نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دوازدهم، شماره ۱، بهار ۱۴۰۰؛ ص ۲۱- ۱

علمی- پژوهشی

طراحی یک شبیه‌ساز حملات سایبری چندگامی برای تولید دادگان جدید

علی‌جبار رشیدی[۱*]، بهزاد نظرپور[۲]

۱- دانشیار و ۲- دانشجوی دکتری مجتمع دانشگاهی برق و الکترونیک، دانشگاه صنعتی مالک اشتر، تهران، ایران

(دریافت: ۱۳۹۸/۱۰/۰۳، پذیرش: ۱۳۹۸/۱۲/۲۸)

چکیده

در حوزه دفاع سایبری همواره پژوهشگران با فقدان یک دادگان مناسب برای ارزیابی نظریه‌ها و روش‌های پیشنهادی خود، مواجه هستند. متأسفانه در دادگان مختلفی که در حوزه سایبری وجود دارند حقیقت زمینه مبهم بوده و سناریوهایی که توسط مهاجمان برای اجرای حمله مورد استفاده قرارگرفته‌اند، نامشخص است. این موضوع موجب خواهد شد تا صحت‌سنجی روش‌ها و پژوهش‌های این حوزه با یک چالش جدی مواجه شود. در این مقاله، روشی ارائه شده است که بر اساس آن می‌توان یک دادگان جدید با حقیقت زمینه مشخص و سناریوهای از پیش تعریف شده برای حملات سایبری چندگامی ایجاد کرد. در این روش از الگوی راهنمای حملات سایبری برای تعیین گام‌های مختلف حمله و از مولد سناریوی حمله نیز برای تعیین سناریوهای مورد استفاده توسط مهاجمان، استفاده شده است. نقشه شبکه به‌عنوان ورودی در نظر گرفته شده و برای ایجاد تنوع در اجراهای مختلف شبیه‌ساز نیز از متغیرهای تصادفی استفاده شده است. همچنین در روش پیشنهادی از فنون مختلفی ازجمله c-means فازی برای خوشه‌بندی، و شبکه‌های عصبی مصنوعی برای طبقه‌بندی استفاده شده است. برای تنظیم مؤلفه‌های شبیه‌ساز پیشنهادی از دادگان CDX استفاده شده و قابلیت آن برای ایجاد یک دادگان جدید از حملات سایبری چندگامی نشان داده شده است. برای ارزیابی روش پیشنهادی از روش امتیازدهی توسط افراد خبره استفاده شده است و درنهایت با متوسط امتیاز ۹۰/۷ از دیدگاه خبرگان این حوزه مورد تأیید قرار گرفته است.

کلیدواژه‌ها: شبیه‌ساز، حملات سایبری چندگامی، تولید دادگان، دفاع سایبری

A multistage cyber-attack simulator to generate a new dataset

A. J. Rashidi[1*], B. Nazarpour[2]

*Associate Professor, Malek Ashtar University of technology, Tehran, Iran

(Received: 24/12/2019; Accepted: 18/03/2020)

Abstract

In the field of cyber defense, researchers always suffer from the lack of a proper dataset to evaluate their proposed theories and methods. Unfortunately, in the various datasets existing in cyber defense scope, the ground truth is ambiguous, and the scenarios used by the attackers to carry out the attacks are unclear. This will lead to a serious challenge to the verification of methods and researches in this area. In this paper, a method is proposed by which a new database can be generated with the explisit ground truth and predetermined scenarios for multistage cyber attacks. In this method, a cyber attack guidance template is used to determine the various stages of the attacks and an attack scenario generator is also used to determine the scenarios used by simulated attackers. Network topology is considered as input, and random variables are used to create variety in simulator performances. Also, in the proposed method, various techniques such as fuzzy c-means for clustering, and artificial neural networks for classification are used. To set the simulator parameters, the CDX dataset is used and its ability to create a new dataset of multistage cyber attacks is well illustrated. To evaluate the proposed method, scoring by SME's is used, and finally with the mean score of 90.7, it had been approved.

Keywords: Simulator, Multistage Cyber-Attacks, Generating Dataset, Cyber Defense

* Corresponding Author E-mail: aiorashid@yahoo.com

۱- مقدمه

در طول سال‌های گذشته هزینه، پیچیدگی و حجم جرائم سایبری افزایش یافته و این روند هر سال رو به گسترش است. سازمان‌های مالی، شرکت‌های خدمات عمومی و انرژی، آژانس‌های دولتی و شرکت‌های فناوری، اهداف عمده حملات سایبری را تشکیل می‌دهند. با این وجود، تقریباً تمامی حوزه‌های تجارت و کسب‌وکار در معرض خطر هستند. تهدید و هزینه فزاینده حمله سایبری به عوامل مختلفی وابسته است که عبارت‌اند از اتکا و وابستگی شدید به شبکه‌های سایبری، تکامل و رشد روش‌های حمله و بهره‌کشی[1] سایبری، و توسعه ضعیف سازوکارهای دفاعی برای پیش‌بینی و جلوگیری از حملات سایبری.

در حوزه دفاع سایبری پژوهش‌های امیدوارکننده‌ای در زمینه‌ی دفاع فعال در مقابل حملات سایبری وجود دارد اما به علت عدم دسترسی به دادگان مناسبی که اطلاعات مربوط به سناریوهای مختلف حملات سایبری را در برداشته باشد، با محدودیت‌های زیادی مواجه هستند و اصولاً امکان ارزیابی و مقایسه دقیق روش‌های مورد مطالعه با یک چالش جدی روبرو شده است.

به‌عبارتی‌دیگر، عمده دادگانی که در این حوزه وجود دارد شامل عبور و مرور شبکه و هشدارهای تشخیص نفوذی هستند که بدون مشخص بودن سناریوی حملات جمع‌آوری شده‌اند. البته در برخی از تحقیقات برای رفع این مشکل از روش برچسب‌گذاری دستی نیز، استفاده شده است اما این موضوع پاسخگوی نیاز واقعی محققان این حوزه نبوده و لازم است که با انجام تحقیقات بیشتر در راستای تولید یک دادگان مناسب با سناریوهای از پیش تعریف شده و حقیقت زمینه[2] مشخص راه‌کارهای مناسبی پیشنهاد گردد. در واقع، یکی از مشکلات دادگان موجود این است که سناریوی حمله در آن‌ها نامعلوم است و وقتی که از دیدگاه مدافع، پس از تحلیل، یک یا چند سناریوی حمله تشخیص داده می‌شود امکان راستی آزمایی آن وجود ندارد و خروجی به‌دست آمده را نمی‌توان با یک خروجی از پیش مشخص شده مقایسه کرد. اما در روش پیشنهادی علاوه بر این‌که حملات متنوعی در رخدادهای تصادفی مختلفی توزیع شده‌اند، برچسب هر رخداد و ارتباط آن با سناریوهای از پیش تعیین شده ذخیره‌سازی شده و کاملا معلوم است که یک تحلیل‌گر باید به چه نتیجه‌ای برسد.

در این مقاله با تمرکز بر روی حملات سایبری چندگامی، که در آن‌ها یک مهاجم برای رسیدن به اهداف خود از چندین گام، مرحله، یا وضعیت مختلف بهره می‌برد، تلاش شده است که با درنظر گرفتن چالش‌های مذکور، با استفاده از شبیه‌سازی، راه‌کار مناسبی برای رفع مشکل فقدان دادگان مناسب، پیشنهاد شود. به‌گونه‌ای که بتواند بر روی یک شبکه با نقشه مشخص، مجموعه‌ای از حملات چندگامی[3] با سناریوهای از پیش تعیین شده را شبیه‌سازی نماید. برای این منظور، با استفاده از فنون مختلف هوش مصنوعی ازجمله طبقه‌بندی و خوشه‌بندی، راه‌کاری برای یادگیری سناریوی حملات، ایجاد الگوی راهنمای حملات[4] و درنهایت تولید سناریوی حملات فرضی پیشنهاد شده است. بدین ترتیب حملاتی که در روش پیشنهادی شبیه‌سازی می‌شوند، دارای یک حقیقت زمینه مشخص به‌همراه مجموعه سناریوهای ازپیش تعیین شده خواهد بود و دادگانی که به این روش ایجاد می‌شود را می‌توان به‌عنوان یک پاسخ مناسب برای ارزیابی پژوهش‌های حوزه سایبری در نظر گرفت.

یکی دیگر از مزایای روش پیشنهادی قابلیت انعطاف آن در یادگیری سناریوی حملات به کمک افراد خبره است که این موضوع موجب خواهد شد علاوه بر این‌که روش پیشنهادی بتواند از روی یک مجموعه داده موجود، مؤلفه‌های خود را تنظیم نماید، تنظیمات لازم با استفاده از دانش افراد خبره نیز بتوانند منظور شوند. استفاده از متغیرهای تصادفی در ساختار روش پیشنهادی نیز به‌گونه‌ای بوده است که تنوع سناریوهای تولید شده تا حد قابل قبولی بالا رفته و امکان تولید دادگان متنوعی فراهم شده است. البته لازم به‌ذکر است که مهاجمان باتجربه، در مقابل دانش افراد خبره، از الگوها و الگوریتم‌های مبهم‌سازی نیز استفاده می‌کنند که، این موضوع محدودیت‌ها و چالش‌های مختلفی را به‌وجود می‌آورد که با توجه به گستردگی آن در این مقاله، مورد بررسی قرار نگرفته و به فعالیت‌های آتی موکول شده است.

در ادامه این مقاله ابتدا مروری بر فعالیت‌های مرتبط انجام شده است؛ سپس در بخش ۲ روش تحقیق ارائه شده و در بخش ۳ ضمن معرفی دادگان، نتایج حاصل از اجرای روش پیشنهادی به همراه ارزیابی آن مورد بحث قرار گرفته است. درنهایت در بخش ۴ نتیجه‌گیری و پیشنهادهایی برای تحقیقات آینده ارائه شده است.

۱-۱- کارهای مرتبط

اولین شبیه‌ساز حمله سایبری توسط فِرِد کوهِن، توسعه داده شده است که از الگوی علت و معلولی برای الگوسازی حملات سایبری استفاده نموده و قادر به الگوسازی رخ‌نماهای[5] مختلف تهدید (مهاجمان)، سازوکارهای حمله و سازوکارهای دفاعی است [۱].

[1] Exploit
[2] Ground Truth
[3] Multi-Stage Attack
[4] Attack Guidance Tempelate
[5] Profile

الگوی علت و معلولی کوهن، پیوندهایی بین مهاجمان و حملات، حملات و روش‌های دفاعی، و حملات یا روش‌های دفاعی را با نتایج آن‌ها برقرار می‌کند.

شبیه‌ساز کوهن مبتنی بر الگوهای از پیش تعریف شده‌ای است که به‌صورت دستی، ایجاد شده و امکان به‌روز نگه‌داشتن آن‌ها تا زمان فعلی غیرعملی است. شبیه‌ساز دیگری توسط پارک و همکارانش، در دانشگاه هانگ‌کونگ کشور کره و در دانشکده مهندسی رایانه توسعه داده شده است که، مبتنی بر شبیه‌ساز کوهن بوده و یک واسط گرافیکی کاربر نیز به آن افزوده شده است [۲]. کاربران با استفاده از این واسط گرافیکی می‌توانند پیکربندی‌های دلخواه شبکه را ایجاد کرده و سازوکارهای دفاع و حمله را نیز مشخص نمایند. هر دو شبیه‌ساز توسعه داده شده توسط کوهن و پارک، از یک نمایش ساده جهت شبکه رایانه‌ای استفاده نموده و بهره‌کشی‌ها و آسیب‌پذیری‌های مشخصی را الگوسازی نمی‌کنند.

کوتنکو و منکوف، در موسسه خودکارسازی[۱] و داده‌ورزی[۲] سنت پترزبورگ روسیه، با هدف انجام تحلیل بر روی آسیب‌پذیری‌های شبکه رایانه‌ای، ابزاری نرم‌افزاری به نام «شبیه‌ساز حمله» ایجاد کرده‌اند [۳]. این شبیه‌ساز از گروه‌های سطح بالای حملات نظیر «شناسایی خدمات میزبان» و «ارتقاء سطح مجوز» برای الگوسازی ماشین‌های حالت احتمالی حمله، استفاده کرده است. ماشین‌های حالت احتمالی نیز برای تعیین ترتیب و توالی گروه‌های سطح بالای حمله مورد استفاده قرارگرفته‌اند. همانند شبیه‌سازهای قبلی، این شبیه‌ساز نیز نمایش ساده‌ای از شبکه را مورد استفاده قرار داده است که برای استانداردهای امروزی، مقیاس‌پذیر نیست.

کُهل و همکاران، با هدف تولید هشدارهای سامانه تشخیص نفوذ و پَروَنجای[۳] حقیقت زمینه، شبیه‌ساز حمله سایبری را در محیط نرم‌افزاری آرِنا[۴] که یک نرم‌افزار شبیه‌سازی تجاری است، توسعه داده‌اند [۴]. این شبیه‌ساز، کاربر را قادر می‌سازد تا شبکه‌ای شامل سه مؤلفه اصلی ارتباط‌دهنده، ماشین و زیرشبکه، ایجاد نماید که در آن زیرشبکه‌ها شامل گروهی از ماشین‌های مشابه هستند. ماشین‌های شبکه، مؤلفه‌هایی نظیر نوع سامانه عامل[۵]، آدرس IP ماشین و وجود حسگر تشخیص نفوذ بر روی ماشین، دارند. این شبیه‌ساز، الگوی راهنما را نیز به‌کار می‌گرفت که مبنای فعالیت الگوی راهنمای سناریو است. این الگوی راهنما از نه گام جداگانه تشکیل شده است که، اقدامات سطح بالای مهاجم در طول یک حمله سایبری را نشان می‌دهد. جهت الگوسازی دنباله‌های بالقوه‌ای از اقدامات یک مهاجم بر مبنای ماشین، این گام‌ها در قالب یک گراف شکل گرفته است. هر حمله بر اساس فهرستی گروه‌بندی شده، متشکل از ۲۲۳۷ بهره‌کشی و در قالب ۵ گروه و ۲۳ زیرگروه انتخاب شده است. در این شبیه‌ساز رفتار پایه حمله نیز با استفاده از سه مؤلفه کارآمدی، مهارت و اختفاء، الگوسازی شده است. در محیط آرنا، این شبیه‌ساز قادر به اجرای ۲۵ حمله با ۲۵۰ مرحله در هر حمله است. همانند سایر شبیه‌سازها، این الگو، یک شبیه‌سازی سطح بالا از حملات سایبری را با بهره‌گیری از نمایش سطح بالای مهاجم و شبکه استخراج کرده است.

