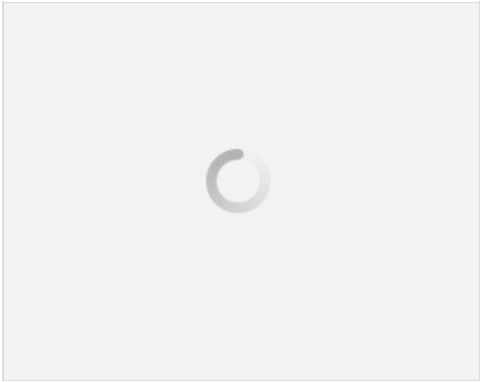
ASLR چیست؟ آشنایی با Address Space Layout Randomization (نسخه PDF)

ASLR چیست؟ همـانطور که در مورد DEP هم گفته شد، ASLR نیز یکی دیگر از مفـاهیمی است که در لوای مفهوم عـامتر حملات Client Side به آن بر خواهید خورد. ASLR را در کنار DEP میتوان دو تکنیک علیه تهدیدات سیستمی دانست که بصورت مجزا و یا بصورت ترکیبی این وظیفه را انجام میدهند.ASLR یک تکنولوژی پیشـگیری کننده امنیتی است که سیستم امنیتی را با افزایش تنوع اهداف حمله تقویت میکند. ASLR بجای آن که امنیت را با از میان بر داشـتن آسیب پذیری ها افزایش دهد، این کار را از طریق مشکل نمودن سوء استفاده از آسیب پذیری های موجود انجام میدهد.

در واقع این تکنولوژی تلاش های موجود در جهت رفع آسیب پذیری های امنیتی را با معرفی آسیب پذیری هایی که هنوز رفع نشده اند و یا شناخته نشده هستند، تکمیل میکند.ASLR را میتوان مکملی برای دیگر روش های پیشگیرانه مانند DEP نیز بشمار آورد؛ ترکیب این دو روش (ASLR و DEP) با یکدیگر، لایه محافظ قدرتمند تری را در مقابل آسیب پذیری های آلوده کننده مموری به نسبت اجرایی شدن فقط یکی از آن ها، ایجاد میکند. تکنیک هایی که در جهت مقابله با سوء استفاده از آسیب پذیری های آلوده کردن مموری ارائه میشوند، به لایه مموری در برنامه ای که هدف قرار داده شده است، حساس میباشند.

ASLR با تصادفی کردن لایه مموری در یک برنامه اجرایی، پیش بینی و تخمین این لایه را کاهش داده که به تبع آن احتمال موفقیت یک اکسـپلویت نیز کمتر خواهد شد. امنیتی که توسط ASLR ارائه میشود، بر اسـاس فاکتورهـای مختلفی است. این پارامترها شامل موارد زیر است : میزان پیش بینی پـذیر بودن لایه مموری یک برنامه، مقـدار مقاومت یک روش اکسـپلویت در برابر تغییرات لایه مموری، و تعـداد تلاش های اکسپلویت یک هکر است که کورکورانه و تخمینی انجام میشود.



ASLR با چندین سیستم عامل محبوب و پرکاربرد یکپارچه شده است. این سیستم عامل ها شامل OpenBSD و لینوکس میباشند که چندین سال است با ASLR یکپارچه شده اند. پیاده سازی ASLR در نسـخه های پیشین ویندوز نیز بصورت Third-party و ارائه محصولات stand-alone یا به عنوان بخشـی از راهکارهای HIPS نیز وجود داشـته است. با ارائه محصول ویندوز ویستا از سوی مایکروسافت، ASLR نیز برای اولین بار با ساختاربندی پیش فرض سیستم عامل ویندوز یکپارچه شد.

سربلند و مانا باشید.

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی