

## روشی مبتنی بر مدل امنیتی برای ارزیابی پویا از خطر حملات چند مرحله‌ای در شبکه‌های کامپیوتری

مرجان کرامتی<sup>۱\*</sup>، فاطمه‌سادات هل‌اتابی<sup>۲</sup>

۱- مریبی دانشگاه سمنان، ۲- مریبی دانشگاه سمنان

(دریافت: ۱۳۹۷/۰۸/۲۵ پذیرش: ۱۳۹۸/۰۷/۰۲)

### چکیده

با گسترش روزافزون آسیب‌پذیری‌ها در شبکه‌های کامپیوتری و وابستگی ابعاد مختلف زندگی بشر به شبکه، امن‌سازی شبکه‌ها در برابر حملات ضروری است. در این راستا مقاوم‌سازی کم‌هزینه به دلیل محدودیت بودجه در زمره چالش‌های مورد توجه مدیران امنیتی است. برآورده‌سازی این هدف، با اولویت‌بندی آسیب‌پذیری‌ها از نظر میزان خطر و انتخاب پرخطرترین آن‌ها برای حذف ممکن می‌شود. در این باره سیستم امتیازدهی به آسیب‌پذیری عام یا CVSS، به‌عنوان پرستفاده‌ترین سیستم برای تعیین میزان خطر ناشی از بهره‌برداری شدن از آسیب‌پذیری‌ها معرفی شده است. اما باید دقت داشت که در CVSS، شدت آسیب‌پذیری تنها بر اساس خصوصیات ذاتی تعیین می‌شود و عوامل زمانی مثل احتمال معرفی ابزارهای بهره‌برداری از آسیب‌پذیری نادیده گرفته می‌شوند. بنابراین، CVSS نمی‌تواند ارزیابی پویایی از خطر داشته باشد. همچنین، CVSS متمایزسازی کارایی از آسیب‌پذیری‌ها از نقطه‌نظر خطر وارده به سیستم را انجام نمی‌دهد بدین دلیل که، تنها تعداد محدودی عدد برای امتیازدهی به انبوهی از آسیب‌پذیری‌ها موجود است. به‌علاوه CVSS، ارزیابی خطر را فقط برای تک آسیب‌پذیری‌ها انجام می‌دهد و ارزیابی عمده حملات که حملات چندمرحله‌ای هستند توسط CVSS ممکن نیست. در این مقاله، به‌منظور بهبود عملکرد CVSS سیستمی برای ارزیابی پویای خطر حملات چندمرحله‌ای با در نظر گرفتن عوامل زمانی ارائه شده است. گوناگونی امتیازات در این سیستم به شکل قابل‌توجهی توسعه یافته است. توسعه سیستم معرفی شده براساس مدل امنیتی و تعریف معیارهای امنیتی مبتنی بر مدل امنیتی، دقت نظری بوده که ارزیابی خطر حملات چند مرحله‌ای را توسط سیستم پیشنهادی ممکن ساخته است. همچنین، قابلیت ارزیابی خطر حملات چند مرحله‌ای روز صفر را می‌توان به‌عنوان یک ویژگی منحصربه‌فرد برای سیستم پیشنهادی معرفی کرد که سیستم‌های امتیازدهی فعلی قادر به انجام آن نیستند.

**واژه‌های کلیدی:** ارزیابی خطر، آسیب‌پذیری، حملات چند مرحله‌ای، حملات روز صفر، گراف حمله، سیستم امتیازدهی به آسیب‌پذیری عام (CVSS)، معیار امنیتی

### ۱. مقدمه

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 [۵]. برای این منظور چندین پایگاه‌داده از آسیب‌پذیری‌هایی از جمله CVE و OSVDB ارائه شده است که در آن‌ها هر آسیب‌پذیری با یک شناسه به نام CVE و یک توضیح

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 آسیب‌پذیری‌ها هستند. آسیب‌پذیری‌های امنیتی موجود در یک نرم‌افزار، از مسائل متعددی نشأت می‌گیرند که از جمله این مسائل عبارتند از خطا در طراحی، پیکره‌بندی نامناسب برای سیستم‌ها یا کاستی‌هایی که عموماً تحت عنوان باگ شناخته می‌شوند [۲]. بهره‌برداری از آسیب‌پذیری‌ها از آنجایی که منجر به خرابی سرویس‌های موجود در شبکه و در

نایاب‌داری اصلاحیه‌های موجود منجر به باقی ماندن آسیب‌پذیری‌های شناخته شده در سازمان می‌گردد [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].

حملاتی که از آسیب‌پذیری‌های موجود 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 [۱۰]. 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. بدین علت 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 مشخص سازی وضعیت امنیتی خود کمک کند. 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 راهبرد 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 امنیتی مبتنی بر گراف حمله استفاده شود، می‌تواند برای ارزیابی کمی برخی از جنبه‌های امنیتی شبکه به‌کار گرفته شود [۱۰].

منظور از شدت یک آسیب‌پذیری 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 بالقوه‌ای است که بهره‌برداری از آن می‌تواند به‌همراه داشته باشد و از آن تحت عنوان تاثیر یاد می‌شود [۱۱]. در هر صورت تا کنون معیار قابل قبولی برای ارزیابی خطر امنیت شبکه معرفی نشده و مشکل موجود در رابطه با روش‌های ارزیابی خطر فعلی این است که این روش‌ها، ارزیابی پویایی از خطر انجام نمی‌دهند [۱۲].

یک معیار امنیتی، درجه برآورده‌سازی اهداف امنیتی را برای یک سیستم مشخص می‌کند. از آنجا که معیارهای امنیتی کمی در

مختصر متناظر است [۷-۶]. ابزارهای پویا از جمله Nessus، هر میزبان شبکه را پوشش می‌کنند و بر مبنای این پایگاه داده‌ها، شرحی از آسیب‌پذیری‌های کشف شده را به همراه شناسه‌های CVE آنها مشخص می‌سازند [۸]. در هر صورت این پایگاه داده‌ها کافی نیستند. زیرا بدون رتبه‌بندی آسیب‌پذیری‌ها کار مدیر امنیتی همچنان سخت است و خود مدیر باید تصمیم‌گیری کند که کدام آسیب‌پذیری خطرناک‌تر بوده و کدام نقطه‌ضعف باید زورتر از بقیه برطرف شود [۹]. 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. برطرف‌سازی آسیب‌پذیری، کاری پرزحمت است و برای سازمان‌های سرتا سر دنیا امری هزینه‌بر به‌شمار می‌آید [۲]. مدیران امنیتی در سازمان اغلب با مشکل بودجه محدود مواجه هستند. به‌همین سبب، لازم است سرمایه‌گذاری در بخش‌های مختلف را با در نظر داشتن پاسخ‌های موجود برای حملات، اولویت‌بندی کنند. به‌کارگیری روش‌های ارزیابی کمی آسیب‌پذیری‌های امنیتی، اولویت‌بندی کارایی از تلاش‌های امنیتی برای برطرف‌سازی آسیب‌پذیری‌های شناسایی شده را ممکن می‌سازد. در نتیجه، مقاوم‌سازی کم هزینه سیستم‌های کامپیوتر میسر می‌شود.

متناظر با شدت هر آسیب‌پذیری باید یک اقدام متقابل برای برطرف‌سازی آسیب‌پذیری یا کاهش اثرات ناخوشایند آن وجود داشته باشد. همچنین، با توجه به مشکل بودجه محدود، باید آسیب‌پذیری‌ها، بر اساس شدتشان اولویت‌بندی شوند [۳]. به بیان دیگر، سرمایه‌گذاری امنیتی باید متناسب با خسارات احتمالی باشند. برای مثال، یک سازمان مبتنی بر اینترنت ممکن است در نتیجه افراط در صرف هزینه برای اقدامات امنیتی، مجبور به افزایش قیمت فروش خود گردد [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

وارد به سیستم انجام نمی‌دهد چرا که، در CVSS تنها تعداد محدودی عدد مختلف برای امتیازدهی به سیل عظیمی از آسیب‌پذیری‌ها موجود است [۱۶].

همچنین قابل ذکر است که تلاش‌های امنیت سنتی در سازمان‌ها، عموماً بر حفاظت از سرمایه‌های کلیدی در برابر مخاطراتی تأکید دارند که بصورت عمومی افشا شده‌اند. اما امروزه مهاجمان پیشرفته در تلاش برای توسعه ابزارهای بهره‌بردار برای آسیب‌پذیری‌هایی هستند که تاکنون افشا نشده‌اند و تحت عنوان حملات روز صفر معروف هستند [۱]. CVSS به‌عنوان یک سیستم پرکاربرد در ارزیابی‌های امنیتی، سنجشی از میزان خطر حملات روز صفر ندارد.

در این مقاله با هدف اولویت‌بندی حملات از نظر میزان خطری که برای شبکه به‌همراه دارند، روشی برای ارزیابی پویای خطر حملات چند مرحله‌ای در شبکه‌های کامپیوتری ارائه شده است. راهکار ارائه شده با در نظر گرفتن احتمال معرفی ابزارهای بهره‌بردار برای آسیب‌پذیری‌ها در کنار خصوصیات ذاتی آنها، میزان خطر حملات چند مرحله‌ای را با گذر زمان مشخص می‌سازد. بنابراین، این روش ارزیابی دقیق‌تری از میزان خطر هر آسیب‌پذیری انجام می‌دهد. از این‌رو، پیش‌بینی میزان خطر برای آینده نیز ممکن خواهد بود. به‌علاوه، روش ارائه شده در این مقاله می‌تواند سنجش‌ای از میزان خطر حملات روز صفر در شبکه داشته باشد.

همچنین، در این مقاله با هدف بهبود نقطه ضعف CVSS در سنجش میزان تأثیر بهره‌بردار از آسیب‌پذیری روی سه پارامتر امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری، راه‌کار جدیدی برای ارزیابی تأثیر معرفی شده است که در نتیجه به‌کارگیری آن، دامنه امتیازات برای ارزیابی خطر نسبت به CVSS به شکل قابل توجهی بهبود پیدا می‌کند. افزایش گستردگی امتیازات در روش ارائه‌شده نسبت به CVSS اولویت‌بندی حملات در شبکه را به شکل کاراتری ممکن می‌سازد.

در روش پیشنهادی، ارزیابی خطر حملات با تعریف تعدادی معیار امنیتی مبتنی بر گراف حمله و معرفی روشی برای تجمیع این معیارهای امنیتی انجام می‌شود. معیارهای امنیتی مذکور با تحلیل گراف حمله شبکه مورد نظر به شکل کمی قابل اندازه‌گیری هستند.