دوگرتی و گونزلاوز، برای آزمایش میزان محافظت نرم‌افزار، یک سامانه انطباقی الگوسازی حملات را توسعه داده‌اند [۵].

چونگ و همکاران، پروژه‌ای به‌نام الگوسازی حمله همبسته را توسعه داده‌اند که در آن سناریوهای حمله از طریق مشاهده هشدارهای واقعی سامانه تشخیص نفوذ الگوسازی شده‌اند و این هشدارها به‌طورکلی می‌توانند با یک گام خاص از حمله مرتبط باشند [۶]. هرچند این شیوه امکان استفاده از حملات واقعی برای توسعه الگوهای حمله را فراهم می‌سازد؛ اما بسیاری از هشدارهای سامانه تشخیص نفوذ نیز ممکن است مثبت کاذب[۶] باشند (عبور و مرور عادی شبکه را اشتباهاً به‌عنوان یک گام حمله در نظر گرفته و هشدار تولید کرده است)؛ بنابراین فرآیند شبیه‌سازی را تحت تأثیر قرار داده است. علاوه‌بر این، ممکن است برخی از گام‌های حمله به‌طور کامل از بین رفته باشند و یا از نظر زمانی کاملاً توزیع شده باشند، که در این صورت فرآیند شبیه‌سازی، با مشکل مواجه خواهد شد.

هُلِندِر و همکاران، با استفاده از فنون نظریه گراف، یک الگوی مبتنی بر گراف را توسعه داده‌اند تا وابستگی بین بهره‌کشی‌ها یا اقدامات یک حمله را تعیین کنند [۷].

فعالیت کستانتینی [۸] نیز همانند کوهن [۱] باهدف تحلیل الگوهای حمله و درک بهتر حملات سایبری انجام گرفته است درحالی‌که برخی شبیه‌سازها مانند [۹] با انگیزه آموزش، ایجاد شده‌اند.

به‌عنوان نمونه‌ای از سایر کارهای انجام شده در این حوزه می‌توان الگوسازی بر اساس گراف حمله توسط جاجودیا و همکاران [۱۰]، الگوسازی بر اساس شبکه بیزین توسط کوئین و لی [۱۱] و همچنین ژی و همکاران [۱۲]، الگوسازی بر اساس

[1] Automation
[2] Informatics
[3] File
[4] Arena
[5] Operating System
[6] False Positive

الگوی گراف، توسط استاتز و سادیت [۱۳]، الگوی پیش‌بینی مارکوف با طول متغیر توسط فاوا و همکاران [۱۴]، الگوسازی عامل مبنا توسط عبدالهی‌ازگمی و عباسی [۱۵] و ترکیب روش‌های مبتنی بر امضاء و الگوریتم نزدیکترین همسایه برای شبیه‌سازی حملات انکار سرویس در محیط رایانش ابری توسط رجایی [۱۶] را نام برد. کارهای دیگری که در راستای الگوسازی رفتار مهاجم انجام‌گرفته‌اند، شامل الگوسازی قابلیت و فرصت، توسط هلسپل و همکاران [۱۷]، استفاده از فرآیند تصمیم مارکوف توسط ژانگ و همکاران [۱۸] و استفاده از نظریه بازی توسط وانگ و همکاران [۱۹] است.

در سال‌های اخیر نیز فعالیت‌های زیادی در حوزه شبیه‌سازی حملات سایبری انجام شده است که به‌عنوان نمونه‌ای از فعالیت‌های انجام شده می‌توان به شبیه‌سازی رفتار سامانه‌های فیزیکی سایبری[1] [۲۰]، چارچوبی برای شبیه‌سازی چند وجهی سامانه‌های تولید محصولات فیزیکی سایبری [۲۱]، الگوی پیشگویانه، برای شبیه‌ساز حملات سایبری [۲۲]، ابزار هکایت برای بررسی آزمایشگاهی حملات به‌صورت بلادرنگ [۲۳]، فرآیند انتخاب کامپوننت در مونتاژ الگوهای شبیه‌سازی و پیاده‌سازی آن‌ها [۲۴ و ۲۵]، اشاره نمود. با وجود تلاش‌هایی که تاکنون انجام شده است، اما هنوز چالش‌های فراوانی وجود دارد که مورد توجه قرار نگرفته‌اند. در این مقاله، با درنظر گرفتن این موضوع، راه‌کاری برای استفاده از شبیه‌سازی برای تولید دادگان سایبری ارائه شده است.

۲- روش تحقیق

از آنجایی‌که هدف اصلی این مقاله ارائه یک طرح جدید برای شبیه‌سازی حملات سایبری چندگامی تحت شبکه‌های رایانه‌ای و در جهت تولید یک دادگان جدید با حقیقت زمینه مشخص و سناریوهای ازپیش تعیین شده است، لذا باید راه‌کارهای مناسبی برای تعیین نقشه شبکه، تعیین الگوی حملات، تولید سناریوهای حمله، ایجاد یک فضای فرضی از مهاجمان و تخصیص هشدارهای تشخیص نفوذ به فعالیت‌های مهاجمان ارائه نمود. در این مقاله نقشه شبکه به‌عنوان ورودی و از پیش تعیین شده فرض شده است. به‌عبارتی دیگر، فرض شده است که محیط سایبری که تحت آن قرار است شبیه‌سازی انجام شود، از قبل مشخص است. بدین ترتیب مسئله شبیه‌سازی حملات را می‌توان با ایجاد سناریوهای تصادفی و تطبیق هشدارهای تشخیص نفوذ به فعالیت‌های مرتبط با سناریوهای حملات، ساده‌سازی نمود. طرح پیشنهادی برای شبیه‌سازی حملات سایبری چندگامی در شکل (۱) نمایش داده شده است. در این طرح، الگوی راهنمای حملات سایبری به همراه همبندی شبکه، به‌عنوان ورودی و دادگان شبیه‌سازی به‌عنوان خروجی سامانه شبیه‌ساز، درنظر گرفته‌شده‌اند. مولد سناریوی حمله، به‌عنوان اصلی‌ترین مؤلفه در طرح پیشنهادی، وظیفه تولید سناریوی حملات مختلف را بر عهده دارد و برای این کار از یک مولد متغیر تصادفی بهره می‌برد. سناریوی حملات بر اساس الگوی راهنمای حملات و همبندی شبکه، تولید شده و سپس هرکدام از فعالیت‌های مرتبط با سناریوی حملات با تطبیق پورت‌ها و آسیب‌پذیری‌ها به توصیف هشدارهای متناسبی نگاشت شده و به ازای هر هشدار یک برچسب زمانی، به همراه شناسه مهاجم و قربانی، به‌صورت تصادفی تولید و تخصیص داده می‌شود. درنهایت پس از مرتب‌سازی هشدارها بر اساس برچسب زمانی، دادگان موردنظر، به‌عنوان خروجی شبیه‌ساز، ذخیره می‌شود.

به‌طورکلی دادگان حاصل از شبیه‌سازی حملات سایبری در کاربردهای بسیار زیادی در حوزه دفاع سایبری می‌تواند مورد استفاده قرار گیرد که ازجمله آن‌ها می‌توان به ردگیری حملات سایبری [۲۶] و تجسم حملات سایبری [۲۷] اشاره نمود.

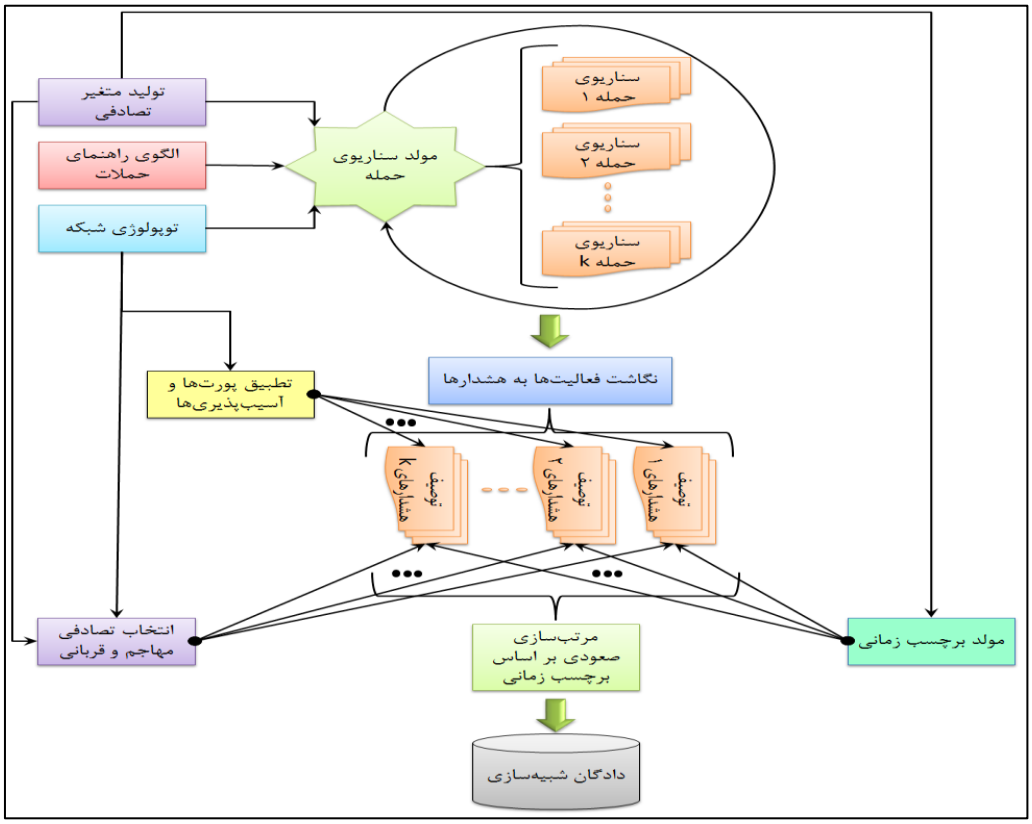
همان‌طور که در شکل (۱) نیز نشان داده شده است طرح پیشنهادی، از مؤلفه‌های مختلفی تشکیل شده است که در ادامه این بخش توضیح داده شده‌اند.

۲-۱- الگوی راهنمای حملات

الگوی راهنمای حملات چندگامی یک نمای مفهومی از مجموعه فعالیت‌هایی که ممکن است یک مهاجم سایبری در جهت اجرای طرح و سناریوی حمله خود اجرا نماید را در یک قالب گرافیکی و قابل‌فهم نمایش می‌دهد. درواقع الگوی راهنمای حملات چندگامی یک طرح مفهومی و جامع است که قابلیت ردگیری گام‌های مختلف حمله را در یک فضای مفهومی فراهم می‌کند. جامعیت الگوی راهنمای حملات ازاین‌جهت مطرح می‌شود که باید بتواند تمامی حالاتی که ممکن است در اجرای یک حمله رخ دهد را نمایش دهد.

در این تحقیق از یک رویکرد مبتنی بر خوشه‌بندی و طبقه‌بندی برای تعیین الگوی راهنمای حملات چندگامی استفاده شده است. به‌عبارتی‌دیگر با استفاده از طبقه‌بندی، حملات در دسته‌هایی مشخص و با برچسب‌های از پیش تعیین‌شده قرار داده می‌شوند و این دسته‌ها گام حملات را نشان می‌دهند. درحالی‌که با استفاده از خوشه‌بندی، به ازای هرکدام از دسته‌های فوق، زیردسته‌های مختلفی به وجود می‌آیند که مبتنی بر توصیف نوع فعالیت‌های مهاجم است و این فعالیت‌ها پس از اینکه توسط ماشین تمیز داده شدند، به‌وسیله افراد خبره نام‌گذاری می‌شوند. درواقع، تفاوت طبقه‌بندی و خوشه‌بندی نیز در همین موضوع است که در هنگام طبقه‌بندی تعداد گام‌های حمله از پیش تعیین‌شده است اما در هنگام خوشه‌بندی تعداد فعالیت‌های هر گام پس از عملیات خوشه‌بندی تعیین می‌شوند.

