بررسی چالش‌های توسعه سیستم‌های ارزیابی خطر آسیب‌پذیری روز صفر و ارائه راهکار

مرجان کرامتی [۱،۱]، فاطمه سادات هل اتایی [۲]

۱- عضو هیات علمی دانشگاه سمنان

۲- عضو هیات علمی دانشگاه سمنان

چکیده

توسعه شبکه‌های کامپیوتری با افزایش سریعی در تعداد حملات سایبری در شرکت‌ها و ادارات دولتی همراه بوده است. از جمله پیامدهای این مسئله می‌توان قطع عملیات تجاری، هتک حرمت و ناثباتی مالی شرکت‌ها را نام برد. عامل ایجاد حملات در شبکه‌های کامپیوتری آسیب‌پذیری‌های هستند. آسیب‌پذیری‌های امنیتی موجود در یک نرم‌افزار، از مسائل متعددی از جمله خطا در طراحی، پیکره‌بندی نامناسب برای سیستم‌ها یا کاستی‌هایی که عموماً تحت عنوان باگ شناخته می‌شوند نشات می گیرند. مادامی که آسیب‌پذیری ناشناخته باقی می‌ماند، امکان توسعه اصلاحیه برای آن وجود ندارد. همچنین نرم افزارهای ضد ویروس میتنی بر امضا نیز قارد نخواهند بود حمله متناظر با این آسیب‌پذیری را تشخیص دهند. بنابراین، پیشگیری و تشخیص این نوع حملات با بکارگیری مکانیزم های امینتی موجود در سیستم های کامپیوتری ممکن نخواهد بود. بهبود سیستم‌های کامپیوتری از نقطه نظر مقاومت در برابر حملات روز صفر نیازمند ارزیابی خطر این نوع حملات در سیستم مورد نظر است.در این مقاله، هدف استخراج چالش‌های موجود برای توسعه سیستم‌های ارزیابی حملات روز صفر و ارائه راهکار در این زمینه است.

کلمات کلیدی: آسیب‌پذیری روز صفر، ارزیابی خطر، مدل امنیتی، معیار امنیتی، سیستم امتیازدهی به آسیب‌پذیری عام (CVSS)

۱. مقدمه

نظر به انقلابی که شبکه‌های کامپیوتری در زندگی بشر ایجاد کرده‌اند، اینترنت را می توان جز جدایی ناپذیر زندگی امروز به حساب آورد. وابستگی به اینترنت به عنوان یک شاهراه ارتباطی و بانک اطلاعاتی به شکل روز افزونی در حال افزایش است. انتقال اطلاعات ضروری از طریق اینترنت و سیل عظیم تراکنش‌های تجارت الکترونیک که به صورت آنلاین انجام می‌شود، این شاهراه ارتباطی را هر چه بیشتر معرض خطر هدف مهاجمان قرار داده است. به صورتی که، نیاز به برقراری امنیت شبکه به یک ضرورت در زندگی بشر تبدیل شده است. اخبار روزمره‌ای که در رابطه با انواع حملات در شبکه های کامپیوتری شنیده می‌شوند، گویای این مسئله هستند. حمله مهاجمان به شبکه های تجاری به منظور اختلال در تبادلات اقتصادی و نفوذ به سیستم‌های صنایع دفاع با هدف سرقت مستندات فوق سری از جمله بارزترین حملاتی است که در شبکه های کامپیوتری انجام می‌شود. فایروال‌ها و سیستم های تشخیص و پیشگیری از نفوذ از جمله تمهیدات امنیتی هستند که به منظور ردیابی مهاجمان در شبکه های کامپیوتری تعبیه شده‌اند.

توسعه شبکه‌های کامپیوتری با افزایش سریعی در تعداد حملات سایبری در شرکت‌ها و ادارات دولتی همراه بوده است. از جمله پیامدهای این مسئله می‌توان قطع عملیات تجاری، هتک حرمت و ناثباتی مالی شرکت‌ها را نام برد. عامل ایجاد حملات در شبکه‌های کامپیوتری آسیب‌پذیری‌های هستند. آسیب‌پذیری‌های امنیتی موجود در یک نرم‌افزار، از مسائل

[1] **Corresponding author: Marjan Keramati**
Email: keramati_marjan@semnan.ac.ir

متعددی از جمله خطا در طراحی، پیکره‌بندی نامناسب برای سیستم‌ها یا کاستی‌هایی که عموماً تحت عنوان باگ شناخته می‌شوند نشات می‌گیرند. مادامی که آسیب‌پذیری ناشناخته باقی می‌ماند، امکان توسعه اصلاحیه برای آن وجود ندارد. همچنین نرم افزارهای ضد ویروس میتنی بر امضا نیز قارد نخواهند بود حمله متناظر با این آسیب‌پذیری را تشخیص دهند. بنابراین، پیشگیری و تشخیص این نوع حملات با بکارگیری مکانیزم های امینتی موجود در سیستم های کامپیوتری ممکن نخواهد بود.

یک آسیب‌پذیری روز صفر قبل از اینکه توسعه دهندگان نرم‌افزار متناظر با آسیب‌پذیری، اطلاعی در مورد آن داشته باشند توسط مهاجمین استفاده شده و یا به اشتراک گذاشته میشود و هکرهای کلاه سفید، صفر روز برای رسیدگی و رفع آسیب‌پذیری فرصت خواهند داشت. به عبارت دیگر، حمله روزصفر در صفرمین روز آگاهی مدیران امنیتی و توسعه‌دهندگان نرم‌افزار از وجود آسیب‌پذیری رخ می‌دهد.

بهبود سیستم‌های کامپیوتری از نقطه نظر مقاومت در برابر حملات روز صفر نیازمند ارزیابی خطر این نوع حملات در سیستم مورد نظر است. چرا که، با توجه به محدودیت در فاکتور هزینه، مقاوم‌سازی کم‌هزینه ضرورت پیدا می کند. برای این منظور، آگاهی از میزان خطر این نوع حملات برای سیستم مورد بررسی اهمیت پیدا می‌کند.