مزایای روش پیشنهادی در مقایسه با سیستم‌های امتیازدهی به آسیب‌پذیری موجود عبارتند از:

- اولویت‌بندی کارای حملات بر اساس میزان خطر وارده به سیستم (گوناگونی قابل توجه امتیازات موجود برای ارزیابی خطر حملات)

سطح وسیع موجود نیستند، جامعه امنیتی اصولاً 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 شبکه خود استفاده می‌کنند. در هر صورت نیاز برای ارزیابی کمی و واقع‌بینانه از امنیت شبکه همچنان باقی خواهد بود [۱۳].

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 به‌کار می‌گیرند [۵].

نمونه‌هایی از سیستم‌های کیفی عبارتند از ISS X-Force از شرکت IBM [۱۴] و سیستم ارزیابی Qualys [۱۵]. از جمله سیستم‌های امتیازدهی کمی می‌توان سیستم امتیازدهی به آسیب‌پذیری US-CERT's و سیستم امتیازدهی به آسیب‌پذیری عام یا CVSS را نام برد [۱۶]. الگوهای اختصاصی بسیاری برای امتیازدهی به آسیب‌پذیری‌های نرم‌افزارها وجود دارد اما، CVSS تنها سیستم شناخته شده است که به‌واسطه ارزیابی کمی از آسیب‌پذیری‌ها از سایر سیستم‌ها مجزا می‌شود. همچنین، CVSS جزئیاتی را در رابطه با ماهیت آسیب‌پذیری مشخص می‌سازد که به کاربران در درک بهتر علت تخصیص امتیاز به آسیب‌پذیری کمک می‌کند [۱۷-۱۸]. به بیان دیگر CVSS، روشی را برای تعیین خصوصیات ذاتی هر آسیب‌پذیری فراهم می‌کند که منعکس‌کننده شدت آن هستند [۱۶].

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 کاربرد محدودی دارد، زیرا سیاست‌های امنیتی هر شبکه و عوامل زمانی از جمله احتمال معرفی راه‌کارهای اصلاحی و ابزارهای بهره‌بردار از آسیب‌پذیری میزان خطر ناشی از بهره‌بردار از آن را با گذر زمان تغییر می‌دهند [۲]. از طرف دیگر CVSS، ارزیابی خطر را تنها برای حملات تک‌مرحله‌ای انجام می‌دهد. در صورتی که بیشتر حملات موجود در شبکه حملات چند مرحله‌ای یا زنجیره بهره‌بردار هستند. مشکل جدی دیگر این است که، CVSS متمایزسازی کارایی از آسیب‌پذیری‌ها از نقطه‌نظر خطر

- قابلیت ارزیابی خطر حملات چند مرحله‌ای
- انجام ارزیابی پویا از خطر حملات
- قابلیت ارزیابی خطر حملات روز صفر

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 اهداف خاصی انجام شده ولی مشخص است هر یک از این معیارها دارای نقاط ضعفی هستند. به‌طور 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 الزاماً نا امن‌تر از آن نیست. به‌منظور غلبه بر کاستی‌های فوق، در این مقاله الگوریتمی برای ترکیب معیارهای فوق پیشنهاد شده است که به‌واسطه آن می‌توان تصمیم‌گیری کرد کدام پیکره‌بندی برای شبکه امن‌تر است.

در [۱۱] 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 روش پیشنهادی در این مقاله، تخمین کمی امنیت با در نظر گرفتن ویژگی‌هایی پویای هر آسیب‌پذیری قابل انجام است.

در [۴] یک مدل برای تخمین سطح خطر بر مبنای احتمال شرطی رخداد حمله و تاثیر منفی رخداد معرفی شده است. برآورد فرکانس رخداد حمله و تاثیر آن با استفاده از CVSS انجام شده است. مدل ارائه‌شده، 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 [۱۳]، 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 موفقیت‌آمیز به شبکه حمله کند. معیار امنیتی کمی معرفی شده به مدیران شبکه این امکان را می‌دهد که یک پیکره‌بندی مناسب 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 ارائه‌شده در [۳]، با در نظر گرفتن صدمات اقتصادی که بهره‌برداری از یک آسیب‌پذیری به‌همراه دارد، ارزیابی کمی از شدت آن انجام می‌دهند. در این روش، نیازمندی‌های امنیتی شبکه‌ی مورد بررسی در ارزیابی خطر مد نظر قرار گرفته شده است. همچنین در این مقاله، تجمیع فاکتورهای اقتصادی به‌منظور ارزیابی شدت آسیب‌پذیری با استفاده از روش‌های تجزیه و تحلیل تصمیم‌گیری چند ضابطه‌ای یا MCDA انجام شده است.

مقاله پیش‌رو، بهبود یافته سیستم امتیازدهی به آسیب‌پذیری است که در مرجع شماره [۴۱] معرفی کرده‌ایم. مزایای سیستم پیشنهادی در مقاله حاضر نسبت به [۴۱] عبارتند از:

- اصلاح روش برآورد تاثیر بهره‌برداری از آسیب‌پذیری روی پارامترهای محرمانگی، یکپارچگی و دسترسی‌پذیری در CVSS
- توانایی ارزیابی خطر حملات روز صفر
- قابلیت تخمین تاثیر رخداد حمله چند مرحله‌ای روی محرمانگی، یکپارچگی و دسترسی‌پذیری شبکه.

در ادامه بعد از مروری کوتاه بر فعالیت‌های مشابه و مفاهیم مرتبط با گراف حمله و CVSS در بخش‌های ۲ و ۳ و ۴، روش پیشنهادی در بخش ۵ معرفی شده است. همچنین در بخش‌های ۶ و ۷ نتایج ارزیابی خطر حملات توسط روش پیشنهادی با CVSS مقایسه شده است.

## ۲- مروری بر کارهای مشابه

همان‌طور که بیان شد، سیستم‌های امتیازدهی به آسیب‌پذیری به دو شکل 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) [۱۹]. سیستم امتیازدهی به آسیب‌پذیری عام یا CVSS نیز یک مثال از سیستم کمی است که توضیح داده شد.

در ادامه مرور کوتاهی داریم بر تعدادی راه‌کار غیر استاندارد که در سالیان اخیر به‌منظور ارزیابی خطر حملات در شبکه‌های کامپیوتری پیشنهاد شده است. مسئله مورد اهمیت در اقدامات صورت گرفته به منظور ایمن‌سازی شبکه‌ها 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 [۱۰] ارائه شده است، یک معیار امنیتی یا ترکیبی از معیارهای امنیتی، شامل یک مقیاس کمی از ویژگی‌های امنیتی اجزای قابل شناسایی سیستم (مثلاً شبکه) است. به کمک تعریف و استفاده از چنین معیارهایی این امکان فراهم می‌شود که قادر به مقایسه میزان امنیت سیستم‌های مختلف باشیم. به‌طور مثال سه معیار امنیتی مبتنی بر گراف حمله معرفی شده در [۱۰]، شامل معیارهای ساده‌ای نظیر کوتاه‌ترین مسیر، تعداد کل مسیرها و میانگین طول 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. به‌طور مثال معیار کوتاه‌ترین مسیر سعی دارد پاسخ این سوال را مشخص کند که کمترین تلاش لازم برای نفوذ به سیستم چقدر است و یا تعداد مسیرهای موجود نیز

پیش رو توسعه یافته مقالات مذکور با هدف ارزیابی پویایی از خطر حملات چند مرحله‌ای (شناخته شده و روز صفر) در شبکه‌های کامپیوتری است.

مدل‌های امنیتی از مرسوم ترین ابزارها برای ارزیابی امنیتی به شمار می‌آیند. در [۴۲] مدلی برای محاسبه اعتماد به کمک شبکه‌های بیزین برای شبکه‌های اجتماعی ارائه شده است

گراف حمله متناظر با یک شبکه با در اختیار داشتن اطلاعات توپولوژی شبکه و آسیب‌پذیری‌های شبکه مورد نظر مدل می‌شود. اطلاعات آسیب‌پذیری متناظر با هر شبکه با استفاده از ابزارهای تست نفوذی مانند Nessus قابل استخراج است [۸]. همچنین، اطلاعات جامعی در رابطه با هر آسیب‌پذیری در پایگاه‌داده‌هایی مانند NVD در دسترس است [۲۳]

بخش بعدی مروری بر مدل گراف حمله و تعدادی مفاهیم مرتبط با آن است.

### ۳- مروری بر مدل امنیتی گراف حمله

همان‌طور که عنوان شد، گراف‌های حمله، تمامی دنباله‌ها یا زنجیره‌های حمله ممکن برای حمله به یک نقطه بخصوص در شبکه را از طریق ارتباطات بین آسیب‌پذیری‌های موجود نشان می‌دهد. یک شیوه مرسوم برای ارزیابی کمی یک شبکه کامپیوتری استفاده از گراف حمله است. برای ساخت گراف‌های حمله حداقل سه مولفه زیر مورد نیاز است [۱۰]:

- ۱- لیست آسیب‌پذیری‌های موجود در میزبان‌ها
- ۲- نحوه اتصال میزبان‌ها به یکدیگر
- ۳- حداقل یک سیاست امنیتی (مثلا یک نقطه هدف)

انواع متفاوتی از گراف‌های حمله وجود دارد. دو نوع مرسوم عبارتند از گراف‌های حمله مبتنی بر حالت و گراف‌های حمله مبتنی بر بهره‌برداری. پیچیدگی ساخت و تحلیل گراف‌های حمله مبتنی بر حالت، تابعی نمایی از تعداد میزبان‌های شبکه است. به همین دلیل گراف‌های حمله مبتنی بر حالت مشکل مقیاس‌پذیری دارند. از این‌رو در این مقاله، از گراف حمله مبتنی بر بهره‌برداری یا گراف حمله فشرده به‌عنوان مدل امنیتی استفاده شده است [۲۴].

گراف حمله فشرده، یک گراف حمله جهت‌دار است که دو نوع گره مختلف دارد: آسیب‌پذیری‌های قابل بهره‌برداری و شرایط امنیتی. در این نوع نمایش، گره‌ها بیانگر شرایط امنیتی و یا آسیب‌پذیری‌ها هستند. پیچیدگی تولید این نوع گراف‌های حمله تابعی چندجمله‌ای از تعداد آسیب‌پذیری‌ها و شرایط امنیتی موجود در شبکه است. در گراف حمله مبتنی بر بهره‌برداری، شرایط امنیتی به دو دسته کلی تقسیم می‌شوند [۲۴]:

روش ارائه شده در [۵] یک سیستم امتیازدهی به آسیب‌پذیری است که پراکندگی امتیازات در آن به‌شکل قابل توجهی از CVSS بالاتر است. نویسنده در [۹] با تغییر و اصلاح روابط در CVSS، روش نوینی را برای امتیازدهی به آسیب‌پذیری‌ها پیشنهاد کرده است. عدم در نظر گرفتن عوامل زمانی در امتیازدهی به آسیب‌پذیری‌ها و فقدان توانایی برای امتیازدهی به حملات چندمرحله‌ای از جمله مشکلات اساسی دو روش مذکور است.

