Journal of Electronical & Cyber Defence
Vol. 9, No. 1, 2021, Serial No. 33

A Security Model Based Approach for Dynamic Risk Assessment of Multi-Step Attacks in Computer Networks

M. Keramati*

*Faculty Member of Semann University

(Received: 07/08/2020, Accepted: 26/10/2020)

ABSTRACT

Multi-facet dependency of human life on computer networks and its widespread vulnerability has made network robustness a necessity. With cost as a limiting factor, network robustness is considered as a great challenge for network administrators. This goal would be achievable by prioritizing the vulnerabilities based on their risk and choosing the most hazardous ones for elimination. Nowadays, CVSS is being used as the most widely used vulnerability scoring system. In CVSS, vulnerability ranking is based on its intrinsic features while temporal features such as the probability of developing exploitation tools, are ignored. So, dynamic risk evaluation is not possible with CVSS and it is incapable of performing effective vulnerability discretion. This is because, only limited number of vulnerabilities are available for prioritization of infinite number of vulnerabilities. In addition, CVSS only ranks single step attacks whilst a wide variety of attacks are multi-step attacks. In this paper, a security system is proposed that is an improvement over CVSS and some other existing vulnerability scoring systems. It performs dynamic risk evaluation of multi-step attacks by considering vulnerabilities' temporal features. As the introduced model is developed based on security metrics of the security model, security evaluation of multi-step attacks is now possible by CVSS. Also, the capability of risk evaluation of zero-day attacks is one unique feature of the proposed system which cannot be accomplished by the present vulnerability scoring systems. In CVSS, the impact of exploiting 35.5% of vulnerabilities on confidentiality, integrity and availability are scored the same. But, in the proposed system, by considering the relative priority of the three mentioned security parameters, vulnerability discrimination of risk score of the mentioned percentage of vulnerabilities may be possible. On the other hand, the continuity of the probability assessment function of the proposed method in comparison to the discrete one in CVSS, improves the score diversity.

Keywords: Risk Assessment, Multi-Step Attacks, Zero-Day Attacks, Attack Graph, Common Vulnerability Scoring System(CVSS), Security Metric

* Corresponding Author Email: keramati_marjan@semnan.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۱، بهار ۱۴۰۰، ص ۱۷۳-۱۵۷

علمی – پژوهشی

روشی مبتنی بر مدل امنیتی برای ارزیابی پویا از خطر حملات چندمرحله‌ای شبکه‌های کامپیوتری

مرجان کرامتی

عضو هیات علمی گروه علوم کامپیوتر دانشگاه سمنان، ایران

(دریافت: ۱۳۹۹/۰۵/۱۷، پذیرش: ۱۳۹۹/۰۸/۰۵)

چکیده

با گسترش روزافزون آسیب‌پذیری‌ها در شبکه‌های کامپیوتری وابستگی ابعاد مختلف زندگی بشر به شبکه، امن‌سازی شبکه‌ها در برابر حملات ضروری است. در این راستا مقاوم‌سازی کم‌هزینه به‌دلیل محدودیت بودجه در زمره چالش‌های مورد توجه مدیران امنیتی است. برآورده‌سازی این هدف، با اولویت‌بندی آسیب‌پذیری‌ها از نظر میزان خطر و انتخاب آسیب‌پذیری‌های پر خطر برای حذف ممکن می‌شود. در این‌باره سامانه امتیازدهی به آسیب‌پذیری عام یا CVSS برای تعیین میزان خطر ناشی از بهره‌برداری شدن از آسیب‌پذیری‌ها معرفی شده است و استفاده فراوانی دارد. 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 سامانه 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 و تعدادی از سامانه‌های ارزیابی خطر موجود، سامانه برای ارزیابی پویای خطر حملات چندمرحله‌ای با در نظر گرفتن عوامل زمانی ارائه شده است. توسعه سامانه معرفی شده بر اساس مدل امنیتی و تعریف معیارهای امنیتی مبتنی بر مدل امنیتی، ایده اصلی مقاله بوده که ارزیابی خطر حملات چندمرحله‌ای را توسط سامانه پیشنهادی ممکن ساخته است. همچنین، قابلیت ارزیابی خطر حملات چند مرحله‌ای روز صفر را می‌توان به‌عنوان یک ویژگی منحصربه‌فرد برای سامانه پیشنهادی معرفی کرد که سامانه‌های امتیازدهی فعلی قادر به انجام آن نیستند. در CVSS، تأثیر مخرب ۳۵/۵ درصد از آسیب‌پذیری‌ها روی سه پارامتر امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری یکسان گزارش می‌شود. در صورتی که در سامانه امتیازدهی پیشنهادی، با در نظر گرفتن اولویت نسبی بین سه پارامتر امنیتی، مجزاسازی درصد مذکور از آسیب‌پذیری‌ها از نقطه‌نظر میزان آسیب به سامانه ممکن می‌شود. همچنین ماهیت پیوسته واحد ارزیابی احتمال پویای سامانه پیشنهادی در مقابل ماهیت گسسته تابع محاسبه احتمال CVSS، گوناگونی امتیازات را گسترش می‌دهد.

کلیدواژه‌ها: ارزیابی خطر، آسیب‌پذیری، حملات چندمرحله‌ای، حملات روز صفر، گراف حمله، سامانه امتیازدهی به آسیب‌پذیری عام (CVSS)، معیار امنیتی

۱- مقدمه

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، تاثیرمنفی بر اعتبار سازمان‌ها و افراد و بروز مشکلات مالی شرکت‌ها را نام برد [۱]. عامل ایجاد حملات در شبکه‌های کامپیوتری آسیب‌پذیری‌ها هستند. آسیب‌پذیری‌های امنیتی موجود در یک نرم‌افزار، از مسائل متعددی نشات می‌گیرند که از جمله این مسائل عبارت‌اند از خطا در طراحی، پیکره‌بندی نامناسب برای سامانه‌ها یا کاستی‌هایی که عموماً تحت عنوان باگ شناخته می‌شوند [۲]. بهره‌برداری از آسیب‌پذیری‌ها ازآنجایی‌که 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

رایانامه نویسنده مسئول: keramati_marjan@semnan.ac.ir

ناشر: دانشگاه جامع امام حسین (ع)

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 خطر بالایی را برای سازمان‌ها به‌همراه دارند [۵]. برای این‌منظور چندین پایگاه‌داده از آسیب‌پذیری‌هایی از جمله CVE[1] و OSVBD[2] ارائه شده است که در آن‌ها هر آسیب‌پذیری با یک شناسه به نام CVE و یک توضیح مختصر متناظر است [۷-۶]. ابزارهای پویش از جمله Nessus، هر میزبان شبکه را پویش می‌کنند و بر مبنای این پایگاه‌داده‌ها، 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 خطرناک بوده و کدام نقطه‌ضعف‌ها باید بقیه برطرف شوند [۹]. به‌کارگیری روش‌های ارزیابی کمی آسیب‌پذیری، برطرف‌سازی آسیب‌پذیری‌های شناسایی شده را ممکن می‌سازد. در نتیجه، مقاوم‌سازی کم‌هزینه سامانه‌های 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]. هزینه واکنش در برابر آسیب‌پذیری مجموع هزینه‌های مستقیم (منابع انسانی بکارگرفته شده، هزینه مجوزها و...) و غیر مستقیم (اتلاف بهره‌وری، قطع عملکردهای سامانه 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 کم 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. پارامترهای زمانی از جمله، سرعت آهسته انتشار اصلاحیه‌ها و ناپایداری 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 بالا 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. 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 تأثیر یاد می‌شود [۱۱]. در هرصورت 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 این‌روش‌ها، ارزیابی پویایی از خطر انجام نمی‌دهند [۱۲].