[1] Cyber-Physical

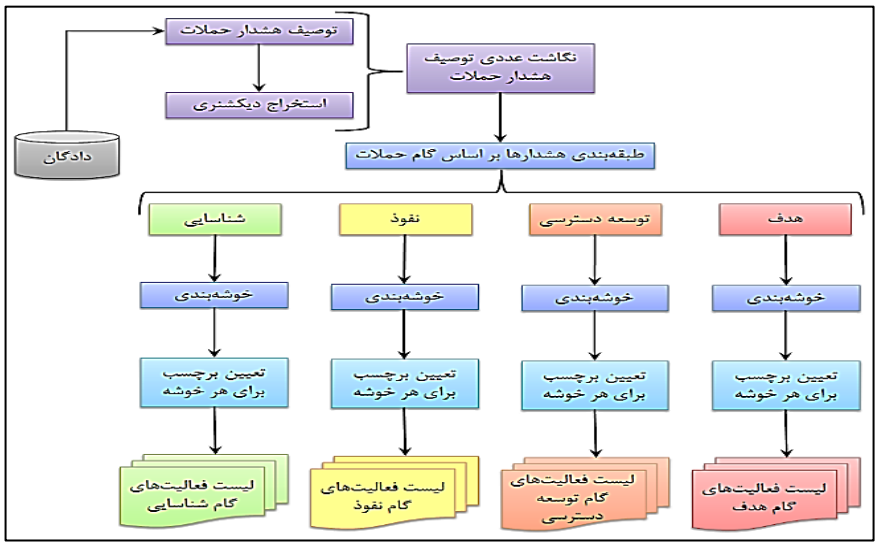


شکل ۱. طرح پیشنهادی: شبیه‌سازی حملات سایبری چندگامی برای تولید دادگان

در این رویکرد ابتدا کلیه اقدامات/فعالیت‌ها در چهار دسته زیر طبقه‌بندی شده‌اند که هرکدام از این دسته‌ها یکی از گام‌های حمله را نشان می‌دهند:

- **گام شناسایی:** مهاجم در این گام تلاش می‌کند تا حداکثر اطلاعات ممکن را در مورد سامانه‌ها و موجودیت‌های موجود در فضای سایبری به دست آورده و میزان شناخت خود را از اهداف احتمالی افزایش دهد. همچنین در این مرحله، مهاجم ضمن جمع‌آوری اطلاعات، یک فهرست از اهداف اولیه‌ای که می‌توانند او را در دست‌یابی به مقصود نهایی یاری رسانند را تهیه کرده و یک سناریوی پیش‌فرض را برای خود تدوین می‌کند. در این سناریو مهاجم اهداف اولیه، میانی و نهایی را به روشی سازمان‌دهی می‌کند که امن‌ترین و کوتاه‌ترین راه ممکن در دست‌یابی به هدف نهایی عملیات را داشته باشد.
- **گام نفوذ:** در این گام، مهاجم تلاش می‌کند تا به یکی از اهداف موردنظر خود (اولیه، میانی، نهایی) دسترسی یافته و به‌طور نامحسوس آن را در اختیار بگیرد. لازم به ذکر است که بدون درنظر گرفتن روش انجام نفوذ، هرکدام از فعالیت‌هایی که در گام قبلی یعنی گام شناسایی برای جمع‌آوری اطلاعات انجام می‌شوند، می‌توانند به روشی متفاوت درنهایت منجر به اجرای یکی از انواع نفوذ گردند. یک مهاجم در این گام از حمله، معمولاً می‌تواند در قالب مهمان، کاربر و یا مدیر نفوذ کرده و فعالیت‌های خود را با سطح دسترسی تعیین‌شده انجام دهد.
- **گام توسعه دسترسی:** در این گام از حمله مهاجم تلاش می‌کند که سطح دسترسی خود را گسترش داده و به‌این‌ترتیب قابلیت‌های تهاجمی خود را افزایش دهد. برای تعیین سطوح مختلف دسترسی روش‌های مختلفی را می‌توان مورد استفاده قرار داد. به‌عنوان نمونه می‌توان بر اساس سلسله‌مراتب موجود در فضای سایبری که شامل شبکه، سامانه، درگاه[1]، خدمت[2]، برنامه، فرآیند و نخ[3] است، سطوح مختلفی را تعریف کرده که دسترسی به هرکدام از آن‌ها توسط مهاجم می‌تواند به‌عنوان دریچه‌ای جدید برای پیشبرد حمله[4] در نظر گرفته شود.
- **گام هدف:** این گام از حمله معمولاً زمانی اتفاق می‌افتد که یک مهاجم تمامی پیش‌نیازها و دسترسی‌های موردنیاز خود را برای اجرای عملیات خرابکارانه به دست آورده باشد. در این مرحله بر اساس سناریوی حمله‌ای که توسط مهاجم از قبل طراحی شده است یک فعالیت مخرب انتخاب و اجرا می‌شود.

[1] Port
[2] Service
[3] Thread
[4] منظور از پیشبرد حمله، اجرای سناریوها و یا برداشتن گام‌هایی در جهت نزدیک شدن به هدف نهایی حمله است.



شکل (۲): روش پیشنهادی برای تعیین فعالیت‌های هر گام حمله.

برای اینکه الگوی راهنمای پیشنهادی یک طرح جامع باشد و تمامی حالت‌های ممکن برای حملات چندگامی را بازنمایی کند، لازم است تمامی روابط ممکن بین گام‌های مختلف حملات را در آن لحاظ کرد. برای انجام این کار، از یال‌های دوطرفه برای اتصال گام‌های مختلف حمله استفاده شده و تمامی یال‌های ممکن بین گام‌های مختلف حمله ترسیم شده است.

یک مهاجم می‌تواند بر اساس قابلیت‌ها و ابزارهایی که در اختیار دارد فعالیت‌های مختلفی را در هر گام از حمله انجام دهد. برای تعیین فعالیت‌ها روش‌های مختلفی وجود دارد. در این مقاله از یک راه‌کار مبتنی بر خوشه‌بندی استفاده شده است. به این صورت که فعالیت‌های مختلف در هر گام از حمله را به‌صورت جداگانه خوشه‌بندی کرده و با تعیین یک برچسب مناسب برای هر خوشه، نوع فعالیت‌های هر گام حمله تعیین شده است. به‌عبارتی‌دیگر خوشه‌بندی و برچسب‌گذاری در دو مرحله مختلف و مجزا انجام می‌شوند. ابتدا خوشه‌بندی، دسته‌هایی را به‌عنوان خوشه تعیین می‌کند و سپس برای هر خوشه، با نظر افراد خبره، یک برچسب تعیین می‌شود. شکل (۲) روش انجام این کار را نمایش می‌دهد.

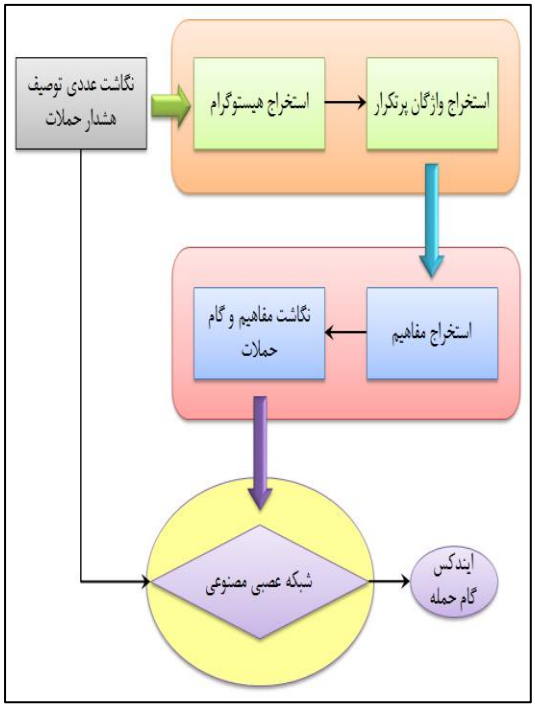
لازم به توضیح است که این روش با بهره بردن از خوشه‌بندی یک روش کاملاً پویا برای تعیین فعالیت‌هایی که یک مهاجم سایبری در هر گام از حمله می‌تواند انجام دهد را به وجود آورده است. بدین‌وسیله در صورت به وجود آمدن دادگان جدید می‌توان فعالیت‌های جدیدی نیز استخراج کرده و مورداستفاده قرار داد.

در ادامه هر یک از بخش‌های روش پیشنهادی برای تعیین فعالیت‌های هر گام حمله با جزئیات بیشتری توضیح داده شده است.

- **استخراج توصیف هشدار حملات:** عموماً هشدارهای تشخیص نفوذ از مؤلفه‌های مختلفی تشکیل شده‌اند که این مؤلفه‌ها درمجموع اطلاعات جامعی از رویدادهای امنیت سایبری را مشخص می‌کنند. در میان این مؤلفه‌ها، مؤلفه توصیف هشدار، یک توصیف زبانی از ماهیت هشدار را در قالب مجموعه‌ای از واژگان ارائه می‌کند که می‌تواند برای تحلیل و درک فعالیت انجام‌شده توسط مهاجم مورد استفاده قرار گیرد. با استخراج این مولفه از دادگان تلاش شده است که روش پیشنهادی بر مبنای تحلیل این توصیف زبانی با استفاده از پردازش متن ایجاد شود.
- **استخراج واژه‌نامه:** درروش پیشنهادی برای استخراج واژه‌نامه، کلیه واژگان غیرتکراری در توصیف هشدارها به ترتیب حروف الفبا مرتب می‌شوند.
- **نگاشت عددی توصیف هشدار حملات:** ازآنجایی‌که توصیف هشدارها به ازای تمامی هشدارها دارای یک طول ثابت نیست لذا لازم است که راه‌کاری ارائه شود که بر اساس آن بتوان توصیف تمام هشدارها را در یک فضای K بعدی نمایش داد. برای انجام این کار یک واژه تهی با نمایه[1] صفر به واژه‌نامه اضافه شده و ابعاد فضای توصیف هشدار حملات، برابر با طولانی‌ترین توصیف قرار داده شده و به ازای بقیه هشدارها از واژه تهی استفاده شده است. بدین ترتیب یک فضای برداری K بعدی از واژگان تشکیل شده و هر توصیف هشدار در آن فضا نمایش داده می‌شود. برای ساده کردن محاسبات در روش پیشنهادی، این فضای برداری از واژگان به یک فضای برداری از اعداد صحیح نگاشت شده و از آن استفاده شده است، برای این منظور به‌جای استفاده از واژه‌ها از نمایه آن‌ها که در واژه‌نامه ذخیره شده است استفاده شده است.
- **طبقه‌بندی هشدارها بر اساس گام حملات:** برای طراحی یک طبقه‌بندی کننده که بتواند هشدارها را بر اساس گام حملات طبقه‌بندی نماید پیشنهاد می‌شود که از یک روش نیمه‌نظارتی[2] استفاده شود. درروش پیشنهادی هم از

[1] index
[2] Semi-Supervised

تجزیه‌وتحلیل خودکار توصیف هشدارها استفاده می‌شود و مفاهیم مرتبط با هر هشدار استخراج می‌گردد و هم یک فرد خبره ارتباط بین مفاهیم را در جهت رسیدن به گام حمله برقرار می‌نماید. درنهایت نیز از یک شبکه عصبی مصنوعی[1] برای طبقه‌بندی هشدارها استفاده می‌شود. شکل (۳) طرح پیشنهادی برای طبقه‌بندی هشدارها بر اساس گام حملات را نمایش می‌دهد.



شکل (۳): روش پیشنهادی برای طبقه‌بندی هشدارها.

همان‌طور که در شکل (۳) نشان داده شده است ابتدا با استفاده از یک تحلیل خودکار که مبتنی بر هیستوگرام است واژگان پرتکرار استخراج شده و سپس با نظر افراد خبره مفاهیم مرتبط با این واژگان مشخص شده و نگاشت مفاهیم با گام حملات تعیین می‌گردد. به‌عبارتی‌دیگر با استفاده از هیستوگرام، فراوانی واژگان استخراج شده و سپس با انتخاب واژگانی که فراوانی بیشتری دارند یک بردار ویژگی به دست آمده است. سپس افراد خبره به هرکدام از این بردارهای ویژگی یک مفهوم را نسبت داده و درواقع، فعالیت منتسب به آن بردار ویژگی را مشخص کرده‌اند. درنهایت نیز از یک شبکه عصبی مصنوعی به‌عنوان یک طبقه‌بندی کننده استفاده شده است. این شبکه عصبی مصنوعی با دریافت بردار عددی توصیف هشدار حمله که از نگاشت واژگان موجود در توصیف هشدار حملات به نمایه معادل آن‌ها در واژه‌نامه به دست آمده است، نمایه گام آن حمله را مشخص می‌کند. پس‌ازاینکه شبکه عصبی مصنوعی با تعداد داده‌های آموزشی مناسبی آموزش داده شد، می‌تواند به‌جای فرد خبره مورداستفاده قرار گیرد و با دیدن داده‌های جدید، عملیات نگاشت توصیف بردار حمله به نمایه گام‌های حمله را انجام دهد. در این مقاله برای پیاده‌سازی این طبقه‌بندی‌کننده از یک شبکه عصبی پیش‌خور[2] پرسپترون[3]، با سه لایه مخفی، تابع انتقال سیگموئید[4] و تابع خطای میانگین مربعات استفاده شده است که به ترتیب دارای ۱۶، ۶۴ و ۸ نورون در لایه‌های مخفی است.

- **خوشه‌بندی هشدارهای مربوط به هر گام حمله:** در این مقاله از خوشه‌بندی فازی c-means استفاده شده است که مبتنی بر کمینه کردن تابع هدف زیر است:

$$J_m = \sum_{i=1}^{D}\sum_{j=1}^{N} \mu_{ij}^{m} \left\|x_i - c_j\right\|^2 \qquad (۱)$$

که در آن، D تعداد داده‌ها، N تعداد خوشه‌ها، m مؤلفه همپوشانی فازی، x_i داده i ام، c_j مرکز j امین خوشه، μ_{ij} تابع تعلق i امین داده به j امین خوشه، است.

الگوریتم مورداستفاده به این صورت است:

الگوریتم (۱): الگوریتم خوشه‌بندی فازی c-means.

۱. به‌طور تصادفی مقادیر عضویت خوشه‌ها را تخصیص دهید.

۲. مراکز خوشه را با استفاده از رابطه (۲) به دست آورید.

$$c_j = \frac{\sum_{i=1}^{D} \mu_{ij}^{m} x_i}{\sum_{i=1}^{D} \mu_{ij}^{m}} \qquad (۲)$$

۳. مقادیر تابع تعلق را با استفاده از رابطه (۳) محاسبه کنید.

$$\mu_{ij} = \frac{1}{\sum_{k=1}^{N} \left(\frac{\left\|x_i - c_j\right\|}{\left\|x_i - c_k\right\|} \right)^{\frac{2}{m-1}}} \qquad (۳)$$

۴. تابع هدف رابطه (۱) را محاسبه کنید.

۵. مراحل ۲ تا ۴ را تا هنگامی‌که تابع هدف از یک حد آستانه کمتر شود یا پس از تعداد مشخصی، تکرار نمایید.