ارزیابی خطر یک آسیب‌پذیری نیازمند تخمین میزان احتمال بهره‌برداری از آسیب‌پذیری و تعیین آثار مخرب ناشی از بهره‌برداری از آن روی پارامترهای امنیتی از جمله محرمانگی، یکپارچگی و دسترسی‌پذیری است. برای این منظور باید تعدادی معیار امنیتی در اختیار داشته باشیم که بتوانند به‌شکل کمی اندازه‌گیری شوند. همچنین، نظر به چند مرحلهاي بودن ماهیت حملات (حملاتی هستند که مهاجمان با بهره‌برداری از چندین آسیب پذیری با یک ترتیب مشخص به سیستم حمله می کنند.) در شبکه‌های کامپیوتری، تخمین میزان خطر یک آسیب پذیری با در نظر گرفتن ماهیت سایر نقاط آسیب پذیر در شبکه امری اجتناب ناپذیر است. لذا، به منظور تعریف و کمی سازی معیارهای امنیتی نیازمند مدل امنیتی مناسبی از شبکه خواهیم بود.

در ادامه بعد از بیان اهمیت ارزیابی خظر حملات روز صفر ومروری کوتاه بر فعالیت های انجام شده در این حوزه تحقیقاتی، چالش‌های موجود برای ارزیابی خظر حملات روز صفر استخراج و راهکارهایی جهت حل این چالش‌ها پیشنهاد می گردد.

۲.طرح مساله

آسیب‌پذیری‌های سخت افزاری و نرم افزاری دو نوع هستند: آسیب‌پذیری‌های شناخته شده و آسیب‌پذیری‌های ناشناخته یا روز صفر. منظور از آسیب‌پذیری‌های شناخته شده مواردی هستند که، شناسایی و برطرف شده‌اند. در مقابل، آسیب‌پذیری‌های روز صفر، نقاط ضعفی هستند که تنها مهاجمان از وجود آنها آگاه هستند. در نتیجه، هیچ راهکار اصلاحی برای آنها وجوند ندارد. این آسیب‌پذیری‌ها به شدت خطرناک و غیر قابل پیش‌بینی هستند. این نوع آسیب‌پذیری‌ها با ایجاد در پشتی در سیستم عامل یا برنامه‌های کاربردی راه مهاجم را برای نفوذ به سیستم باز می‌کنند. نکته قابل توجه این است که تعداد حملاتی که از طریق آسیب‌پذیری‌های روز صفر انجام می‌شود، به شدت در حال افزایش است. این نوع حملات که اغلب با اهداف سیاسی و اقتصادی انجام می‌شوند را می‌توان یک ابزار قدرتمند برای مهاجمان به حساب آورد. همین است که این نوع حملات را می‌توان بزرگترین دغدغه زیرساخت‌های سیاسی و اقتصادی دانست. اپل، فیسبوک، مایکروسافت و توییتر نمونه سرویس‌دهنده های مشهوری هستند که طعمه حملات روز صفر بوده‌اند . شرکت امنیتی FireEye نیز در سال ۲۰۱۳، یازده عدد آسیب پذیری که اینترنت اکسپلورر، جاوا، ادبی فلش، پی دی اف و ActiveX را مورد حمله قرار داده بودند ، شناسایی کردند.

حملات روز صفر همواره مورد توجه متخصصان امنیتی بوده است. اما تا کنون هیچ مکانیزم امنیتی واحد و قابل اطمینانی برای مقاوم‌سازی سیستم‌های کامپیوتری در برابر این نوع حملات توسعه داده نشده است. توسعه زیرساخت‌های امن، وجود ضد ویروس با دقت بالا، بروز رسانی منظم سیستم، بکارگیری سیستم‌های پیشگیری تشخیص و اصلاح نفوذ، انجام تست های نفوذ و ... همه و همه فاکتورهایی هستند که می توانند مقاومت سیستم‌های کامپیوتری را در مقابل حملات روز صفر بالا ببرند. اما با این حال نباید فراموش کرد که هیچ امنیت مطلقی وجود ندارد.

شناسایی این گونه حملات توسط ابزارهای امنیتی از جمله ابزارهای تست نفوذ ممکن نیست. لذا، تخصیص هزینه کافی به منظور شناسایی و برطرف سازی این گونه حملات از اهمیت ویژه ای برخوردار است.منظور از حفاظت در برابر چنین حملاتی، قابلیت مسدود سازی و پیشگیری از وقوع آنها قبل از افشای عمومی و یا پیش از توسعه اکسپلویت برای آنها توسط مهاجم است.

برخی سازمان‌ها برای مقابله با اینگونه حملات، متخصصانی را استخدام می‌کنند که وظیفه آنها کشف آسیب‌پذیری‌های نهفته در سازمان و برطرف‌سازی آنها پیش از وقوع هرگونه حمله سایبری است. هدف اصلی این متخصصان این است که، به محض کشف آسیب‌پذیری در نرم افزار آن را سریعاً به مسوولان امنیتی سازمان اطلاع رسانی کرده و به دنبال راهکار و انتشار اصلاحیه های امنیتی در جهت رفع آن آسیب‌پذیری‌ها باشند. در این راستا، ارزیابی خطر حملات شناسایی شده با هدف پیدا کردن پرخطر ترین حملات و تلاش برای مقاوم سازی کم هزینه در شبکه‌های کامپیوتری از ضروریات است.

یک آسیب‌پذیری امنیتی یک اشکال برنامه‌نویسی است که در زمان تست نرم افزار نادیده گرفته شده است. اگر این آسیب‌پذیری به هنگام تست نفوذ یا قبل از این که توسط هکرها کشف شود، مورد شناسایی قرار بگیرد، به فرآیند توسعه و اعمال اصلاحیه وارد خواهد شد. در غیر این صورت مجرمان سایبری آسیب‌پذیری را کشف، از آن بهره‌برداری و برای یک حمله ناشناخته مورد استفاده قرار می‌دهند.

کشف و بهره‌برداری از آسیب‌پذیری‌های ناشناخته همواره یکی از روش های حمله برای مهاجمان حرفه ای بوده است. مهاجمان از طریق این نوع آسیب‌پذیری‌ها (آسیب‌پذیری روز صفر) بدون اینکه کاربر از وجود آنها کوچکترین اطلاعی داشت باشد، صدمات جبران ناپذیری از جمله تخریب و سرقت اطلاعات و از دسترس خارج کردن سرویس‌های ضروری در سازمان‌ها را ایجاد خواهند کرد.

