چهارمین کنفرانس بین المللی
مطالعات نوین درعلوم کامپیوتر و فناوری اطلاعات
4th International Conference
On New studies Of Computer And IT
وزارت علوم تحقیقات و فناوری
دانشگاه هنر صنعتی سجاد
ISC
Islamic World Science Citation Center
مشهد
۰۵ اسفند ماه ۱۳۹۶
FEBRUARY 24 ,2018

مروری بر تهدیدها و مقایسه تکنیک‌های امنیتی در سیستم‌عامل مکینتاش،یونیکس،ویندوز

فرهنگ پدیداران مقدم[۱] ، رسول نعیمی[۲]

۱-استادیار گروه کامپیوتر، موسسه آموزشی عالی اشراق بجنورد

۲-دانشجوی کارشناسی ارشد مهندسی نرم‌افزار، موسسه آموزشی عالی اشراق بجنورد

چکیده

امروزه با توجه به آسیب‌هایی که از سمت مهاجمان و نفوذ گران می‌شود و همچنین باوجود تهدیدهایی از قبیل (ویروس‌ها، تروجان ها، کرم‌ها و ...) مبحث امنیت از اهمیت بسیار بالایی برخوردار است. این مقاله یک مرور کلی از تکنیک‌های مورداستفاده برای محافظت از سیستم‌عامل MAC را ارائه می‌دهد و در بعضی از تکنیک‌ها مقایسه‌ای نیز با سیستم‌عامل‌های ویندوز NT و Unix انجام‌گرفته است و به نقاط قوت و ضعف آن‌ها اشاره‌شده است. این مقاله شامل سه بخش عمده (۱- حفاظت از حافظه۲- امنیت رمز عبور۳- حملات) است که در هر بخش آن شامل تکنیک‌ها و مکانیزم مایی است که توضیح داده می‌شود، تجزیه‌وتحلیل می‌شود. در اینجا دستورالعمل را برای هر تکنیک و همچنین روش امنیتی زیرمجموعه‌ای که برای هر تکنیک استفاده می‌شود معرفی می‌کنیم، علاوه بر این، نیز نقاط قوت و ضعف هر روش ارزیابی خواهد شد. گزارش‌های زیادی در رابطه با امنیت ویندوز و یونیکس در مورد طراحی هسته و فلسفه وجود دارد و همچنین درباره ویژگی‌های امنیتی مربوط به کاربران معمولی و حملات رایج صحبت خواهیم کرد. بسیاری از سیستم های مبتنی بر یونیکس وجود دارد، هر یک از آن‌ها دارای ویژگی‌های امنیتی و ساختارهای مختلف هستند. در این پژوهش در یک مقایسه ساده، به‌جای استفاده از سیستم‌های عمومی یونیکس بر روی امنیت MAC تمرکز خواهیم کرد. برای انجام کلیه نظری که تا حد امکان روشن است، هر یک از روش‌های امنیتی را به‌صورت جداگانه با توجه به روش حملات احتمالی و سناریوهای امنیتی موردبحث قرار خواهیم داد، دودسته بزرگ از حمله وجود خواهند داشت: حمله محلی و حمله از راه دور. طبق این دودسته بزرگ، بسته به هدف حملات، زیر دسته‌های مختلفی نیز وجود خواهد داشت.

کلیدواژه‌ها: امنیت، تهدید، مکینتاش، ویندوز، یونیکس