هشتمین کنفرانس بین‌المللی انجمن رمز ایران
دانشگاه فردوسی مشهد -۲۳ و ۲۴ شهریور ۱۳۹۰

چارچوب شبیه‌سازی سطح بالای حملات سایبری به منظور ارزیابی دسترس‌پذیری

مهرداد آشتیانی[۱] و محمد عبداللهی ازگمی[۲]

[۱] آزمایشگاه ارزیابی کارایی و اتکاپذیری، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران
m_ashtiani@comp.iust.ac.ir

[۲] آزمایشگاه ارزیابی کارایی و اتکاپذیری، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران
azgomi@iust.ac.ir

چکیده

امروزه حملات سایبری به شبکه‌های کامپیوتری به یکی از چالش‌های بزرگ مدیران شبکه‌ها تبدیل شده است. برای مشخص کردن تاثیرت حملات گوناگون بر روی شبکه‌های مختلف در پیکربندی‌های متفاوت، از مدل‌سازی حملات استفاده می‌شود. روش‌های فراوانی برای مدل کردن حملات سایبری به کار گرفته شده است. در این مقاله از شبکه‌های پتری رنگی زمانی سلسله مراتبی، برای مدل‌سازی حملات استفاده شده است. یکی از اهداف این مقاله نشان دادن قدرت و انعطاف بالای شبکه‌های پتری رنگی در مدل‌سازی حملات سایبری با جزئیات بالا و در سطوح انتزاع مختلف است.

در مدل پیشنهادی، عناصر اصلی و موثر در حملات سایبری همانند کامپیوترهای میزبان، دیواره‌های آتش، سیستم‌های تشخیص و پیش‌گیری‌کننده از نفوذ و سرویس‌دهنده‌ها به صورت عناصر قابل استفاده مجدد مدل‌سازی شده‌اند. با کنار هم قرار دادن این عناصر، شبکه‌های مختلف با پیکربندی‌های متفاوت قابل مدل‌سازی است. با شبیه‌سازی مدل ایجاد شده، می‌توان تاثیرات حملات مختلف را تفکیک کرده و معیارهای متفاوتی را برای آن محاسبه کرد. در ادامه چارچوب شبیه سازی توزیع شده حملات سایبری بر اساس مبانی مدل‌سازی انجام شده معرفی خواهد گردید.

کلمات کلیدی

آسیب‌پذیری، تطبیق امضا، حملات سایبری، دسترس‌پذیری، شبکه‌های پتری رنگی،کدهای بهره‌برداری

۱- مقدمه

در این مقاله ما از شبکه‌های پتری رنگی زمانی سلسله مراتبی برای مدل‌سازی عناصر شبکه و سپس شبیه‌سازی فرایند نفوذ به آن استفاده می‌کنیم. یکی از انگیزه‌های استفاده از این روش، ارائه چارچوبی است که به وسیله آن مدیران شبکه قادر باشند عناصر شبکه خود را کنار هم قرار داده و اقدام به شبیه‌سازی حمله و مشاهده نتایج آن بنمایند. به عبارت بهتر به دلیل سلسله مراتبی بودن مدل ایجاد شده، در بالاترین سطح، اجزای شبکه به صورت عناصر قابل استفاده مجددی دیده خواهند شد که می‌توانند به سادگی کنار هم قرار گرفته و شبکه‌های مختلفی را مدل‌سازی کنند.

در این روش سعی شده است که پارامترهای موثر در موفقیت و زمان حملات، در مدل در نظر گرفته شود. همچنین در مدل، برای حمله‌کننده و مدیر سیستم سه سطح توانایی پایین، متوسط و بالا در نظر گرفته شده و چگونگی نفوذ در هرکدام از این سه سطح برای حمله‌کننده تفاوت خواهد کرد. از طرف دیگر چگونگی پیشگیری و مقابله با حملات برای مدیران سیستم نیز با توجه به سطح در نظر گرفته شده متفاوت خواهد بود. در دنیای واقعی، شبکه‌های کامپیوتری دارای ابزارهای دفاعی مختلفی همانند دیواره‌های آتش و سیستم‌های تشخیص و پیشگیری‌کننده از نفوذ هستند. بنابراین در مدل ایجاد شده، سعی گردیده است که رفتار این سیستم‌ها نیز مدل‌سازی گردد.