یک معیار امنیتی، درجه برآورده‌سازی اهداف امنیتی را برای یک سامانه مشخص می‌کند. 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 شبکه خود استفاده می‌کنند. در هر صورت نیاز برای ارزیابی کمی واقع‌بینانه از امنیت شبکه همچنان باقی خواهد بود [۱۳].

به‌دلیل اهمیت بالای ارزیابی امنیت سامانه‌های اطلاعاتی، تعداد زیادی از سازمان‌ها، شرکت‌ها و محققین سامانه‌هایی را

[1] Common Vulnerabilities and Exposures
[2] Open Source Vulnerability Data Base

برای ارزیابی آسیب‌پذیری‌ها توسعه داده‌اند. دو دسته‌بندی کلی از سامانه‌های امتیازدهی به آسیب‌پذیری موجود هستند، کیفی و کمی. روش‌های کیفی، شدت هر آسیب‌پذیری را مشخص می‌سازند. در صورتی‌که، روش‌های کمی گستره بالایی از امتیازات را برای توصیف آسیب‌پذیری‌ها به‌کار می‌گیرند [۵].

نمونه‌هایی از سامانه‌های کیفی عبارت‌اند از ISS X-Force از شرکت IBM [۱۴] و سامانه ارزیابی Qualys [۱۵]. از جمله سامانه‌های امتیازدهی کمی می‌توان سامانه امتیازدهی به آسیب‌پذیری US-CERT's و سامانه امتیازدهی به آسیب‌پذیری عام یا CVSS را نام برد [۱۶].

الگوهای اختصاصی بسیاری برای امتیازدهی به آسیب‌پذیری-های نرم‌افزارها وجود دارد اما، CVSS تنها سامانه شناخته شده است که به‌واسطه ارزیابی کمی از آسیب‌پذیری‌ها از سایر سامانه‌ها مجزا می‌شود. همچنین، CVSS[1] جزئیاتی را در رابطه با ماهیت آسیب‌پذیری مشخص می‌سازد که به کاربران در درک مناسب علت تخصیص امتیاز به آسیب‌پذیری کمک می‌کند [۱۸- ۱۷]. به بیان دیگرCVSS، 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 حملات، دقت پایینی دارد. زیرا، سیاست‌های امنیتی هر شبکه و عوامل زمانی از جمله احتمال معرفی راه‌کارهای اصلاحی و ابزارهای بهره‌برداری از آسیب‌پذیری هستند که میزان خطر ناشی از بهره‌برداری از آن را با گذر زمان تغییر می‌دهند [۲]. و این در صورتی است که CVSS ارزیابی خطر را بدون در نظر گرفتن عوامل زمانی انجام می‌دهد.

از طرف دیگر CVSS، ارزیابی خطر را تنها برای حملات تک‌مرحله‌ای انجام می‌دهد. در صورتی که اکثر حملات موجود در شبکه حملات چندمرحله‌ای یا زنجیره بهره‌برداری هستند. مشکل جدی دیگر این است که، CVSS متمایزسازی کارایی از آسیب‌پذیری‌ها از نقطه‌نظر خطر وارده به سامانه 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 تاکید دارند که به‌صورت عمومی افشا شده‌اند. اما امروزه مهاجمان پیشرفته در تلاش برای توسعه ابزارهای بهره‌برداری برای آسیب‌پذیری‌هایی هستند که تاکنون افشا نشده‌اند و تحت عنوان حملات روز صفر معروف هستند [۱]. CVSS به‌عنوان یک سامانه 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 چندمرحله‌ای در شبکه‌های کامپیوتری ارائه شده است. راهکار ارائه شده با در نظر گرفتن احتمال معرفی ابزارهای بهره‌برداری برای آسیب‌پذیری‌ها در کنار خصوصیات ذاتی آنها، میزان خطر حملات چندمرحله‌ای را با گذر زمان مشخص می‌سازد. بنابراین، این‌روش ارزیابی دقیقی 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 بهره‌برداری 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 بهبود پیدا می‌کند. افزایش گستردگی امتیازات در روش ارائه‌شده نسبت به CVSS اولویت‌بندی حملات در شبکه را به شکل کارا 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 به‌شکل کمی قابل اندازه‌گیری هستند.

روش پیشنهادی بهبودی است بر تعدادی از سامانه امتیازدهی به آسیب‌پذیری موجود از جمله CVSS ، [۱۹] و [۱۰] که در ادامه معرفی خواهد شد.

مزایای روش پیشنهادی در مقایسه با سامانه‌های امتیازدهی به آسیب‌پذیری موجود عبارت‌اند از:

[1] Common Vulnerability Scoring System

- قابلیت ارزیابی خطر حملات چندمرحله‌ای
- انجام ارزیابی پویا از خطر حملات با در نظر گرفتن عوامل زمانی
- قابلیت ارزیابی خطر حملات روز صفر
- اولویت‌بندی کارای حملات بر اساس میزان خطر وارده به سامانه (گوناگونی قابل توجه امتیازات موجود برای ارزیابی خطر حملات)

مقاله پیش‌رو، بهبود یافته سامانه امتیازدهی به آسیب‌پذیری است که در مرجع شماره [۱۹] معرفی کرده‌ایم .مزایای سامانه پیشنهادی در مقاله حاضر نسبت به [۱۹] عبارتند از:

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

از نقطه‌نظر کمی، بهبود روش پیشنهادی نسبت به سامانه امتیازدهی CVSS، به شرح زیر است:

- ارزیابی احتمال وقوع رخداد یک حمله: ماهیت پیوسته تابع پیشنهادی برای تخمین احتمال رخداد حمله، در مقایسه با CVSS با ماهیت گسسته (کمتر از ۱۰۰ امتیاز برای مجزاسازی سیل عظیمی از آسیب‌پذیری‌ها)، مجزاسازی حملات در یک شبکه را ممکن می‌سازد.
- ارزیابی تأثیر بهره‌برداری از آسیب‌پذیری روی محرمانگی، یکپارچگی و دسترسی‌پذیری: ۳۵/۵درصد از آسیب‌پذیری‌های شناخته‌شده بر اساس CVSS، از نظر میزان تأثیر روی پارامترهای امنیتی یکسان امتیازدهی می‌شوند. در صورتی‌که، روش پیشنهادی با اولویت‌بندی سه پارامتر امنیتی مذکور وزن دهی به آن‌ها، تأثیر بهره‌برداری متفاوتی را برای این کسر از آسیب‌پذیری گزارش می‌کند.

