نام مقاله: آشنایی با پایگاه داده ای SAM
سطح مقاله: متوسط
کاربران: دانشجویان کامپیوتر و مدیران امنیتی

سلام دوستان ، در این درس راجع به پایگاه داده SAM که یکی از اصلی ترین ارکان ویندوز NT است صحبت می کنیم. برای اینکه با پایگاه Sam به خوبی آشنا شویم باید یک مقدار با معماری ویندوز NT آشنا باشیم. معماری ویندوز 2000 به دو حالت تقسیم می شود: 1- حالت کاربری (User Mode) 2- حالت هسته (Kernel Mode)
در حالت کاربری همانطور که از اسم آن مشخص است فعالیت های کاربران و ارتباطات آنها با ویندوز 2000 را پشتیبانی می کند که آنها هم به زیرمجموعه هایی تقسیم می شود که به آنها هم زیر سیستم یا Sub سیستم می گویند. یکی از این زیر سیستم ها که نقش حساسی در امنیت ویندوز 2000 دارد، زیر سیستم Security است که به LSA (Local Security Authority) نیز معروف است و تعیین می کند که آیا تلاش های Login معتبر است یا خیر. وقتی که یک کاربر Username و کلمه عبورش را در سیستم وارد می کند، زیر سیستم Security این اطلاعات را به یک سیستم بنام مدیر Account های امنیتی یا همان SAM (Security Accounts Manager) می فرستد. Sam یک پایگاه داده اعتبار سنجی دارد که به آن پایگاه داده Sam می گویند و معمولاً برای هر Account کاربری در پایگاه داده Sam دو قسمت رمز ورود وجود دارد. یکی که نمایش LM رمز ورود نامیده می شود شامل نمایش رمز ورود کاربر برای اهداف سازگاری با محصولات قدیمی تر یا با پیچیدگی کمتر مایکروسافت مثل LanMan که LM از آن گرفته شده است یا Windows for Workgroups می باشد که به این قسمت LM می گویند و قسمت دوم در پایگاه داده Sam، NT Hash یا درهم سازی NT نامیده می شود و رمز ورود درهم شده مورد استفاده برای سازگاری با سیستم های ویندوز NT / 2000 را در خود دارد. بنابراین به طور پیش فرض پایگاه داده Sam شامل دو نمایش از هر رمز ورود است. نمایش LM و NT Hash و همچنین اطلاعات دیگری هم می تواند در این فایل قرار بگیرد که اختیاری است.
نمایش LM و NT Hash از رمز ورود برای هر Account در ویندوز NT به دو روش متفاوت به دست می آیند. در ویندوز NT حداکثر طول رمز ورود 14 کاراکتر است. البته کاربر می تواند بیش از 14 کاراکتر وارد کند ولی سیستم فقط 14 کاراکتر ابتدایی را می گیرد. نمایش LM با تنظیم طول رمز ورود به دقیقاً 14 کاراکتر با حذف کاراکترهای اضافی و یا با اضافه کردن کاراکتر جای خالی (Blank) به دست می آید و رشته به دست آمده به دو قسمت مساوی تقسیم می شود. یک کاراکتر توازن مورد نیاز برای رمزنگاری داده ها DES (Data Encryption Standard) به هر قسمت اضافه می شود و در هر قسمت از یک عدد شانزدهی به عنوان کلیدی برای رمزنگاری DES مورد استفاده قرار می گیرد. در کل نمایش LM بسیار ضعیف است. تقسیم رشته به دو قسمت 7 کاراکتری برای به دست آوردن نمایش LM به مهاجمان و هکرها امکان می دهد تا قسمت های رمز ورود را مستقل از هم حدس بزنند و این امر کار حدس زدن رمز ورود را ساده تر می کند و در کل زمان عمل Crack پسورد توسط هکر را کاهش می دهد. اما قسمت NT Hash یا درهم سازی NT بسیار قوی تر است ولی شکست ناپذیر نیست. در این حالت طول رمز ورود دقیقاً 14 کاراکتر تنظیم می شود سپس الگوریتم های درهم سازی MD-4 (Message Digest 4) سه بار اعمال می شود تا رمز ورود درهم شده به دست آید. توجه داشته باشید که نمایش LM نه یک رمز ورود درهم شده است و نه یک رمز ورود به رمز درآمده، بلکه چیزی جز یک عدد به رمز درآمده و ثابت هگزا نیست که در آن رمز ورود به عنوان یک کلید مورد استفاده قرار گرفته است ولی نمایش NT یک رمز ورود درهم شده است زیرا برای به دست آوردن آن از یک الگوریتم درهم سازی استفاده شده است. اما حالت NT Hash هم یک نقص بزرگ دارد و آنهم این است که برای همه Account ها از یک الگوریتم درهم سازی رمز استفاده می شود که اصطلاحاً می گویند پسوردها Salted نیست. Salting یعنی از بین الگوریتم های مختلف رمز نگاری یکی بر حسب تصادف انتخاب بشود که این عمل کار پیدا کردن الگوریتم مورد استفاده در پسورد را خیلی سخت می کند و

این روش در سیستمهای مبتنی بر Unix استفاده می شود و سیستم های یونیکس از Salt استفاده می کنند تا عمل شکستن رمز ورود از طریق یک ابزار مبتنی بر فرهنگ لغات را بسیار سخت تر کنند. از آنجا که پسوردهای ویندوز NT، Salted نیستند شکنندگان فرهنگ لغتی رمز ورود تنها باید یک رمزنگاری یا درهم سازی را برای هر رمز ورود کاندید و امتحان کنند و این امر روند شکستن رمز ورود را به میزان قابل توجهی تسریع می کند.
در دنیای هکرها حمله به پسوردها و کلمات عبور خیلی معمول و رایج است، هکرها اغلب سعی می کنند تا کلمات عبور پیش فرض سیستم ها را برای دسترسی از طریق دستی و یا با استفاده از اسکریپت ها حدس بزنند. Password Cracking عبارت است از دریافت کلمات عبور رمزنگاری شده و درهم شده از یک سیستم و استفاده از ابزارهای اتوماتیک برای تعیین کلمه عبور اولیه. ابزارهای Crack یا شکستن کلمه عبور، یک کلمه عبور اتفاقی را ایجاد کرده و آن را کدگذاری/درهم سازی می کنند و بعد نتیجه را با کلمه عبور رمز شده/درهم یافته مقایسه می نمایند. کلمه عبور اتفاقی (حدس زده شده) می تواند از طریق یک دیکشنری، روش Brute Force و یا تکنیک دورگه به دست آید. یکی از بهترین ابزارهای Crack و شکستن کلمات عبور و پسوردها در ویندوز NT - 2000 - XPبرنامه L0pht Crack نام دارد که در دنیای هکرها به LC معروف است که هم اکنون نسخه 5 آن در دسترس مدیران شبکه ها و هکرها قرار گرفته است و برای شکستن پسوردهای سیستم های یونیکس نیز برنامه John The Ripper برنامه معروف و سودمندی است که این کار را به راحتی و با قدرت انجام می دهد که در درس های آینده راجع به این ابزارها و طرز کار آنها مفصل توضیح خواهم داد.
موفق و پیروز باشید .

نویسنده مقاله : بهروز کمالیان