در حیطه مدل‌سازی فرایند نفوذ کارهای فراوانی صورت گرفته است. بسیاری از کارهای انجام شده مبتنی بر ایجاد مدل و سپس بررسی مدل ایجاد شده و تولید فضای حالتی است که این مدل‌ها ایجاد می‌نمایند. یکی از مشکلات بزرگ این روش انفجار فضای حالت است[1]. به عبارت بهتر این مدل‌ها تنها برای شبکه‌های بسیار کوچک و غیر واقعی مناسبند. رویکردهای بسیار مختلفی برای مدل‌سازی فرایند نفوذ وجود دارد. بسیاری از کارها مبتنی بر درخت‌های حمله و گراف‌های حمله هستند[2,3]. بسیاری از مدل‌سازی‌ها نیز بر اساس زنجیره‌های مارکوف انجام شده است[4]. این روش‌ها در عین داشتن مزایای بسیار، از گسترش‌پذیری و انعطاف کمی برخوردار هستند. در مورد کارهای مشابه انجام گرفته در حیطه مدل‌سازی فرایند نفوذ به وسیله شبکه‌های پتری رنگی، تا به حال دو کار عمده انجام شده است. در [5] به چگونگی تبدیل درخت حمله به شبکه‌های پتری رنگی پرداخته شده است. در این مقاله نشان داده شده است که تمامی عملیاتی که توسط درخت‌های حمله قابل نمایش و مدل‌سازی است، توسط شبکه‌های پتری رنگی نیز قابل نمایش است. در [6] از شبکه‌های پتری رنگی سلسله مراتبی برای نمایش و مدل‌سازی حملات در دو سطح عام و خاص استفاده شده است. موضوع اصلی این مقاله حملات چند مرحله‌ای است. در [7] یک چارچوب شبیه‌سازی توزیع شده معرفی گردیده است. در این شبیه‌سازی مبتنی بر رخداد، سیستم‌های IPS در نظر گرفته شده‌اند. همچنین اعمال متداول برای پیشگیری از حملات توسط این سیستم‌ها نیز معرفی گردیده است.

۲- تعاریف و مفاهیم

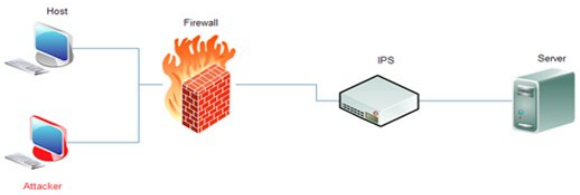
حمله‌کنندگان برای نفوذ به سیستم‌ها از آسیب‌پذیری‌های[1] موجود در آن‌ها استفاده می‌کنند. برای این کار نفوذگران از کدهای بهره‌برداری[2] که برای آن آسیب‌پذیری‌ها نوشته شده استفاده کرده و در صورت استفاده موفقیت آمیز کد بهره‌برداری از آن آسیب‌پذیری، اقدام به بهره‌برداری از سیستم می‌نمایند. به عبارت دیگر همانطور که در [1] بیان شده است، این فرایند از قدم‌های زیر تشکیل می‌شود:

- جمع‌آوری اطلاعات در مورد سیستم هدف
- تعیین آسیب‌پذیری‌های سیستم هدف
- ارسال و اجرای کد بهره‌برداری برای استفاده از آسیب‌پذیری
- بهره‌برداری از سیستم

یکی از دلایل استفاده از شبکه‌های پتری رنگی برای مدل‌سازی حمله نیز همین مسئله است. شبکه‌های پتری رنگی برخلاف شبکه‌های پتری معمولی این اجازه را می‌دهند که به هریک از نشانه‌ها رنگ مشخصی داده شود. این کار باعث می‌شود که بتوان در مدل‌سازی با نشانه‌های مختلفی که با رنگ‌های متفاوت در مکان‌های مختلف قرار می‌گیرند، رفتار منحصر بفردی داشت. بنابراین جداسازی تاثیرات دسترس‌پذیری، محرمانگی و جامعیت به سادگی قابل جداسازی و نمایش است.

۳- مدل‌سازی چندسطحی فرایند نفوذ

در ساده‌ترین حالت فرض کنید که شبکه نشان داده شده در شکل ۱ را می‌خواهیم به وسیله شبکه پتری رنگی زمانی سلسله مراتبی مدل‌سازی کنیم. برای این کار نیازمند آن هستیم که هرکدام از عناصر موجود در این شبکه را مدل‌سازی کرده و در بالاترین سطح از کنار هم قرار دادن هر کدام از این مدل‌ها شبکه‌های پیچیده‌تری را خلق نماییم. مدل این شبکه در شکل ۲ آورده شده است.