در [۱۱] با استفاده از CVSS و بر مبنای معیارهای پایه، زمانی و محیطی روش جدیدی برای تخمین شدت یک آسیب‌پذیری 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 را مشخص می‌سازد.

در [۲۰] یک بررسی آماری روی امتیازات تولید شده توسط سه پایگاه داده آسیب‌پذیری‌های معروف ( IBM ISS X-Force, CVSS, Vupen Security ) با هدف بررسی تفاوت‌های سیستم‌های موجود و یافتن مزایای نسبی آنها از نقطه نظر آماری انجام شده است. در این مقاله، یک سیستم امتیازدهی به آسیب‌پذیری معرفی شده که در پیاده‌سازی آن مزایای سه سیستم فوق اعمال شده است و ارزیابی آسیب‌پذیری‌ها را به صورت کیفی و کمی انجام می‌دهد. در این مقاله بهبودی روی CVSS با هدف سازگار کردن نتایج با توزیع نرمال انجام شده است.

در [۲۱] روشی برای ارزیابی میزان مقاومت یک شبکه در برابر حملات ناشناخته معرفی شده است. همچنین در [۲۲] با در نظر گرفتن آسیب‌پذیری‌های ناشناخته، روشی برای تخمین متوسط زمان مورد نیاز برای تصاحب حملات چند مرحله‌ای ارائه شده است. 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 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. در مقاله پیش‌رو با در نظر داشتن ضرورت انجام مقاوم‌سازی کم‌هزینه در شبکه‌های کامپیوتری، سیستم امتیازدهی به آسیب‌پذیری با ویژگی‌های مذکور توسعه داده شده است که ارزیابی خطر هر شبکه را با دریافت گراف حمله آن ممکن می‌سازد.

در [۳۹]، ما روشی مبتنی برای مدل امنیتی برای پیش‌بینی خطر حملات روز صفر ارائه دادیم. همچنین، در [۴۰] ما روشی برای ارزیابی پویایی خطر حملات تک مرحله‌ای معرفی کرده‌ایم. مقاله

بهره‌برداری و معیار تاثیر منعکس کننده پیامد مستقیم بهره‌برداری از یک آسیب پذیری روی سه پارامتر امنیتی محرمانگی، یکپارچگی و دسترسی پذیری است. گروه زمانی منعکس کننده خصوصیات از آسیب پذیری است که به مرور زمان تغییر می‌کند. از جمله مثال‌هایی برای معیارهای زمانی، وجود ابزارهای بهره‌برداری از آسیب پذیری است که امتیاز آسیب پذیری را افزایش می‌دهد یا توسعه اصلاحیه برای آسیب پذیری که امتیاز آن را کاهش می‌دهد. گروه محیطی نمایانگر ویژگی‌هایی از یک آسیب پذیری است که منحصر به یک محیط بخصوص است. معیارهای پایه امتیاز بین ۰ تا ۱۰ را برای یک آسیب پذیری مشخص می‌سازند که می‌تواند با امتیازدهی به معیارهای زمانی و محیطی تغییر کند [۱۶].

چالش موجود در رابطه با این سیستم امتیازدهی این است که گروه معیارهای زمانی و محیطی برای آسیب پذیری‌ها در هیچ یک از نسخه های ۲ و ۳ مقدار دهی نشده‌اند، بنابراین امتیازی که CVSS برای هر آسیب پذیری تخصیص می‌دهد تنها منعکس کننده خصوصیات ذاتی آسیب پذیری‌ها است و در نتیجه، میزان خطر گزارش شده مقدار دقیقی نیست و ارزیابی خطر پویا توسط CVSS ممکن نخواهد بود. در این مقاله، تلاش شده است با تخمین خصوصیات زمانی هر آسیب پذیری در کنار خصوصیات ذاتی آن که توسط CVSS قابل استخراج است روشی برای ارزیابی پویای خطر ارائه شود. دامنه امتیازات روش پیشنهادی نسبت به CVSS به شکل قابل توجهی بالاتر است. بنابراین مجزاسازی کاراتری از آسیب پذیری‌ها توسط روش پیشنهادی ممکن خواهد بود.

## ۵- روش پیشنهادی

در این مقاله روشی برای ارزیابی خطر حملات چندمرحله‌ای پیشنهاد شده است. یکی از ویژگی‌های مهم روش ارائه شده این است که عوامل زمانی در کنار خصوصیات ذاتی هر آسیب پذیری برای ارزیابی خطر مورد استفاده قرار می‌گیرد. بنابراین خطر محاسبه شده ماهیت پویا خواهد داشت که پیش‌بینی میزان خطر در آینده را نیز ممکن می‌سازد.

طبق تعریف، میزان خطر یا ریسک به صورت (۱) محاسبه می‌شود [۲۵]:

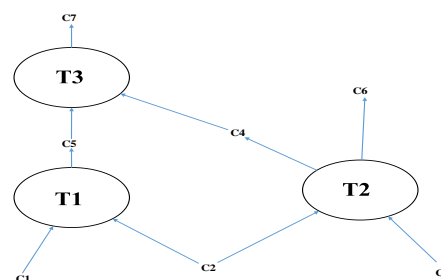
$$Risk = Likelihood of an adverse event \times Impact of the adverse event. \quad (1)$$

در این مقاله، تعیین خصوصیات ذاتی در ارزیابی خطر حملات چندمرحله‌ای بر اساس CVSS انجام شده است. برای هر آسیب پذیری شناخته شده بر اساس شناسه CVE، میزان خطر

- شرایط اولیه: این نوع شرایط فقط به عنوان شرط لازم برای بهره‌برداری از آسیب پذیری‌ها هستند و نتیجه بهره‌برداری از هیچ آسیب پذیری دیگری نیستند.
- شرایط میانی: شرایطی هستند که نتیجه بهره‌برداری از آسیب پذیری‌های موجود در شبکه هستند.

یکی دیگر از مفاهیم مهم در رابطه با گراف حمله؛ مسیر حمله است. یک مسیر حمله مجموعه‌ای از آسیب پذیری‌هایی است که با یک ترتیب مشخص بهره‌برداری می‌شوند تا مهاجم به نقطه هدف خود برسد. به عبارت دیگر، هر مسیر حمله معادل با یک زنجیره بهره‌برداری است. در گراف حمله، مسیرهای حمله موفق، منجر به این می‌شود که مهاجم به تعدادی از وضعیت‌های هدف مطلوب خود دست یابد.

یک نمونه از گراف حمله مبتنی بر بهره‌برداری در شکل (۱) نشان داده شده است. در این گراف C1 و C2 و C3 شرایط اولیه و C4 یک نمونه شرط میانی است. آسیب پذیری‌های قابل بهره‌برداری نیز با Ti نمایش داده شده است. T1، T3 یک نمونه مسیر حمله است که مهاجم از طریق آن می‌تواند امتیاز C7 را در شبکه کسب کند.



شکل (۱): نمونه گراف مبتنی بر بهره‌برداری

## ۴- سیستم امتیازدهی CVSS

آسیب پذیری‌های سخت‌افزاری و نرم‌افزاری برای سازمان‌هایی که بر مبنای شبکه‌های کامپیوتری عمل می‌کنند خطر جدی به شمار می‌آیند و طبقه‌بندی و برطرف‌سازی آن‌ها امری دشوار است.

در حال حاضر محاسبه‌گر امتیاز برای نسخه دو از CVSS موجود و نسخه ۳ از آن در حال توسعه است. لازم به ذکر است، نسخه ۳ در حال حاضر برای امتیازدهی به دامنه محدودی از آسیب پذیری‌ها (آسیب پذیری‌های ثبت شده از سال ۲۰۱۶ به بعد) قابل استفاده است [۱۶].

CVSS شامل سه گروه معیار است: پایه، زمانی و محیطی. گروه پایه نمایانگر خصوصیات ذاتی یک آسیب پذیری است که در طول زمان و در خلال شبکه‌های مختلف ثابت هستند. گروه معیارهای پایه شامل دو دسته معیار است: معیارهای قابلیت بهره‌برداری و معیار تاثیر. معیارهای قابلیت بهره‌برداری منعکس کننده سادگی

محیطی برای آسیب‌پذیری‌ها مقدار دهی نشده‌اند، پارامتر مذکور قابل استفاده نخواهد بود. از این رو، در این مقاله با هدف تخمین پارامتر  $Exploitability(V_i)$  در (۲) برای هر تک آسیب‌پذیری، از مدل توزیع احتمال Pareto در (۴) استفاده شده است [۲۶]. در این رابطه،  $x$  سن یک آسیب‌پذیری است که برابر است با تعداد روزهایی که از زمان افشا شدن این آسیب‌پذیری می‌گذرد.

$$Prob(V_i) = \frac{AccessComplexity(V_i)}{\times Exploitability(V_i)} \quad (2)$$

$$EaseOfExploitDegree(V_i) = 100 \times Prob(V_i) \quad (3)$$

$$F(x) = 1 - \left(\frac{k}{x}\right)^\alpha \quad (4)$$

$k = 0.00161, \alpha = 0.260$

تلاش صورت‌گرفته در این مقاله برای تخمین احتمال بهره‌برداری شدن یک حمله چندمرحله‌ای، در راستای بهبود روش ارائه شده در [۱۰] است. در [۱۰] ارزیابی خطر حملات بر مبنای تعدادی از معیارهای امنیتی مبتنی بر مسیر حمله انجام شده است. نقطه ضعف اساسی مقاله [۱۰]، نادیده گرفتن ماهیت آسیب‌پذیری‌های موجود در مسیرهای حمله است. به عبارت دیگر در مقاله مذکور فرض شده، درجه آسانی بهره‌برداری تمامی آسیب‌پذیری‌های موجود در هر شبکه یکسان بوده که این فرضی غیر واقعی است. از این رو، در این مقاله، روشی برای ارزیابی درجه آسانی بهره‌برداری از هر آسیب‌پذیری با تعریف تعدادی از معیارهای امنیتی مبتنی بر خصوصیات ذاتی و زمانی یک آسیب‌پذیری پیشنهاد شده است. (رابطه (۳)). بنابراین، در این مقاله به‌عنوان بهبودی بر مقاله [۱۰]، مسیرهای حمله وزن‌دار شده، برای ارزیابی خطر مورد استفاده قرار گرفته‌اند.

در هر شبکه، متناظر با هر حمله چند مرحله‌ای عموماً بیش از یک مسیر حمله وجود دارد. بنابراین، در این مقاله، در ارزیابی خطر حملات چندمرحله‌ای اثر تمامی این مسیرها توأم در نظر گرفته شده است. احتمال رخداد یک حمله چندمرحله‌ای از روی درجه آسانی هر آسیب‌پذیری که در بخش قبل توضیح داده شد، استخراج شده است.