هیچ گونه ابزار خودکار یا روند مستند شده‌ای برای بازیابی یک سیستم بعد از رخداد حمله روز صفر در آن وجود ندارد. کاهش بهره‌وری سیستم‌های تجاری را می‌توان یکی از پیامدهای قابل توجه رخداد حملات روز صفر دانست. دسترسی به داده های محرمانه در سیستم های نظامی سیاسی نیز یکی دیگر از صدمات جبران ناپذیری است که می تواند پیامدهای قانونی به همراه داشته باشد. باید دقت داشت که، فایروال‌ها و سیستم‌های تشخیص نفوذ قادر به مقاومت در برابر حملات روز صفر نیستند.

یکی از مشکلاتی که در رابطه با حملات روز صفر وجود دارد، سرعت انتشار روزافزون این نوع حملات است. برای مثال در سال ۲۰۰۳ توسعه اکسپلویت برای آسیب پذیری SQL Slammer حدود ۸ ماه به طول انجامید. در صورتی که، در حال حاضر متوسط زمان بین کشف آسیب پذیری و توسعه اکسپلویت برای آن به تنها چند روز محدود شده است.

بسیاری از حملات روز صفر کرم های خود انتشاری هستند که تنها در چند دقیقه محدوده قابل توجهی از سیستم ها را تحت تاثیر قرار می دهد.

همچنین لازم به ذکر است، ارزیابی خطر توسط سیستم‌های امتیازدهی به آسیب‌پذیری موجود از جمله CVSS , فقط برای آسیب پذیری های شناخته شده ممکن است. همچنین تمهیدات امنیتی موجود برای مقابله با حملات روز صفر از جمله Symantec، Zscaler و غیره در دسته سیستم‌های تشخیص نفوذ قرار دارند و بعد از پیش‌روی حمله در برابر آن عکس العمل

نشان می‌دهند. در نتیجه، وجود یک سیستم پیشگیری از نفوذ در شبکه با هدف پیش بینی پرخطر ترین حملات روز صفر احتمالی و مقاوم سازی شبکه در برابر این حملات از ضروریات است.

در ادامه راهکارهای موجود برای ارزیابی های امنیتی و ارزیابی خطر حملات روز صفر بیان می گردند.

۳.فعالیت‌های پژوهشی انجام شده برای ارزیابی‌های امنیتی و سنجش خطر حملات روز صفر

توسعه شبکه‌های کامپیوتری با افزایش سریعی در تعداد حملات سایبری در شرکت‌ها و ادارات دولتی همراه بوده است که از جمله پیامدهای این مسئله می‌توان قطع عملیات تجاری، هتک حرمت و ناثباتی مالی شرکت‌ها را نام برد [۱]. عامل ایجاد حملات در شبکه‌های کامپیوتری آسیب‌پذیری‌های هستند. آسیب‌پذیری‌های امنیتی موجود در یک نرم‌افزار، از مسائل متعددی از جمله خطا در طراحی، پیکره‌بندی نامناسب برای سیستم‌ها یا کاستی‌هایی که عموما تحت عنوان باگ شناخته می‌شوند نشات می‌گیرند [۲]. بهره‌برداری از آسیب‌پذیری‌ها از آنجایی که منجر به خرابی سرویس‌های موجود در شبکه و در نتیجه مختل کردن پارامترهای محرمانگی، یکپارچگی و دسترسی‌پذیری می‌شود هزینه زیادی برای سازمان‌ها به‌همراه خواهد داشت [۳]. برای مثال، حمله عدم پذیرش سرویس برای یک سازمان مبتنی بر اینترنت می‌تواند منجر به مختل شدن عملیات تجاری شود[۴].رشد روزافزون آسیب‌پذیری‌ها برای سازمان‌های عمومی و خصوصی همیشه یک چالش بوده است. با این حال برای تمامی آسیب‌پذیری‌ها راهکار اصلاحی ارائه نشده است [۳]. از آنجا که تعداد آسیب‌پذیری‌ها به سرعت در حال افزایش است، ضروری است که مدیران امنیتی توجه خود را به آسیب‌پذیری‌هایی معطوف سازند که بیشترین خطر را برای سازمان‌ها به‌همراه دارند [۴]. برای این‌منظور چندین پایگاه‌داده از آسیب‌پذیری‌هایی از جمله CVE و OSVBD ارائه شده است که در آن‌ها هر آسیب‌پذیری با یک شناسه به نامCVE و یک توضیح مختصر متناظر است [۶]و [۷]. ابزارهای پویش از جمله Nessus، هر میزبان شبکه را پویش می‌کنند و بر مبنای این پایگاه‌ها، شرحی از آسیب‌پذیری‌های کشف شده را به همراه شناسه‌های CVE آنها مشخص می‌سازند در هر صورت این پایگاه داده‌ها کافی نیستند. چرا که، بدون رتبه‌بندی آسیب‌پذیری‌ها کار مدیر امنیتی همچنان سخت است و خود مدیر باید تصمیم‌گیری کند که کدام آسیب‌پذیری خطرناک‌تر است و کدام نقطه‌ضعف باید زورتر از بقیه برطرف شود [۸]. از جمله امور مهم در مدیریت رویدادهای امنیتی، تجزیه و تحلیل و برطرف‌سازی آسیب‌پذیری‌ها است که یکی از پیچیده‌ترین فعالیت‌ها در مدیریت امنیت سازمانی به‌شمار می‌آید. برطرف سازی آسیب‌پذیری یک کار پرزحمتی است و برای سازمانهای سرتا سر دنیا یک امر هزینه‌بری به‌شمار می‌آید [۲]. از آنجا که مدیران امنیتی در سازمان اغلب با مشکل بودجه محدود مواجه هستند، آنان نیازمند این هستند که با در نظر داشتن واکنش‌های موجود برای حملات، سرمایه‌گذاری در بخش‌های مختلف را اولویت‌بندی کنند. بکارگیری روش‌های ارزیابی کمی آسیب‌پذیری‌های امنیتی، اولویت‌بندی کارایی از تلاش‌های امنیتی و سرمایه‌گذاری بهینه را به‌منظور برطرف‌سازی آسیب پذیری‌های شناسایی شده ممکن می‌سازد.