شکل(۱): شبکه‌ای ابتدایی متشکل از عناصر تاثیرگذار در فرایند نفوذ

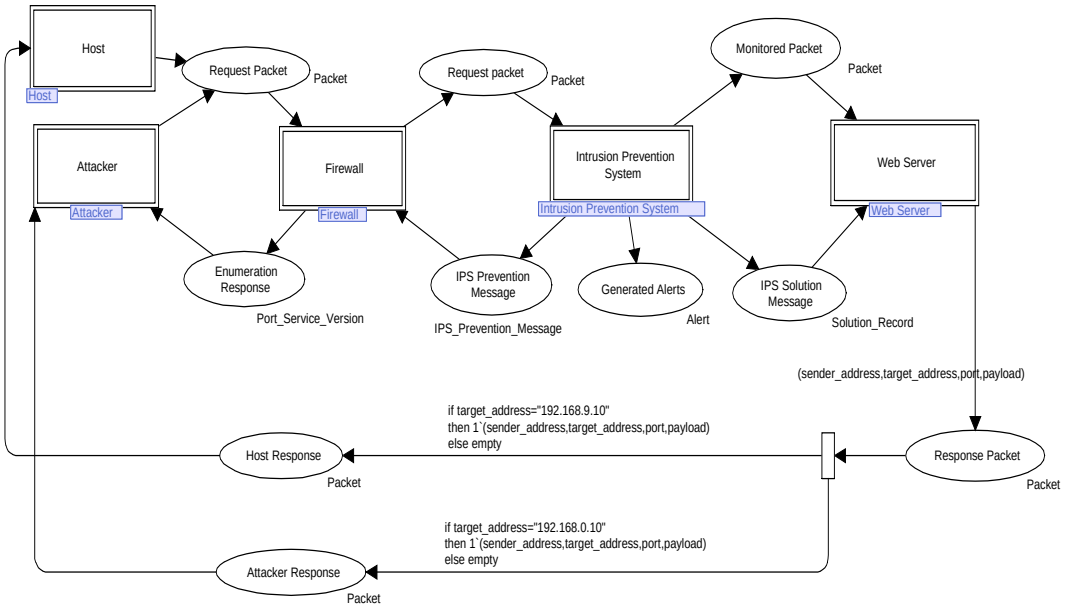
این بالاترین سطح در سلسله مراتب مدل‌های ایجاد شده برای این شبکه است. همانطور که مشاهده می‌کنید هرکدام از عناصر شبکه در قالب یک انتقال نمایش داده شده است. در سطوح پایین‌تر هر کدام از این انتقال‌ها خود دارای مدل مشخصی هستند. بنابراین از کنار هم قرار دادن این عناصر می‌توان شبکه‌های متفاوت و پیچیده‌ای را مدل‌سازی کرد. در این مدل کامپیوتر میزبان(و حمله‌کننده) با نرخ نمایی در طول زمان بسته‌های درخواست خود را به سرویس‌دهنده می‌فرستد.

این بسته‌ها ابتدا از دیواره آتش عبور می‌کنند. در صورتی که بسته برای درگاه بازی، بر روی سرویس‌دهنده ارسال شده باشد، دیواره آتش اجازه عبور بسته را می‌دهد. در غیر این صورت بسته بلوکه خواهد شد. پس از عبور از دیواره آتش، بسته به IPS فرستاده می‌شود. سیستم IPS محموله بسته را با مجموعه امضای کدهای بهره‌برداری موجود خود مطابقت می‌دهد. در صورتی که تطبیق انجام شد، IPS پیغام هشدار مناسب را تولید کرده و با توجه سه سطح توانایی مدیر سیستم پیشگیری مناسب نیز انجام می‌شود. در صورتی که بسته بی خطر و معمولی تشخیص داده شود، به سرویس‌دهنده ارسال می‌شود. سرویس‌دهنده نیز پس از پردازش بسته، پاسخ مربوط به آن را ایجاد کرده و به فرستنده بسته ارسال می‌کند. مدل‌سازی کامپیوتر میزبان در زیرمدل انتقال مربوط به میزبان انجام شده است. پارامتر سطح توانایی، معیار مهمی برای نحوه انتخاب کدهای بهره‌برداری توسط حمله‌کننده است. موفقیت حمله نیز به میزان زیادی از نوع و چگونگی انتخاب کدهای بهره‌بردار، ناشی می‌شود. برای بررسی نحوه انتخاب کدهای آسیب‌پذیری توسط مهاجم، بهتر است ابتدا نگاهی به دسته‌بندی کدهای بهره‌برداری داشته باشیم و سپس به نحوه انتخاب آنها توسط مهاجم بپردازیم. برای دسته‌بندی کدهای بهره‌برداری، از اطلاعات قرار گرفته بر روی پایگاه داده آسیب‌پذیری OSVDB استفاده شده است[8]. این دسته‌بندی عبارتست از:

۱- کدهای بهره‌برداری عمومی: این دسته از کدهای بهره‌برداری، به صورت عمومی در سطح اینترنت گسترش پیدا کرده‌اند. اطلاعات کاملی در مورد این کدهای بهره‌برداری در دست بوده و امضای این کدها در سطح وسیعی در پایگاه‌های داده آسیب‌پذیری موجود است.

۲- کدهای بهره برداری تجاری: این دسته از کدهای بهره‌برداری، توسط تیم‌های حرفه‌ای امنیتی برای ابزارهای تجاری نوشته شده برای بررسی آسیب‌پذیری سیستم‌ها نوشته شده است. این کدها معمولا بسیار موثر بوده و هنوز به صورت وسیعی در پایگاه داده‌های آسیب‌پذیری گسترش پیدا نکرده‌اند.

