هک چیست و هکر کیست و چگونه میشود هک کرد؟

حالا که فرق یک هکر و کناکر رو میدونین پس مطمئن باشین مطالبي که در اینجا خواهید خواند ذهن شما رو در بسیاري از مسائل روشن خواهد کرد.

بمب های میل :

بمبهاي میل سریالي از میلها رو به طرف میل سرور شما سرازیر میکنند. صحبت از ۱۰ یا ۲۰ ایمیل نیست صحبت از هزاران هزار ایمیلي است که در ظرف چند دقیقه در میل سرور شما لنگر انداخته و کارهاي شما رو مختل میکنند.و از همه مهمتر به خاطر مدت زمان طولاني که براي داون لود شدن و پاک شدن احتیاج دارند سرعت شبکه رو به طرز عجیبي پایین مي آورند. کاربران شبکه اي که مورد حمله این قبیل بمبها قرار میگیرند موظف هستند روتین و طرز عملکرد آنها را شناسایي کنند. مسلما این کار از حمله بعدي جلوگیري نخواهد کرد ولي از حمله ناآگاهانه اعضاي شبکه به بقیه جلوگیري خواهد کرد. بله این وظیفه یک مدیر شبکه است . ولي چطور میشه فهمید که یک بمب ایمیل چطور کار میکند؟

امیدوارم که در اینجا به حرف من رسیده باشین که زبده ترین و با اعتمادترین و کارکشته ترین مدیران شبکه هکرها هستند.

معروفترین بمبهاي ایمیل و داده هاي مربوط به آن :

UPYOURS3.ZIP,UPYOURS3.EXE,MAILCHEK.EXE,UPYOURSX Yours Up

KABOOM.ZIP,KABOOM3.EXE,KABOOM3!.ZIP,WSERR.DLL Kaboom

Unabomber UNA.EXE,KWANTAM.NFO The

Email Bomber BOMB.EXE,BOMB.TXT,BOMB02B.ZIP The Windows

Gatemail GATEMAIL.C

Mail-Bomber MAILBOMB.C Unix

یک راه براي کمتر کردن (نه جلوگیري کردن) این حمله ها این خواهد بود که یک اسکریپت برنامه نویسي کنید که در ازاي هر میلي که دریافت میکنید یک اخطار ۱۰ صفحه اي براي فرستنده بفرستد. ممکن است که پرووایدر ایمیل سرور او متوجه این کار شده و اقدام به جلوگیري از این کار کند .

چیست؟ Service – Denial – of حمله

عملکردي بسیار شبیه به بمبهاي ایمیل دارد DoS این حمله با علامت اختصاري

ولي با این تفاوت که خطرناکتر و مخربتر هستند مخصوصا وقتي شما یک شبکه بیزینسي رو دارا هستیند و یا یک پرووایدر اینترنت رو مدیریت میکنید این حمله ها میتوانند خسارات جبران ناپذیري رو به باربیاورند. مثلا خواهند توانست در ظرف مدت کوتاهي کل شبکه شما رو فلج کنند. اولین اینها که قشنگ و تر و تمیز کار میکرد موریس نام داشت. موریس در زمان خود حدود ۵۰۰۰۰ کامپیوتر رو در ظرف چندساعت خراب میکرد. در اون زمان یعن سال ۱۹۸۸ این رقم سرسام آوري بود . امروزه امثال موریس میلیونها کامپیوتر رو در عرض چند

ساعت خراب خواهند کرد.

هدف همه حمله هاي

Denial – of – Service

يک چيز است: قطع ارتباط کامپيوتر از شبکه. اين نوع حمله در طبقه حمله هاي باهوش قرار دارد دليل: دي او اس نميتواند روي همه پلات فورمها و سيستمها کار کند ولي به محض اينکه فهميد روي سيستمي نميتواند کار کند خود را مخفي کرده و شروع به تکميل و تطبيق خود با سيستم مورد نظر ميکند و بعد از اينکه از کارآرايي خود مطمئن شد شروع به کار ميکند. به جرات ميتوان گفت که هر دو هفته يک بار نوع جديدي از دي او اس در دنياي کامپيوتر عرضه ميشود. کاربراني که براي رد يابي کردن طرز عملکرد دي او اس مخصوصا دي او اس را در شبکه خود راه اندازي ميکنند ميدانند که با چه چيز مخربي روبرو هستند.