متناظر با شدت هر آسیب‌پذیری باید یک اقدام متقابل برای برطرف‌سازی یا کاهش اثرات ناخوشایند آن وجود داشته باشد و با توجه به مشکل بودجه محدود، آسیب‌پذیری‌ها باید بر اساس شدتشان اولویت‌بندی شوند[۳]. به بیان دیگر، سرمایه گذاری امنیتی باید متعادل با خسارات احتمالی باشد. برای مثال، یک سازمان مبتنی براینترنت ممکن است در نتیجه افراط در هزینه برای اقدامات امنیتی مجبور شود قیمت فروش خود را بالا ببرد. [۴]. هزینه واکنش در برابر آسیب‌پذیری مجموع هزینه‌های مستقیم (منابع انسانی بکارگرفته شده، هزینه مجوزها و...) و غیر مستقیم (اتلاف بهره‌وری، قطع عملکردهای سیستم به‌دلیل راه‌اندازی مجدد زمان‌بندی نشده بعد از اعمال اصلاحیه‌ها) در نظر گرفته می‌شود. انتخاب یک راهکار مناسب برای واکنش در برابر آسیب‌پذیری به معنای انتخاب روشی است که آسیب‌پذیری مورد نظر را در زمان قابل قبول و با هزینه کمتری نسبت به روش‌های دیگر برطرف سازد.

مسئله قابل توجه دیگر این است که، حتی زمانی که آسیب‌پذیریها معلوم هستند و شناسایی شده‌اند، ممکن است هیچ راهکار مناسبی برای رسیدگی کردن به آنها وجود نداشته باشد. مسائل زمانی از جمله، سرعت آهسته انتشار اصلاحیه‌ها و ناپایداری اصلاحیه‌های موجود منجر به باقی ماندن آسیب‌پذیری‌های شناخته شده در سازمان می‌شود [۷]. در نظر گرفتن اطلاعات زمانی از این قبیل، ارزیابی کاراتری از شدت واقعی یک آسیب‌پذیری را به‌همراه دارد و اولویت‌بندی آسیب‌پذیری‌ها را بهبود می‌بخشد. در نتیجه اقدامات امنیتی با کارایی بالاتری انتخاب می‌شوند[۲]. منظور از شدت یک آسیب پذیری به‌عنوان شاخصی برای اولویت‌بندی آسیب‌پذیری‌ها، میزان خطری است که بهره‌برداری از آن برای شبکه به همراه دارد. منظور از ارزیابی خطر، تخمین احتمال بهره‌برداری از یک حمله و همچنین آسیب بالاقوه‌ای است که بهره‌برداری از آن می‌تواند به‌همراه داشته باشد (تاثیر) [۹]. در هرصورت تا کنون معیار قابل‌قبولی برای ارزیابی خطر امنیت شبکه معرفی نشده است و مشکلی نیز که در رابطه با روش‌های ارزیابی خطر موجود وجود دارد این است که، این روش‌ها ارزیابی پویای از خطر انجام نمی‌دهند. [۱۰].

حملاتی که آسیب‌پذیری‌های موجود را برای نقض سیاست‌های امنیتی استفاده می‌کنند ممکن است توسط یک حمله واحد یا دنباله‌ای از حملات تک‌مرحله‌ای انجام شوند. به دنباله حملات تک‌مرحله‌ای گاهاً زنجیره بهره‌برداری نیز گفته می‌شود. زنجیره بهره‌برداری، از وابستگی‌های موجود بین آسیب‌پذیری‌ها به‌عنوان ابزاری برای مختل کردن سیاست‌های امنیتی استفاده می‌کند. [۱]. مجموعه تمامی زنجیره‌های بهره‌برداری که سیاست‌های امنیتی را نقض می‌کنند می‌توانند توسط یک گراف حمله مشخص شوند. شماری از اطلاعات امنیتی یک شبکه با تجزیه و تحلیل گراف حمله آن قابل استخراج است. چرا که، گراف حمله نمایش خلاصه‌ای از تمامی راه‌های ممکن برای نفوذ به شبکه و مختل کردن سیاست‌های امنیتی است. گراف حمله به‌عنوان یک ابزار ارزیابی آسیب‌پذیری می‌تواند به یک سازمان کمک کند که وضعیت امنیتی خود را مشخص سازد. یک سازمان می‌تواند از گراف حمله برای تعیین چگونگی نفوذ مهاجم به شبکه استفاده کند. بر اساس مسیرهای مشخص شده، یک سازمان قادر خواهد بود راهکارهایی را برای کاهش خطر پیشنهاد دهد. اگر یک مهندس امنیتی از معیارهای امنیتی مبتنی بر گراف حمله استفاده کند، می‌تواند یک استراتژی را برای انتخاب اقدامات متقابل بکارگیرد یا امنیت دو پیکره‌بندی متفاوت از شبکه مورد نظر را با هم مقایسه کند. زمانی که گراف حمله در کنار معیارهای امینتی مبتنی بر گراف حمله استفاده می‌شود، می‌تواند برای ارزیابی کمی شماری از جنبه‌های امینتی شبکه استفاده شود[۱].

یک معیار امنیتی درجه برآورده‌سازی اهداف امنیتی برای یک سیستم را مشخص می‌سازد. از آنجا که معیارهای امنیتی کمی در سطح وسیع موجود نیستند، جامعه امنیتی اصولا از معیارهای کیفی به‌منظور ارزیابی امنیت استفاده می‌کند. در حال حاضر بیشتر دست‌اندرکاران امنیتی از روش‌های کیفی وابسته به طرز فکر شخصی (بر مبنای عقاید و بینش‌ها) برای ارزیابی امنیت شبکه‌شان استفاده می‌کنند. در هر صورت نیاز برای ارزیابی کمی و واقع‌بینانه از امنیت شبکه همچنان باقی خواهد بود [۱۱].

به دلیل اهمیت بالای ارزیابی امنیت سیستم‌های اطلاعاتی، تعداد زیادی از سازمان‌ها، شرکت‌ها و محققین سیستم‌هایی را برای ارزیابی آسیب‌پذیری‌ها توسعه داده‌اند. دو دسته‌بندی کلی از سیستم‌های امتیازدهی به آسیب‌پذیری موجود هستند، کیفی و کمی. روش‌های کیفی شدت هر آسیب‌پذیری را مشخص می‌سازند در صورتی که روش‌های کمی گستره بالاتری از امتیازات را برای توصیف آسیب‌پذیری‌ها بکار می‌گیرند [۵].