۳- کدهای بهره‌برداری خصوصی: این دسته از کدهای بهره‌برداری، توسط نفوذگران حرفه‌ای نوشته می‌شوند. این کدها اصلا در سطح عمومی گسترش پیدا نکرده و در دنیای زیر زمینی نفوذگران باقی می‌مانند. نفوذگران معمولا پس از گذشت چند ماه از نوشتن کدهای بهره‌برداری خود، آنها را به صورت عمومی منتشر می‌کنند. تا قبل از این زمان، کد بهره‌برداری خصوصی بوده و سیستم‌های امنیتی و مدیران شبکه‌ها از وجود آنها و آسیب‌پذیری‌های مربوطه با خبر نیستند(کدهای بهره‌برداری روز صفر).



شکل(۲): مدل سطح بالای شبکه نشان داده شده در شکل۱ به وسیله شبکه‌های پتری رنگی زمانی سلسله مراتبی

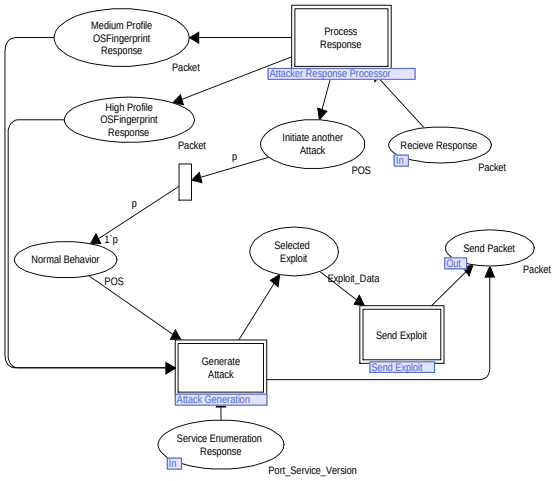
هر کدام از این دسته کدهای بهره‌برداری توسط حمله‌کنندگانی با سطوح مختلف توانایی مورد استفاده قرار می‌گیرند. اما سه سطح توانایی پایین، متوسط و بالا برای حمله‌کننده نیز باید به دقت تعریف شده و ویژگی‌های هریک نیز مشخص شود. در زیر تعاریفی برای این سه سطح توانایی آورده شده است.

۱- مهاجم با سطح توانایی پایین: مهاجمینی که دارای سطح توانایی پایین ارزیابی می‌شوند، معمولا دارای دانش برنامه‌نویسی نبوده و درک چندانی نیز از اطلاعات لازم برای نفوذ به هدف ندارند. این مهاجمین در اغلب اوقات به برنامه‌ها و کدهای بهره‌برداری نوشته شده توسط نفوذگران حرفه‌ای تکیه می‌کنند. البته استفاده آن‌ها از این کدهای بهره‌برداری معمولا به صورت کورکورانه و بدون دقت در مشخصات آنها انجام می‌گیرد. به همین علت این مهاجمین تنها متکی بر کدهای بهره‌برداریی هستند که در اختیار عموم قرار دارند. از طرف دیگر این مهاجمین معمولا بدون توجه به مشخصات سیستم هدف(همانند سیستم عامل، سرویس‌های نصب شده و پورت‌های باز و غیره) دست به انتخاب کدهای بهره‌برداری می‌زنند.

۲- مهاجم با سطح توانایی متوسط: مهاجم دارای سطح توانایی متوسط، معمولا با ابزارهای حرفه‌ای نفوذ آشنا بوده و به کدهای بهره‌برداری تجاری نیز دسترسی دارد. این دسته از مهاجمین با اطلاعات لازم برای نفوذ به سیستم‌های هدف آشنایی داشته و مراحل نفوذ را به درستی طی می‌کنند. البته همچنان دانش برنامه‌نویسی (و در نتیجه ایجاد کدهای بهره‌برداری جدید) چندانی برای این دسته از مهاجمین نمی‌توان متصور بود. در اینجا لیست کدهای بهره‌برداری در اختیار مهاجم، با کدهای بهره‌برداری در حالت قبلی متفاوت است. در این حالت مهاجم میان مجموعه‌ای از کدهای بهره‌برداری عمومی و تجاری، کد بهره‌برداری خود را انتخاب می‌کند. احتمال آنکه امضای کدهای بهره‌برداری تجاری در سیستم‌های تشخیص نفوذ قرار گیرد کمتر از کدهای بهره‌برداری عمومی است. این معیار باعث می‌شود که میزان موفقیت حملات مهاجمین با سطح توانایی متوسط نسبت به مهاجمینی با سطح توانایی پایین بیشتر شود. توجه کنید که در این حالت نیز مهاجم همچنان به کدهای بهره‌برداری خصوصی دسترسی ندارد. نکته مهم دیگر در این حالت آن است که کدهای بهره‌برداری انتخاب شده بر اساس سیستم عامل و سرویس‌های در حال اجرای سیستم هدف انتخاب می‌شوند. همین مساله به مراتب احتمال موفقیت آمیز بودن حمله توسط مهاجم با سطح توانایی متوسط را به نسبت مهاجم با سطح توانایی پایین، بیشتر می‌کند.