علت اصلي خطرناک بودن دي او اس اين است که با اينکه دي او اس سيستم و عملکرد بسيار پيچيده اي دارد ولي اشخاصي که حتي تجربه کمي از کامپيوتر دارند نيز ميتوانند به راحتي با آن کار کنند.

من فرض رو براين ميگيرم که شما الان يک دي او اس روي هارد ديسک داريد! و ميخواهيد عملکرد دي او اس را تجربه کنيد! و سوالاتي در اين زمينه داريد! مثلا:

Dataname

اينجا بايد اسمي را وارد کنيد که حمله شما با اون اسم صورت ميگيره. اين رو هميشه در نظر داشته باشين که اين اسم فقط در ۱ يا ۲ حمله اول استفاده خواهد شد و در حمله هاي بعدي عوض خواهد شد (اين اسم را فايل اصلي برنامه نيز دارا ميباشد.)

Autor

اينجا معمولا يک آدرس ايمل بعضي مواقع هم يک اسم داده ميشود. اگر دوست داريد يک شبه معروف شويد اسم و آدرس خودتون رو بدين. البته اگر اين کار رو بکنيد يک شبه معروف خواهيد شد ولي فقط همون يک شب معروف خواهيد ماند.

URL

در اينجا شما ميتوانيد سورس دي او اس را داون لود کنيد و اقدام به عوض کردن آن بکنيد ولي اين آدرس بستگي به تاريخ دي او اسي که شما داريد دارد چون مطمئنن سورس دي او اس روي اينترنت و روي يک آدرس وب مدت زمان زيادي آنلاين نخواهد ماند.

System

اينجا نشان داده خواهد شد که دي او اس با چه پلات فورمي نوشته شده و تحت چه سيستمي کار ميکند

معروفترين دي او اس ها :

Bionk Bonk and

است . bonk.c اسم فايلي كه اين دي او اس رو دارد

معرفي كرده. ROOTSHEL.COM نويسنده خودش رو تحت

اين دي او اس به خاطر علاقه شديد به ويندوز ان تي و ويندوز ۹۵ اينها را در عرض چند ثانيه از كار خواهد انداخت.

Hanson

استhanson.c اسم فايل

myn@efinet نويسنده :

اين دي او اس با لينوكس نوشته شده و كار اصلي آن اين است كه ام آي ار سي سايلنت را از شبكه بيرون ميانداز.

بقيه معروفترين دي او اس ها را با اسامي فايلهادر زير مشاهده ميكنيد:

Inetinfo.exe inetfo – inetfo.c – inetfo.pl
Jolt.c Jolt
Land Land.c
Newtear Newtear.c
Pong Pong.c
Real Audio pnserver.c
land.c Solaris Land solaris_land.c
Teartop teartop.c
Der Pentium-bug Pentium_bug.c

Phreaken چيست؟

معني دقيق كلمه Phreaken را ميشود در يک جمله خلاصه كرد : رجيستر شدن و استفاده كردن از Paysiteها با اطلاعات غلط. يا به طور مستقيم : استفاده كردن مجاني از همه چيز!

مسلما انجام دادن همچين كاري ممنوع است ولي اطلاعات زير به وب مسترها (هم) كمک خواهد كردكه چگونه جلوي همچين كارهايي را بگيرند.!

در اينجا ما مستقيم سراغ بهترين روش استفاده ار همچين سايتهايي ميرويم:

استفاده كردن با كارتهاي اعتباري! :

در همچين مواردي كاربر به صورت آنلاين شماره و مشخصات كارت اعتباري را وارد ميكند و سپس كد و رمز هاي مربوطه را براي استفاده

کردن از سایت در یافت میکند.

