هانیه اسدی

مرکز آپا دانشگاه کردستان

دفترچه تقلب
لاگ‌های امنیتی ویندوز

SIRT

مقدمه

لاگ فایل ویندوز (Event Logs) در واقع فایل‌هایی هستند که همه رخدادها و اتفاقات سیستم در آن‌ها ثبت می‌گردد، برای نمونه خاموش و روشن‌کردن سیستم، توقف و استارت‌کردن سرویس‌ها، نصب برنامه‌های کاربردی، تغییر سیاست‌های امنیتی سیستم، تلاش‌های موفق و ناموفق ورود به سیستم، تلاش برای حذف یا تغییر فایل‌های مهم و سایر رویدادهای مهم را می‌توان اشاره کرد. هر رویداد شامل اطلاعات بسیار مهمی است که جزئیات مورد نیاز برای عیب‌یابی و رفع مشکل را در اختیار ما قرار می‌دهد. بدون مطالعه دقیق لاگ‌ها علت بروز بسیاری از اشکالات مشخص نخواهد شد.

لاگ‌های امنیتی ویندوز (Security Logs) چگونه به جلوگیری از هک و سرقت اطلاعات کمک می‌کند؟

امروزه موضوع امنیت یکی از مهم‌ترین نگرانی همه سازمان‌ها و شرکت‌ها شده است. رخدادهایی مانند نفوذ، هک و سرقت اطلاعات روزبه‌روز در حال افزایش است و سبب شده است تا مدیران فناوری اطلاعات و راهبران شبکه با چالش‌هایی جدی در خصوص ایمن‌سازی زیرساخت‌ها و سرورها روبرو شوند. مطالعات مختلف نشان داده است درصد قابل توجهی از موارد سرقت اطلاعات در سازمان‌ها در نتیجه تلاش‌های غیرقانونی و مکرر ورود به سیستم صورت پذیرفته است. بنابراین نظارت بر تلاش‌های ناموفق ورود به سیستم موجب کاهش ریسک نفوذ و سرقت اطلاعات خواهد شد. دسترسی غیرمجاز و مشکوک به سیستم و فایل‌ها، پایگاه‌های داده و برنامه‌های کاربردی، موضوعی است که بدون مانیتورینگ دائمی لاگ‌های ویندوز امکان آگاهی از آن‌ها وجود ندارد.

در ادامه دفترچه تقلب برای دسترسی سریع‌تر به لاگ‌های امنیتی در ویندوز نشان داده خواهد شد.

رویدادهای مربوط به احراز هویت کنترل کننده دامنه		
٤٧٦٨	تیکت احراز هویت Kerberos (TGT) درخواست شد.	
٤٧٧١	احراز هویت اولیه Kerberos ناموفق بود.	دیدن کدهای ناموفق Kerberos
٤٨٢٠	Kerberos TGT رد شد زیرا دستگاه محدودیت‌های کنترل دسترسی را برآورده نمی‌کند.	

تغییرات حساب کاربری			
٤٧٢٠	ساخته شده	٤٧٢٢	فعال شده
٤٧٢٣	کاربر رمز عبور خود را تغییر داد.		
٤٧٢٤	کاربر ممتاز رمز عبور این کاربر را تغییر داد.		
٤٧٢٥	غیر فعال شده	٤٧٢٦	حذف شده
٤٧٣٨	تغییرداده شده	٤٧٤٠	قفل شده
٤٧٦٧	باز شده	٤٧٨١	تغییر نام

رویدادهای Logon Session		
٤٦٢٤	ورود موفق	فعال شده
٤٦٤٧	خروج از سیستم توسط کاربر	
٤٦٢٥	خطای ورود	
٤٧٧٨	جلسه Remote desktop دوباره برقرار شد.	
٤٧٧٩	جلسه Remote desktop دوباره قطع شد.	
٤٨٠٠	ایستگاه کاری قفل شده است.	
٤٨٠١	ایستگاه کاری باز شده است.	
٤٨٠٢	Screen Saver فراخوانی شد.	
٤٨٠٣	Screen Saver رد شد.	

انواع Logon	
٢	محاوره‌ای
٣	شبکه (مثال: mapped drive)
٤	Batch (مثال: schedule task)
٥	سرویس (Startup سرویس)
٧	Unlock
٨	Network Cleartext (اغلب یک ورود به IIS را با «basic authentication» نشان می دهد.)
١٠	Remote Desktop
١١	ورود با اطلاعات احراز هویت کش شده

کدهای خطای Logon	
0xC0000064	نام کاربری وجود ندارد.
0xC000006A	نام کاربری صحیح است اما رمزعبور اشتباه است.
0xC0000234	کاربر در حال حاضر قفل شده است.
0xC0000072	حساب کاربر در حال حاضر غیرفعال است.
0xC000006F	کاربر سعی کرد خارج از محدودیت‌های روز هفته یا ساعات روز خود وارد سیستم شود.
0xC0000070	محدودیت‌های ایستگاه کاری
0xC00000193	انقضای حساب کاربری
0xC0000071	رمز عبور منقضی شده
0xC0000133	ساعت‌های بین DC و سیستم‌های دیگر خیلی از همگام‌سازی فاصله گرفته است.
0xC0000224	کاربر باید در ورود بعدی رمزعبور خود را تغییر دهد.
0xC0000225	ظاهراً یک باگ در ویندوز رخ داده است نه یک ریسک امنیتی.
0xC000015b	در این دستگاه به کاربر اجازه ورود داده نشده است.

کدهای خطای kerberos	
0*6	نام کاربری اشتباه
0*7	حساب کاربری جدید در سیستم؟
0*9	مدیر باید رمزعبور را بازنشانی کند.
0*c	محدودیت ایستگاه کاری
0*12	حساب غیرفعال، منقضی شده، قفل شده، محدودیت ساعات ورود به سیستم
0*17	رمزعبور کاربر منقضی شده است.
0*18	رمزعبور اشتباه
0*20	Frequently logged توسط حساب‌های کاربری
0*25	ساعت ایستگاه کاری خیلی از همگام سازی با DC فاصله گرفته است.

تغییرات Group		ساخته‌شده	تغییرداده‌شده	حذف‌شده	Member	
					اضافه‌شده	انتقال دادن
امنیت	Local	۴۷۳۱	۴۷۳۵	۴۷۳۴	۴۷۳۲	۴۷۳۳
	Global	۴۷۲۷	۴۷۳۷	۴۷۳۰	۴۷۲۸	۴۷۲۹
	Universal	۴۷۵۴	۴۷۵۵	۴۷۵۸	۴۷۵۶	۴۷۵۷
توزیع	Local	۴۷۴۴	۴۷۴۵	۴۷۴۸	۴۷۴۶	۴۷۴۷
	Global	۴۷۴۹	۴۷۵۰	۴۷۵۳	۴۷۵۱	۴۷۵۲
	Universal	۴۷۵۹	۴۷۶۰	۴۷۶۳	۴۷۶۱	4762