نمونه‌هایی از سیستم‌های کیفی عبارتند از ISS X-Force از شرکت IBM [۱۲] و سیستم ارزیابی Qualys [۱۳]. از جمله سیستم‌های امتیازدهی کمی می‌توان سیستم امتیازدهی به آسیب‌پذیری US-CERT's و سیستم امتیازدهی به آسیب پذیری عام یا CVSS* را نام برد [۱۴]. الگوهای اختصاصی بسیاری برای امتیازدهی به آسیب‌پذیری‌های نرم‌افزارها وجود

* Common Vulnerability Scoring System

دارد اما، CVSS تنها سیستم شناخته شده باز است که بواسطه ارزیابی کمی از آسیب‌پذیری‌ها از سایر سیستم‌ها مجزا می‌شود. CVSS همچنین جزئیاتی را در رابطه با ماهیت آسیب‌پذیری مشخص می‌سازد که به کاربران کمک می‌کند تا این درک را داشته باشند که چرا این آسیب‌پذیری این امتیاز را کسب کرده است[۱۵]. به بیان دیگر CVSS، روشی را برای تعیین خصوصیات ذاتی هر آسیب‌پذیری فراهم می‌کند که منعکس‌کننده شدت آن هستند[۱۴].

CVSS با ارائه یک معیار امنیتی که شدت آسیب‌پذیری را مشخص می‌کند می‌تواند در امر اولویت‌بندی کمک‌کننده باشد. پژوهشگران و مدیران امنیتی به این موضوع پی برده‌اند که شدت آسیب‌پذیری‌ها با گذر زمان و به‌واسطه قرار گرفتن در بافت‌های سازمانی مختلف تغییر قابل توجهی دارد. بنابراین پارامترهای ارائه شده توسط CVSS برای استفاده به‌منظور اولویت‌بندی کاربردمحدودی دارد چرا که، سیاست‌های امنیتی هر شبکه و عوامل زمانی از جمله، احتمال معرفی راهکارهای اصلاحی و ابزارهای بهره‌برداری از آسیب‌پذیری میزان خطر ناشی از بهره‌برداری از آن را با گذر زمان تغییر می‌دهند [۲]. از طرف دیگر CVSS، ارزیابی خطر را تنها برای حملات تک‌مرحله‌ای انجام می‌دهد. این در حالی است که، بیشتر حملات موجود در شبکه حملات چند مرحله‌ای یا زنجیره بهره‌برداری هستند. مشکل جدی دیگری که وجود دارد این است که، CVSS متمایزسازی کارایی از آسیب‌پذیری‌ها از نقطه‌نظر خطر وارده به سیستم انجام نمی‌دهد چرا که در CVSS تنها تعداد محدودی عدد مختلف برای امتیازدهی به سیل عظیمی از آسیب‌پذیری‌ها موجود است (CVSS).

همچنین قابل ذکر است که، تلاش‌های امنیت سنتی در سازمان‌ها عموماً بر حفاظت از سرمایه‌های کلیدی در برابر مخاطراتی تاکید دارند که، به‌صورت عمومی افشا شده‌اند. اما امروزه مهاجمان پیشرفته در تلاش برای توسعه ابزارهای بهره برداری برای آسیب‌پذیری‌هایی هستند که تاکنون افشا نشده‌اند و تحت عنوان حملات ناشناخته معروف هستند[۲]. CVSS به عنوان یک سیستم پرکاربرد در ارزیابی‌های امنیتی، سنجشی از میزان خطر حملات ناشناخته ندارد.

همان‌طور که بیان شد، سیستم‌های امتیازدهی به آسیب‌پذیری به دوشکل موجود هستند: کیفی و کمی. نمونه‌ای از یک سیستم کیفی Mozilla است که این سیستم، میزان خطر آسیب‌پذیری‌ها را با چهار سطح امنیتی مشخص می‌سازد. (بحرانی، بالا، متوسط و پایین)[۱۶]. سیستم امتیازدهی به آسیب‌پذیری عام یا CVSS نیز یک مثال از سیستم کمی است که توضیح داده شد.

در ادامه مروری کوتاه داریم بر تعدادی راهکار غیر استاندارد که در سالیان اخیر به‌منظور ارزیابی خطر حملات در شبکه‌های کامپیوتری پیشنهاد شده است. در اقداماتی که به منظور ایمن‌سازی شبکه‌ها صورت می‌گیرد مسئله‌ای که اهمیت پیدا می‌کند این است که بتوان، احتمال بروز حملات، تخمین صدمات ممکن ناشی از آنها در شبکه و کارایی اقدامات ایمن‌سازی را به‌صورت کمی مشخص کرد. بنابراین، ارزیابی خطر ناگزیر با تعریف تعدادی معیار امنیتی قابل انجام خواهد بود. .بر اساس تعریفی که توسط SSECMM در [۱] ارائه شده است، یک معیار امنیتی یا ترکیبی از معیارهای امنیتی، شامل یک مقیاس کمی از ویژگی‌های امنیتی اجزای قابل شناسایی سیستم (مثلا شبکه) است. به کمک تعریف و استفاده از چنین معیارهایی این امکان فراهم می‌شود که قادر به مقایسه میزان امنیت سیستم‌های مختلف باشیم. به طور مثال سه معیار امنیتی مبتنی بر گراف حمله که در[۱] معرفی شده است، شامل معیارهای ساده‌ای نظیر کوتاه‌ترین مسیر، تعداد کل مسیرها و طول میانگین مسیرهای موجود در گراف است که هر یک از این معیارها سعی در ارائه پاسخ به یکی از سوالات مهم و اساسی در زمینه امنیت شبکه را دارند. به طور مثال معیار کوتاه‌ترین مسیر سعی دارد تا پاسخ این سوال را مشخص کند که کمترین تلاشی که برای نفوذ به سیستم لازم است چقدر است و یا تعداد مسیرهای موجود نیز معرف تعداد راه‌های مختلفی است که مهاجم برای نفوذ به سیستم در اختیار دارد. همچنین، میانگین طول مسیرهای موجود نیز بیانگر میزان تلاش نوعی مهاجم برای نفوذ به سیستم است. هر چند تعریف این معیارها با هدف‌های خاصی انجام شده است ولی مشخص است هر یک از این معیارها دارای نقاط ضعفی هستند. به طور مثال معیار کوتاه‌ترین مسیر و یا میانگین طول مسیرهای موجود در گراف تعداد راه‌هایی که مهاجم می‌تواند از آنها استفاده نماید را نادیده می‌گیرند. به عبارت دیگر، همواره گرافی که اندازه