هکرهاي کارکشته در اینگونه موارد از پاکتهاي گمنام اینترنتي استفاده میکنند که در راس همه بسته (تست اینترنت با AOL) قرار دارد که در اکثر مجله هاي کامپیوتر در اروپا به طور رایگان عرضه میشود. در این بسته شرکت AOL ۲ ماه استفاده مجاني از اینتر نت را عرضه میکند .

تنها کاري که باید بکنیم:

وارد کردن اسم و مشخصات خیالي

وارد کردن اسم یکي از بانکهاي معروف اروپا

وارد کردن یک عدد دلخواه ضربدر ۴ به عنوان شماره حساب!

و دقیقا ۲ ثانیه بعد استفاده رایگان به مدت ۲ ماه از اینترنت.

مشکلي که در این موارد ممکن است پیش آید تست صحت وجود داشتن شماره حساب به وسیله AOL است. که پیدا کردن یک شماره حساب بانک در اینترنت و یا در روزنامه نباید مشکلي براي ما ایجاد کند.

در اینجا باید بغیر از AOL یادي هم ازشرکت OKEY.NET کنیم که امکانات فوق را دارد!

مشکل بعدي انتخاب Paysite و بدست آوردن شماره کارت اعتباري است. که اینکار کمي مشکل تر ولي مسلما غیر ممکن نخواهد بود.

معمولترین روش بدست آوردن آن استفاده از Credit Card-Generatorها است. مانند : Credit Wizrd و یا Cardpro و یا Creditmaster

مثالي تصویري از یک Credit Card-Generator

http://www.elte.hu/~kincses/konf/almere/ccard1.jpg

شاید که با رفتن به سایت http://www.metacrawler.com/ و جستجو کردن عبارت: Credit Card-Generator بتوانید به این برنامه ها دسترسي پیدا کنید.

چیزي که باید دانست: هیچ وقت نمیشود آلاین امتحان کرد که آیا همچین شماره کارتي وجود خارجي دارد یا به چه کسي تعلق دارد. بنابراین شماره اي که از Credit Card-Generatorها میگیریم را به راحتي استفاده میکنیم ولي Credit Card-Generatorها تاریخ اعتبار کارت را نمیگویند براي بدست آوردن آن چه باید کرد؟

در اکثر برنامه هاي Credit Card-Generator از یک شماره کارت اعتباري واقعي شماره هاي شبیه سازي شده بدست مي آید. این کار در اینترنت تحت اصطلاح Extrapolation شناخته میشود.شماره هاي جعلي اکثرا در رقمهاي آخري با شماره اصلي و معتبر کارت فرق دارند.

شاید تعجب کنید اگر بشنوید : وقتي مثلا شماره کارت اعتباري خود را به Credit Card-Generatorها میدهید و یک شماره جعلي از آن Extrapolation میکنید میتوانید از تاریخ اعتبار کارت خود استفاده کنید! این کار ۹۹% با موفقیت همراه است.

واقعا هم هیچ جاي ترسي نیست که کسي ردپاي شما را دنبال کند چون کساني که با بسته هاي گمنام AOL و ...در اینترنت هستند با بالاترین درصد گمنام بودن از اینترنت استفاده میکنند.

براي اطمینان بیشتر از گمنام ماندن میتوانید سري به www.anonymizer.com بزنید شاید در آنجا بتوانید مثلا تولزي پیدا کنید که آدرس آي پي شما را مخفي کند یا غیر قابل تعقیب!!

ولي توجه داشته باشيد : اگر از يكي از روشهاي بالا استفاده نمي كنيد دست به همچين كاري نزنيد چون در غير اين صورت مدير سايتي كه شما در آن از شماره جعلي كارت اعتباري وارد ميكنيد آدرس آي پي شما را كه در سرور سايت پروتكل ميشود بدست آورده . و يک تماس با پرووايدر اينترت شما و دادن آدرس آي پي شما به پرووايدر كافي است تا پرووايدر با يک گزارش .i.d.R به پليس و اثبات اينكه شما با اين آدرس آي پي آنلاين بوديد شما را به جرم جعل كارت اعتباري روانه زندان كند.

محمد سيستم

E-Mail : mohammad4763@yahoo.com