لازم به توضیح است که در مرحله ۵ این الگوریتم از دو شرط برای خاتمه استفاده می‌شود که هرکدام از این دو شرط نقض شود موجب خاتمه الگوریتم خواهد شد. همچنین در این الگوریتم در ابتدا مراکز خوشه‌ها به‌صورت تصادفی تعیین می‌شوند و در هر بار تکرار مراکز خوشه‌ها به‌صورت پویا تغییر می‌کنند.

[1] Artificial neural networks

[2] Feedforward
[3] Perceptron
[4] Sigmoid

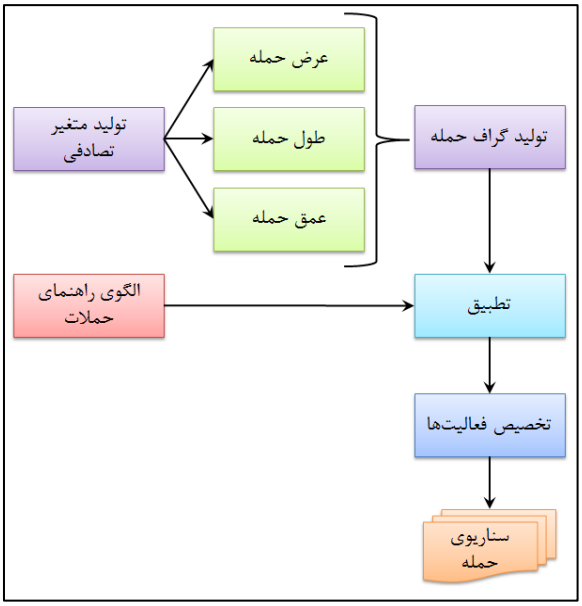
- **تعیین برچسب برای هر خوشه:** برای تعیین تعداد خوشه‌ها و همچنین برچسب هر خوشه از دانش افراد خبره استفاده شده است. جدول (۱) برچسب هر خوشه که نشان‌دهنده فعالیت انجام‌شده در هر گام حمله است را نشان می‌دهد. لازم به توضیح است که اطلاعات این جدول بر اساس نظرات افراد خبره تدوین شده است.

جدول (۱): فعالیت‌های مربوط به هر گام حمله.

هدف	توسعه	نفوذ	شناسایی
انکار	شبکه	مهمان	پویش
اخلال	سیستم		شنود
تزریق	پورت	کاربر	شمارش
تغییر	سرویس		بررسی
تخریب	برنامه	مدیر	درخواست
سرقت	فرآیند		شکار
حذف	نخ	سایر	جعل
انتشار	متغیر		فریب

۲-۲- مولد سناریوی حمله

یافتن سناریوی حمله واقعی یکی از چالش‌های اصلی در انواع دادگان موجود است و موجب می‌شود که در اکثر دادگان، حقیقت زمینه[1] که شامل مجموعه رخدادهای واقعی در فضای فیزیکی است، مخفی بماند؛ اما درروش پیشنهادی از یک مولد سناریوی حمله برای تعیین فعالیت‌هایی که مهاجم فرضی (شبیه‌سازی‌شده) انجام می‌دهد استفاده شده است. شکل (۴) طرح پیشنهادی برای مولد سناریوی حمله را نشان می‌دهد.



شکل (۴): طرح پیشنهادی برای مولد سناریوی حمله.

[1] Ground Truth

همان‌طور که در شکل (۴) نیز نشان داده شده است، برای تولید سناریوی حمله، ابتدا یک گراف تصادفی تشکیل داده می‌شود. این گراف که بر اساس ۳ متغیر تصادفی برای مشخص کردن مؤلفه‌های عرض[2]، طول[3] و عمق[4] حمله ایجاد می‌شود، مبنای اصلی یک سناریوی حمله تصادفی خواهد بود. پس‌ازآنکه گراف حمله[5] تولید شد آن را با الگوی راهنمای حملات تطبیق داده و هرکدام از گره‌های آن با یکی از گره‌های موجود در الگوی راهنمای حملات متناظر می‌شود. سپس برچسب گره متناظر به همراه یال‌های موجود در الگوی راهنمای حملات بر روی گراف موردنظر درج شده تا فعالیت‌های مربوط به الگوی راهنمای حملات به همراه یال‌های مربوطه در گراف تصادفی ذخیره گردند. اکنون این گراف یک سناریوی حمله[6] را نشان می‌دهد که درواقع یک زیرگراف[7] از الگوی راهنمای حملات است.

در ادامه بخش‌های مختلف طرح پیشنهادی با جزئیات بیشتری توضیح داده شده است.

- **تولید متغیر تصادفی عرض، طول و عمق حمله:** اگر بخواهیم که حملات چندگامی را با جزئیات بیشتری مورد بررسی قرار دهیم باید بتوانیم مشخصه‌هایی از آن‌ها را که قابل مشاهده هستند به‌عنوان مؤلفه‌های حمله تعیین کرده و تأثیر آن‌ها را بر روی حملاتی که توسط مهاجمین مختلف انجام می‌شوند مورد بررسی قرار دهیم. در این تحقیق بر اساس شکل ظاهری گراف حمله، سه ویژگی جدید تحت عنوان عرض، طول و عمق حمله، به شرح زیر، تعریف شده است:

  - **عرض حمله (W):** ما حداکثر تعداد فعالیت‌های متفاوت و منحصربه‌فردی که در یک گام از حمله انجام می‌شوند را عرض حمله تعریف می‌کنیم. بر اساس این تعریف می‌توان بر مبنای مؤلفه عرض حمله به چند نکته دقت نمود. اولاً، عرض حمله با قابلیت‌های مهاجم رابطه مستقیمی دارد و نشان می‌دهد که یک مهاجم چقدر با فعالیت‌های مختلفی که می‌توان در هر گام از حمله انجام داد آشنایی دارد. ثانیاً، نشان‌دهنده میزان تلاشی است که یک مهاجم برای تکمیل یک گام از حمله انجام می‌دهد.

  - **طول حمله (L):** ما حداکثر تعداد فعالیت‌هایی که یک مهاجم برای تکمیل سناریوی حمله خود انجام می‌دهد را طول حمله تعریف می‌کنیم. بر اساس این تعریف می‌توان بر

[2] Width
[3] Length
[4] Depth
[5] Attack Graph
[6] Attack Scenario
[7] Subgraph

اساس مؤلفه طول حمله به چند نکته توجه نمود. اولاً هرچه طول یک حمله کمتر باشد نشان‌دهنده این موضوع است که مهاجم توانسته است با کمترین فعالیت‌ها به مقصود خود برسد. ثانیاً اگر طول حمله بزرگ باشد نشان‌دهنده عدم توانایی مهاجم یا پیچیدگی محیط عملیات خواهد بود.

- **عمق حمله (D)**: ما برای تعریف مؤلفه عمق حمله که نشان‌دهنده شدت حمله است به هر گام از حمله یک عدد متناسب با جایگاه آن گام در الگوی راهنمای حملات نسبت داده‌ایم؛ یعنی به ترتیب گام‌های شناسایی، نفوذ، توسعه دسترسی، هدف را از ۱ تا ۴ شماره‌گذاری کرده‌ایم. سپس تعداد فعالیت‌های هر گام را در این شماره ضرب کرده و مجموع آن را بر تعداد کل فعالیت‌ها تقسیم می‌کنیم. رابطه زیر نحوه محاسبه عمق حمله را نشان می‌دهد.

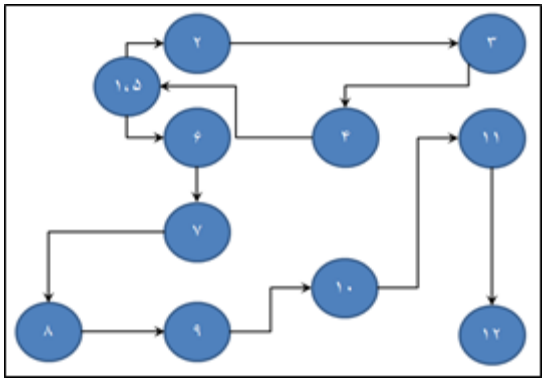
$$\text{عمق حمله} = \frac{\sum_{i=1}^{4}(\mathrm{n}_i \times Action_i)}{N_A} \qquad (۴)$$

که در آن، $Action_i$ نشان‌دهنده تعداد فعالیت‌های گام i، n_i نشان‌دهنده شماره گام حمله و N_A نشان‌دهنده تعداد کل فعالیت‌ها است.

همان‌طور که از رابطه (۴) نیز می‌توان نتیجه‌گیری کرد، هرچه عمق حمله بیشتر باشد نشان‌دهنده این موضوع است که فعالیت‌های مهاجم به گام‌های پایانی نزدیک‌تر است. اثبات این موضوع در تعریفی که برای عمق حمله ارائه شده است نهفته است. در واقع ضریب n_i در رابطه (۴) متضمن این موضوع است که هرچه فعالیت‌های انجام‌شده مربوط به گام‌های پایانی حمله باشد، آن‌گاه مقدار بیشتری برای عمق حمله به دست خواهد آمد.

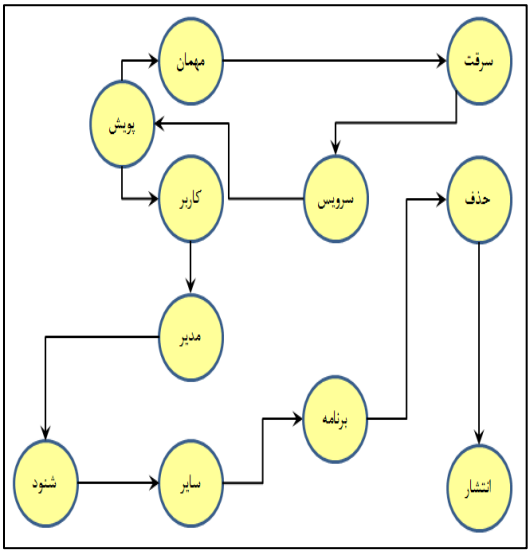
حال با توجه به مؤلفه‌های فوق می‌توان یک گراف تصادفی را ایجاد نمود. ما برای این کار از یک تولیدکننده متغیر تصادفی استفاده می‌کنیم. بدین ترتیب که ابتدا بر اساس دادگان محدوده مؤلفه‌های فوق را اندازه‌گیری کرده و سپس با استفاده از یک توزیع تصادفی یک متغیر در آن محدوده تولید کرده و به مؤلفه موردنظر تخصیص می‌دهیم.

- **تولید گراف حمله:** گراف حمله درواقع یک زیرگراف از الگوی راهنمای حملات است. همان‌طور که قبلاً نیز بیان گردید ما برای تولید این گراف به‌صورت تصادفی از سه مؤلفه تصادفی طول، عرض و عمق حمله استفاده کرده و بر اساس آن یک گراف تصادفی را تولید می‌کنیم. شکل (۵) نمونه‌ای از گراف تولید شده را نشان می‌دهد.



شکل (۵): تولید گراف حمله.

- **تطبیق گراف حمله با الگوی راهنما و تخصیص فعالیت‌ها:** گراف حمله یک زیرگراف تصادفی است که برچسب گره‌های آن نیز به ترتیب پیمایش آن مشخص شده است. برای تطبیق این گراف با الگوی راهنمای حملات کافی است بر اساس عمق هر گره، یکی از فعالیت‌های موجود در گام حمله به‌صورت تصادفی انتخاب و به آن گره نسبت داده شود. شکل (۶) یک نمونه از این تطبیق را نشان می‌دهد.



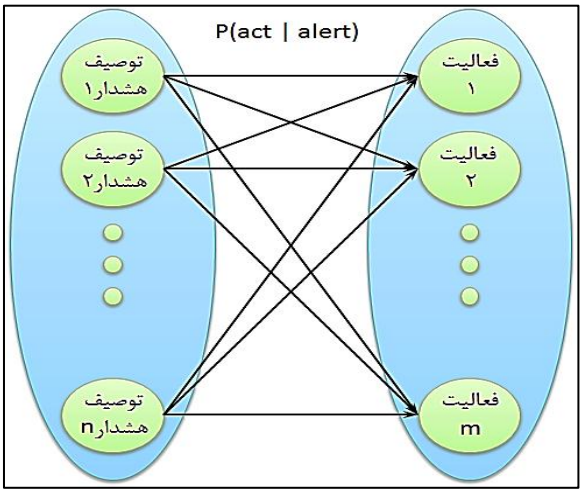
شکل (۶): تطبیق گراف حمله با الگوی راهنمای حملات.

۲-۳. نگاشت فعالیت‌ها به هشدارها

اولین کاری که برای طراحی یک شبیه‌ساز حمله باید انجام شود، مشخص کردن قالب خروجی آن است. لذا لازم است که ابتدا فضای هشدارها را به فضای فعالیت‌ها نگاشت نماییم. به‌عبارتی‌دیگر باید مشخص نماییم که هرکدام از هشدارها بر اساس چه فعالیتی ایجاد شده‌اند.

ازآنجایی‌که ما در الگوی راهنمای پیشنهادی فعالیت‌ها را با استفاده از خوشه‌بندی هشدارها ایجاد نموده‌ایم، با یک پیمایش

ساده بر روی آن‌ها می‌توانیم مشخص کنیم که کدام هشدار با کدام فعالیت ارتباط دارد. لذا الگو احتمالاتی نگاشت فضای هشدار به فضای فعالیت‌ها را مطابق شکل (۷) تشکیل می‌دهیم.



شکل (۷): نگاشت هشدارها به فعالیت‌ها.

همان‌طور که در شکل (۷) نیز نشان داده شده است فعالیت‌ها بر اساس توصیف هشدارها که یکی از ویژگی‌های موجود در دادگان است به وجود آمده‌اند. لذا ما نیز برای نمایش این نگاشت از همان ویژگی توصیف هشدارها استفاده می‌کنیم. با فرض اینکه n هشدار منحصربه‌فرد در دادگان وجود داشته باشد و درمجموع نیز m فعالیت مختلف استخراج شده باشد احتمال وقوع فعالیت j ام به‌شرط مشاهده هشدار i ام به‌صورت زیر محاسبه می‌شود [۲۸].

