به نام خدا

اسماعیل زارع

معرفی ۴ نوع حمله به پسوردها در هک : چگونه رمز عبور هک می شود؟

معرفی انواع حملات به پسورها یا رمز عبور ، کرک کردن پسوردها یکی از دشوارترین روش های پیدا کردن پسورد سیستم ها و ورود به آنها است. پسورد کرکینگ برای پیدا کردن پسوردهای فراموش شده کاربران نیز مورد استفاده قرار می گیرد اما اگر بصورت غیرمجاز استفاد شود می تواند دسترسی های غیرمجاز بسیار خطرناکی را در سطح شبکه و سیستم های شما ایجاد کند. حملات هکری که بر روی پسوردهای شما انجام می شوند بر اساس روشی که هکر برای کرک کردن پسورد شما مورد استفاده قرار می دهد طبقه بندی می شوند که معمولا به شکل های زیر طبقه بندی می شوند:

روش ۱ : حملات آنلاین غیرفعال(Passive Online Attacks)

هرگاه صحبت از حملات Passive یا غیرفعال شود به این معناست که هیچوقت هیچ تاثیری کارهایی که هکر انجام می دهد بر روی سیستم واقعی نخواهد داشت و حملات در جای دیگری انجام می شوند. این نوع حمله در واقع بیشتر در بحث مانیتور کردن و ثبت و ضبط کردن داده ها مورد استفاده قرار می گیرد. در چنین حملاتی مهاجم صرفا داده هایی که از مسیر عبور می کنند را شنود می کند یا از میان لینک ارتباطی خودش عبور می دهد و ضبط می کند ، در واقع در این میان حمله ای انجام نمی شود بلکه داده های مورد نیاز برای انجام یک حمله جمع آوری می شود.

بصورت کلی سه نوع حمله آنلاین غیرفعال یا Passive Online Attack داریم که شنود کردن یا Sniffing در وایرلس یا شبکه های کابلی ، حمله MITM یا Man In The Middle و حله Replay از جمله این نوع حملات هستند. این نوع حملات با توجه به اینکه در مسیر واقعی ارتباط انجام می شوند و فعال هستند Online هستند اما با توجه به اینکه هیچ تغییری در اطلاعات عبوری از مسیر نمی دهند به عنوان Passive شناخته می شوند طبیعی است که اگر در میان مسیر تغییری در پسوردها یا داده ها انجام شود دیگر حمله Passive محسوب نمی شود. توجه کنید که در چنین نوع حمله ای شما هیچوقت بصورت مستقیم به سیستم هدف متصل نمی شوید.

روش ۲ : حملات آنلاین فعال(Active Online Attacks)

در این نوع حمله به پسوردها که از نظر بسیاری از هکرها ساده ترین روش حمله به پسوردها می باشد شما می توانید دسترسی در سطح مدیریتی به سیستم مقصد به دست بیاورید ، این نوع حملات معمولا به چهار نوع طبقه بندی می شوند که از آن جمله می تواند به حدس زدن پسوردها اشاره کرد که شما مستقیما به جاییکه پسوردها وارد می شود متصل شده و پسوردها را مرتب تست می کنید تا احتمالا یکی از آنها پسورد واقعی باشد ، روش دوم استفاده از بدافزارهای ویژه جمع آوری و ارسال پسورد است که بصورت خلاصه Trojan ها ، جاسوس افزارها یا Spyware ها و همچنین Keylogger ها از جمله این نوع حملات هستند ، البته حملاتی مثل Hash Injection و Phishing که بعضا در طبقه بندی های سایر حملات مانند مهندسی اجتماعی هم قرار می گیرند در این دسته بندی قرار می گیرند.

روش ۳ : حملات آفلاین به پسوردها(Offline Password Attacks)

زمانیکه صحبت از حملات آفلاین می شود یعنی ما هیچگونه ارتباطی برای کرک کردن پسورد با سیستم هدف نداریم. در چنین مواقتی بررسی صحت و کرک پسوردها از طریق سیستمی که در اختیار هکر است انجام می شود. در چنین حملاتی همیشه هکر از نحوه ذخیره سازی پسوردها در قالب پایگاه داده یا فایل خاص بر روی سیستم هدف خبر دارد و می داند که از کجا می تواند فایل رمزنگاری شده یا مقدار Hash پسورد را مشاهده و ثبت کند.

سپس آن فایل یا محتویات Hash بدست آمده را کرک می کند و به پسورد اصلی دست پیدا کرده و به سیستم هدف حمله می کند. حملات آفلاین همانطور که بصورت مختصر قبلا هم اشاره کردیم بعضا بسیار زمانبر هستند ، اگر از الگوریتم های ضعیف رمزنگاری مثل LM استفاده کنید احتمال Offline کرک شدن پسورد شما با توجه به ضعف الگوریتم بسیار بالاتر است. تکنیک های بسیار زیادی برای کرک کردن پسوردها در اینترنت وجود دارد که قبلا هم در خصوص آنها بصورت مفصل در ITPRO توضیح داده ایم اما بصورت کلی برای جلوگیری از حملات Offline Cracking می توانید موارد زیر را برای امنیت بیشتر انجام بدهید:

۱. از پسوردهای قوی استفاده کنید
۲. از LM Hash برای نگهداری پسورد استفاده نکنید

توجه کنید که بصورت کلی سه نوع حمله به پسورد بصورت آفلاین وجود دارد که استفاده کردن از پایگاه داده های Hash های از قبل Crack شده ، استفاده از شبکه های توزیع شده محاسباتی برای کرک پسورد ها و همچنین استفاده از Rainbow Table از انواع این روش ها می باشند. قویترین روش مقابله با هر نوع کرک پسورد استفاده از پسوردهای بسیار قوی و دارای استانداردهای لازم است.

روش ۴ : حملات غیر الکترونیکی به پسوردها(Non-Electronic Attacks)

اما آخرین نوع از حملات به پسوردها تقریبا هیچ ارتباطی به کامپیوتر ندارد و روشی کاملا غیر الکترونیک است ، این نوع حملات را حملات غیرفنی هم نامگذاری می کنند. شما به عنوان یک هکر در چنین حملاتی اصلا نیازی به داشتن دانش فنی در خصوص نفوذ به سیستم یا کرک کردن پسورد ندارید و به همین دلیل هم این نوع حملات غیرفنی محسوب می شوند.بصورت کلی سه نوع از اینگونه حملات وجود دارد که اولین آنها به عنوان Shoulder Surfing شناخته می شود که بعضا حداقل یکبار شما این نوع حمله را تجربه کرده اید!

در چنین حملاتی مهاجم زمانیکه شما می خواهید پسورد خودتان را وارد کنید کنار شما می ایستد یا پشت شما می ایستد و به مواردی که شما وارد می کنید نگاه می کند. نوع دوم مهندسی اجتماعی یا Social Engineering است که برای خودش کتابها مطلب و محتوا دارد و استفاده از روش های روانشناسی برای حمله و گول زدن هدف حمله محسوب می شود. آخرین نوع هم Dumpster Divingاست یا زباله گردی !! این نوع حملات یعنی مهاجم سطل های زباله و جاهایی که ممکن است شما یا هدف حمله کاغذهای اسناد بلااستفاده خودتان را به زباله می اندازید را جستجو می کند و اطلاعات بعضا بسیار جالبی برای حمله پیدا می کند که بسیار هم در عین سادگی حمله موفقی است.