درجه آسانی یک مسیر حمله طبق رابطه (۵)، با مد درجه آسانی آسیب‌پذیری‌های موجود در یک مسیر حمله رابطه مستقیم دارد. در (۵)،  $mode(EaseOfExploitDegree(V_i))$  شاخص آماری مد است که برای تخمین درجه آسانی بهره‌برداری از  $n$  آسیب‌پذیری که در مسیر  $path$  وجود دارند، استفاده می‌شود. دقت داشته باشید که متنوع بودن آسیب‌پذیری‌هایی که در یک مسیر حمله

یک آسیب‌پذیری که بر اساس ویژگی‌های ذاتی آن تعیین می‌شود از سیستم محاسبه‌گر CVSS نسخه ۲ قابل استخراج هستند. همچنین برای تعدادی از آسیب‌پذیری‌ها، امتیاز متناظر با آسیب‌پذیری از نسخه ۳ نیز قابل استخراج است. از این رو با این هدف که سیستم پیشنهادی با هر دو نسخه CVSS سازگار باشد، در این مقاله پارامترهایی از CVSS در تعریف معیارهای امنیتی برای ارزیابی خطر مورد استفاده قرار گرفته‌اند که بین هر دو نسخه مشترک هستند.

در ادامه، سیستم پیشنهادی در سه بخش مجزای چگونگی سنجش احتمال رخداد یک حمله چندمرحله‌ای، روند تخمین میزان تاثیر بهره‌برداری شدن از آن روی سه پارامتر امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری و روش ارزیابی خطر حملات روز صفر معرفی شده است.

## ۵-۱. ارزیابی احتمال بهره‌برداری از یک حمله چندمرحله‌ای

ارزیابی میزان احتمال رخداد حملات چندمرحله‌ای نیازمند تعیین احتمال بهره‌برداری از تک آسیب‌پذیری‌هایی است که حمله چند مرحله‌ای را موجب می‌شوند. از این رو در این مقاله روشی برای تخمین میزان احتمال بهره‌برداری از یک آسیب‌پذیری بر اساس خصوصیات ذاتی و زمانی آن پیشنهاد شده که در ادامه معرفی می‌شود.

گروه معیارهای پایه در CVSS نمایانگر خصوصیات از یک آسیب‌پذیری هستند که در ارزیابی احتمال بهره‌برداری از آن تعیین کننده هستند. در روش پیشنهادی، تنها پارامتر پیچیدگی دسترسی که بین دو نسخه CVSS مشترک است، در تخمین میزان احتمال بهره‌برداری شدن از یک آسیب‌پذیری مورد استفاده قرار می‌گیرد.

در تعیین احتمال رخداد یک حمله تک‌مرحله‌ای باید دقت داشت که هر چه پیچیدگی دسترسی کمتر باشد (یا پارامتر پیچیدگی دسترسی گزارش شده از CVSS برای یک آسیب‌پذیری بالاتر باشد) و ابزارهای بهره‌برداری با احتمال بیشتری در دسترس مهاجم باشند، آسیب‌پذیری با احتمال بالاتری توسط مهاجم مورد بهره‌برداری قرار می‌گیرد. با این استدلال، رابطه (۲) برای تخمین احتمال بهره‌برداری از یک تک آسیب‌پذیری پیشنهاد شده است. رابطه (۳) نیز، درجه آسانی بهره‌برداری از تک آسیب‌پذیری را مشخص می‌سازد.

متناظر با کیفیت ابزارهای بهره‌برداری از یک آسیب‌پذیری، پارامتری تحت عنوان  $Exploitability$  در گروه معیارهای موقتی یا زمانی CVSS موجود است. اما از آنجایی که معیارهای زمانی و

$$\prod_{i=1}^n a_{ij}^{w_i} \quad \text{و} \quad \sum_{i=1}^n w_i = 1 \quad (7)$$

$$\text{EaseOfExploitDegree}(\text{MultiStageAttack}) = \text{SLength}^{SPP} \times \text{TrimedMean}^{TMP} \times \text{LLength}^{LPP} \quad (8)$$

$$TMP = 1 - (SPP + LPP) \quad (9)$$

$$\text{Prob}(\text{MultiStageAttack}) = \frac{\text{EaseOfExploitDegree}(\text{MultiStageAttack})}{100 * \text{constant}} \quad (10)$$

$$\begin{cases} \text{Version 2 constant} = 0.71 \\ \text{Version 3 constant} = 0.77 \end{cases}$$

طبق استدلالی که در [۱۰] وجود دارد، معیار کوتاه‌ترین مسیر و میانگین طول مسیرهای موجود در گراف، تعداد راه‌هایی که مهاجم می‌تواند از آنها بهره بگیرد را نادیده می‌گیرد. بنابراین، در این مقاله، علاوه بر وزن دار کردن مسیرها با روابط مذکور در کنار معیار کوتاه‌ترین مسیر، سایر مسیرهای حمله متناظر با حمله چندمرحله‌ای نیز با محاسبه میانگین پیراسته به شرح بالا (رابطه ۸)، به‌نوعی در ارزیابی خطر در نظر گرفته شده‌اند.

طبق استدلالی که در [۱۰] وجود دارد، معیار کوتاه‌ترین مسیر و میانگین طول مسیرهای موجود در گراف، تعداد راه‌هایی که مهاجم می‌تواند از آنها بهره بگیرد را نادیده می‌گیرد. بنابراین، در این مقاله، علاوه بر وزن دار کردن مسیرها با روابط مذکور در کنار معیار کوتاه‌ترین مسیر، سایر مسیرهای حمله متناظر با حمله چندمرحله‌ای نیز با محاسبه میانگین پیراسته به شرح بالا (رابطه ۸)، به‌نوعی در ارزیابی خطر در نظر گرفته شده‌اند.

بنابر (۱)، به‌منظور ارزیابی خطر حملات، علاوه بر تخمین احتمال، سنجش تاثیر بهره‌برداری شدن از آسیب‌پذیری روی پارامترهای امنیتی شبکه (محرمانگی، یکپارچگی و دسترسی‌پذیری) نیز ضروری است. در بخش ۵-۲، روش پیشنهادی برای ارزیابی تاثیر رخداد یک حمله چندمرحله‌ای روی سه پارامتر امنیتی شبکه توضیح داده شده است.

## ۵-۲. سنجش میزان تاثیر رخداد یک حمله چندمرحله‌ای روی پارامترهای امنیتی شبکه

برای هر تک آسیب‌پذیری شناخته شده در پایگاه داده CVSS، میزان تاثیر بهره‌برداری از آن روی پارامترهای امنیتی شبکه قابل استخراج است و طبق مستندات CVSS توسط رابطه (۱۱) محاسبه می‌شود. در (۱۱)  $I_C, I_I, I_A$  به ترتیب از راست به چپ، تاثیر بهره‌برداری شدن از تک آسیب‌پذیری روی سه پارامتر

وجود دارد، بهره‌برداری از آن را برای مهاجم سخت می‌سازد. از این‌رو، در محاسبه درجه آسانی بهره‌برداری از یک مسیر حمله، درجه گوناگونی آسیب‌پذیری‌های موجود در یک مسیر حمله (*Diversity (path)*) (درصد آسیب‌پذیری‌های منحصربه‌فرد نیز) در نظر گرفته شده و با استفاده از رابطه (۶) قابل محاسبه است.

$$\text{EaseOfExploitDegree}(\text{path}) = \text{mode}(\text{EaseOfExploitDegree}(V_i)) \times (1 - \text{Diversity}(\text{path})) \quad (5)$$

$$\begin{aligned} i &= 1:n \\ \text{Diversity}(\text{path}) &= \frac{\text{Number of unique vulnerabilities}(\text{path})}{\text{Total Number of Vulnerabilities}(\text{path})} \quad (6) \end{aligned}$$

برای هر مسیر حمله متناظر با حمله چندمرحله‌ای، وزن این مسیرها که معادل با درجه آسانی بهره‌برداری از این مسیرها است، طبق رابطه (۵) محاسبه شده و در تخمین احتمال بهره‌برداری از یک حمله چندمرحله‌ای در رابطه (۱۰) مورد استفاده قرار گرفته است. در رابطه (۱۰)، تقسیم به پارامتر constant با هدف نرمال‌سازی انجام شده است.

فرآیند محاسبه درجه آسانی رخداد حمله چندمرحله‌ای پیشنهادی در این مقاله، یک مسئله تجزیه و تحلیل تصمیم‌گیری چند معیاره یا MCDA است. در این نوع مسئله، رتبه بندی اعضای یک مجموعه متناهی براساس تعدادی معیار انجام شود. برای هر معیار دخیل در امتیازدهی، بر اساس درجه اهمیت آن در رتبه‌بندی، یک وزن در نظر گرفته می‌شود و مجموع این وزن‌ها برابر یک است [۲۷]. چندین روش برای حل مسائل MCDA وجود دارد که با توجه به نیازمندی‌های مسئله تخمین درجه آسانی رخداد حمله چندمرحله‌ای، روش "مدل ضرب وزن دار شده" در (۷) برای این منظور انتخاب شده است.

رابطه (۸) درجه سادگی بهره‌برداری از حمله چندمرحله‌ای را محاسبه می‌کند. پارامترهای موجود در (۸) به شرح زیر هستند:

- $SLength$  و  $LLength$ : به ترتیب اندازه مسیر با کم‌ترین و بیش‌ترین وزن است.
- $TrimedMean$ : میانگین پیراسته وزن مسیرها است که، با حذف مسیرهایی با کم‌ترین وزن و بیش‌ترین وزن از مجموعه مسیرها و محاسبه میانگین حسابی روی مسیرهای باقیمانده محاسبه می‌شود.
- $SPP$  و  $LPP$ : به ترتیب درصد مسیرهای با کم‌ترین و بیش‌ترین وزن در مجموعه مسیرهای حمله است.
- $TMP$ : طبق رابطه (۹) محاسبه می‌شود.



$$Impact = \begin{cases} 6.42 \times ISC_{Base}, & \text{Scope Unchanged} \\ 7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}, & \text{Scope Changed} \end{cases}$$

$$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})] \quad (۱۲)$$

پراکندگی پارامتر *Impact* برای تمامی آسیب‌پذیری‌های شناخته شده از نسخه ۲ CVSS استخراج شده و نتایج در جدول (۲) نشان داده شده است. هر ترکیب نوشته شده در جدول (۲)، به ترتیب از چپ به راست بیانگر تاثیر بهره‌برداری از یک آسیب‌پذیری روی سه پارامتر امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری است و ستون با نام درصد نشانگر کسری از آسیب‌پذیری‌های شناخته شده است که بهره‌برداری از آنها پارامترهای امنیتی شبکه را به شکل بیان شده در ستون ترکیب، تحت تاثیر قرار می‌دهد. در راستای نشان‌دادن کارایی روش پیشنهادی برای ارزیابی تاثیر، لازم به ذکر است که بنا به نتایج موجود در جدول (۲)، تاثیر بهره‌برداری از ۳۵/۵ درصد آسیب‌پذیری‌های موجود روی پارامترهای امنیتی، ترکیب‌های NNP, PNP, PNN است. CVSS طبق رابطه‌های (۱۱) و (۱۲)، تاثیر بهره‌برداری از این کسر از آسیب‌پذیری‌ها را یکسان گزارش می‌کند در صورتی که بر اساس روش پیشنهادی (جدول ۲)، تاثیر بهره‌برداری از آسیب‌پذیری‌های متعلق به این سه دسته با هم متفاوتند. بنابراین، روش ارائه شده در این مقاله، مجزاسازی کارتری از آسیب‌پذیری‌ها را نسبت به CVSS از نظر میزان خطر وارده به سیستم ممکن می‌سازد.