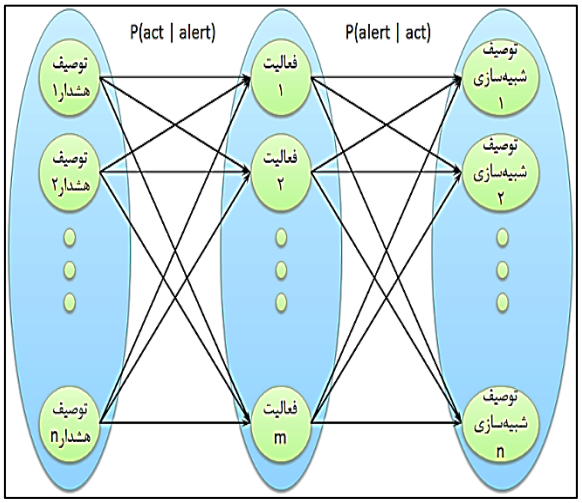
$$P(act_j|alert_i) = \frac{P(act_j \cap alert_i)}{P(alert_i)} \qquad (۵)$$

تا اینجا توانسته‌ایم نگاشت هشدارها به فعالیت‌ها را مشخص نماییم؛ اما آنچه که در شبیه‌سازی حملات چندگامی به آن نیاز داریم عکس این موضوع است یعنی باید بتوانیم با مشخص بودن فعالیت‌ها، هشدارهای مناسب و مرتبط را ایجاد نماییم. به‌عبارتی‌دیگر باید بتوانیم احتمال وقوع هشدار iام را به‌شرط انجام فعالیت jام محاسبه نماییم. برای این کار ما از رابطه (۶) استفاده می‌کنیم [۲۸].

$$P(alert_i|act_j) = \frac{P(act_j|alert_i)P(alert_i)}{P(act_j)} \qquad (۶)$$

با مشخص شدن احتمالات فوق می‌توان الگوی نگاشت فعالیت‌ها به هشدارهای شبیه‌سازی را ایجاد نمود این الگو در شکل (۸) نشان داده شده است.

همان‌طور که در شکل (۸) نشان داده شده است نگاشت سمت چپ توصیف هشدارهای موجود در دادگان را به فعالیت‌های مهاجم نگاشت می‌کند و نگاشت سمت راست فعالیت‌ها را به توصیف هشدارهای شبیه‌سازی نگاشت می‌کند. ما در ادامه برای انجام شبیه‌سازی از نگاشت سمت راست استفاده می‌کنیم.



شکل (۸): نگاشت هشدارها به فعالیت‌ها و فعالیت‌ها به هشدارهای شبیه‌سازی.

۲-۴- توضیح عملکرد شبیه‌ساز پیشنهادی

در طرح پیشنهادی مولد سناریوی حمله به‌صورت تصادفی k مرتبه فراخوانی می‌شود تا این‌که k سناریوی حمله مختلف را تولید نماید. سپس با استفاده از ماژول نگاشت فعالیت‌ها هرکدام از سناریوهای حمله به مجموعه‌ای از توصیف‌های هشدار نگاشت می‌شوند. سپس بر اساس نقشه شبکه دو شناسه برای مهاجم و قربانی انتخاب شده و به هشدارها تخصیص داده می‌شوند. لازم به توضیح است که به ازای هر سناریو انتخاب مهاجم و قربانی تکرار می‌گردد. به‌این‌ترتیب دو ویژگی دیگر از هشدارها تکمیل می‌گردد. همچنین برای انتخاب مهاجم و قربانی، تطبیق درگاه‌ها و آسیب‌پذیری‌های مربوطه نیز بررسی می‌گردند. در مرحله بعدی به ازای هر هشدار در هر سناریو یک برچسب زمانی منحصربه‌فرد به‌صورت تصادفی تولید شده و به‌عنوان ویژگی برچسب زمانی به هر هشدار اضافه می‌شود. اگرچه این برچسب زمانی به ازای هر سناریو منحصربه‌فرد است اما این امکان نیز وجود دارد که به دو هشدار از دو سناریوی مختلف برچسب یکسانی تخصیص داده شود. درنهایت نیز تمامی هشدارها بر اساس این برچسب زمانی مرتب می‌شوند و بدین ترتیب هشدارهای مربوط به سناریوهای مختلف درهم‌سازی می‌شوند. در این مرحله دادگان شبیه‌سازی‌شده، آماده ذخیره‌سازی و استفاده است.

۳- نتایج و بحث

برای پیاده‌سازی روش پیشنهادی لازم است که مؤلفه‌های مختلف آن تنظیم شوند. این کار می‌تواند توسط افراد خبره، داده‌های موجود و یا ترکیبی از آن‌ها انجام شود. در این مقاله برای تنظیم مؤلفه‌های طرح پیشنهادی از دادگان CDX به همراه تجربیات افراد خبره بهره گرفته شده است.

۳-۱- معرفی دادگان

دادگان CDX[1] در سال ۲۰۰۹ میلادی، بر اساس یک مسابقه دفاع سایبری ۴ روزه، بین یک گروه از آکادمی نظامی ایالات‌متحده آمریکا معروف به وست پوینت[2] و یک گروه از آژانس امنیت ملی آمریکا، ایجاد گردیده است.

در این مسابقه دو نوع رقابت دفاعی[3] و تهاجمی[4] در نظر گرفته شده است. در رقابت تهاجمی، هر گروه به دیگری حمله کرده و تلاش می‌کند حملات گروه مقابل را دفع کند. علاوه بر این، یک مجموعه اهداف مشترک نیز وجود دارد که هر دو گروه به آن‌ها حمله می‌کنند.

در این رقابت هر گروه هم نقش مدافع و هم نقش مهاجم را بر عهده دارد و باید یک سری از خدمات مثل وب، رایانامه[5] و گفتگو را فعال نگهدارند. فعالیت این خدمات توسط داوران نظارت شده و مدت‌زمان کارکرد خدمات ملاک قضاوت داوران بوده است. رقابت دفاعی، نسبت به رقابت تهاجمی، در این مورد تفاوت می‌کند که گروه‌ها مجاز به حمله به یکدیگر نبوده و می‌بایست امنیت شبکه خود را تأمین کرده و خدماتی پایدار[6] ارائه کنند.

در این حالت یک گروه اداری به هر دو گروه شرکت‌کننده در مسابقه حمله می‌کند. در این مسابقه، عبور و مرور شبکه که شامل سه نوع عبور و مرور عادی، تهاجمی و دفاعی است ذخیره‌سازی شده و به‌عنوان یک مجموعه داده استاندارد معرفی شده است. جدول (۲) نمونه‌ای از توصیف هشدارهای این دادگان را نشان می‌دهد. به‌عنوان‌مثال، ردیف ۹، توصیف هشداری را نشان می‌دهد که در اثر تلاش برای اجرای از راه دور یک کد ایجاد شده است.

[1] Cyber Defense Exercise
[2] West Point
[3] defensive
[4] offensive
[5] Email
[6] consistent

جدول (۲): نمونه‌ای از توصیف هشدار حملات.

ردیف	توصیف هشدار حمله
۱	(http_inspect) ANOMALOUS HTTP ' 'SERVER ON UNDEFINED HTTP PORT
۲	(http_inspect) WEBROOT DIRECTORY ' ' TRAVERSAL
۳	(smtp) Attempted header name buffer ' ' overflow: 121 chars before colon
۴	(smtp) Attempted specific command buffer ' ' overflow: ETRN, 507 chars
۵	' (spp_frag3) Fragmentation overlap'
۶	BACKDOOR sensepost.exe command shell ' ' attempt
۷	' BAD-TRAFFIC IP Proto 103 PIM'
۸	ET CURRENT_EVENTS NS query for a ' ' single dot, possible ddos
۹	ET EXPLOIT Awstats Remote Code ' ' Execution Attempt
۱۰	ET EXPLOIT XML-RPC for PHP Remote ' ' Code Injection
۱۱	ET SCAN Brute Force Exploit Detector ' ' HTTP Buffer Overflow Detection
۱۲	' ET SCAN Nessus User Agent'
۱۳	' ET SCAN NMAP -sS'
۱۴	ET WEB Barracuda Spam Firewall img.pl ' ' Remote Directory Traversal Attempt
۱۵	ET WEB PHP Remote File Inclusion ' ' (monster list http)
۱۶	ET WEB_SPECIFIC phpBB Remote Code ' ' Execution Attempt
۱۷	' SHELLCODE base64 x86 NOOP'
۱۸	' SMTP AUTH user overflow attempt'
۱۹	' SMTP MAIL FROM overflow attempt'
۲۰	' SQL generic sql update injection attempt'
۲۱	' WEB-CGI /cgi-bin/ access'
۲۲	' WEB-CGI service.cgi access'
۲۳	' WEB-COLDFUSION displayfile access'
۲۴	' WEB-FRONTPAGE service.pwd'
۲۵	' WEB-IIS JET VBA access'
۲۶	WEB-MISC Cisco Catalyst command ' ' execution attempt
۲۷	' WEB-MISC viewcode access'
۲۸	' WEB-PHP /_admin access'

۳-۲- نتایج

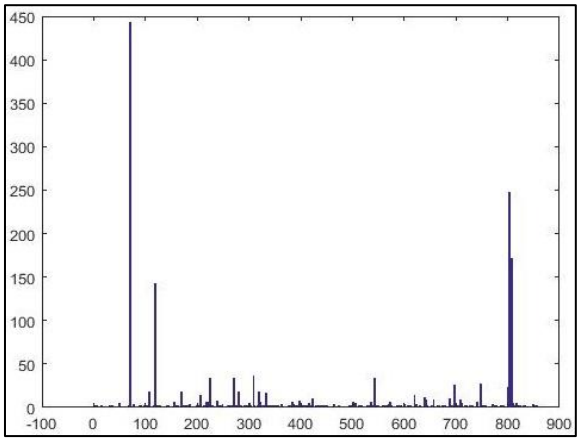
برای پیاده‌سازی طرح پیشنهادی برای شبیه‌سازی حملات سایبری چندگامی از نرم‌افزار MATLAB 2016b استفاده شده است. جدول (۳) نمونه‌هایی از نگاشت توصیف هشدار حملات را به بردارهای عددی نشان می‌دهد. به‌عنوان‌مثال در ردیف اول، بردار [589 401 760 535 661 401 103 4] نشان‌دهنده یک توصیف هشدار حمله است که شامل ۸ واژه است و به ترتیب اعدادی که در این بردار قرار دارند جایگاه واژه‌های مربوط به

توصیف حمله را در واژه‌نامه نشان می‌دهند. یادآوری می‌گردد که 0 ها نیز برای هم‌ترازی بردارها اضافه شده‌اند.

جدول (۳): نمونه‌هایی از بردارهای عددی توصیف هشدار حملات.

بردار عددی توصیف هشدار حمله												
4	103	401	661	535	760	401	589	0	0	0	0	0
6	123	388	504	173	546	49	211	159	227	1	0	0
313	251	526	608	347	69	692	289	591	266	1	0	0
712	741	483	360	855	228	426	122	1	0	0	0	0
806	733	475	337	275	750	122	1	0	0	0	0	0
811	304	243	693	645	398	414	730	672	743	443	122	1

شکل (۹) هیستوگرام واژگان توصیف هشدار حملات را نشان می‌دهد. لازم به توضیح است که این هیستوگرام بر اساس هشدارهای منحصربه‌فرد استخراج شده است و شامل ۸۵۶ واژه مختلف است که از ۶۵۷ هشدار غیرتکراری استخراج شده‌اند. همچنین همان‌طور که در تصویر نیز نشان داده شده است محور افقی مقدار عددی هر واژه را نشان می‌دهد که درواقع همان نمایه واژه‌نامه است و محور عمودی نیز تعداد تکرار هر واژه را در این هشدارها نشان می‌دهد.



شکل (۹): هیستوگرام واژگان توصیف هشدار حملات.

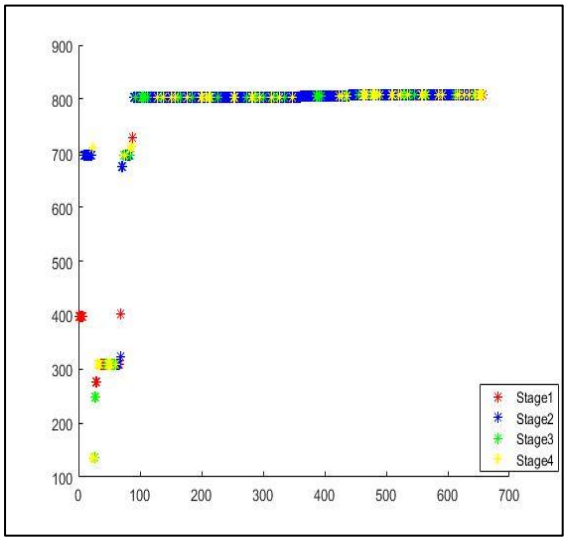
جدول (۴) فهرستی از واژگان پرتکرار که بر اساس هیستوگرام[1] شکل (۹) استخراج شده‌اند را نشان می‌دهد. همان‌طور که در این جدول نشان داده شده است، این واژگان حاوی مفاهیمی هستند که بیانگر نوع رویداد می‌باشد. علاوه بر این، در این جدول نگاشت عددی هر واژه نیز نشان داده شده است که نشان‌دهنده نحوه تبدیل رشته متنی به بردار عددی است.

[1] Histogram

جدول (۴): واژگان پرتکرار موجود در توصیف هشدار حملات.