در ادامه بعد از مروری کوتاه بر فعالیت‌های مشابه و مفاهیم مرتبط با گراف حمله و CVSS در بخش‌های ۲و ۳و 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، سامانه‌های امتیازدهی به آسیب‌پذیری به دو شکل موجود هستند: کیفی و کمی. نمونه‌ای از یک سامانه کیفی Mozilla است که این سامانه، میزان خطر آسیب‌پذیری‌ها را با چهار سطح امنیتی مشخص می‌سازد. (بحرانی، بالا، متوسط و پایین) [۲۰]. سامانه امتیازدهی به آسیب‌پذیری عام یا CVSS نیز یک مثال از سامانه کمی است که توضیح داده شد.

در ادامه مرور کوتاهی داریم بر تعدادی راه‌کار غیراستاندارد که در سالیان اخیر به‌منظور ارزیابی خطر حملات در شبکه‌های کامپیوتری پیشنهاد شده است. مسئله مورد اهمیت در اقدامات صورت گرفته به‌منظور 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 در [۱۰] ارائه شده است، یک معیار امنیتی یا ترکیبی از معیارهای امنیتی، شامل یک مقیاس کمی از ویژگی‌های امنیتی اجزای قابل شناسایی سامانه (مثلاً شبکه) است. به کمک تعریف و استفاده از چنین معیارهایی این امکان فراهم می‌شود که قادر به مقایسه میزان امنیت سامانه‌های 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 سامانه چقدر است و یا تعداد مسیرهای موجود نیز معرف تعداد راه‌های مختلفی است که مهاجم برای نفوذ به سامانه در اختیار دارد. همچنین، میانگین طول مسیرهای موجود نیز بیانگر میزان تلاش نوعی مهاجم برای نفوذ به سامانه 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 ناامن‌تر 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 امن 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 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 تأثیر منفی رخداد معرفی شده است. برآورد فرکانس رخداد حمله و تأثیر آن با استفاده از CVSS انجام شده است. مدل ارائه‌شده، هر آسیب‌پذیری را به یک سطح سرویس نظیر می‌کند. سطوح سرویس تعیین‌کننده سطوح خطر بالقوه 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 معرفی‌شده 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 این‌روش، نیازمندی‌های امنیتی شبکه مورد بررسی در ارزیابی خطر مدنظر 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[1] انجام شده است.

روش ارائه‌شده در [۵] یک سامانه 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 [۲۱] یک بررسی آماری روی امتیازات تولیدشده توسط سه پایگاه داده آسیب‌پذیری‌های معروف (IBM ISS X-Force, Vupen Security , CVSS) با هدف بررسی تفاوت‌های سامانه‌های موجود و یافتن مزایای نسبی آن‌ها از نقطه‌نظر آماری انجام شده است. در این مقاله، یک سامانه امتیازدهی به آسیب‌پذیری معرفی شده که در پیاده‌سازی آن مزایای سه سامانه 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 [۲۲] روشی برای ارزیابی میزان مقاومت یک شبکه در برابر حملات ناشناخته معرفی شده است. همچنین در [۲۳] با در نظر گرفتن آسیب‌پذیری‌های ناشناخته، روشی برای تخمین متوسط زمان مورد نیاز برای تصاحب حملات چندمرحله‌ای 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 سامانه به‌همراه دارند و تعیین حملات خطرناک به‌منظور مقاوم‌سازی است. همچنین، در نظر گرفتن وجود حملات ناشناخته در مدل امنیتی، حملات پرخطر در شبکه را با دقت بالا مشخص می‌سازد. در حال حاضر، مدیران امنیتی سامانه 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، سامانه امتیازدهی به آسیب‌پذیری با ویژگی‌های مذکور توسعه داده شده است که ارزیابی خطر هر شبکه را با دریافت گراف حمله آن ممکن می‌سازد.

در [۴۱]، ما روشی مبتنی برای مدل امنیتی برای پیش‌بینی خطر حملات روز صفر ارائه دادیم. همچنین، در [۱۹] ما روشی برای ارزیابی پویای خطر حملات تک‌مرحله‌ای معرفی کرده‌ایم. مقاله پیش رو توسعه‌یافته مقالات مذکور با هدف ارزیابی پویایی از خطر حملات چندمرحله‌ای (شناخته شده و روز صفر) در شبکه‌های کامپیوتری 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 تست‌نفوذی مانند Nessus قابل استخراج است [۸]. همچنین، اطلاعات جامعی در رابطه با هر آسیب‌پذیری در پایگاه‌داده‌هایی مانند NVD در دسترس است [۲۴]

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

مدل‌سازی امنیتی همواره مورد توجه پژوهشگران بوده است. برای مثال، در [۴۳] با ارائه طبقه‌بندی جدیدی در روش‌های

[1] Multiple Criteria Decision and Analysis

مبهم‌سازی، روشی مبتنی بر فن افزودن حمله برای مدل‌سازی حملات سایبری مبهم، پیشنهاد شده است.

در [۴۴] با هدف بهبود سامانه امتیازدهی CVSS، روشی برای ارزیابی خطر آسیب‌پذیری‌ها با در نظر گرفتن عوامل محیطی ارائه شده است.

در [۴۵] مدلی مبتنی بر سامانه امتیازدهی CVSS، با هدف ارزیابی خطر حملات در سامانه‌های کنترل صنعتی ارائه شده است.

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 به‌خصوص 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 مؤلفه زیر مورد نیاز است [۱۰]:

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

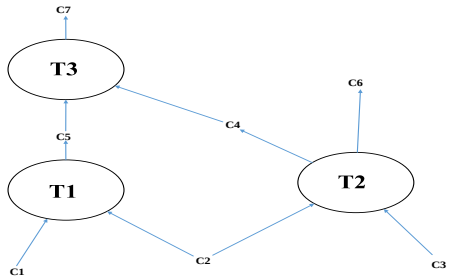
انواع متفاوتی از گراف‌های حمله وجود دارد. دو نوع مرسوم عبارت‌اند از گراف‌های حمله مبتنی بر حالت و گراف‌های حمله مبتنی بر بهره‌برداری. پیچیدگی ساخت و تحلیل گراف‌های حمله مبتنی بر حالت، تابعی نمایی از تعداد میزبان‌های شبکه است. به همین دلیل گراف‌های حمله مبتنی بر حالت مشکل مقیاس‌پذیری دارند. از این‌رو در این مقاله، از گراف حمله مبتنی بر بهره‌برداری یا گراف حمله فشرده به‌عنوان مدل امنیتی استفاده شده است [۲۵].

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 [۲۵]:

- شرایط اولیه: این نوع شرایط فقط به‌عنوان شرط لازم برای بهره‌برداری از آسیب‌پذیری‌ها هستند و نتیجه بهره‌برداری از هیچ آسیب‌پذیری دیگری نیستند.
- شرایط میانی: شرایطی هستند که نتیجه بهره‌برداری از آسیب‌پذیری‌های موجود در شبکه هستند.