دقت شود که بررسی آماری فوق روی نسخه ۲ از CVSS انجام شده است. عدم انجام بررسی آماری روی نسخه ۳ از CVSS، محدود بودن پایگاه داده آن به آسیب‌پذیری‌هایی است که از سال ۲۰۱۶ به بعد ثبت شده‌اند. از طرف دیگر، تفاوت روند ارزیابی تاثیر بهره‌برداری از آسیب‌پذیری روی سه پارامتر امنیتی فوق در معادل کمی است که در دونسخه فوق به آسیب‌پذیری نسبت داده می‌شود.

برای هر یک از آسیب‌پذیری‌های موجود در هر مسیر حمله، پارامتر تاثیر از جدول ۲ استخراج شده و تاثیر یک مسیر حمله طبق رابطه (۱۳)، میانگین هندسی تاثیر آسیب‌پذیری‌هایی خواهد بود که در این مسیر حمله قرار دارند. استفاده از میانگین هندسی به جای میانگین حسابی بدین دلیل است که میانگین هندسی به میزان کمتری تحت تاثیر داده‌های خیلی بزرگ قرار دارد. در (۱۳)،  $Impact(vul_i)$  از تقسیم رتبه متناظر با آسیب‌پذیری از جدول (۲) بر ۲/۷ حاصل می‌شود.

امنیتی دسترسی‌پذیری، یکپارچگی و محرمانگی است که توسط CVSS در سه سطح بدون تاثیر، جزئی و کامل امتیازدهی می‌شود. معادل عددی این سطوح کیفی در دونسخه ۲ و ۳ از CVSS در جدول (۱) نشان داده شده است.

جدول (۱): معادل کمی پارامتر Impact در دو نسخه CVSS

سطح کیفی Impact	معادل کمی در نسخه ۲	معادل کمی در نسخه ۳
بدون تاثیر	۰	۰
جزئی	۰/۲۷۵	۰/۲۲
کامل	۰/۶۶	۰/۵۶

مشکل اساسی رابطه (۱۱)، ماهیت متقارن آن است. زیرا منجر به این مسئله می‌شود که میزان تاثیر دو آسیب‌پذیری با پارامترهای تاثیر متفاوت، یکسان گزارش شود. این مسئله گوناگونی امتیازات برای رتبه‌بندی آسیب‌پذیری‌ها را محدود می‌سازد و مانع از این می‌شود که اولویت‌بندی کارایی از حملات داشته باشیم. برای مثال در نسخه ۲، دو آسیب‌پذیری که زیرپارامترهای تاثیر آنها عبارتست از (۰/۲۷۵ و ۰/۶۶) و (۰ و ۰/۶۶) پارامتر تاثیر آنها بنابر CVSS یکسان و برابر ۷/۸ گزارش می‌شود. اما در واقعیت ماهیت این دو آسیب‌پذیری متفاوت هست.

علاوه بر این، در CVSS، اهمیت نسبی این سه پارامتر امنیتی نادیده گرفته شده است. طبق [۵]، در بین سه پارامتر امنیتی مذکور، تاثیر مخرب محرمانگی از یکپارچگی و یکپارچگی از دسترسی‌پذیری بیشتر است. زیرا سرعت افشای تاثیر مخرب مختل شدن پارامتر محرمانگی روی سرویس‌های امنیتی از یکپارچگی و یکپارچگی از دسترسی‌پذیری پایین‌تر است. در نتیجه، در نظر گرفتن اهمیت نسبی مذکور در بین سه پارامتر امنیتی به منظور ارزیابی دقیق از میزان خطر یک حمله از ضروریات است.

در این مقاله، با در نظر گرفتن اهمیت نسبی این سه پارامتر امنیتی، راه‌کاری برای حل چالش ماهیت متقارن چگونگی محاسبه تاثیر در CVSS پیشنهاد شده است که آسیب‌پذیری‌ها را بر اساس میزان تاثیر آنها روی سه پارامتر امنیتی، طبق جدول ۲ در ۲۷ سطح مختلف قرار می‌دهد. این در صورتی است که بر اساس (۱۱)، CVSS نسخه ۲، حداکثر ۱۱ سطح مختلف از تاثیر را برای امتیازدهی به سیل عظیمی از آسیب‌پذیری‌های موجود در نظر می‌گیرد.

$$Impact = 10.41 \times (1 - (1 - I_C) \times (1 - I_I) \times (1 - I_A)) \quad (۱۱)$$

همچنین، طبق رابطه (۱۲) در نسخه ۳ از CVSS، تنها ۲۲ امتیاز برای امتیازدهی به انبوهی از آسیب‌پذیری‌ها استفاده می‌شود.

آسانی آن، با استفاده از روابط (۲) تا (۴) انجام می‌شود. دقت شود از آنجایی که معیارهای CVSS تنها برای آسیب‌پذیری‌های شناخته‌شده قابل استخراج است. برای مقاردهی به پارامتر پیچیدگی دسترسی به آسیب‌پذیری‌هایی روز صفر، از سیاست CVSS برای امتیازدهی به آسیب‌پذیری‌های شناخته شده‌ای استفاده شده که اطلاعات کافی برای مقاردهی به معیارهای CVSS از آنها در دسترس نیست. بنابراین CVSS، چنین آسیب‌پذیری‌هایی کمترین پیچیدگی دسترسی (۰/۷۱) در نسخه ۲ و ۰/۷۷ در نسخه ۳ را دارا هستند [۱۶]. پارامتر Exploitability نیز برابر با کمترین مقدار تابع توزیع Pareto با پارامترهای مشخص شده در (۴) در نظر گرفته می‌شود که با ۰/۸۱۲۲ برابر است.

تاثیر بهره‌برداری از آسیب‌پذیری ناشناخته روی پارامترهای امنیتی شبکه: براساس اطلاعات موجود در جدول (۲)، آسیب‌پذیری‌های با تاثیر PPP بر روی پارامترهای امنیتی، بالاترین درصد را در بین تمامی ترکیبات ممکن از تاثیر دارا هستند. از این‌رو در این مقاله، تاثیر برای آسیب‌پذیری‌های ناشناخته برابر امتیاز متناظر با PPP یا ۱۷ در نظر گرفته می‌شود.

به این ترتیب، محاسبه میزان خطر حملات روز صفر توسط سیستم پیشنهادی قابل انجام و ارزیابی خطر سایر حملات چند مرحله‌ای با در نظر گرفتن وجود آسیب‌پذیری‌های روز صفر نیز، ممکن خواهد بود.

این تقسیم به منظور نرمال سازی Impact برای قرار گرفتن در محدود ۰ تا ۱۰ (همانند CVSS) انجام می‌شود.

$$Impact(path) = \left( \prod_{i=1}^n Impact(vul_i) \right)^{1/n} \quad (13)$$

همان‌طور که گفته شد متناظر با هر حمله، عموماً بیش از یک مسیر حمله وجود دارد. بنابراین، برای ارزیابی تاثیر یک حمله چندمرحله‌ای، تمامی مسیرهای حمله باید توأم در نظر گرفته شوند. در این رابطه دقت شود که از آنجایی که مهاجم در یک زمان نمی‌تواند بیش از یک مسیر حمله را طی کند، تاثیر بهره‌برداری از یک حمله چندمرحله‌ای را برابر با تاثیر بهره‌برداری از مسیری در نظر می‌گیریم که پارامتر تاثیر آن در بین تمامی مسیرهای منتهی به آن حمله بالاتر باشد. (رابطه (۱۴))

بنابراین، با استفاده از روش پیشنهادی تخمین خطر حمله چند مرحله‌ای با استفاده از رابطه (۱) ممکن خواهد بود.

$$Impact(Attack) = \max\{Impact(path_i)\}, \quad (14)$$

$i = 1: \text{number of paths}$

### ۵-۳- چگونگی تخمین خطر برای حملات ناشناخته

ویژگی مهم سیستم ارزیابی خطر پیشنهادی در این مقاله، توانایی ارزیابی خطر حملات چندمرحله‌ای با در نظر گرفتن تاثیر وجود آسیب‌پذیری‌های روز صفر در شبکه‌های کامپیوتری است. احتمال بهره‌برداری از یک آسیب‌پذیری روز صفر و تاثیر رخداد آن روی پارامترهای امنیتی شبکه بصورت زیر قابل تخمین است:

- احتمال بهره‌برداری از آسیب‌پذیری روز صفر: محاسبه احتمال بهره‌برداری از آسیب‌پذیری روز صفر و درجه

جدول (۲): رتبه بندی پارامتر Impact برای ترکیب‌های ممکن از تاثیر بهره‌برداری از آسیب‌پذیری روی محرمانگی، یکپارچگی و دسترسی پذیری

ترکیب	رتبه	درصد	ترکیب	رتبه	درصد	ترکیب	رتبه	درصد
NNN	۱	۰/۰۳۰۳	NPP	۵	۱/۱	CPN	۲۲	۰/۰۱
PPP	۱۷	۳۳	PPN	۱۶	۲/۷	PCN	۱۹	۰
CCC	۲۷	۳۱	PNP	۱۱	۰	PNC	۱۲	۱/۰۴۴ ۰۱
NNP	۲	۹/۶	NCC	۹	۰/۱۴	PCC	۲۱	۰/۰۱
NPN	۴	۱۶	CCN	۲۵	۰/۰۹	CPC	۲۴	۰
PNN	۱۰	۹/۹	CNC	۱۵	۰	CCP	۲۶	۰
NNC	۳	۳/۹	NCP	۸	۰	PPC	۱۸	۰/۰۸
NCN	۷	۰/۱	CNP	۱۴	۰	CPP	۲۳	۰/۰۳
CNN	۱۳	۰/۹۳	NPC	۶	۰/۰۴۲۷	PCP	۲۰	۰

در ارزیابی خطر حملات، نتایج ارزیابی خطر چارچوب پیشنهادی با تخمین CVSS از خطر این حملات مقایسه شده است. دقت شود که CVSS، علاوه بر ارزیابی کمی، براساس مقادیر امتیاز پایه ارزیابی کیفی نیز از میزان خطر آسیب‌پذیری‌ها به‌صورت جدول (۳) انجام می‌دهد. از آنجایی که اطلاعات متناظر با آسیب‌پذیری‌های شبکه تحت بررسی تنها در نسخه ۲ از CVSS موجود هستند، استخراج اطلاعات آسیب‌پذیری‌ها از نسخه ۲ انجام شده و سطوح کیفی فقط برای نسخه ۲ در جدول (۳) نمایش داده شده است.