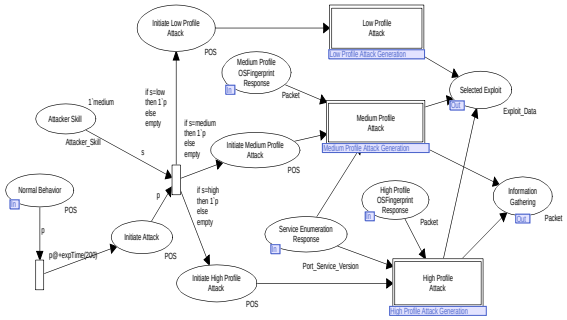
۳- مهاجم با سطح توانایی بالا: مهاجمین با سطح توانایی بالا معمولا دارای دانش عمیقی از برنامه‌نویسی بوده و با ابزارهای حرفه‌ای نفوذ آشنا هستند. این مهاجمین با اطلاعات لازم برای نفوذ به سیستم‌ها کاملا آشنا بوده و مراحل نفوذ به سیستم هدف را نیز به طور کامل طی می‌کنند. این مهاجمین می‌توانند آسیب‌پذیری‌ها را در سیستم‌های کامپیوتری تشخیص داده و برای بهره‌برداری از آنها شروع به ایجاد کدهای بهره‌برداری جدید بنمایند. بنابراین این گونه از مهاجمین معمولا دارای ابزارهای منحصر به فرد و کدهای بهره‌برداری خصوصی خود هستند. در این حالت مجموعه کدهای بهره‌برداری که در اختیار مهاجم قرار خواهد گرفت، متفاوت است. مجموعه کدهای بهره‌برداری که در اختیار مهاجم قرار داده شده است، متشکل از کدهای بهره‌برداری خصوصی و کدهای بهره‌برداری حرفه‌ای تجاری است. این مجموعه کدهای بهره‌برداری به مهاجم سطح بالا اجازه می‌دهند که با احتمال بسیار زیادی از تشخیص سیستم‌های IDS/IPS در امان باقی بمانند. در شکل ۳ مدل سطح بالای حمله‌کننده آورده شده است. دو بخش اصلی مدل، قسمت تولید حمله و پردازش پاسخ است. بخش پردازش پاسخ، پاسخ‌های

رسیده از سرویس‌دهنده را پردازش کرده و محموله مناسب را استخراج می‌کند. در قسمت تولید حمله، برحسب تعاریفی که از سطوح مختلف حمله‌کننده آورده شد، سه بخش تولید حمله در سطوح مختلف مدل‌سازی شده است. بر حسب سطح توانایی انتخاب شده در مکان *Attacker Skill* و مطابق شکل ۴ یکی از این انتقال‌ها اجرا خواهد شد.



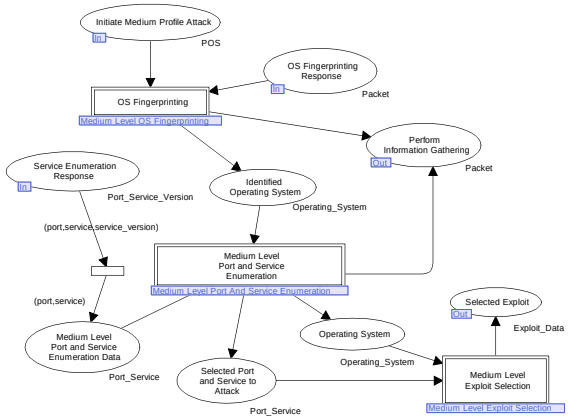
شکل(۳): مدل سطح بالای حمله‌کننده

برای مهاجم با سطح توانایی متوسط مدل‌سازی فرایند نفوذ به صورت شکل ۵ صورت گرفته است. همانطور که مشاهده می‌کنید، این مهاجم ابتدا، اقدام به جمع‌آوری اطلاعات در مورد سیستم هدف می‌نماید. برای این کار مهاجم ابتدا نوع سیستم عامل سرویس‌دهنده را استخراج کرده و سپس اقدام به شمارش درگاه‌های باز و سرویس‌های در حال اجرا بر روی هریک از آنها می‌کند. پس از به دست آوردن این اطلاعات (و با توجه به آنها) کد بهره‌برداری مناسب انتخاب می‌شود. ساختار رنگ کدهای بهره‌برداری در مدل ایجاد شده به صورت نشان داده شده در شکل ۶ تعریف شده است.