یکی دیگر از مفاهیم مهم در رابطه با گراف حمله؛ مسیر حمله است. یک مسیر حمله مجموعه‌ای از آسیب‌پذیری‌هایی است که با یک ترتیب مشخص بهره‌برداری می‌شوند تا مهاجم به نقطه هدف خود برسد. به‌عبارت 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. آسیب‌پذیری‌های 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- سامانه امتیازدهی CVSS

آسیب‌پذیری‌های 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 آسیب‌پذیری‌ها (آسیب‌پذیری‌های ثبت‌شده 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 آسیب‌پذیری 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 تأثیر. معیارهای قابلیت بهره‌برداری منعکس‌کننده سادگی بهره‌برداری و معیار تأثیر منعکس‌کننده

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

چالش موجود در رابطه با این سامانه امتیازدهی این است که گروه معیارهای زمانی و محیطی برای آسیب‌پذیری‌ها در هیچ یک از نسخه‌های ۲و ۳ مقداردهی نشده‌اند، بنابراین، امتیازی که CVSS برای هر آسیب‌پذیری تخصیص می‌دهد تنها منعکس‌کننده خصوصیات ذاتی آسیب‌پذیری‌ها است و در نتیجه، میزان خطر گزارش‌شده مقدار دقیقی نیست و ارزیابی خطر پویا توسط CVSS ممکن نخواهد بود. در این مقاله، تلاش شده است با تخمین خصوصیات زمانی هر آسیب‌پذیری در کنار خصوصیات ذاتی آن‌که توسط CVSS قابل استخراج است روشی برای ارزیابی پویای خطر ارائه شود. بنابراین، ارزیابی خطر توسط روش پیشنهادی نسبت به CVSS دقیق‌تر خواهد بود.

۵- روش پیشنهادی

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

همان‌طور که پیش‌تر نیز به آن اشاره شد، مزایای روش پیشنهادی در مقایسه با سامانه‌های امتیازدهی به آسیب‌پذیری موجود عبارت‌اند از:

- قابلیت ارزیابی خطر حملات چندمرحله‌ای
- انجام ارزیابی پویا از خطر حملات با در نظر گرفتن عوامل زمانی
- قابلیت ارزیابی خطر حملات روز صفر
- اولویت‌بندی کارای حملات بر اساس میزان خطر وارده به سامانه (گوناگونی قابل توجه امتیازات موجود برای ارزیابی خطر حملات)

روش پیشنهادی، بهبودی است بر سامانه‌های امتیازدهی به آسیب‌پذیری CVSS و [۱۹] . همچنین، تعدادی از معیارهای امنیتی استفاده شده، اصلاح شده معیارهای مرجع [۱۰] است که در ادامه شرح داده شده‌اند.

طبق تعریف، میزان خطر یا ریسک به‌صورت (۱) محاسبه می‌شود [۲۶].

در (۱) منظور از Probability، احتمال بروز حمله و منظور از Impact تأثیر مخرب رخداد حمله روی پارامترهای امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری است.

$$Risk = Probability \times Impact \quad (1)$$

در این مقاله، تعیین خصوصیات ذاتی در ارزیابی خطر حملات چندمرحله‌ای بر اساس CVSS انجام شده است. برای هر آسیب‌پذیری شناخته‌شده بر اساس شناسه CVE، میزان خطر یک آسیب‌پذیری که بر اساس ویژگی‌های ذاتی آن تعیین می‌شود از سامانه محاسبه‌گر CVSS نسخه ۲ قابل استخراج هستند. همچنین برای تعدادی از آسیب‌پذیری‌ها، امتیاز متناظر با آسیب‌پذیری از نسخه ۳ نیز قابل استخراج است. از این‌رو با این هدف که سامانه 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، سامانه پیشنهادی در سه بخش مجزای چگونگی سنجش احتمال رخداد یک حمله چندمرحله‌ای، روند تخمین میزان تأثیر 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 چندمرحله‌ای را موجب می‌شوند. از این‌رو 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 خصوصیاتی از یک آسیب‌پذیری هستند که در ارزیابی احتمال بهره‌برداری از آن تعیین‌کننده هستند. در روش پیشنهادی، تنها پارامتر پیچیدگی دسترسی که بین دو نسخه CVSS مشترک است و 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 گزارش‌شده 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 .

در رابطه (۲)، پارامتر $AccessComplexity(V_i)\times$ برای هر آسیب‌پذیری (V_i) از سامانه امتیازدهی به آسیب‌پذیری CVSS استخراج شده است.

در رابطه با پارامتر $Exploitability(V_i)$ قابل ذکر است که، متناظر با کیفیت ابزارهای بهره‌برداری از یک آسیب‌پذیری، پارامتری تحت عنوان Exploitability در گروه معیارهای موقتی یا زمانی CVSS موجود است. اما ازآنجایی‌که معیارهای زمانی و محیطی برای آسیب‌پذیری‌ها مقداردهی نشده‌اند، پارامتر مذکور قابل استفاده نخواهد بود. از این‌رو، در این مقاله با هدف تخمین پارامتر Exploitability ($Exploitability(V_i)$ در (۲)) برای هر تک آسیب‌پذیری، از مدل توزیع احتمال Pareto در (۴) استفاده شده است [۲۷]. در این رابطه، x سن یک آسیب‌پذیری است که برابر است با تعداد روزهایی که از زمان افشا شدن این آسیب‌پذیری می‌گذرد.

$$Prob(V_i) = AccessComplexity(V_i) \times Exploitability(V_i) \quad (۲)$$

$$EaseOfExploitDegree(V_i) = 100 \times Prob(V_i) \quad (۳)$$

$$F(x) = 1 - \left(\frac{k}{x}\right)^{\alpha}. \quad k = 0.00161,\ \alpha = 0.260 \quad (۴)$$

تلاش صورت‌گرفته در این مقاله برای تخمین احتمال بهره‌برداری شدن یک حمله چندمرحله‌ای، در راستای بهبود روش ارائه‌شده 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 غیرواقعی است. از این‌رو، 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 چندمرحله‌ای عموماً بیش از یک مسیر حمله وجود دارد. بنابراین، در این مقاله، در ارزیابی خطر حملات چندمرحله‌ای اثر تمامی این مسیرها توامان 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)، $mode\left(\text{EaseOfExploitDegree}(V_i)\right)$ 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 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.

$$EaseOfExploitDegree(path) = mode\left(EaseOfExploitDegree(V_i)\right) \times \left(1 - Diversity\ (path)\right) \quad (۵)$$
$$\mathrm{i} = 1{:}\,\mathrm{n}$$

$$Diversity\ (path) = \frac{Number\ of\ unique\ vulnerabilities(path)}{Total\ Number\ of\ Vulnerabilities(path)} \quad (۶)$$

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، رتبه‌بندی اعضای یک مجموعه متناهی بر اساس 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 [۲۸]. چندین روش برای حل مسائل MCDA وجود دارد که با توجه به نیازمندی‌های مسئله تخمین درجه آسانی رخداد حمله چندمرحله‌ای، روش "مدل ضرب وزن‌دار 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:

- $LLength$ و $SLength$: به‌ترتیب 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.
- LPP و SPP: به‌ترتیب درصد مسیرهای با کم‌ترین و بیش‌ترین وزن در مجموعه مسیرهای حمله است.
- TMP: طبق رابطه (۹) محاسبه می‌شود.

$$\prod_{i=1}^{n} a_{ij}{}^{w_i} \quad \text{و} \quad \sum_{i=1}^{n} w_i = 1 \qquad (۷)$$

$$EaseOfExploitDegree(MultiStageAttack) = SLength^{SPP} \times TrimedMean^{TMP} \times LLength^{LPP} \qquad (۸)$$

$$TMP = 1 - (SPP + LPP) \qquad (۹)$$

$$Prob(MultiStageAttack) = \frac{EaseOfExploitDegree(MultiStageAttack)}{100 * \text{constant}} \qquad (۱۰)$$

$$\begin{cases} Version2\ constant = 0.71 \\ Version\ 3\ constant = 0.77 \end{cases}$$

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 وزن‌دار 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 وزن‌دار 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.