پیکره‌بندی شبکه مورد تست در شکل (۲) و گراف حمله متناظر با حمله مهاجم به شبکه برای دستیابی به دسترسی سطح ریشه روی میزبان شماره ۳ نیز در شکل (۳) نشان داده شده است. اطلاعات پیکره‌بندی شبکه در قالب قوانین فایروال در جدول (۴) و اطلاعات آسیب‌پذیری‌های آن نیز در جدول (۵) آمده است. جدول (۶)، نتایج اعمال چارچوب پیشنهادی روی این شبکه است.

در جدول (۶)، مقدار خطر محاسبه شده برای حملات چندمرحله‌ای شبکه شکل (۲) توسط روش پیشنهادی و میزان خطری که CVSS تحت عنوان امتیاز پایه برای این حملات در نظر می‌گیرد، نشان داده شده است. با تجزیه و تحلیل اطلاعات جدول (۶)، نتایج زیر قابل استخراج هستند:

نتایج موجود در این جدول منعکس‌کننده بالاتر بودن پراکندگی خطر آسیب‌پذیری‌ها در روش پیشنهادی نسبت به CVSS است بدین دلیل که بر خلاف CVSS، روش پیشنهادی میزان خطر مجزایی را برای هر حمله چند مرحله‌ای مشخص می‌سازد. این ویژگی، اولویت‌بندی آسیب‌پذیری‌ها را بر اساس میزان خطر وارده به سیستم به‌منظور مقاومت‌سازی کم‌هزینه ممکن می‌سازد.

کاهش سطوح کیفی در روش پیشنهادی، یکی دیگر از نتایج اعمال سیستم پیشنهادی روی شبکه مذکور است که منجر به صرفه‌جویی در بودجه امنیتی در فرآیند مقاومت‌سازی خواهد شد. واضح است تخصیص هزینه برای مقاومت‌سازی سیستم‌های کامپیوتری در برابر حملات، بر اساس سطح کیفی خطر حمله انجام می‌شود.

کاهش قابل توجه در میزان خطر هر آسیب‌پذیری به دلایل زیر اتفاق افتاده است:

جدول (۳): تفسیر کیفی CVSS از خطر آسیب‌پذیری‌ها

سطح کیفی	محدوده امتیاز پایه
پایین	[۰-۳/۹]
متوسط	[۴-۶/۹]
بالا	[۷-۱۰]

## ۶- مقایسه روش پیشنهادی با CVSS جهت ارزیابی کارایی

طبق مستندات CVSS، تنها تعداد محدودی امتیاز مختلف (کمتر از ۱۰۰ امتیاز) برای امتیازدهی به سیل عظیمی از آسیب‌پذیری‌های موجود قابل استفاده هستند [۱۶]. این مسئله، استفاده از این سیستم امتیازدهی را در مجزاسازی آسیب‌پذیری‌ها از نقطه‌نظر خطر وارده به سیستم محدود می‌سازد.

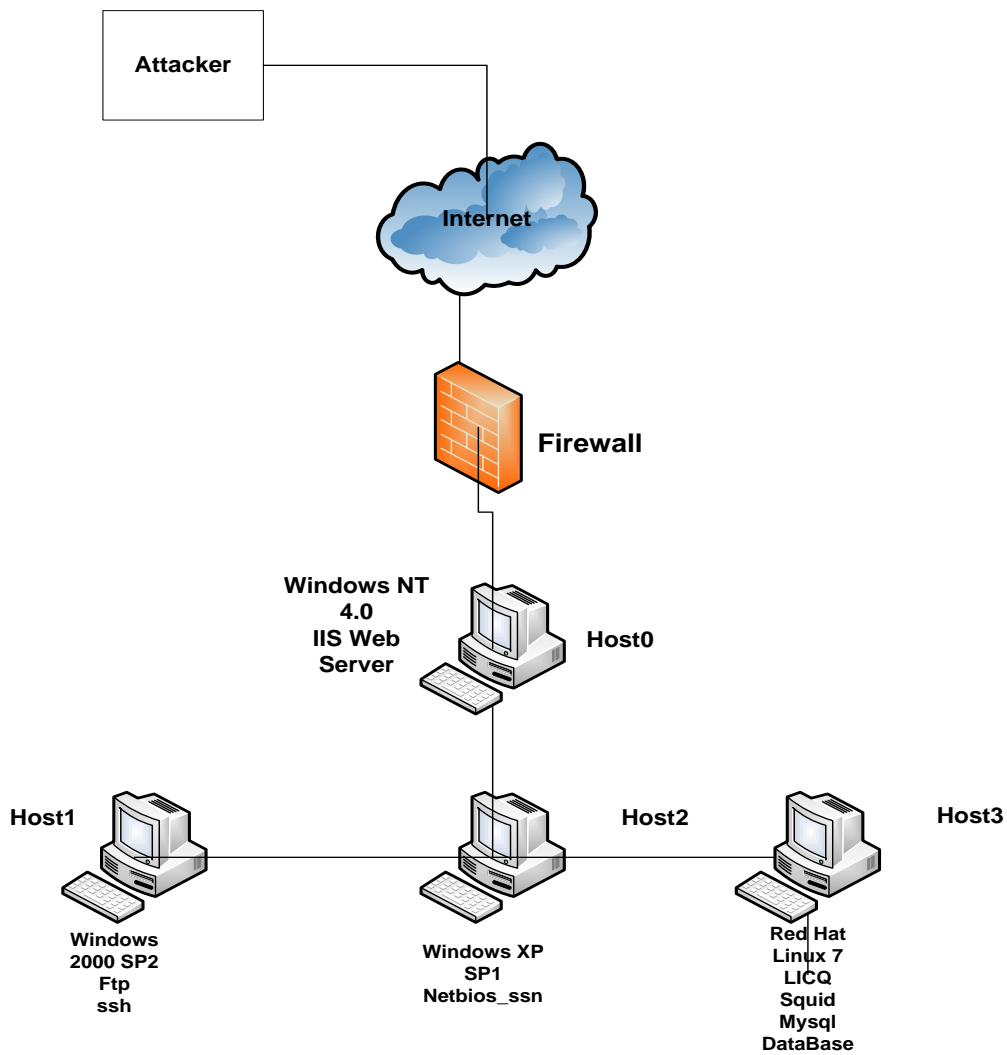
در این مقاله، در نظر گرفتن عوامل زمانی در تخمین احتمال رخداد حملات و پیشنهاد راهکار جدید برای تخمین تاثیر رخداد حملات روی پارامترهای امنیتی با هدف بهبود مشکل فقدان گوناگونی امتیازات بوده است. بنا بر (۴)، برد تابع توزیع Pareto در محدوده [۰/۸۱۲۲ و ۱] قرار دارد. از آنجایی که برد این تابع بی‌شمار امتیاز مختلف را پوشش می‌دهد و این تابع یک به یک است، بی‌شمار امتیاز مختلف برای مجزاسازی احتمال بهره‌برداری از آسیب‌پذیری‌ها با سنین متمایز در دسترس است.

از طرفی، همان‌طور که گفته شد، طبق جدول (۲)، تاثیر بهره‌برداری از ۳۵/۵ درصد آسیب‌پذیری‌های موجود روی پارامترهای امنیتی، ترکیب‌های NNP, NPN, PNN است. CVSS طبق (۱۲) و (۱۳)، تاثیر بهره‌برداری از این کسر از آسیب‌پذیری‌ها را یکسان گزارش می‌کند. به‌عبارت دیگر، ۳۵/۵ درصد از آسیب‌پذیری‌های شناخته شده براساس CVSS، از نظر میزان تاثیر روی پارامترهای امنیتی یکسان هستند. در صورتی‌که، روش پیشنهادی (جدول ۲)، تاثیر بهره‌برداری از آسیب‌پذیری‌های متعلق به این سه دسته را متفاوت گزارش می‌کند. این ویژگی تاییدی است بر بهبود روش پیشنهادی نسبت به CVSS در مجزاسازی حملات از نقطه‌نظر خطر وارده به سیستم‌های کامپیوتری.

در بخش آتی نتایج اعمال روش پیشنهادی روی دو نمونه شبکه نوعی نشان داده شده است.

## ۷- نتایج تجربی

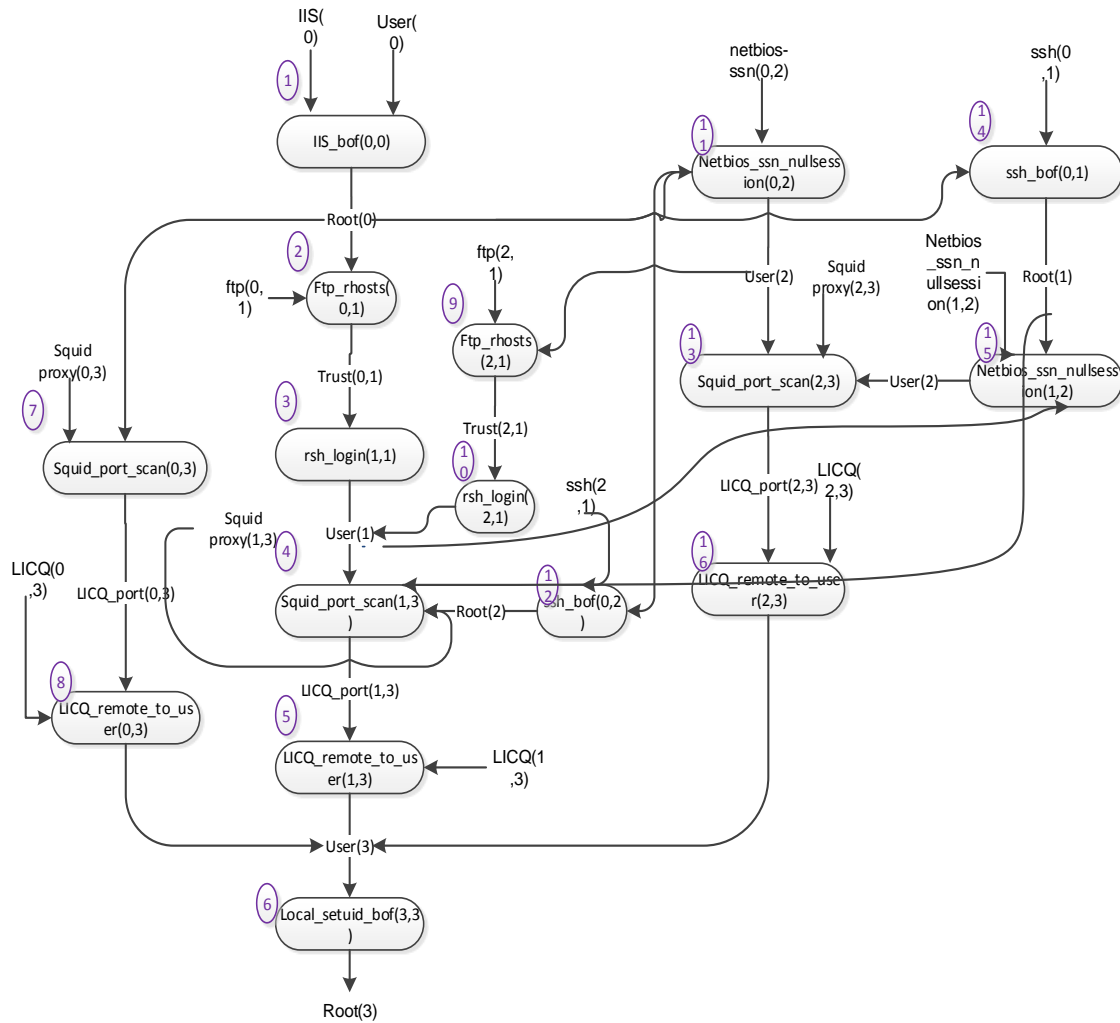
پیاده‌سازی چارچوب پیشنهادی توسط نرم‌افزار Matlab و در یک سیستم کامپیوتری با RAM با اندازه ۸ گیگا بایت و CPU با قدرت ۲/۲ گیگا هرتز انجام شده است. روش پیشنهادی با دریافت گراف حمله هر شبکه میزان خطر بهره‌برداری از آسیب‌پذیری‌های آن را مشخص می‌سازد. سیستم پیشنهادی روی تعدادی شبکه نوعی که در کارهای مشابه از جمله [۲۸] استفاده می‌شود اعمال شده و نتایج ارزیابی خطر برای یک نمونه از این شبکه‌ها در ادامه بیان شده است. به‌منظور بیان توانایی روش پیشنهادی