شکل(٤): مدل‌سازی تولید حمله در سطوح متفاوت

پس از دریافت شدن بسته توسط سرویس‌دهنده، دو اتفاق ممکن است رخ دهد. یا بسته یک بسته طبیعی درخواست بوده که سرویس‌دهنده به آن پاسخ می‌دهد و یا بسته، یک بسته بهره‌برداری است که توانسته از لایه‌های دفاعی شبکه عبور کرده و به سرویس‌دهنده برسد. در این حالت باید مشخص شود که آیا این بسته بهره‌برداری می‌تواند به سرویس‌دهنده آسیب زده و از آن بهره‌برداری کند یا خیر. تعیین این موضوع در واحد *Exploit infiltration success probability* انجام می‌شود. در صورتی که کد بهره‌برداری امکان آسیب‌رسانی را داشته باشد، مرحله تخریب آغاز خواهد شد. مدل‌سازی این مرحله در واحد *Exploiting Stage* انجام شده است. در نهایت نیز با توجه به اطلاعات استخراج شده از کد بهره‌برداری میزان تاثیر آن بر دسترس‌پذیری، محرمانگی و جامعیت سیستم مشخص خواهد شد.



شکل(٥): مدل‌سازی فرایند نفوذ مهاجم با سطح توانایی متوسط

```
colset Exploit_Signature=string;
colset Exploit_ID=int;
colset Access_Complexity=with High | Medium | Low;
colset Exploit_Data= product Exploit_Signature * Disclosure
  * Access_Complexity * Operating_System * Port_Service_Version;
colset Exploit= product Exploit_ID * Exploit_Data;
colset Signature=string;
```

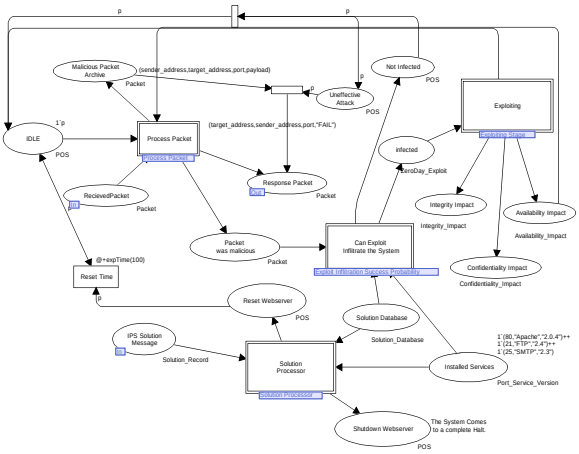
شکل (٦): ساختار رنگ کد بهره‌برداری

همچنین واحد پردازش‌کننده راه حل نیز وظیفه نصب و نگهداری راه حل‌های رسیده از IPS را بر عهده دارد. در شکل ۷ مدل ایجاد شده برای سرویس‌دهنده آورده شده است. یکی از مهمترین بخش‌های این مدل تعیین آن است که آیا کد بهره‌برداری می‌تواند به سیستم آسیب برساند یا خیر. برای تعیین این موضوع باید پارامترهایی همانند سیستم عامل، درگاه‌های باز و سرویس‌های در حال اجرا بر روی سیستم‌های هدف، شماره نسخه سرویس‌ها، بردار دسترسی و وجود راه حل برای آسیب‌پذیری مورد حمله قرار گرفته در نظر گرفته شوند. واحد تعیین احتمال موفقیت کد بهره‌برداری وظیفه تطبیق این پارامترها را بر عهده دارد. پس از دریافت یک کد بهره‌برداری، ابتدا بردار دسترسی آن بررسی می‌شود. اگر بردار دسترسی با نحوه دسترسی مهاجم به سرویس‌دهنده مطابقت داشته باشد به مرحله بعد در تطبیق‌دهی می‌رویم. در استاندارد امتیاز دهی امنیتی CVSS [10] برای بردار دسترسی سه دسته کلی در نظر گفته شده است:

۱- محلی: در این حالت برای آنکه کد بهره‌برداری بر روی سیستم هدف موثر باشد، حمله‌کننده یا باید به سیستم هدف دسترسی فیزیکی داشته باشد و به صورت محلی کد بهره‌برداری را بر روی سیستم اجرا کند و یا باید در یک شبکه محلی با سیستم هدف قرار داشته باشد.

۲- شبکه مجاور: در این حالت برای موثر بودن کد بهره‌برداری، حمله کننده (و یا نقطه فرستاده شدن کد بهره‌برداری) باید در شبکه مجاور سیستم هدف باشد. به عنوان مثال اگر آدرس فرستنده کد بهره‌برداری ۱۹۲.۱۶۸.۰.۱ و آدرس سیستم هدف ۱۹۲.۱۷۶.۱۰.۲ باشد، به دلیل آنکه مهاجم در زیر شبکه مجاور سیستم هدف قرار ندارد، کد بهره‌برداری او نمی‌تواند تاثیر گذار باشد.

۳-راه دور: در این حالت کد بهره‌برداری تولید شده توسط مهاجم می‌تواند از راه دور و بدون نیاز به دسترسی محلی یا قرار داشتن در شبکه مجاور، موثر واقع شود.