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

۵-۲- سنجش میزان تأثیر رخداد یک حمله چندمرحله‌ای روی پارامترهای امنیتی شبکه

برای هر تک آسیب‌پذیری شناخته‌شده در پایگاه داده CVSS، میزان تأثیر 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 به‌ترتیب از راست به چپ، تأثیر بهره‌برداری شدن از تک آسیب‌پذیری روی سه پارامتر امنیتی دسترسی‌پذیری، یکپارچگی و محرمانگی است که توسط CVSS در سه سطح بدون تأثیر، جزئی و کامل امتیازدهی می‌شود. معادل عددی این سطوح کیفی در دو نسخه ۲ و ۳ از CVSS در جدول (۱) نشان داده شده است.

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

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

مشکل اساسی رابطه (۱۱)، ماهیت متقارن آن است. زیرا منجر به این مسئله می‌شود که میزان تأثیر دو آسیب‌پذیری با پارامترهای تأثیر 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 تأثیر آن‌ها عبارت است از (۰/۲۷۵ و ۰/۶۶و ۰) و (۰/۶۶و ۰و۰/۲۷۵)، پارامتر تأثیر 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، تأثیر مخرب محرمانگی از یکپارچگی و یکپارچگی

از دسترسی‌پذیری بیشتر است. زیرا سرعت افشای تأثیر 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 به‌منظور 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 تأثیر در CVSS پیشنهاد شده است که آسیب‌پذیری‌ها را بر اساس میزان تأثیر 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 تأثیر را برای امتیازدهی به سیل عظیمی از آسیب‌پذیری‌های موجود در نظر می‌گیرد.

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

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

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

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

پراکندگی پارامتر Impact برای تمامی آسیب‌پذیری‌های شناخته‌شده از نسخه ۲ CVSS استخراج شده و نتایج در جدول (۲) نشان داده شده است. هر ترکیب نوشته‌شده در جدول (۲)، به ترتیب از چپ به راست بیانگر تأثیر 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 بیان‌شده در ستون ترکیب، تحت تأثیر قرار می‌دهد. در راستای نشان دادن کارایی روش پیشنهادی برای ارزیابی تأثیر، لازم به ذکر است که بنا به نتایج موجود در جدول (۲)، تأثیر بهره‌برداری از ۳۵/۵ درصد آسیب‌پذیری‌های موجود روی پارامترهای امنیتی، ترکیب‌های NNP ,NPN,PNN است. CVSS طبق رابطه‌های (۱۱) و (۱۲)، تأثیر بهره‌برداری از این کسر از آسیب‌پذیری‌ها را یکسان گزارش می‌کند در صورتی‌که بر اساس روش پیشنهادی (جدول ۲)، تأثیر بهره‌برداری از آسیب‌پذیری‌های متعلق به این سه دسته با هم متفاوت‌اند. بنابراین، روش ارائه‌شده در این مقاله، مجزاسازی دقیقی از آسیب‌پذیری‌ها را نسبت به CVSS از نظر میزان خطر وارده به سامانه 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 تأثیر بهره‌برداری از آسیب‌پذیری روی سه پارامتر امنیتی فوق در معادل کمی است که در دو نسخه فوق به آسیب‌پذیری نسبت داده می‌شود.

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

این تقسیم به‌منظور نرمال‌سازی Impact برای قرار گرفتن در محدود ۰ تا ۱۰ (همانند CVSS) انجام می‌شود.

$$Impact\ (path) = \left(\prod_{i=1}^{n} Impact\ (vul_i)\right)^{1/n} \quad (۱۳)$$

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

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

$$Impact(Attack) = \max\{Impact\ (path_i)\}, \quad i = 1: number\ of\ paths \quad (۱۴)$$

۵-۳- چگونگی تخمین خطر برای حملات ناشناخته

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

- احتمال بهره‌برداری از آسیب‌پذیری روز صفر: محاسبه احتمال بهره‌برداری از آسیب‌پذیری روز صفر و درجه آسانی آن، با استفاده از روابط (۲) تا (۴) انجام می‌شود. دقت شود، ازآنجایی‌که معیارهای CVSS تنها برای آسیب‌پذیری‌های شناخته‌شده قابل استخراج است، برای مقداردهی به پارامتر پیچیدگی دسترسی به آسیب‌پذیری‌هایی روز صفر، از سیاست CVSS برای امتیازدهی به آسیب‌پذیری‌های شناخته شده‌ای استفاده شده که اطلاعات کافی برای مقداردهی به معیارهای CVSS از آن‌ها در دسترس نیست. بنابر 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.
- تأثیر بهره‌برداری از آسیب‌پذیری ناشناخته روی پارامترهای امنیتی شبکه: بر اساس اطلاعات موجود در جدول (۲)، آسیب‌پذیری‌های با تأثیر PPP بر روی پارامترهای امنیتی، بالاترین درصد را در بین تمامی ترکیبات ممکن از تأثیر دارا هستند. از این‌رو، در این مقاله، تأثیر برای آسیب‌پذیری‌های ناشناخته برابر امتیاز متناظر با PPP یا ۱۷در نظر گرفته می‌شود.

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

جدول (۲): رتبه‌بندی پارامتر Impact برای ترکیب‌های ممکن از تأثیر بهره‌برداری از آسیب‌پذیری روی محرمانگی، یکپارچگی و دسترسی‌پذیری

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	۰۱/۰۴۴
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

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 سامانه امتیازدهی را در مجزاسازی آسیب‌پذیری‌ها از نقطه‌نظر خطر وارده به سامانه محدود می‌سازد. چرا که، تعداد قابل توجهی از آسیب‌پذیری‌ها از نظر میزان خطر وارده به سامانه یکسان گزارش می‌شوند و در نتیجه، اولویت‌بندی حملات جهت مقاوم‌سازی کم‌هزینه، ممکن نخواهد بود.