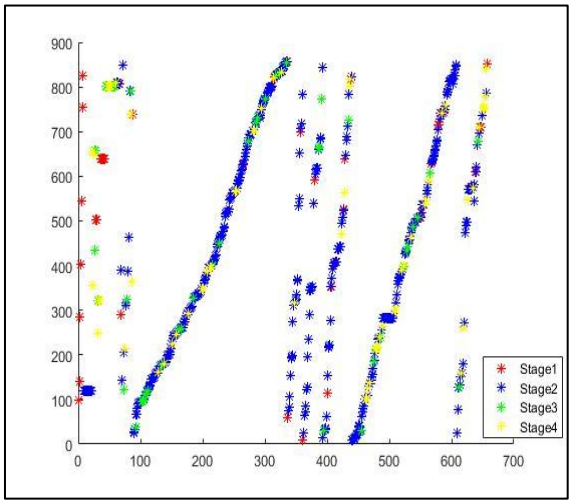
ردیف	واژه	نگاشت عددی	تعداد تکرار
۱	'access'	71	444
۲	'web-cgi'	803	248
۳	'web-misc'	808	172
۴	'attempt'	118	143
۵	'web-php'	809	49
۶	'web-iis'	806	47
۷	'et'	309	37
۸	'command'	224	34
۹	'directory'	271	34
۱۰	'overflow'	542	34
۱۱	'web-frontpage'	805	32
۱۲	'transversal'	747	27
۱۳	'smtp'	697	26
۱۴	'web'	801	24
۱۵	web-' 'coldfusion	804	24
۱۶	'arbitrary'	107	19
۱۷	'buffer'	169	19
۱۸	'execution'	320	19
۱۹	'domino'	281	18
۲۰	'file'	333	17
۲۱	'attempted'	119	14
۲۲	'chars'	207	14
۲۳	'remote'	620	14
۲۴	'scan'	639	12
۲۵	'injection'	422	10
۲۶	'site'	689	10

شکل‌های (۱۰ و ۱۱) توزیع طبقه‌بندی هشدارها را بر اساس روش پیشنهادی نشان می‌دهد. نگاشت توصیف هشدار حملات به بردارهای عددی که قبلا توضیح داده شد، موجب می‌شود که هشدارها در فضای بردارهای عددی نمایش داده شوند. بدین ترتیب مجموعه هشدارها به‌صورت یک ماتریس نمایش داده می‌شود و هر ستون از این ماتریس یک ویژگی را نشان می‌دهد. لازم به توضیح است که هر شکل مبتنی بر یکی از ویژگی‌های بردار عددی هشدارها است و انتخاب یک ویژگی صرفاً برای امکان ترسیم توزیع هشدارها در صفحه انجام شده است. همچنین محور x نشان‌دهنده شماره هشدار و محور y ویژگی انتخابی را نشان می‌دهد. برای نمایش بهتر از رنگ‌بندی برای تفکیک گام حملات استفاده شده است و به ترتیب رنگ‌های قرمز، آبی، سبز و زرد گام‌های ۱ تا ۴ را که نشان‌دهنده شناسایی، نفوذ، توسعه دسترسی و هدف هستند را نشان می‌دهند.



شکل (۱۰): نمایش توزیع طبقه‌بندی هشدارها بر اساس اولین ویژگی.

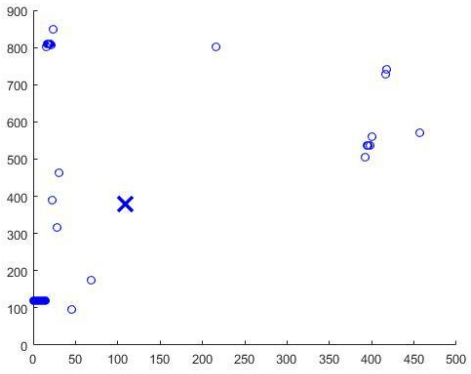
بر اساس شکل (۱۰)، اولین ویژگی قابلیت تفکیک‌کنندگی مناسبی ندارد و استفاده از آن به‌تنهایی نمی‌تواند برای تحلیل داده‌ها ارزشمند باشد. برای انتخاب یک ویژگی مناسب که بتواند توزیع داده‌ها را به‌خوبی نشان دهد، با انجام آزمایش‌های مختلف، هرکدام از ویژگی‌ها مورد بررسی قرار گرفتند و درنهایت دومین ویژگی برای این منظور انتخاب شده است.



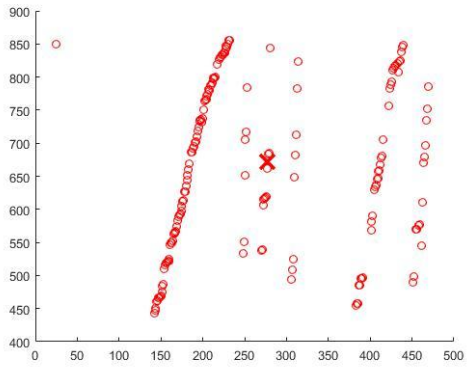
شکل (۱۱): نمایش توزیع طبقه‌بندی هشدارها بر اساس دومین ویژگی

بر اساس شکل (۱۱)، دومین ویژگی قابلیت تفکیک‌کنندگی نسبتاً خوبی دارد توزیع دادگان را به شکلی معنادار نمایش می‌دهد. به همین جهت در شکل‌های (۱۲ الف – د) از این ویژگی برای نمایش توزیع داده‌ها استفاده شده است.

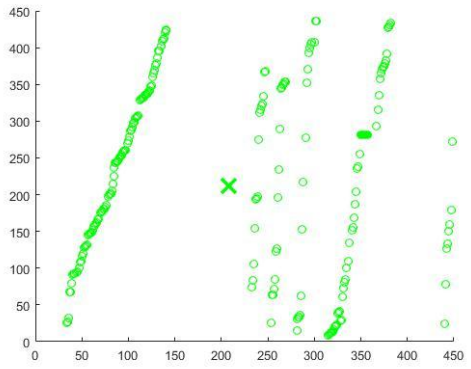
شکل‌های (۱۲ الف – د) به‌عنوان نمونه، خوشه‌بندی گام نفوذ را نشان می‌دهند. سایر خوشه‌بندی‌ها برای سایر گام‌ها نیز به همین ترتیب انجام شده است. این شکل‌ها صرفا نمایش خوشه‌های گام نفوذ و مراکز خوشه‌ها است و توضیح خاصی ندارند.



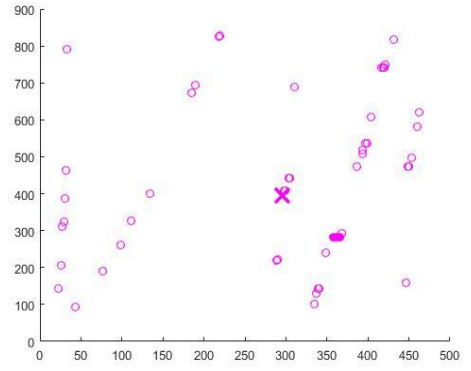
(الف)



(ب)



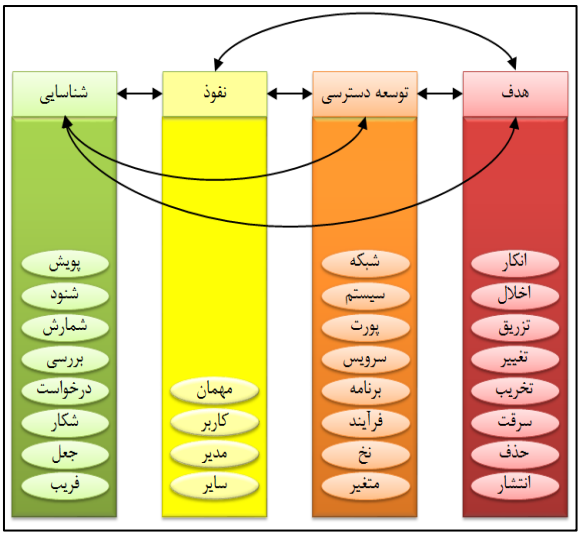
(ج)



(د)

شکل (۱۲): خوشه‌بندی گام نفوذ.

با توجه به اینکه الگوی راهنمای حملات چندگامی یک طرح مفهومی است و برای تشخیص گام حملات و فعالیت‌هایی که در هر گام حمله انجام می‌شود مورد استفاده قرار می‌گیرد. لذا طرح پیشنهادی برای الگوی راهنمای حملات چندگامی، یک ساختار سلسله مراتبی است که در سطح اول آن گام حملات و ارتباطات بین گام‌های مختلف و در سطح دوم آن فعالیت‌های مربوط به هر گام حمله است. شکل (۱۳) این ساختار سلسله مراتبی را نمایش می‌دهد.



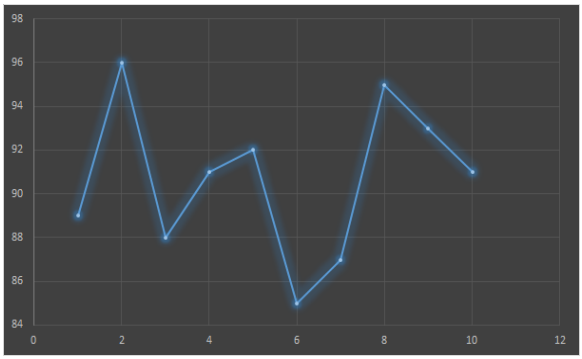
شکل (۱۳): طرح پیشنهادی برای الگوی راهنمای حملات چندگامی

۳-۳- تولید دادگان جدید با استفاده از شبیه‌سازی

با اجرای روش پیشنهادی برای شبیه‌سازی حملات چندگامی می‌توان دادگان متنوع و جدیدی را تولید نمود. جدول (۵) که در پیوست قرار دارد، یک نمونه از دادگان تولید شده را نشان می‌دهد. به‌عنوان نمونه، یکی از سناریوهای موجود در این دادگان نشان‌دهنده حمله‌ای است که از شناسه 7.204.241.161 شروع شده و پس از دسترسی و جمع‌آوری اطلاعات از طریق شناسه 10.1.10.10 موفق به دسترسی به شناسه 7.204.241.161 شده و درنهایت با نفوذ به زیرشبکه 31.154.241.1 موفق می‌شود به سایر سامانه‌های موجود در آن دسترسی داشته باشد.

۳-۴- بحث

اصولاً برای ارزیابی و صحت‌سنجی شبیه‌سازهای حملات سایبری در ادبیات موضوع ازنظر خبرگان استفاده می‌شود؛ اما هدف اصلی در این تحقیق، شبیه‌سازی و تولید یک زیرمجموعه از دادگان واقعی موجود، با سناریوی از پیش تعیین‌شده است. لذا برای اثبات درستی طرح پیشنهادی کافی است نشان دهیم که دادگانی که به این روش تولید می‌شوند یک زیرمجموعه از دادگان واقعی است که در صورت اجرای همان سناریوها در فضای واقعی تولید خواهند شد. برای این منظور با اجرای شبیه‌سازی و ذخیره نمودن دادگان حاصل از شبیه‌سازی و سپس مقایسه نتایج با دادگان واقعی می‌توان به این مهم دست یافت. برای این کار ۱۰ بار روش پیشنهادی اجرا شده و دادگان تولیدشده توسط گروهی ۷ نفره شامل کارشناسان امنیتی و متخصصین حوزه، مورد ارزیابی قرار گرفته است. حاصل تطبیق هر نمونه از دادگان با استفاده از امتیازدهی بین ۰ تا ۱۰۰ انجام شده و سپس با میانگین‌گیری درستی هرکدام از آن‌ها مورد بررسی قرار گرفته است. نمودار زیر نتایج حاصل از این بررسی را نمایش می‌دهد.



شکل (۱۴): نمودار بررسی درستی روش پیشنهادی.

همان‌طور که در شکل (۱۴) نیز نشان داده شده است محور x ها شماره آزمایش‌ها و محور y ها میانگین امتیاز دادگان تولیدشده در هر آزمایش را نشان می‌دهد. در این بررسی در بدترین حالت درستی روش پیشنهادی امتیاز ۸۵ و در بهترین حالت امتیاز ۹۶ را به دست آورده است. به‌طور متوسط نیز با امتیاز ۹۰,۷ می‌توان نتیجه گرفت که درستی روش پیشنهادی از دیدگاه خبرگان این حوزه مورد تأیید قرار گرفته است.

۴- نتیجه‌گیری

فقدان یک دادگان مناسب با حقیقت زمینه مشخص و سناریوهای از پیش تعیین‌شده در تحقیقات مرتبط با دفاع سایبری یک چالش اساسی است و انجام تحقیقات بیشتر در این خصوص به‌عنوان یکی از نیازهای اصلی همواره مورد توجه محققان قرار گرفته است. در این مقاله با درنظر گرفتن این نیاز یک طرح جامع برای شبیه‌سازی حملات سایبری ارائه شده است که دانش موردنیاز خود را با استفاده از روش‌های طبقه‌بندی و خوشه‌بندی مبتنی بر هوش مصنوعی، شامل شبکه‌های عصبی مصنوعی و خوشه‌بندی فازی و همچنین الگوهای احتمالاتی، از سایر دادگان موجود استخراج کرده و به کمک افراد خبره مؤلفه‌های موردنیاز را تنظیم می‌کند. نتایج حاصل از انجام آزمایش‌ها کارایی روش پیشنهادی را برای تولید یک دادگان شبیه‌سازی‌شده جدید، نمایش می‌دهد. مهم‌ترین مزیتی که در دادگان تولیدشده توسط روش پیشنهادی وجود دارد این است که سناریوی حملات مشخص بوده و امکان ارزیابی دقیق را برای سایر تحقیقات فراهم می‌کند. به‌عبارتی‌دیگر، با توجه به امکان ذخیره‌سازی سناریوهای

تولیدشده در شبیه‌سازی می‌توان نتایج تحقیقات مربوط به ردگیری حملات سایبری را با سناریوهای از پیش ذخیره‌شده مورد مقایسه و ارزیابی قرار داد. مزیت دیگری که این روش نسبت به سایر روش‌هایی که به‌صورت دستی انجام می‌شوند این است که تا حد امکان خودکار بوده و احتمال خطای انسانی را به حداقل می‌رساند.