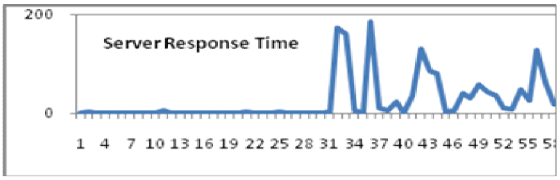


شکل(۷): مدل سرویس‌دهنده

در مرحله دوم سیستم عامل مورد نیاز کد بهره‌برداری با سیستم عامل سرویس‌دهنده تطبیق داده می‌شود. در صورت تطبیق، در مرحله بعد، درگاه‌های باز و سرویس‌های در حال اجرا بر روی هرکدام از آنها تطبیق داده خواهد شد. در نهایت نیز بررسی می‌گردد که آیا برای آسیب‌پذیریی که کد بهره‌برداری از آن استفاده می‌نماید، راه حلی نصب و اجرا شده است یا خیر. اگر به عنوان مثال آن آسیب‌پذیری وصله شده باشد، کد بهره‌برداری قادر به تخریب سیستم و بهره‌برداری از آن نخواهد بود. پس از آنکه کد بهره‌برداری تاثیرگذار تشخیص داده شد، وارد مرحله تخریب می‌شویم. در این قسمت مدت زمانی طول خواهد کشید که کد بهره‌برداری با موفقیت اجرا شده و تاثیر خود را بر روی سرویس‌دهنده بگذارد. این زمان، که برای آن اصطلاح زمان تخریب آورده شده است به میزان زیادی به پیچیدگی دسترسی کد بهره‌برداری وابسته است. به هر میزان که پیچیدگی کد بهره‌برداری بیشتر باشد مدت زمان اجرای موفق آن نیز بیشتر خواهد شد.

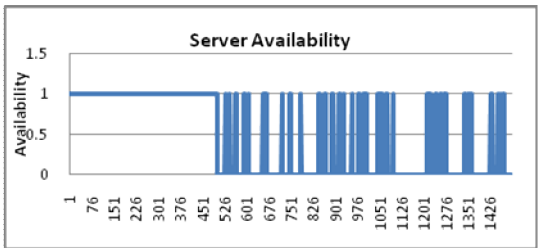
٤- ارزیابی مدل

برای ارزیابی مدل و نمایش معیارهای عملیاتی باید سناریویی را در نظر گرفت. پس از تعیین سناریو و پیکربندی مناسب عناصر، مدل توسط ابزار CPN Tool[11] شبیه‌سازی شده و معیارهای مختلف از طریق تعریف جمع‌آوری‌کننده‌های داده مناسب، محاسبه می‌شوند. برای هر کدام از این سناریوها شبکه ساده نشان داده شده در شکل ۱ در نظر گرفته شده است. سرویس‌دهنده دارای سیستم عامل لینوکس بوده و سرویس‌های FTP، Apache و SMTP به ترتیب بر روی درگاه‌های ۲۱،۸۰ و ۲۵ در حال اجرا هستند. دیواره آتش نیز تنها به ترافیک ورودی به درگاه‌های ۲۱ و ۸۰ اجازه عبور می‌دهد.. در نمودار شکل ۸، تغییرات زمان پاسخ سرویس‌دهنده در طول شبیه‌سازی آورده شده است.

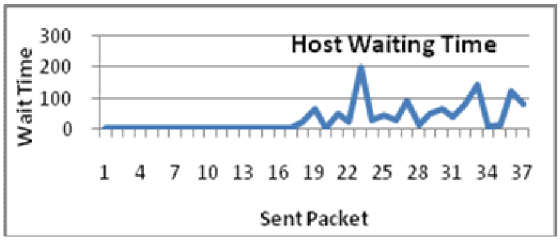


شکل(۸): زمان پاسخ سرویس‌دهنده در حمله‌ای با تاثیر جزئی بر دسترس‌پذیری

این نمودار به دست آمده منطبق بر تعریفی است که در مستندات CVSS در مورد تاثیر جزئی بر دسترس پذیری آورده شده است. برای شبیه‌سازی تاثیرپذیری جزئی، از یک فرایند روشن/خاموش با طول بازه‌های تصادفی استفاده شده است. از آنجایی‌که دسترس‌پذیری به صورت جزئی تحت تاثیر قرا گرفته است، زمان پاسخ نیز دچار نوسانات شدید می‌شود. تغییرات دسترس‌پذیری سرویس‌دهنده نیز در طول شبیه‌سازی مطابق شکل ۹ است.