در این مقاله، در نظر گرفتن عوامل زمانی در تخمین احتمال رخداد حملات و پیشنهاد راه‌کار جدید برای تخمین تأثیر رخداد حملات روی پارامترهای امنیتی، با هدف بهبود مشکل فقدان گوناگونی امتیازات بوده است. بنا بر (۴)، برد تابع توزیع Pareto در محدوده [۱و۰/۸۱۲۲] قرار دارد. ازآنجایی‌که 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. بنابراین، بر خلاف CVSS، با استفاده از سامانه پیشنهادی، اولویت‌بندی آسیب‌پذیری‌ها جهت مقاوم‌سازی کم‌هزینه ممکن می‌شود.

از طرفی، همان‌طور که گفته شد، طبق جدول (۲)، تأثیر بهره‌برداری از ۳۵/۵ درصد آسیب‌پذیری‌های موجود روی پارامترهای امنیتی، ترکیب‌های NNP,NPN,PNN است. CVSS طبق (۱۲) و (۱۳)، تأثیر بهره‌برداری از این کسر از آسیب‌پذیری‌ها را یکسان گزارش می‌کند. به‌عبارت دیگر، ۳۵/۵درصد از آسیب‌پذیری‌های شناخته‌شده بر اساس CVSS، از نظر میزان تأثیر روی پارامترهای امنیتی یکسان هستند. در صورتی‌که، روش پیشنهادی (جدول ۲)، تأثیر بهره‌برداری از آسیب‌پذیری‌های متعلق به این سه دسته را متفاوت گزارش می‌کند. این ویژگی تأییدی است بر بهبود روش پیشنهادی نسبت به CVSS در مجازاسازی حملات از نقطه‌نظر خطر وارده به سامانه‌های 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 سامانه 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. سامانه پیشنهادی روی تعدادی شبکه نوعی که در کارهای مشابه از جمله [۲۹] استفاده می‌شود، اعمال شده و نتایج ارزیابی خطر برای یک نمونه از این شبکه‌ها در ادامه بیان شده است. به‌منظور بیان توانایی روش پیشنهادی 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، بر اساس مقادیر امتیاز پایه، ارزیابی کیفی نیز از میزان خطر آسیب‌پذیری‌ها به‌صورت جدول (۳) انجام می‌دهد. ازآنجایی‌که 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 آزمون 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 محاسبه‌شده 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. در جدول (۶)، سطوح کیفی بر اساس قرار داد CVSS برای تعیین سطح کیفی (جدول (۳)) تعیین شده‌اند.

با تجزیه و تحلیل اطلاعات جدول (۶)، نتایج زیر قابل استخراج هستند:

نتایج موجود در این جدول منعکس‌کننده بالا 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 چندمرحله‌ای مشخص می‌سازد. این ویژگی، اولویت‌بندی آسیب‌پذیری‌ها را بر اساس میزان خطر وارده به سامانه به‌منظور مقاوم‌سازی کم‌هزینه ممکن می‌سازد.

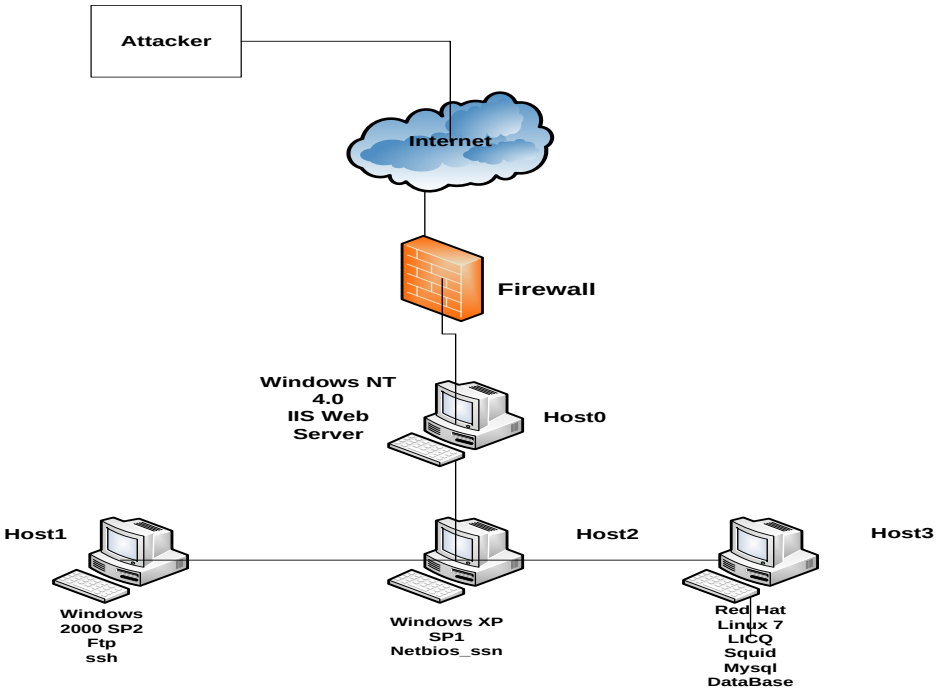
کاهش سطوح کیفی در روش پیشنهادی، یکی دیگر از نتایج اعمال سامانه پیشنهادی روی شبکه مذکور است که منجر به صرفه‌جویی در بودجه امنیتی در فرآیند مقاوم‌سازی خواهد شد. واضح است تخصیص هزینه برای مقاوم‌سازی سامانه‌های کامپیوتری در برابر حملات، بر اساس سطح کیفی خطر حمله انجام می‌شود.