کوتاه‌ترین مسیر آن نسبت به یک گراف دیگر کمتر است الزاما نا امن‌تر از آن نیست. به‌منظور غلبه بر کاستی‌های فوق، در این پژوهش، الگوریتمی برای ترکیب معیارهای فوق پیشنهاد شده است که بواسطه آن می‌توان تصمیم‌گیری کرد که کدام پیکره‌بندی برای شبکه امن‌تر است.

در [۱] به‌منظور ارزیابی خطر مبتنی بر گراف حمله، یک مدل محاسبه احتمال با در نظر گرفتن فاکتورهای زمانی متناظر با هر آسیب‌پذیری ارائه شده است. با استفاده از چارچوب پیشنهادی تخمین کمی امنیت با در نظر گرفتن ویژگی‌هایی پویای هر آسیب‌پذیری که به مرور زمان تغییر می‌کند، قابل انجام است.

در [۴] یک مدل برای تخمین سطح خطر بر مبنای احتمال شرطی رخداد حمله و تاثیر منفی رخداد آن معرفی شده است. برآورد فرکانس رخداد حمله و تاثیر با استفاده از CVSS انجام شده است. مدل ارائه شده، هر آسیب‌پذیری را به یک سطح سرویس نظیر می‌کند. سطوح سرویس تعیین‌کننده سطوح خطر بالاقوه هستند و به شکل یک فرآیند مارکوف مدل شده‌اند و برای پیش‌بینی سطح خطر در یک زمان مشخص استفاده خواهند شد.

در [۱۱]، یک معیار امنیتی کمی مبتنی بر تجزیه و تحلیل گراف حمله معرفی شده است. معیار مذکور قدرت امنیتی شبکه را بر اساس قدرت ضعیف‌ترین مهاجمی ارزیابی می‌کند که می‌تواند به‌صورت موفقیت آمیز به شبکه حمله کند. معیار امنیتی کمی معرفی شده به مدیران شبکه این امکان را می‌دهد که یک پیکره‌بندی مناسب را برای شبکه خود انتخاب کنند.

در [۲] با هدف مدیریت کمی امنیت، تخمینی از احتمال موجود بودن ابزارهای بهره‌برداری از آسیب‌پذیری و معرفی اصلاحیه‌ها انجام شده است.

روش ارائه شده در [۳]، با درنظر گرفتن صدمات اقتصادی که بهره‌برداری از یک آسیب‌پذیری به‌همراه دارد، یک ارزیابی کمی از شدت آن انجام می‌دهند. در این روش، نیازمندی‌های امنیتی شبکه مورد بررسی نیز در ارزیابی خطر مد نظر قرار می‌گیرد. همچنین، تجمیع فاکتورهای اقتصادی به‌منظور ارزیابی شدت آسیب‌پذیری با استفاده از تکنیک‌های تجزیه و تحلیل تصمیم‌گیری چندضابطه‌ای یا MCDA انجام شده است.

[۵] یک سیستم امتیازدهی به آسیب‌پذیری است که پراکندگی امتیازات در آن به‌شکل قابل توجهی از CVSS بالاتر است. نویسنده در [۸] با تغییر و اصلاح روابط در CVSS، روش نوینی را برای امتیازدهی به آسیب‌پذیری‌ها پیشنهاد کرده است. عدم درنظر گرفتن عوامل زمانی در امتیازدهی به آسیب‌پذیری‌ها و فقدان توانایی برای امتیازدهی به حملات چندمرحله ای از جمله مشکلات اساسی دو روش مذکور است.

در [۹] با استفاده از CVSS و بر مبنای معیارهای پایه، زمانی و محیطی روش جدیدی برای تخمین شدت یک آسیب پذیری ارائه شده است که با ترکیب امتیازات فرعی مرتبط با هر بخش و با مدل کردن پارامترهای مسئله در قالب یک چارچوب ریاضی، شدت یک آسیب‌پذیری مشخص می‌کند.

در [۱۷] یک بررسی آماری روی امتیازات تولید شده توسط سه پایگاه داده آسیب‌پذیری‌های معروف (IBM ISS X-Force, Vupen Security , CVSS) با هدف بررسی تفاوت‌های سیستم‌های موجود و یافتن مزایای نسبی آنها از نقطه‌نظر آماری انجام شده است. در این مقاله، یک سیستم امتیازدهی به آسیب‌پذیری معرفی شده است که در پیاده‌سازی آن مزایای سه سیستم فوق اعمال شده است و ارزیابی آسیب‌پذیری‌ها را به‌صورت کیفی و کمی انجام می‌دهد. در این مقاله بهبودی روی CVSS با هدف سازگار کردن نتایج با توزیع نرمال انجام شده است.

در [۱۸] روشی برای ارزیابی میزان مقاومت یک شبکه در برابر حملات ناشناخته معرفی شده است. همچنین در [۱۹] با در نظر گرفتن آسیب‌پذیری‌های ناشناخته روشی برای تخمین متوسط زمان مورد نیاز برای تصاحب حملات چند مرحله‌ای ارائه شده است.

در، [۲۰] ما یک سیستم مبتنی بر مدل امنیتی برای ارزیابی خطر حملات روز صفر چند مرحله‌ای توسعه داده‌ایم.

آنچه یک مدیر امنیتی به‌منظور مقاوم‌سازی کم‌هزینه برای شبکه خود نیاز دارد، ارزیابی پویایی از میزان خطری است که حملات چندمرحله‌ای برای سیستم به‌همراه دارند و تعیین پرخطرترین حملات به‌منظور مقاوم‌سازی است. همچنین، در نظر گرفتن وجود حملات ناشناخته در مدل امنیتی حملات پرخطر در شبکه را با دقت بالاتری مشخص می‌سازد. در حال حاضر، مدیران امنیتی سیستم جامعی با ویژگی‌های مذکور را به‌منظور تعیین خطر حملات چندمرحله‌ای در اختیار ندارند.

