسیسات ارتباطات راه دور
- تاسیسات شرکت های برق
- تاسیسات تولید، ذخیره سازی و حمل و نقل انرژی

- سیستمهای بانکداری و مالی
- تاسیسات حمل و نقل زمینی، هوایی و دریایی
- تاسیسات تامین آب
- خدمات اورژانس
- خدمات دولتی

۴ (ویروسها

- اسبهای تروا
- خرگوش ها
- کرمها
- بمب های منطقی
- هیولای کلوچه

۵ (جرائم جنسی

- هرزه نگاری سایبر: انتشار متون/ تصاویر/ فیلمها و نقاشی های مستهجن
- دلالی فحشا
- دسترسی کودکان و نوجوانان به هرزه نگاری سایبر
- هرزه نگاری کودکان و نوجوانان نوجوانان
- مزاحمت جنسی سایبر
- فریب کودکان و نوجوانان از طریق ارتباط رایانه ای
- فریب دختران و زنان

۶ (مزاحمت

- از طریق انتشار اطلاعات غلط
- افشاگری در مورد اطلاعات و تصاویر شخصی
- تهدید به آزار جنسی

وضعیت محیط سایبر در ایران

مجلس آمادگي تصويب قوانين بازدارنده جرايم سايبري را دارد

مرکز پژوهش‌های مجلس شورای اسلامی یکی از مهم‌ترین نیازمندی‌های تقنینی فضای تبادل اطلاعات (فضای سایبر) را قانون جرایم رایانه‌ای ذکر کرده و افزود: دامنه‌ی کاربری فناوری اطلاعات و نقشی که در تمام عرصه‌های زندگی بشری می‌گذارد، بی‌همتاست و از همین رو از يك سو شاهد ورود این فناوری به عرصه‌های جدید و توسعه‌ی کاربردها و خدمات الکترونیکی و از سوی دیگر با معضلات و اعمال قابل سرزنش کاربران مواجه هستیم که به دلیل عدم وجود تدابیر کیفری و غیر کیفری متناسب تعداد و نوع سوءاستفاده‌ها رو به افزایش است. ضمن این‌که در سال‌های اخیر رویکرد دیگری نیز در دستور کار قرار گرفته نظیر استفاده از مضامین کیفری مشابه و اصلاحات قانونی به صورت بخشی که این رویه به دلیل فقدان آیین دادرسی خاص جرایم رایانه‌ای و عدم جرم‌انگاری عناوین مجرمانه جدید روند بررسی پرونده‌های سوء استفاده را با مشکلات جدی مواجه می‌کند، که در این میان تصویب قانون جرایم رایانه‌ای با اصلاحاتی که باید به دلیل گذشت چهار سال از زمان ارایه و تغییرات بسیاری که در عرصه‌ی فناوری جرایم فناوری اطلاعات و دامنه‌ی کاربری اتفاق افتاده در آن اعمال شود و نیز عدم تصویب قوانین

بخشی، بهترین راهکار قانونی برای اعمال حاکمیت نظام جمهوری اسلامی ایران در جهت سالم‌سازی فضای سایبر است.

پیوست مقاله

زبان هکری

گاهی هکرها در هنگام نوشتن به جای تعدادی از حروف انگلیسی معادل‌های قراردادی‌به کار می‌روند که لیست آنها را در زیر می‌بینید:

0 <= O
1 <= L; I
2 <= Z
3 <= E
4 <= A
5 <= S
6 <= G
7 <= T
8 <= B
| <= L; I
@ <= at (duh)
$ <= S
)(<= H
}{ <= H
/\/ <= N
\/\/ <= W
/\/\ <= M
|> <= P; D
|< <= K
ph <= f
z <= s

مثال

/\/\0}{4/\/\/\/\4|> R324 $0|74/\/| = محمد رضا سلطانی
}{3 $|>34|< z <= he speak

نتیجه گیری:

هکرها و افراد سودجو همیشه در کمین ما هستند باید با اطلاع از وضعیت امنیت فضای اینترنتی و سایبری اقدام به استفاده از اینترنت کنیم.

از آخرین نسخه های بروز نرم افزارها استفاده کنیم.

از یا آنتی ویروس بروز و فایروال مناسب بهره ببریم.

مراقب رفتار خود در اینترنت به خصوص فضای گفتگو (چت) باشیم. وبه کسی اعتماد نکنیم.

به هر سایتی بدون شناخت قبلی وارد نشویم چرا که به محض ورود به آن سایت ممکن است کدهای مخربی وارد سیستم شما بشود.و در موقعیت مناسب اطلاعات شما را انقال دهد.

از پسوردهای مناسب استفاده کنیم.

حدالامکان از کافی نت ها استفاده نکنیم.

از اطلاعات مهم خود در سیستم BACK UP بگیریم و از هارد آن را پاک کنیم دقت داشته باشید حتی با پاک کردن عکسها و فیلمها از هارد باز هم هکرها قادر به بازیابی آنها هستند.

هر برنامه ای را در کامپیوتر خود نصب نکنیم چرا که ممکن است داخل آنها کدهای مخرب وجود داشته باشد.

حرف آخر :

از همه دوستان و اساتیدی که من را در تهیه این مقاله یاری کردند تشکر میکنم.

از آنجایی که علم بشر خالی از نقص نیست از همراهان عزیز میخواهم اشتباهات و یا انتقادات خود را در میان بگذارند. **yahooID: shayan881 Email: mr.soltany66@gmail.com**

انسانها به ۱۰ گروه تقسیم می شوند. آنهایی که باینری می فهمند و آنهایی که نمی فهمند

منابع:

آموزش قدم به قدم هک , آزار صمدی

هک , نیما الولن فروش , 1385

مباحثی پیرامون هونی پوت ها , نویسنده استانیک سولفول , 2007

ماهنامه شبکه - خرداد ۱۳۸۶ شماره 76 بهروز نوعي پور

Panda Security بخش تحقیقات و پژوهش امنیت اطلاعات در شرکت ترجمه: اسماعیل ذبیحي

خـبرگزاري مجلس شوراي اسـلامي http://news.parliran.ir/News

آژانس خبری پرشین هک http://www.persianhack.com

راههای مقابله با هک WWW.AFTAB.IR

و سایتهای :

http://madreseha.com

www.webgostarco.com/pages/Learning/Hack

hackcity.blogfa.com

danesh.bizhat.com/Computer/HackNetwork

www.dothack.com

www.pnu4u.tk

hackaday.com

hacker.blogfa.com

http://www.atcce.com

www.abc.net.au/triplej/hack

..: M R S :.. Email: mr.soltany@yahoo.com