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

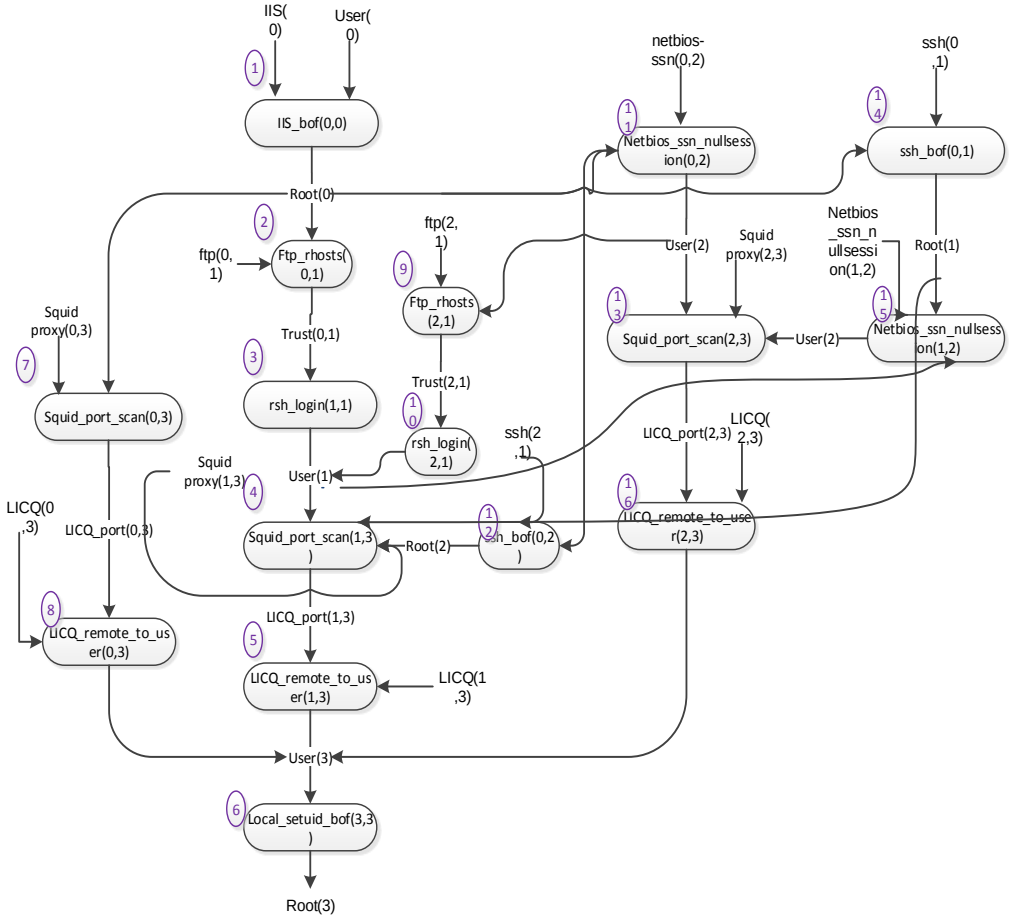
- در نظر گرفتن ارتباط بین آسیب‌پذیری‌ها: بر اساس گراف حمله، بهره‌برداری از یک آسیب‌پذیری مستلزم بهره‌برداری از تعدادی دیگر از آسیب‌پذیری‌ها است که این مسئله بهره‌برداری از آن را دشوارتر می‌سازد. در نتیجه، میزان خطر واقعی آن نسبت به میزان خطر گزارش‌شده توسط CVSS کمتر است.
- در نظر گرفتن عوامل زمانی: ارزیابی 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 بالا رفتن احتمال بهره‌برداری از آن توسط مهاجمان را در گذر زمان مدنظر قرار می‌دهد.

جدول (۳): تفسیر کیفی CVSS از خطر آسیب‌پذیری‌ها

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



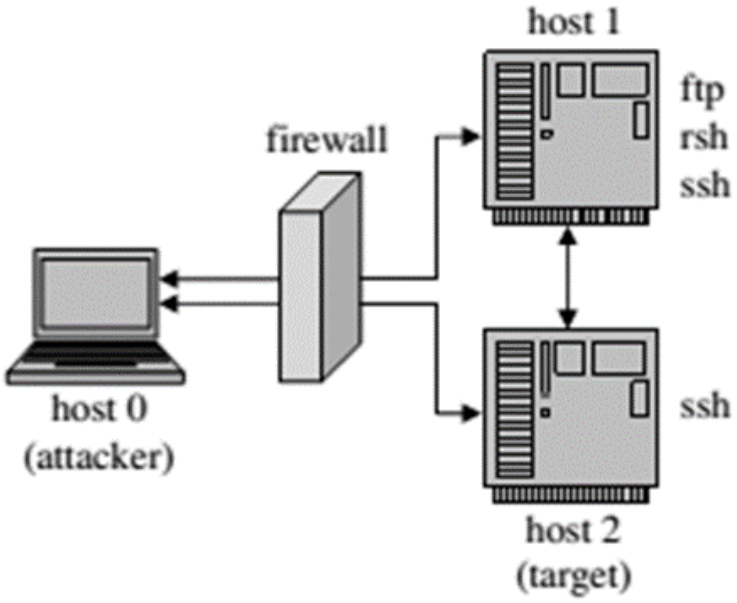
شکل (۲): شبکه مورد آزمون [۲۹]



شکل (۳):: گراف حمله شبکه مورد آزمون [۲۹]

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

میزبان	مهاجم	H0	H1	H2	H3
مهاجم	localhost	IIS	هیچ‌یک	هیچ‌یک	هیچ‌یک
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 (۴): شبکه شامل آسیب‌پذیری ناشناخته [۲۲]

جدول (۵): اطلاعات آسیب‌پذیری شبکه شکل (۲)

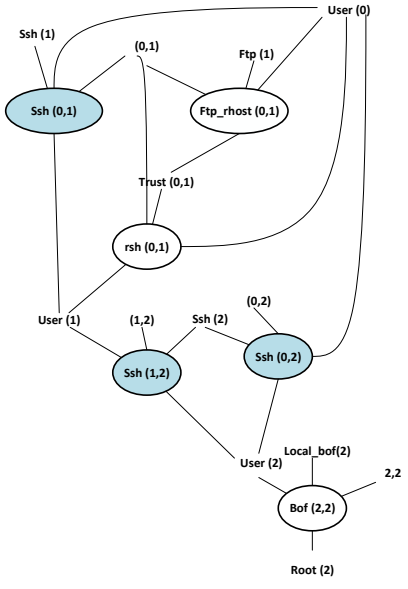
CVE	آسیب‌پذیری	محرمانگی	یکپارچگی	دسترسی‌پذیری	پیچیدگی دسترسی	سن تا تاریخ (۲۰۱۵/۱۱/۱۱)
CVE-2002-0364	IIS buffer overflow	p	p	p	۰/۷۱	۴۸۵۴
CVE-2008-1396	ftp rhost overwrite	p	n	n	۰/۶۱	۲۷۶۸
CVE-1999-1455	Sshd bufferoverflow	p	p	p	۰/۷۱	۵۷۶۶
CVE-2003-0661	Net bios ssn nullsession	p	n	n	۰/۷۱	۴۳۸۲
CVE-1999-0180	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 آزمون

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

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

در این بخش، نتایج به‌کارگیری سامانه 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.



شکل (۵): گراف حمله شبکه شامل آسیب‌پذیری ناشناخته [۲۲].

این مثال نوعی، در کارهای مشابه از جمله [۲۲]، به‌منظور ارزیابی 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 CVE-۱۹۹۹-۱۴۵۰ را به سامانه اضافه کرده است.

CVE-۲۰۱۰-۳۸۱۴ آسیب‌پذیری سرریز بافر است که در میزبان شماره ۲ وجود دارد. علاوه بر این، سرویس ssh که روی هر دو میزبان وجود دارد، آسیب‌پذیری شناخته‌شده‌ای ندارد. در این شبکه همچنین فرض شده است که فایروال در مقابل حملات مقاوم است. هدف مقاومت شبکه در برابر کسب دسترسی سطح ریشه روی میزبان شماره ۲ توسط مهاجم ماست. 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 شناخته‌شده نیز قابل تخمین است.

جدول (۷): ارزیابی خطر شبکه شکل (۴) توسط چارچوب پیشنهادی

آسیب‌پذیری	*Prob* (احتمال)	*Impact* (تأثیر)	*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، امن سازی شبکه‌های کامپیوتری در برابر حملات یک نیازمندی اجتناب‌ناپذیر به شمار می‌آید.

محدودیت در بودجه سازمان‌ها مقاوم‌سازی به‌صورت کم‌هزینه را به یک ضرورت اجتناب‌ناپذیر تبدیل کرده است. این امر ممکن نخواهد بود جز با امتیازدهی به آسیب‌پذیری‌ها به‌منظور پیدا کردن حملات پرخطر.