۴.نمونه هایی از سیستم های موجود برای ارزیابی خطر حملات روز صفر

در رابطه با فعالیت های مشابه که در سطح دنیا انجام شده است آشنا می شویم. قابل ذکر است که، مکانیزم های حفاظتی در برابر حملات روز صفر موجود عموما:

- با تشخیص نفوذ بعد از پیشروی حمله از سیستم های کامپیوتری موجود محافظت می کنند.
- پیشگیری از بروز حمله روز صفر را برای یک سیستم واحد و نه در یک شبکه انجام می دهند.

این در صورتی است که، لازم است یک سیستم ارزیابی خطر روز صفر با پیش بینی پرخطرترین حملات روز صفر احتمالی در یک شبکه کامپیوتری، قبل از رخداد حملات، شبکه را در برابر حملات چند مرحله‌ای روز صفر توسط مهاجمان محافظت می‌کند. این مسئله حائز اهمیت است. چرا که، بکارگیری سیستم های پیشگیری به جای تشخیص، صدمات ناشی از بروز حمله را به شکل قابل توجهی کاهش می دهند.

ادامه این بخش اشاره ای است به تعدادی از سیستم های حفاظتی موجود در برابر حملات روز صفر

- Watchdog

در سیستم مذکور، وجود مکانیزم امنیتی لایه‌ای هوشمند در کنار فایروال‌های موجود در لایه کاربرد، محافظت در برابر حملات روز صفر را انجام می‌دهند [۲۱].

- Zscaler

ادعا شده است که طراحی این سیستم با این هدف بوده است که، اتصال به اینترنت از طریق امن را با برقراری مکانیزم‌های محرمانگی، یکپارچگی و دسترسی پذیری برای کاربران ممکن سازد. در این سیستم، تشخیص و پیشگیری از حملات روز صفر با بررسی محتوا و تحلیل پویای ترافیک انجام می‌شود. [۲۲].

- Symantec

این سیستم محافظت از زیرساخت وب را در برابر حملات ناشناخته انجام می‌دهد [۲۳] .

- Adaptive Defense 360

شرکت پاندا محصولی تحت عنوان «Adaptive Defense 360» را به تمامی مدیران آی تی و سازمان‌ها پیشنهاد می کند. این محصول، تمام برنامه‌های کاربردی موجود در سیستم را نظارت می‌کند و همچنین با استفاده از تکنیک «یادگیری ماشین» و استفاده از پلاتفرم‌های کلان داده، قادر به آنالیز کردن رفتار برنامه‌های کاربردی به صورت زنده است.

سیستم مذکور ، قادر است در حالتی تحت عنوان «Extended Block Mode» از اجرای برنامه های نامطلوب و غیر کاربردی جلوگیری کند. در این حالت تنها برنامه هایی که به عنوان(خوب افزار) دسته بندی شده اند قابل اجرا خواهند بود و سایر برنامه ها بصورت خودکار متوقف خواهند شد[۲۴] .

در ادامه، چالش‌های موجود بر سر راه توسعه یک سیستم ارزیابی خطر برای حملات روز صفر به همراه راهکارهای پیشنهادی بیان شده‌اند:

- نظر به ماهیت ناشناخته بودن این نوع حملات برای جامعه امنیتی، استخراج خصوصیات ذاتی این نوع آسیب‌پذیری‌ها از سیستم‌های امتیازدهی مثل CVSS ممکن نیست.

راهکار: استخراج خصوصیات ذاتی آسیب‌پذیری‌های شناخته شده، بررسی شاخصه‌های آماری و پیش بینی خصوصیات ذاتی آسیب پذیری‌های روز صفر موجود براساس شاخصه های آماری مشاهده شده.

- مدیریت و تحلیل حملات چندمرحله‌ای توسط نیروی انسانی کار دشواری است و پتانسیل خطای بالایی نیز دارد.

راهکار : خودکارسازی این فرآیند، پیچیدگی و احتمال بروز خطا را به شکل قابل توجهی کاهش می دهد. منظور از خودکارسازی مدیریت و تحلیل حملات چند مرحله‌ای، توسعه سیستمی برای آنالیز مدل امنیتی شبکه تحت بررسی و استخراج حملات چند مرحله ای موجود در یک شبکه است.

- پیچیدگی استخراج مدل امنیتی

به منظور مشخص کردن تمامی حملات ممکن در شبکه، نه تنها اطلاعات پیکربندی شبکه مورد نیاز است بلکه، ارتباطات متقابل بین آنها نیز باید مشخص باشد. به عبارت دیگر هم ارتباطات فیزیکی و منطقی کامپیوترهای موجود در شبکه و هم اطلاعات مربوط به هر کدام از میزبان‌ها در آن برای شناسایی حملات باید مشخص باشند.

چالش اساسی در طراحی یک سیستم تحلیل آسیب‌پذیری، مشخص کردن جزئیات مورد نیازی است که شبکه باید بر آن اساس مدل شود.

راهکار: در مدل‌سازی امنیتی یک سیستم، عموماً مدل را به اندازه‌ای جزئی در نظر می‌گیرند که مورد نیاز است. به عبارت دیگر تنها جنبه‌هایی از سیستم را که در تحلیل و ارزیابی مورد نیاز است، مدل می‌نمایند. به طور مثال پیشنهاد می‌شود به جز اطلاعات مربوط به آسیب‌پذیری میزبان‌ها و ارتباطات آنها با یکدیگر، پیش‌شرط‌های مورد نیاز برای حملات شناخته شده و نتایج حاصل از بروز آن حملات در سیستم برای مدل‌سازی مورد استفاده قرار گرفته‌اند.

گراف حمله مبتنی بر بهره برداری، نمونه ای از مدل امنیتی است که اطلاعات مذکور را پوشش می دهد. لازم به ذکر است، این نوع گراف حمله با پیچیدگی زمانی قابل قبول (چند جمله‌ای) گزینه مناسبی برای مدل سازی شبکه های بزرگ در یک زمان معقول است.