اگرچه به نظر می‌رسد که روش پیشنهادی یک پاسخ مناسب برای مسئله مطرح شده است، اما بازهم نیاز به انجام تحقیقات بیشتر در این خصوص وجود دارد و لازم است که در تحقیقات آینده ابعاد شناختی مرتبط با رفتار مهاجمان سایبری نیز در نظر گرفته شود و ویژگی‌های شناختی بیشتری برای تعیین نحوه رفتار مهاجمان مورد بررسی قرار گیرند. به‌عبارتی‌دیگر پیشنهاد می‌شود که با استفاده از علوم شناختی، تحلیل عمیق‌تری بر روی رفتار مهاجمان سایبری انجام شده و آنچه موجب می‌شود تا یک انسان در شرایط مختلف، تصمیمات متنوعی اتخاذ نماید را مورد تجزیه‌وتحلیل قرار داده و از آن در شبیه‌سازی حملات سایبری استفاده شود. یکی دیگر از پیشنهادهایی که می‌توان به آن اشاره نمود، توجه به فنون مبهم‌سازی و مخفی‌سازی حملات است که در این تحقیق درنظر گرفته نشده‌اند. لذا پیشنهاد می‌شود که ضمن مطالعه دقیق فنون مبهم‌سازی و مخفی‌سازی حملات که توسط مهاجمان باتجربه انجام می‌شود، برای نحوه پیاده‌سازی این فنون در شبیه‌ساز حملات سایبری، راه‌کار مناسبی ارائه شود.

توجه به روش‌های یادگیری عمیق نیز به‌عنوان یکی دیگر از پیشنهادهایی که ممکن است در ادامه این تحقیق به نتایج قابل‌توجهی منجر شود، می‌تواند مفید باشد؛ بنابراین پیشنهاد می‌شود که با استفاده از فنون یادگیری عمیق، راه‌کاری مورد بررسی قرار گیرد که به‌طور توأمان عملیات استخراج ویژگی و طبقه‌بندی یا خوشه‌بندی را انجام داده و تا حد امکان نیاز به دانش افراد خبره را کاهش دهد. استفاده از فنون یادگیری تقویتی نیز می‌تواند قابلیت انعطاف روش پیشنهادی را در مواجهه با دادگان جدید ارتقاء دهد. درواقع پیشنهاد می‌شود که محققان امکان ترکیب دانش پیشین و دانشی که پس از تنظیم پارامترهای الگو، حاصل می‌شود، به همراه دانشی که در آینده ممکن است اضافه شود را در معماری شبیه‌ساز حملات سایبری مورد بررسی قرار دهند.

سناریوهای مختلفی که برای تولید یک دادگان مورد استفاده قرار می‌گیرند بایستی از نظر منطقی درست بوده و با واقعیت زمینه[1] حملات مطابقت داشته باشند. در این تحقیق فرض شده است که سناریوهای مورد استفاده از نظر منطقی درست هستند و اقدامی برای اثبات درستی آنها انجام نشده است. بنابراین، پیشنهاد می‌گردد که به عنوان یک فعالیت تکمیلی در ادامه این تحقیق، صحت منطق این سناریوها که در قالب الگوی راهنمای حملات ارائه شده‌اند، مورد ارزیابی قرار گرفته و با استفاده از روش‌هایی درستی آن‌ها اثبات گردد.

۷- مراجع

[1] Cohen, F. "Simulating Cyber Attacks, Defences, And Consequences"; J. Com. Sec. 1999, 18, 479-518.

[2] Park, J. S.; Lee, J.S.; Kim, H. K.; Jeong, J. R.; Yeom, D. B.; Chi, S. D. "Secusim: A Tool For The Cyber-Attack Simulation"; Proc. Int. Conf. Inf. Comm. Sec. 2001, 471-475.

[3] Kotenko I.; Mankov E. "Experiments With Simulation Of Attacks Against Computer Networks"; Proc. Int. Conf. Math. Meth. Mod. Arch. Com. Net. Sec. 2003, 183-194.

[4] Kuhl, M. E.; Kistner, J.; Costantini, K.; Sudit, M. "Cyber Attack Modeling And Simulation For Network Security Analysis"; Proc. Conf. Wint. Sim. 2007, 1180-1188.

[5] Gonsalves, P. G.; Dougherty, E. T. "Adaptive Cyber-Attack Modeling System" Sens. & C3I Tech. for Hom. Sec. & Def. 2006, 62-104.

[6] Cheung, S.; Lindqvist, U.; Fong, M. W.; "Modeling Multistep Cyber Attacks For Scenario Recognition"; Proc. DARPA Inf. Surv. Conf., 2003, 284-292.

[7] Sudit, M.; Stotz, A.; Holender, M.; "Situational Awareness Of A Coordinated Cyber Attack"; Data Min. Intr. Det. Inf. Assur. & Data Net. Sec. 2005, 114-129.

[8] Costantini, K.; "Development Of A Cyber Attack Simulator For Network Modeling And Cyber Security Analysis"; Msc. Thesis, RIT university, Rochester, 2007.

[9] Brown, B.; Cutts, A.; McGrath, D.; Nicol, D. M.; Smith, T. P.; Tofel, B.; "Simulation Of Cyber Attacks With Applications In Homeland Defense Training"; Sens. & C3I Tech. for Hom. Sec. & Def., 2003, 63-71.

[10] Jajodia, S.; and Noel, S.; "Advanced Cyber Attack Modeling Analysis And Visualization"; George. Mason. Univ. Fairfax. Va., 2010.

[11] Qin, X.; Lee, W.; "Attack Plan Recognition And Prediction Using Causal Networks"; Proc. Comp. Sec. App. Conf., 2004, 370-379.

[12] Xie, P.; Li, J. H.; Ou, X.; Liu, P.; Levy, R.; "Using Bayesian Networks For Cyber Security Analysis"; Inter. Conf. Dep. Sys. & Net. (DSN), 2010, 211-220.

[1] Ground Truth

[13] Stotz, A.; Sudit, M.; "Information Fusion Engine For Real-Time Decision-Making (INFERD): A Perceptual System For Cyber Attack Tracking"; Inter. Conf. Inf. Fus., 2007, 1-8.

[14] Fava, D. S.; Byers, S. R.; Yang, S. J.; "Projecting Cyberattacks Through Variable-Length Markov Models"; J. IEEE. Trans. Inf. Forens. & Sec., 2008, 3, 359-369.

[15] Abbasi, M.; A Azgomi, M.; "Simulation and Modeling Basis Agent of the Smarf DOS Cyber Attack Using Arena Simulation Software"; Proc. Conf. Com. Sci., 2016, (In Persian).

[16] Rajaie, A.; "Security Assessment in Cloud Computing and Cyber Attack Simulation "; Proc. Conf. Elec. Bank. Pay. Sys., 2018, (In Persian).

[17] Holsopple, J.; Yang, S. J.; "Fusia: Future Situation And Impact Awareness"; Inter. Conf. Inf. Fus., 2008, 1-8.

[18] Zhang, Z.; Nait-Abdesselam, F.; Ho, P. H.; "Boosting Markov Reward Models For Probabilistic Security Evaluation By Characterizing Behaviors Of Attacker And Defender"; Inter. Conf. Avail. Reli. & Sec., 2008, 352-359.

[19] Wang, B.; Cai, J.; Zhang, S.; Li, J.; "A Network Security Assessment Model Based On Attack-Defense Game Theory"; Inter. Conf. Comp. App. & Sys. Mod., 2010, 639- 643.

[20] Canadas, N.; Machado, J.; Soares, F.; Barros, C.; Varela, L.; "Simulation Of Cyber Physical Systems Behaviour Using Timed Plant Models"; J. Mechatronics., 2018, 54, 175-185.

[21] Brandstetter V.; Wehrstedt, J. C.; "A Framework For Multidisciplinary Simulation Of Cyber-Physical Production Systems" J. IFAC, 2018, 51, 809-814.

[22] Kour, R.; Thaduri, A.; Karim R; "Predictive model for multistage cyber-attack simulation"; Int. J. Syst. Assur. Eng. Manag, 2020, 1-14.

[23] Aggarwal, P.; Gonzalez, C.; Dutt, V.; "HackIt: A Real-Time Simulation Tool for Studying Real-World Cyberattacks in the Laboratory"; Springer International Publishing: Cham, 2020.

[24] Mayfield, K.P.; Petty, M.D.; Whitaker, T.S.; Cantrell, W.A.; Hice, S.M.; McClendon, J.; Reyes, P.J.; "Component Selection Process in Assembling Cyberattack Simulation Models"; Proc. Int. Conf. Sec. & Manag. 2019, 168-174.

[25] Mayfield, K.P.; Petty, M.D.; Whitaker, T.S.; Bland, J.A.; Cantrell, W.A.; "Component-based implementation of cyberattack simulation models", Proc. ACM. Conf. 2019, 64-71.

[26] Heidarpour, M.; Rashidi, A. J.; Ahmadi, K. D.; "Cyber Situational Awareness Using Intelligent Information Fusion Engine"; J. Sci., 2015, 36, 3218-3229.

[27] Rashidi, A. J.; Jafari, M.; Ahmadi, K. D.; "Projection Of Cyber Attacks By Damage Estimation And Combining Capability And Opportunity Based On Transferable Belief Model"; J. Elec. & Cyb. Def., 2019, 6, 1-12.

[28] Zalta, E. N. "Bayes Theorem"; https://plato.stanford.edu/archives/spr2019/entries/bayes-theorem/, 2019

پیوست

جدول ۵. نمونه‌ای از دادگان تولید شده با شبیه‌ساز پیشنهادی

'Description'	'SourceIP'	'SourcePort'	'DestinationIP'	'Destination Port'	'sTime'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.2'	'1296'	'09:58:56.275385'
'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'51451'	'10.1.10.10'	'25'	'10:00:04.236747'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51451'	'10:00:07.126084'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51451'	'10:00:11.265069'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51451'	'10:00:15.182329'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51451'	'10:00:19.221401'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51451'	'10:00:27.276080'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51451'	'10:00:43.176329'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.2'	'1340'	'10:03:18.591461'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.1'	'1309'	'10:17:49.493157'
'Data sent on stream not accepting data '	'3.75.190.181'	'50523'	'154.241.88.201'	'443'	'10:18:48.857969'
'Data sent on stream not accepting data '	'3.75.190.181'	'55795'	'154.241.88.201'	'443'	'10:19:47.611091'
'TCP Timestamp is outside of PAWS window '	'154.241.88.201'	'80'	'3.75.190.181'	'58667'	'10:20:47.585829'
'TCP Timestamp is outside of PAWS window '	'3.75.190.181'	'57017'	'180.242.137.181'	'5222'	'10:21:46.984272'
'TCP Timestamp is outside of PAWS window '	'154.241.88.201'	'80'	'3.75.190.181'	'49207'	'10:21:46.990027'
'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'57669'	'10.1.10.10'	'25'	'10:22:46.018780'
'TCP Timestamp is outside of PAWS window '	'154.241.88.201'	'80'	'3.75.190.181'	'51429'	'10:22:46.662615'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57669'	'10:22:52.902780'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57669'	'10:23:01.748308'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57669'	'10:23:10.444543'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57669'	'10:23:19.223159'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57669'	'10:23:36.461665'
'Data sent on stream not accepting data '	'3.75.190.181'	'51875'	'154.241.88.201'	'443'	'10:23:48.161817'
'TCP Timestamp is outside of PAWS window '	'3.75.190.181'	'59050'	'180.242.137.181'	'5222'	'10:24:46.981794'
'TCP Timestamp is outside of PAWS window '	'154.241.88.201'	'80'	'3.75.190.181'	'56000'	'10:28:40.920265'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'31.154.241.11'	'1604'	'10:28:42.867602'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'31.154.241.11'	'1606'	'10:28:45.554177'
'TCP Timestamp is outside of PAWS window '	'154.241.88.201'	'80'	'3.75.190.181'	'55945'	'10:29:55.524022'
'TCP Timestamp is outside of PAWS window '	'154.241.88.201'	'80'	'3.75.190.181'	'52329'	'10:31:00.239223'
'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'25'	'3.75.190.181'	'58744'	'10:31:00.267549'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'222.100.5.233'	'3312'	'10:33:07.293811'
'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'51135'	'10.1.10.10'	'25'	'10:33:07.505887'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51135'	'10:33:10.944304'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51135'	'10:33:15.405796'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51135'	'10:33:19.758989'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51135'	'10:33:24.112439'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51135'	'10:33:32.930771'
'TCP Timestamp is outside of PAWS	'154.241.88.201'	'443'	'10.1.60.203'	'51733'	'10:33:48.866696'

window '					

ادامه جدول (۵): نمونه‌ای از دادگان تولید شده با شبیه‌ساز پیشنهادی.