سامانه 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 سامانه، منعکس‌کننده خطر واقعی نخواهد بود.

همچنین، CVSS تعداد محدودی امتیاز مختلف (کمتر از ۱۰۰) را به‌منظور امتیازدهی به سیل عظیمی از آسیب‌پذیری‌ها به‌کار می‌برد. در نتیجه، مجزاسازی دقیق حملات به‌منظور تعیین حملات پرخطر توسط این سامانه ممکن نخواهد بود.

در این مقاله، با هدف تعیین حملات پرخطر به‌منظور مقاوم‌سازی کم‌هزینه، سامانه 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 تأثیر رخداد حملات روی پارامترهای امنیتی شبکه، گستردگی آسیب‌پذیری‌ها را نسبت به CVSS بهبود داده است.

قابلیت ارزیابی خطر حملات چندمرحله‌ای، انجام ارزیابی پویا از خطر حملات با در نظر گرفتن عوامل زمانی و ارزیابی خطر حملات روز صفر را می‌توان به‌عنوان ویژگی‌های منحصربه‌فرد سامانه پیشنهادی در مقابل با CVSS نام برد.

ماهیت پیوسته تابع پیشنهادی برای تخمین احتمال رخداد حمله، در مقایسه با CVSS با ماهیت گسسته (کمتر از ۱۰۰ امتیاز برای مجزاسازی سیل عظیمی از آسیب‌پذیری‌ها)، مجزاسازی حملات در یک شبکه را ممکن می‌سازد.

در CVSS، تأثیر مخرب ۳۵/۵ درصد از آسیب‌پذیری‌ها روی سه پارامتر امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری یکسان گزارش می‌شود. در صورتی که در سامانه امتیازدهی پیشنهادی، با در نظر گرفتن اولویت نسبی بین سه پارامتر امنیتی مذکور، مجزا سازی درصد مذکور از آسیب‌پذیری‌ها از نقطه‌نظر میزان آسیب به سامانه ممکن می‌شود.

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

۹- مراجع

[1] S. Abraham and S. Nair, "A Predictive Framnework for Cyber Security Analytics Using Attack Graphs," International Journal of Computer Networks & Communications (IJCNC), vol. 7, no. 1, pp. 1-17, 2015.

[2] C. Frühwirth and T. Männistö, "Improving CVSS-based vulnerability prioritization and response with context information," Proceeedings 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 an Scoring," https://cve.mitre.org/, 2018.

[7] OSVBD, "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-35.ibm.com/services/us/iss/xforce/faqs.html, 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] 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.

[20] Mozilla, "Mozilla Foundation Security Advisories," "http://www.mozilla.org/security/announce/, 2018.

[21] Q. Liu and Y. Zhang, "VRSS: A new system for rating and scoring vulnerabilities," Computer Communications, vol. 34, no. 3, pp. 264-273, 2011.

[22] 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.

[23] 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.

[24] NVD, "National Vulnerability DataBase," https://nvd.nist.gov, 2018.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] A. V. Sathanur and D. J. Haglin, "A novel centrality measure for network-wide cyber vulnerability assessment," 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, pp. 1-5, 2016.

[34] 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.

[35] A. Younis, Y. K. Malaiya, and I. Ray, "Evaluating CVSS Base Score Using Vulnerability Rewards Programs," In: Hoepman J. H., 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.

[36] 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. 37-50, 2017.

[37] 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.

[38] 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.

[39] 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.

[40] M. Keramati, "An Attack Graph Based Method for Predictive Risk Evaluation of Zero-Day Attacks," IJICTR, vol. 9, no. 3, pp. 7-16, 2017.

[41] M. Keramati, "Dynamic Risk Assessment System for the Vulnerability Scoring," IJICTR., vol. 9, no.4, pp. 57-68, 2017.

[42] V. Hosseinnezhad and A. Pourhaji Kazem, "Bayesian Networks Based Trust Model in Social Networks," Journal of Electronical & Cyber Defence, vol. 6 , no 4, pp. 29-38, 2018.

[43] K. Shoushian, A. J. Rashidi, and M. Dehghani, "Modeling of cyber-attacks obfuscation based on the attack analogous to the to the technique of insertion attacks," Journal of Electronical & Cyber Defence, vol. 7, no. 4, pp. 59-74, 2020. (In Persian)

[44] W. Wang, F. Shi, M. Zhang, C. Xu, and J. Zheng, "A Vulnerability Risk Assessment Method Based on Heterogeneous Information Network," In IEEE Access, vol. 8, pp. 148315-148330, 2020. doi: 10.1109/ACCESS.2020.3015551.

[45] A. Ur-Rehman, I. Gondal, J. Kamruzzaman, et al., "Vulnerability Modelling for Hybrid Industrial Control System Networks," J. Grid Computing, 2020. https://doi.org/10.1007/s10723-020-09528-w

Journal of Electronical & Cyber Defence
Vol. 9, No. 1, 2021, Serial No. 33

A Security Model Based Approach for Dynamic Risk Assessment of Multi-Step Attacks in Computer Networks

M. Keramati*

*Faculty Member of Semann University

(Received: 07/08/2020, Accepted: 26/10/2020)

ABSTRACT

Multi-facet dependency of human life on computer networks and its widespread vulnerability has made network robustness a necessity. With cost as a limiting factor, network robustness is considered as a great challenge for network administrators. This goal would be achievable by prioritizing the vulnerabilities based on their risk and choosing the most hazardous ones for elimination. Nowadays, CVSS is being used as the most widely used vulnerability scoring system. In CVSS, vulnerability ranking is based on its intrinsic features while temporal features such as the probability of developing exploitation tools, are ignored. So, dynamic risk evaluation is not possible with CVSS and it is incapable of performing effective vulnerability discretion. This is because, only limited number of vulnerabilities are available for prioritization of infinite number of vulnerabilities. In addition, CVSS only ranks single step attacks whilst a wide variety of attacks are multi-step attacks. In this paper, a security system is proposed that is an improvement over CVSS and some other existing vulnerability scoring systems. It performs dynamic risk evaluation of multi-step attacks by considering vulnerabilities' temporal features. As the introduced model is developed based on security metrics of the security model, security evaluation of multi-step attacks is now possible by CVSS. Also, the capability of risk evaluation of zero-day attacks is one unique feature of the proposed system which cannot be accomplished by the present vulnerability scoring systems. In CVSS, the impact of exploiting 35.5% of vulnerabilities on confidentiality, integrity and availability are scored the same. But, in the proposed system, by considering the relative priority of the three mentioned security parameters, vulnerability discrimination of risk score of the mentioned percentage of vulnerabilities may be possible. On the other hand, the continuity of the probability assessment function of the proposed method in comparison to the discrete one in CVSS, improves the score diversity.

Keywords: Risk Assessment, Multi-Step Attacks, Zero-Day Attacks, Attack Graph, Common Vulnerability Scoring System(CVSS), Security Metric

* Corresponding Author Email: keramati_marjan@semnan.ac.ir