شکل (۲): شبکه مورد تست [۲۸]

جدول (۴): اطلاعات پیکره‌بندی شبکه شکل (۲)

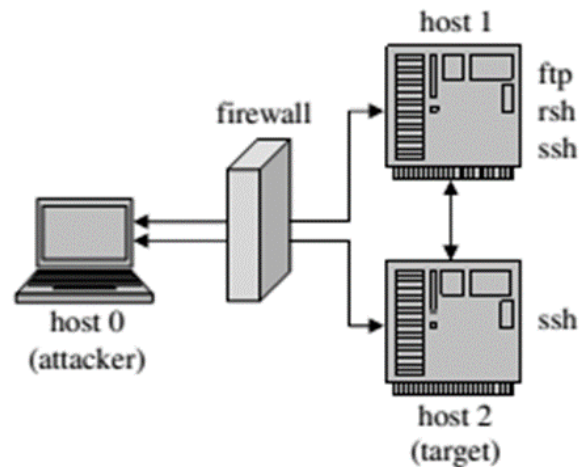
میزبان	مهاجم	H0	H1	H2	H3
مهاجم	localhost	IIS	هیچ یک	هیچ یک	هیچ یک
H0	همه	localhost	ftp,ssh	همه	Squid, LICQ
H1	همه	IIS	localhost	همه	Squid, LICQ
H2	همه	IIS	ftp,ssh	localhost	Squid, LICQ
H3	همه	IIS	ftp,ssh	همه	localhost



شکل (۳): گراف حمله شبکه مورد تست [۲۸]

در نظر گرفتن ارتباط بین آسیب‌پذیری‌ها: بر اساس گراف حمله، بهره‌برداری از یک آسیب‌پذیری مستلزم بهره‌برداری از تعدادی دیگر از آسیب‌پذیری‌ها است که این مسئله بهره‌برداری از آن را دشوارتر می‌سازد. در نتیجه، میزان خطر واقعی آن نسبت به میزان خطر گزارش شده توسط CVSS کمتر است.

در نظر گرفتن عوامل زمانی: ارزیابی خطر آسیب‌پذیری با در نظر گرفتن عوامل زمانی از جمله، احتمال در دسترس بودن ابزارهای مورد نیاز برای بهره‌برداری از آن، کاهش میزان سختی بهره‌برداری از آسیب‌پذیری و بالاتر رفتن احتمال بهره‌برداری از آن توسط مهاجمان را در گذر زمان مد نظر قرار می‌دهد.



شکل (۴): شبکه شامل آسیب‌پذیری ناشناخته [۲۱]

جدول (۵): اطلاعات آسیب‌پذیری شبکه شکل ۲

CVE	آسیب‌پذیری	محرمانگی	یکپارچگی	دسترسی‌پذیری	پیچیدگی دسترسی	سن تا تاریخ (۲۰۱۵/۱۱/۱۱)
CVE-2002-0364	IIS buffer overflow	p	p	p	۰/۷۱	۴۸۵۴
CVE-2008-1396	ftp rhost overwrite	p	n	n	۰/۶۱	۲۷۶۸
CVE-1999-1455	Sshd bufferoverflow	p	p	p	۰/۷۱	۵۷۶۶
CVE-2003-0661	Net bios ssn nullsession	p	n	n	۰/۷۱	۴۲۸۲
CVE-1999-0180	rsh login	p	p	p	۰/۷۱	۶۸۶۱
CVE-2001-0439	LICQ remote to user	p	p	p	۰/۷۱	۵۲۲۰
CVE-2001-1030	Squid-port-scan	p	p	p	۰/۷۱	۵۲۰۴
CVE-2006-3368	Local -setuid-bof	p	n	n	۰/۷۱	۳۳۹۱

جدول (۶): نتایج اعمال چارچوب پیشنهادی روی شبکه مورد تست

شماره آسیب‌پذیری	امتیاز پایه CVSS	سطح کیفی (CVSS)	Prob (احتمال)	Impact (تاثیر)	Risk (خطر)	سطح کیفی (روش پیشنهادی)	اولویت برای حذف (طبق روش پیشنهادی)
۱	۷/۵	بالا	۰/۶۹۵۳	۶/۲۹۶۳	۶/۱۶۶۱	متوسط	۵
۲	۴/۳	متوسط	۰/۵۹۵۴	۴/۸۲۹۰	۴/۰۴۹۶	متوسط	۱۳
۳	۷/۵	بالا	۰/۶۹۶۶	۶/۲۹۶۳	۶/۱۷۷۳	متوسط	۱
۴	۷/۵	بالا	۰/۴۷۶۱	۶/۲۹۶۳	۴/۲۲۲۵	متوسط	۱۲
۵	۷/۵	بالا	۰/۵۱۱۷	۶/۲۹۶۳	۴/۵۳۷۸	متوسط	۱۰
۶	۵	متوسط	۰/۵۳۷۴	۶/۲۹۶۳	۴/۷۶۵۶	متوسط	۸
۷	۷/۵	بالا	۰/۶۹۵۶	۶/۲۹۶۳	۶/۱۶۸۵	متوسط	۴
۸	۷/۵	بالا	۰/۶۹۵۶	۶/۲۹۶۳	۶/۱۶۸۶	متوسط	۳
۹	۴/۳	متوسط	۰/۵۹۵۴	۴/۴۲۰۳	۳/۷۰۶۹	پایین	۱۵
۱۰	۷/۵	بالا	۰/۶۹۶۶	۵/۵۱۴۱	۵/۴۰۹۹	متوسط	۶
۱۱	۵	متوسط	۰/۶۹۴۹	۴/۸۲۹۰	۴/۷۲۶۵	متوسط	۹
۱۲	۷/۵	بالا	۰/۶۹۶۰	۵/۲۷۵۶	۵/۱۷۱۳	متوسط	۷
۱۳	۷/۵	بالا	۰/۴۸۶۳	۵/۶۶۲۳	۳/۸۷۸۴	پایین	۱۴
۱۴	۷/۵	بالا	۰/۶۹۶۰	۶/۲۹۶۳	۶/۱۷۱۸	متوسط	۲
۱۵	۵	متوسط	۰/۴۵۴۸	۵/۵۱۴۱	۳/۵۳۲۵	پایین	۱۶
۱۶	۷/۵	بالا	۰/۵۲۳۹	۵/۷۶۳۴	۴/۲۵۲۵	متوسط	۱۱

خطر شبکه در برابر حملات روز صفر و بررسی مقاومت شبکه در برابر حملات روز صفر استفاده شده است.

در این شبکه سرویس انتقال فایل (ftp) شامل آسیب‌پذیری CVE-2001-0886 است و سرویس rsh آسیب‌پذیری ۱۴۵۰- CVE-۱۹۹۹ را به سیستم اضافه کرده است.

CVE-۲۰۱۰-۳۸۱۴ آسیب‌پذیری سرریز بافر است که در میزان شماره ۲ وجود دارد. علاوه بر این، سرویس ssh که روی هر دو میزبان وجود دارد آسیب‌پذیری شناخته شده‌ای ندارد. در این شبکه همچنین فرض شده فایروال در مقابل حملات مقاوم

#### ۱-۷. نتایج اعمال روش پیشنهادی روی یک شبکه شامل آسیب‌پذیری‌های ناشناخته

در این بخش، نتایج به‌کارگیری سیستم ارزیابی خطر پیشنهادی برای یک شبکه شامل آسیب‌پذیری‌های روز صفر نمایش داده شده است. شبکه مورد نظر در شکل (۴) و گراف حمله متناظر با حمله اتخاذ سطح ریشه روی میزبان شماره ۲ این شبکه، در شکل (۵) نشان داده شده است.

این مثال نوعی، در کارهای مشابه از جمله [۲۱]، به‌منظور ارزیابی

آسیب‌پذیری‌ها را به شکل قابل توجهی نسبت به CVSS بهبود داده است.

در آینده قصد داریم، با در نظر گرفتن سایر عوامل زمانی تاثیر گذار در تخمین خطر بهره‌برداری شدن از آسیب‌پذیری از جمله، احتمال معرفی اصلاحیه‌ها در گذر زمان و مد نظر قرار دادن عوامل محیطی مانند سیاست‌های امنیتی شبکه مورد بررسی، ارزیابی دقیق‌تری از رخداد حملات در شبکه‌های مختلف داشته باشیم.