'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'51135'	'10:33:50.449567'
'TCP Timestamp is outside of PAWS window '	'3.75.190.181'	'59012'	'180.242.137.181'	'5222'	'10:37:12.474011'
'TCP Timestamp is outside of PAWS window '	'154.241.88.201'	'80'	'3.75.190.181'	'60384'	'10:37:12.859632'
'TCP Timestamp is outside of PAWS window '	'10.2.195.248'	'36231'	'154.241.88.201'	'443'	'10:39:55.135541'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.1'	'1386'	'10:51:35.684805'
'DNS named version attempt '	'10.2.195.248'	'50917'	'65.190.233.37'	'53'	'11:07:42.866316'
'DNS named authors attempt '	'10.2.195.248'	'47243'	'65.190.233.37'	'53'	'11:07:43.346095'
'TCP Timestamp is outside of PAWS window '	'10.2.195.248'	'38405'	'7.204.241.161'	'25'	'11:08:01.584327'
'TCP Timestamp is outside of PAWS window '	'10.2.195.248'	'51242'	'7.204.241.161'	'25'	'11:08:08.944800'
'ET SCAN NMAP -f -sS '	'10.2.195.248'	'27460'	'7.204.241.161'	'25'	'11:08:32.588672'
'ET SCAN NMAP -sS '	'10.2.195.248'	'27460'	'7.204.241.161'	'25'	'11:08:32.588672'
'TCP Timestamp is outside of PAWS window '	'10.2.195.248'	'6164'	'7.204.241.161'	'25'	'11:08:32.593412'
'TCP Timestamp is outside of PAWS window '	'10.2.195.248'	'18953'	'7.204.241.161'	'25'	'11:08:40.868728'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1695'	'154.241.88.201'	'443'	'11:08:51.101590'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1696'	'154.241.88.201'	'443'	'11:08:51.165970'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1697'	'154.241.88.201'	'443'	'11:08:51.276316'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1698'	'154.241.88.201'	'443'	'11:08:51.285920'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1699'	'154.241.88.201'	'443'	'11:08:51.574372'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57406'	'11:25:20.825420'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57406'	'11:25:26.033318'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57406'	'11:25:36.377330'
'ET SCAN NMAP -f -sS '	'10.2.199.239'	'61562'	'180.242.137.181'	'5222'	'11:25:41.773271'
'ET SCAN NMAP -sS '	'10.2.199.239'	'61562'	'180.242.137.181'	'5222'	'11:25:41.773271'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'57406'	'11:25:46.707192'
'ET SCAN NMAP -f -sS '	'10.2.199.239'	'50164'	'154.241.88.201'	'80'	'11:27:55.527349'
'ET SCAN NMAP -sS '	'10.2.199.239'	'50164'	'154.241.88.201'	'80'	'11:27:55.527349'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1174'	'154.241.88.201'	'80'	'11:28:13.846962'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1178'	'154.241.88.201'	'80'	'11:28:24.003146'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.199.239'	'1178'	'154.241.88.201'	'80'	'11:28:24.003146'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1182'	'154.241.88.201'	'80'	'11:28:29.049649'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1184'	'154.241.88.201'	'80'	'11:28:34.056903'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1187'	'154.241.88.201'	'80'	'11:28:39.193936'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1193'	'154.241.88.201'	'80'	'11:28:44.425012'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.199.239'	'1193'	'154.241.88.201'	'80'	'11:28:44.425012'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1196'	'154.241.88.201'	'80'	'11:28:49.501313'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1200'	'154.241.88.201'	'80'	'11:28:54.574714'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.199.239'	'1200'	'154.241.88.201'	'80'	'11:28:54.574714'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1203'	'154.241.88.201'	'80'	'11:28:59.606025'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.199.239'	'1203'	'154.241.88.201'	'80'	'11:28:59.606025'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1205'	'154.241.88.201'	'80'	'11:29:04.649385'
'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1207'	'154.241.88.201'	'80'	'11:29:09.659498'

'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.199.239'	'1207'	'154.241.88.201'	'80'	'11:29:09.659498'

ادامه جدول (۵): نمونه‌ای از دادگان تولید شده با شبیه‌ساز پیشنهادی.

'ET WEB-MISC Poison Null Byte '	'10.2.199.239'	'1209'	'154.241.88.201'	'80'	'11:29:14.674060'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.199.239'	'1209'	'154.241.88.201'	'80'	'11:29:14.674060'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1413'	'11:31:33.188733'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1413'	'11:31:47.970582'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1413'	'11:32:03.732045'
'TCP Timestamp is outside of PAWS window '	'10.1.60.253'	'52270'	'180.242.137.181'	'5222'	'11:33:10.845062'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'31.154.241.11'	'1726'	'11:35:21.935448'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1727'	'154.241.88.201'	'443'	'11:35:24.334867'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1421'	'11:41:36.308295'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1424'	'11:46:35.907195'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'52263'	'11:51:40.635189'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'52263'	'11:52:16.653339'
'ET SCAN NMAP -f -sS '	'10.2.194.250'	'45015'	'154.241.88.201'	'443'	'12:01:35.013413'
'ET SCAN NMAP -sS '	'10.2.194.250'	'45015'	'154.241.88.201'	'443'	'12:01:35.013413'
'WEB-MISC robots.txt access '	'10.2.194.250'	'45330'	'154.241.88.201'	'80'	'12:01:38.271328'
'TCP Timestamp is outside of PAWS window '	'10.2.196.244'	'33371'	'154.241.88.201'	'443'	'12:02:20.940883'
'TCP Timestamp is outside of PAWS window '	'10.2.196.244'	'33371'	'154.241.88.201'	'443'	'12:02:20.941690'
'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'62219'	'10.1.10.10'	'25'	'12:02:42.504870'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'62219'	'12:02:46.095708'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'62219'	'12:02:50.850481'
'TCP Timestamp is outside of PAWS window '	'10.2.196.244'	'33373'	'154.241.88.201'	'443'	'12:02:51.722006'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'62219'	'12:02:55.650368'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.1'	'1513'	'12:04:32.387310'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.2'	'1669'	'12:04:45.514726'
'TCP Timestamp is outside of PAWS window '	'10.2.192.252'	'34923'	'154.241.88.201'	'443'	'12:05:15.229832'
'ET SCAN NMAP -sA (2) '	'10.2.196.244'	'43109'	'154.241.88.201'	'80'	'12:06:12.619533'
'ET SCAN NMAP -f -sS '	'10.2.196.244'	'43109'	'154.241.88.201'	'80'	'12:06:12.738513'
'ET SCAN NMAP -sS '	'10.2.196.244'	'43109'	'154.241.88.201'	'80'	'12:06:12.738513'
'TCP Timestamp is outside of PAWS window '	'10.2.196.244'	'52024'	'154.241.88.201'	'443'	'12:06:57.734302'
'Data sent on stream after TCP Reset '	'10.1.50.2'	'3488'	'154.241.88.201'	'443'	'12:07:31.718671'
'Data sent on stream after TCP Reset '	'10.1.50.2'	'3497'	'154.241.88.201'	'443'	'12:07:54.901829'
'ET SCAN NMAP -f -sS '	'10.2.197.242'	'55433'	'7.204.241.161'	'25'	'12:08:04.601502'
'ET SCAN NMAP -sS '	'10.2.197.242'	'55433'	'7.204.241.161'	'25'	'12:08:04.601502'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1420'	'12:09:37.729538'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1420'	'12:10:00.020955'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1736'	'154.241.88.201'	'443'	'12:11:50.122361'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1737'	'154.241.88.201'	'443'	'12:11:50.178087'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1738'	'154.241.88.201'	'443'	'12:11:50.235426'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1743'	'154.241.88.201'	'443'	'12:11:54.362676'
'Data sent on stream after TCP Reset '	'31.154.241.11'	'1744'	'154.241.88.201'	'443'	'12:11:55.229651'
'TCP Timestamp is outside of PAWS window '	'10.2.196.243'	'53275'	'154.241.88.201'	'443'	'12:20:36.141564'

'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'59735'	'10.1.10.10'	'25'	'12:23:36.267657'

ادامه جدول (۵): نمونه‌ای از دادگان تولید شده با شبیه‌ساز پیشنهادی.

'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59735'	'12:23:40.850343'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59735'	'12:23:46.839381'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59735'	'12:23:52.826180'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59735'	'12:23:58.805653'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59735'	'12:24:10.661189'
'TCP Timestamp is outside of PAWS window '	'3.75.190.181'	'58281'	'180.242.137.181'	'5222'	'12:24:10.679262'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59735'	'12:24:34.609910'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'49491'	'154.241.88.201'	'443'	'12:24:54.221891'
'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'59684'	'10.1.10.10'	'25'	'12:25:19.429426'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59684'	'12:25:23.677829'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59684'	'12:25:51.556287'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'39047'	'154.241.88.201'	'443'	'12:25:56.482811'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'59684'	'12:26:13.841893'
'Bad segment, adjusted size <= 0 '	'7.204.241.161'	'61800'	'10.1.10.10'	'25'	'12:26:17.401246'
'TCP Timestamp is outside of PAWS window '	'7.204.241.161'	'61800'	'10.1.10.10'	'25'	'12:26:17.740892'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'61800'	'12:26:22.800058'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'39051'	'154.241.88.201'	'443'	'12:26:51.158692'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'39051'	'154.241.88.201'	'443'	'12:26:51.159803'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'39051'	'154.241.88.201'	'443'	'12:26:51.282687'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'61800'	'12:26:54.563180'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'61800'	'12:27:20.167690'
'TCP Timestamp is outside of PAWS window '	'10.2.190.254'	'45781'	'154.241.88.201'	'443'	'12:31:07.691980'
'ET WEB-MISC Poison Null Byte '	'10.2.193.250'	'43993'	'154.241.88.201'	'80'	'12:31:18.247029'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.193.250'	'43993'	'154.241.88.201'	'80'	'12:31:18.247029'
'ET WEB-MISC Poison Null Byte '	'10.2.193.250'	'43993'	'154.241.88.201'	'80'	'12:31:18.461009'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'39265'	'154.241.88.201'	'443'	'12:31:24.182132'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'63064'	'12:38:50.088604'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'63064'	'12:39:02.053831'
'SMTP ClamAV recipient command injection attempt '	'10.1.70.131'	'58530'	'7.204.241.161'	'25'	'12:39:18.352973'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'56408'	'154.241.88.201'	'443'	'12:39:25.416251'
'Data sent on stream not accepting data '	'10.1.10.10'	'25'	'7.204.241.161'	'63064'	'12:39:25.981037'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'56411'	'154.241.88.201'	'443'	'12:39:26.024279'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'56411'	'154.241.88.201'	'443'	'12:39:26.133991'
'TCP Timestamp is outside of PAWS window '	'10.2.196.243'	'49345'	'154.241.88.201'	'443'	'12:39:30.975304'
'TCP Timestamp is outside of PAWS window '	'10.2.196.243'	'49348'	'154.241.88.201'	'443'	'12:39:31.583969'
'TCP Timestamp is outside of PAWS window '	'10.2.196.243'	'49350'	'154.241.88.201'	'443'	'12:39:45.700446'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1426'	'12:39:55.938693'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1426'	'12:39:56.580059'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1427'	'12:44:20.661772'

'TCP Timestamp is outside of PAWS window '	'10.2.190.254'	'39864'	'154.241.88.201'	'443'	'12:44:20.734593'

ادامه جدول (۵): نمونه‌ای از دادگان تولید شده با شبیه‌ساز پیشنهادی.

'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1427'	'12:44:23.217458'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1427'	'12:44:28.329254'
'TCP Timestamp is outside of PAWS window '	'10.2.196.243'	'49247'	'154.241.88.201'	'443'	'12:44:38.379986'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1427'	'12:44:38.551772'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1427'	'12:44:58.993527'
'TCP Timestamp is outside of PAWS window '	'10.2.193.250'	'44442'	'154.241.88.201'	'443'	'12:45:01.464838'
'TCP Timestamp is outside of PAWS window '	'10.2.190.254'	'39868'	'154.241.88.201'	'443'	'12:45:51.266066'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.3'	'61810'	'12:49:09.411744'
'Data sent on stream not accepting data '	'154.241.88.201'	'443'	'10.1.90.5'	'1487'	'12:50:05.258836'
'Data sent on stream not accepting data '	'7.204.241.161'	'993'	'31.154.241.2'	'1831'	'12:55:46.348366'
'ET SCAN NMAP -sA (2) '	'10.2.190.254'	'48801'	'154.241.88.201'	'80'	'13:01:09.323148'
'TCP Timestamp is outside of PAWS window '	'10.1.60.253'	'55958'	'154.241.88.201'	'443'	'13:01:15.210071'
'ET SCAN NMAP -f -sS '	'10.2.190.254'	'48801'	'154.241.88.201'	'80'	'13:01:27.938144'
'ET SCAN NMAP -sS '	'10.2.190.254'	'48801'	'154.241.88.201'	'80'	'13:01:27.938144'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'49193'	'154.241.88.201'	'80'	'13:01:50.364589'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'45885'	'154.241.88.201'	'80'	'13:01:50.589097'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'34412'	'154.241.88.201'	'80'	'13:01:58.665642'
'WEB-IIS nsiislog.dll access '	'10.2.190.254'	'50559'	'154.241.88.201'	'80'	'13:01:58.880651'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'36626'	'154.241.88.201'	'80'	'13:01:58.895402'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.190.254'	'50559'	'154.241.88.201'	'80'	'13:01:58.972141'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'36887'	'154.241.88.201'	'80'	'13:01:59.165085'
'WEB-PHP test.php access '	'10.2.190.254'	'44986'	'154.241.88.201'	'80'	'13:01:59.372095'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'45646'	'154.241.88.201'	'80'	'13:01:59.528836'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'59697'	'154.241.88.201'	'80'	'13:01:59.705919'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'43080'	'154.241.88.201'	'80'	'13:02:21.262448'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'49250'	'154.241.88.201'	'80'	'13:02:22.318897'
'WEB-IIS nsiislog.dll access '	'10.2.190.254'	'55772'	'154.241.88.201'	'80'	'13:02:22.477276'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.190.254'	'55772'	'154.241.88.201'	'80'	'13:02:22.653806'
'(http_inspect) OVERSIZE REQUEST-URI DIRECTORY '	'10.2.190.254'	'52039'	'154.241.88.201'	'80'	'13:02:22.794526'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.190.254'	'52039'	'154.241.88.201'	'80'	'13:02:22.794530'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'52122'	'154.241.88.201'	'80'	'13:02:22.932173'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'42451'	'154.241.88.201'	'80'	'13:02:24.023389'
'WEB-PHP viewtopic.php access '	'10.2.190.254'	'45865'	'154.241.88.201'	'80'	'13:02:30.658068'
'WEB-IIS nsiislog.dll access '	'10.2.190.254'	'48741'	'154.241.88.201'	'80'	'13:02:31.209115'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.190.254'	'48741'	'154.241.88.201'	'80'	'13:02:31.286693'
'EXPLOIT HP OpenView CGI parameter buffer overflow attempt '	'10.2.190.254'	'41570'	'154.241.88.201'	'80'	'13:02:31.952234'
'(http_inspect) BARE BYTE UNICODE ENCODING '	'10.2.190.254'	'41570'	'154.241.88.201'	'80'	'13:02:31.999655'