- عدم وجود استانداردی برای تعریف، اندازه‌گیری و تجمیع معیارهای امنیتی

راهکار: نظر به عدم وجود استاندارد واحد برای تعریف و اندازه گیری معیارهای امنیتی، به منظور ارزیابی کمی خطر، تعریف معیارهای امنیتی مبتنی بر مدل امنیتی و خصوصیات ذاتی آسیب پذیری‌ها پیشنهاد می‌شود. تحلیل مدل امنیتی و در اختیار داشتن خصوصصیات ذاتی آسیب پذیری‌ها، اندازه گیری کمی معیارهای مذکور را ممکن می سازد.

۵.جمع بندی و کارهای آینده

در حال حاضرهیچ گونه ابزار خودکار یا روند مستند شده‌ای برای بازیابی یک سیستم بعد از رخداد حمله روز صفر در آن وجود ندارد. کاهش بهره‌وری سیستم‌های تجاری را می‌توان یکی از پیامدهای قابل توجه رخداد حملات روز صفر دانست. دسترسی به داده های محرمانه در سیستم های نظامی سیاسی نیز یکی دیگر از صدمات جبران ناپذیری است که می تواند

پیامدهای قانونی به همراه داشته باشد. باید دقت داشت که، فایروال‌ها و سیستم‌های تشخیص نفوذ قادر به مقاومت در برابر حملات روز صفر نیستند. در این مقاله، تلاش شد تا با بررسی سیستم‌های امنیتی موجود برای حفاظت از حملات روز صفر، چالش‌های موجود برای توسعه سیستم‌های ارزیابی خطر حملات روز صفر استخراج و راهکارهایی پیشنهاد گردد. در ادامه قصد داریم، با توسعه یک چارچوب مبتنی بر مدل امنیتی شبکه، روشی برای ارزیابی خطر حملات روز صفر احتمالی در یک شبکه پیشنهاد دهیم. خروجی سیستم پیشنهادی که میزان خطر رخداد حملات روز صفر قبل از وقوع آنها در یک شبکه خواهد بود، به‌عنوان ابزاری برای انجام مقاوم‌سازی کم‌هزینه در اختیار مدیران امنیتی شبکه قرار می‌گیرد. تلاش تیم امنیتی برای ممانعت از بهره برداری از پرخطرترین آسیب پذیری های روز صفر گزارش شده توسط سیستم پیشنهادی، احتمال وقوع حملات روز صفر پرخطر و صدمات ناشی از رخداد آن‌ها را به مراتب کاهش می‌هد.

۶. مراجع

1. Idika N., Bhargava B.,(2010), Extending Attack Graph-based Security Metrics and Aggregating Their Application, IEEE Transactions on Dependable and Secure Computing, pp. 1-12.

2. Frühwirth C., Männistö T.,(2009), Improving CVSS-based vulnerability prioritization and response with context information, Proceeedings of International Workshop on Security Measurement and Metrics (MetriSec), PP. 535-544.

3. Ghani H., Luna j., Suri N.,(2013), Quantitative assessment of software vulnerabilities based on economic-driven security metrics, International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1-8.

4. Houmb S. H.,. Franqueira V. N. L, (2009), Estimating ToE Risk Level Using CVSS, International Conference on Availability, Reliability and Security, pp.718-725,

5. Spanos G., Sioziou A., Angelis L., (2013), WIVSS: a new methodology for scoring information systems, pp.83-90

6. https://cve.mitre.org/, MITRE CVE,(Accessed September 2018)

7. http://osvdb.org/, OSVBD, (Accessed September 2018)

8. GALLON L., (2010), Vulnerability discrimination using CVSS framework, In New Technologies", Mobility and Security (NTMS), 4th IFIP International Conference, pp. 1 –6.

9. Hamid T., Maple C., and Sant P. , (2012), Methodologies to Develop Quantitative Risk Evaluation Metrics, International Journal of Computer Applications, Vol.48, No.14, pp.17-24.

10. Xie L., Zhang X., Zhang J.,(2013), Network Security Risk Assessment Based on Attack Graph, Journal of Computers, Vol. 8, No. 9, pp. 2339-2347.

11. Pamula J., Jajodia S., Ammann P., and Swarup V.,(2006), A Weakest-Adversary Security Metric for Network Configuration Security Analysis," Proc. Second ACM Workshop Quality of Protection, pp. 31-38,.

12. http://www-935.ibm.com/services/us/iss/xforce/faqs.html, IBM. X-Force frequently asked questions, (Accessed September 2018)

13. http://www.qualys.com/research/knowledge/severity/ , Qualys. Severities KnowledgeBase, (Accessed September 2018)

14. https://www.first.org/cvss, Common Vulnerability Scoring System (CVSS), (Accessed September 2018)

15. Scarfone K., Mell P.,(2009), An Analysis of CVSS Version 2 Vulnerability Scoring, Proceeding of 3rd International Symposium on Empirical Software Engineering and Measurement, PP. 516 – 525.

16. http://www.mozilla.org/security/announce/, Mozilla Foundation Security Advisories, (Accessed September 2018).

17. Liu Q., Zhang Y.,(2011), VRSS: A new system for rating and scoring vulnerabilities, Computer Communications, Vol. 34, No. 3, PP. 264-273.

18. Albanese M., Jajodia S., Singhal A., Wang L., (2014), An Efficient Framework for Evaluating the Risk of Zero-Day Vulnerabilities. In E-Business and Telecommunications, Springer. PP. 322-340.

19. Nzoukou W., Wang L., Jajodia S., Singhal A.,(2013), A unified framework for measuring a network's mean time-to-compromise. Proc. 32nd Int'l. Symp. on Reliable Distributed Systems (SRDS). pp. 215-224.

20. Keramati, M. (2018).Dynamic Risk Assessment System for the Vulnerability Scoring. International Journal of Information & Communication Technology Research, 9(4), 57-68.

21. https://www.watchdogsecurity.co.nz/,Watchdog , (Accessed September 2018)

22. https://www.zscaler.com/ ,Zscaler (Accessed September 2018)

23. https:www.symantec.com/,Symantec (Accessed September 2018)

24. https://www.pandasecurity.com/mediacenter/panda.../why-adaptive-defense-360/ ,Adaptive Defense 360 (Accessed September 2018)