## ۹. مراجع

- [1] S. Abraham and S. Nair, "A Predictive Framework for Cyber Security Analytics Using Attack Graphs", International Journal of Computer Networks & Communications (IJNC), vol. 7, no. 1, pp. 1-17, 2015.
- [2] C. Frühwirth and T. Männistö, "Improving CVSS-based vulnerability prioritization and response with context information". Proceedings of International Workshop on Security Measurement and Metrics (MetriSec), pp. 535-544, 2009.
- [3] H. Ghani, J. Luna and N. Suri, "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, 2013.
- [4] S. H. Houmb and V. N. L. Franqueira, "Estimating ToE Risk Level Using CVSS", International Conference on Availability, Reliability and Security, pp. 718-725, 2009.
- [5] G. Spanos, A. Sioziou and L. Angelis, "WIVSS: a new methodology for scoring information systems vulnerabilities". Panhellenic Conference on Informatics, pp. 83-90, 2013.
- [6] MITRE CVE, "Common Vulnerabilities and Scoring", <https://cve.mitre.org/>, 2018.
- [7] OSVDB, "Open Sourced Vulnerability Database", <http://osvdb.org/>, 2018.
- [8] Nessus, "Vulnerability Assessment Solution", <http://www.tenable.com/products/nessus-vulnerability-scanner>, 2018.
- [9] L. GALLON, "Vulnerability discrimination using cvss framework", In New Technologies", Mobility and Security (NTMS), 4th IFIP International Conference, pp. 1-6, 2010.
- [10] N. Idika and B. Bhargava, "Extending Attack Graph-based Security Metrics and Aggregating Their Application", IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1 pp. 1-12, 2010.
- [11] T. Hamid, C. Maple, and P. Sant, "Methodologies to Develop Quantitative Risk Evaluation Metrics", International Journal of Computer Applications, vol. 48, no. 14, pp. 17-24, 2012.
- [12] L. Xie, X. Zhang and J. Zhang, "Network Security Risk Assessment Based on Attack Graph", Journal of Computers, vol. 8, no. 9, pp. 2339-2347, 2013.
- [13] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A Weakest-Adversary Security Metric for Network Configuration Security Analysis," Proc. Second ACM Workshop Quality of Protection, pp. 31-38, 2006.
- [14] IBM, "X-Force frequently asked questions", <http://www-935.ibm.com/services/us/iss/xforce/faqs.html>, 2018

است. هدف مقاومت شبکه در برابر کسب دسترسی سطح ریشه روی میزبان شماره ۲ توسط مهاجم می‌باشد. نتایج اعمال روش پیشنهادی روی شبکه مذکور در جدول (۷) نشان داده شده است. همان‌طور که گفته شد، با استفاده از روش پیشنهادی، علاوه بر میزان خطر آسیب‌پذیری‌های صفر، میزان خطر آسیب‌پذیری‌های شناخته شده نیز قابل تخمین است.

جدول (۷): ارزیابی خطر شبکه شکل (۵) توسط چارچوب پیشنهادی

آسیب‌پذیری	Prob (احتمال)	Impact (تاثیر)	Risk (خطر)
Ssh(0,1)	۰/۵۷۶۶	۶/۲۹۶۳	۵/۱۱۳۶
Ssh (1,2)	۰/۳۳۲۹	۶/۲۹۶۳	۲/۹۵۲۴
Ssh (0,2)	۰/۵۷۶۶	۶/۲۹۶۳	۵/۱۱۳۶
Ftp_rhost(0,1)	۰/۵۷۶۶	۶/۲۹۶۳	۵/۱۱۳۶
Rsh(0,1)	۰/۵۷۶۶	۶/۲۹۶۳	۵/۱۱۳۶
Bof (2,2)	۰/۳۶۳۳	۱۰	۵/۱۱۳۶

## ۸. نتیجه‌گیری

نفوذ شبکه‌های کامپیوتری در عرصه‌های مختلف تجاری، اقتصادی، آموزشی، پزشکی و ...، بروز حملات در شبکه‌های کامپیوتری را به یک مسئله ویرانگر در زندگی بشر تبدیل کرده است. از این‌رو، امن‌سازی شبکه‌های کامپیوتری در برابر حملات یک نیازمندی اجتناب‌ناپذیر به‌شمار می‌آید.

محدودیت در بودجه سازمان‌ها مقاومت‌سازی به صورت کم‌هزینه را به یک ضرورت اجتناب‌ناپذیر تبدیل کرده است. این امر ممکن نخواهد بود جز با امتیازدهی به آسیب‌پذیری‌ها به منظور پیدا کردن پرخطرترین حملات. پرستفاده‌ترین سیستم امتیازدهی موجود یا CVSS، توصیفی کمی را از میزان خطر یک آسیب‌پذیری مشخص می‌سازد. اما، این کمی‌سازی، تنها بر اساس خصوصیات ذاتی و صرف‌نظر کردن از عوامل زمانی از جمله احتمال وجود ابزارهای بهره‌برداری از آن آسیب‌پذیری صورت می‌گیرد. بنابراین، میزان خطر مشخص شده توسط این سیستم، منعکس‌کننده خطر واقعی نخواهد بود. همچنین، CVSS تعداد محدودی امتیاز مختلف (کمتر از ۱۰۰) را به منظور امتیازدهی به سیل عظیمی از آسیب‌پذیری‌ها به کار می‌برد. در نتیجه، مجزاسازی دقیق حملات به منظور تعیین پرخطرترین آنها توسط این سیستم ممکن نخواهد بود. در این مقاله، با هدف تعیین حملات پرخطر به منظور مقاوم‌سازی کم‌هزینه، سیستمی برای امتیازدهی به آسیب‌پذیری‌ها معرفی شده است که تعیین میزان خطر را با در نظر گرفتن عوامل زمانی انجام می‌دهد. در نظر گرفتن عوامل زمانی و معرفی راه‌کار جدیدی برای سنجش تاثیر رخداد حملات روی پارامترهای امنیتی شبکه، گسترده‌تری

- Homeland Security (HST)*, Waltham, MA, pp. 1-5 , 2016.
- [33] E. Weintraub, "Evaluating Damage Potential in Security Risk Scoring Models". *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 5, pp. 345-353, 2016.
- [34] A. Younis, Y.K. Malaiya and I. Ray, "Evaluating CVSS Base Score Using Vulnerability Rewards Programs". In: Hoepman JH., Katzenbeisser S. (eds) *ICT Systems Security and Privacy Protection. SEC 2016. IFIP Advances in Information and Communication Technology*, Springer, Cham, vol. 471, pp. 62-75, 2016.
- [35] P. Johnson, A. Vernotte, D. Gorton, M. Ekstedt and L. Robert. "Quantitative Information Security Risk Estimation Using Probabilistic Attack Graphs", (eds) *Risk Assessment and Risk-Driven Quality Assurance. RISK 2016. Lecture Notes in Computer Science*, vol 10224. Springer, Cham, pp. 37-5., 2017.
- [36] I. Kotenko and A. Chechulin, "Fast Network Attack Modeling and Security Evaluation based on Attack Graphs". *Journal of Cyber Security and Mobility*. Vol. 3, pp. 27-46., 2014.
- [37] J. C. Acosta, E. Padilla and J. Homer, "Augmenting attack graphs to represent data link and network layer vulnerabilities," *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Baltimore, MD, pp. 1010-1015 , 2016.
- [38] W. Zhou, H. Zhang and Li. Q.-M. "A network risk assessment method based on attack-defense graph model", *Journal of Computers (Taiwan)*. vol. 28. pp. 105-118, 2017
- [39] Keramati M. "An Attack Graph Based Method for Predictive Risk Evaluation of Zero-Day Attacks" , *IJICTR*, vol. 9, no. 3, pp. 7-16, 2017
- [40] Keramati M. "Dynamic Risk Assessment System for the Vulnerability Scoring" . *IJICTR.*, vol. 9, no.4, pp. 57-68, 2017.
- [41] M.Keramati, "Attack Graph Based system for Risk Assessment of Multi-Step Attacks", *Proceedings of the 2nd International Conference on Combinatorics, Cryptography and Computation (I4C2017)*, pp. 171-182, 2017
- [42] V. Hosseinnezhad, A. Pourhaji Kazem, "Bayesian Networks Based Trust Model in Social Networks" , *Journal of Electrical & Cyber Defence*, vol. 6 , no 4, pp. 29-38, 2018.
- [15] Qualys, "Severities Knowledge Base "http://www.qualys.com/research/knowledge/severity/ , 2018
- [16] CVSS," Common Vulnerability Scoring System " https://www.first.org/cvss, , 2018
- [17] CVE," Common Vulnerabilities and Exposures" , https://cve.mitre.org/, ,2018
- [18] K. Scarfone and P. Mell. "An Analysis of CVSS Version 2 Vulnerability Scoring," *Proceeding of 3rd International Symposium on Empirical Software Engineering and Measurement*, pp. 516 – 525, 2009.
- [19] " Mozilla, "Mozilla Foundation Security Advisories" "http://www.mozilla.org/security/announce/, 2018.
- [20] Q. Liu and Y. Zhang, "VRSS: A new system for rating and scoring vulnerabilities", *Computer Communications*, vol. 34, no. 3, pp. 264-273, 2011
- [21] M. Albanese, S. Jajodia, A. Singhal and L. Wang. "An Efficient Framework for Evaluating the Risk of Zero-Day Vulnerabilities". In *E-Business and Telecommunications*, Springer. pp. 322-340, 2014.
- [22] W. Nzoukou, L. Wang, S. Jajodia and A. Singhal, "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, 2013.
- [23] NVD." National Vulnerability DataBase", https://nvd.nist.gov, 2018.
- [24] F.Chen, D.Liu,Y.Zhang and J.Su, "A Scalable Approach to Analyzing Network Security using Compact Attack Graphs", *Journal Of Networks*, vol. 5 ,no. 5, pp. 543-550, 2010.
- [25] H. Joh and Y. K. Malaiya, "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics". *Proc. Int. Conference on Security and Management*. pp. 10-16, 2011.
- [26] S. Frei, S. May, U. Fiedler and B. Plattner. "Large-scale vulnerability analysis", *LSAD '06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*. pp. 131–138, 2006.
- [27] E. Triantaphyllou and K. Baig," The Impact of Aggregating Benefit and Cost Criteria in Four MCDA Methods", *IEEE Transactions on Engineering Management*, vol. 52, no. 2, pp. 213-226, 2005.
- [28] N.Ghosh and S.K.Ghosh, "An Approach for Security Assessment of Network Configurations Using Attack Graph", *1st International Conference on Networks and Communications*, IEEE, pp. 283-288, 2009.
- [29] S. Abraham and S. Nair., "Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains". *Journal of Communications.*, vol. 9 , no. 12, pp. 899-907, 2014.
- [30] Y. Ru *et al.*, "Risk assessment of cyber attacks in ECPS based on attack tree and AHP," 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Changsha, pp. 465-470 , 2016.
- [31] S. c. Liu and Y. Liu, "Network security risk assessment method based on HMM and attack graph model," 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Shanghai, pp. 517-522, 2016.
- [32] A. V. Sathanur and D. J. Haglin, "A novel centrality measure for network-wide cyber vulnerability assessment," 2016 *IEEE Symposium on Technologies for*