شکل(۹): دسترس‌پذیری سرویس‌دهنده در حمله‌ای با تاثیر جزئی بر دسترس‌پذیری



شکل(۱۰): زمان انتظار میزبان در حمله‌ای با تاثیر جزئی بر روی دسترس‌پذیری

٥- شبیه‌ساز توزیع‌شده حملات سایبری

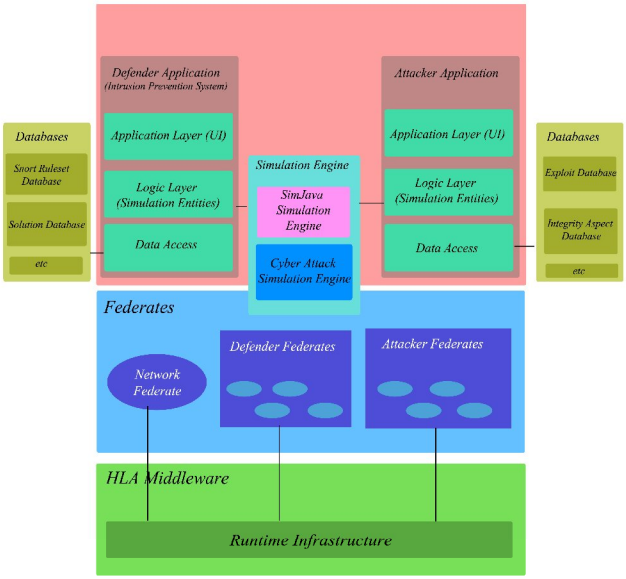
بر مبنای مفاهیم تئوری مطرح‌شده در بخش قبلی، در این قسمت یک شبیه ساز توزیع‌شده حملات سایبری معرفی خواهد گردید. شبیه‌ساز طراحی شده که در شکل ۱۱ نیز نشان داده شده است، مبتنی بر معماری سطح بالا پیاده‌سازی شده است. در این معماری بخش‌های مستقل شبیه‌سازی می‌توانند در قالب فدرال‌های مختلفی به فدراسیون شبیه‌سازی متصل شده و با یکدیگر ارتباط برقرار کنند. معماری سطح بالا برای برقراری ارتباط میان فدرال‌ها از دو مکانیزم کلی Publish/Subscribe و فرستادن Interaction استفاده می‌کند. در شبیه‌ساز حملات سایبری توزیع‌شده، سه دسته کلی از فدرال‌ها وجود دارد. این سه دسته عبارتند از:

۱- فدرال شبکه: این فدرال بخش اصلی شبیه‌سازی است. در این فدرال قسمت‌های مختلفی قرار گرفته است که مهمترین آنها عبارتند از طراح شبکه، شبیه ساز و بخش گزارش گیری.

۲-فدرال مهاجم: در این فدرال، حمله‌کننده به وسیله برنامه‌ای که در اختیارش قرار می‌گیرد شروع به حمله می‌نماید. مهاجم می‌تواند از امضای کدهای بهره‌برداری موجود در پایگاه داده آسیب‌پذیری OSVDB استفاده کند. همچنین حمله‌کننده در حالت اجرای تعاملی شبیه‌سازی قادر است اعمال لازم برای نفوذ به سیستم‌ها همانند شمارش سیستم عامل و سرویس‌ها و پویش پورت‌های باز را نیز انجام دهد.

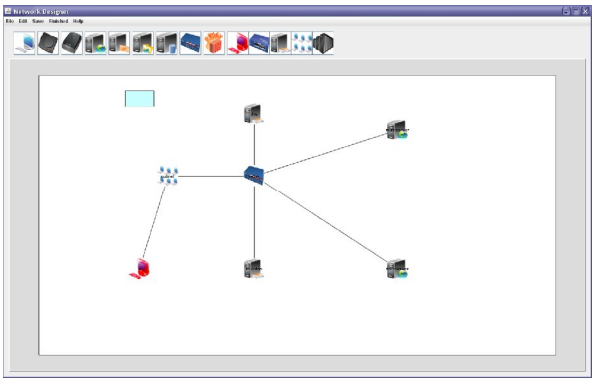
۳- فدرال مدافع: این فدرال‌ها به دو دسته کلی سیستم‌های تشخیص نفوذ و سیستم‌های پیشگیری‌کننده از نفوذ تقسیم‌بندی می‌شوند. برای شبیه سازی سیستم‌های تشخیص نفوذ از نحوه کار IDS های مبتنی بر امضا که

گونه رایج موجود در شبکه‌های امروزی هستند الگو برداری شده است. برای این کار نیز از مجموعه قواعد Snort استفاده شده است.



شکل (۱۱): معماری شبیه‌ساز توزیع‌شده حملات سایبری

نمونه ای از سناریوی جعل سرویس دهنده نام طراحی شده در شبیه ساز در شکل ۱۲ نمایش داده شده است.



شکل (۱۲): شبکه طراحی شده برای حمله جعل سرویس‌دهنده نام در شبیه‌ساز

از آنجایی‌که ترافیک موجود در اینترنت دارای خاصیت خود-شباهت[3]است[12]، برای شبیه‌سازی ترافیک از فرایند انفجاری پواسن- پارتو[4] استفاده شده است.

٦- نتیجه‌گیری

مدل‌سازی فرایند نفوذ به وسیله شبکه‌های پتری رنگی زمانی سلسله مراتبی، دارای مزایای فراوانی است. بزرگترین مزیت این روش توانایی ایجاد چارچوبی از عناصر قابل استفاده مجدد و قابل اتصال به هم برای مدل‌سازی شبکه‌های مختلف با پیکربندی‌های متفاوت است. همچنین با گسترش این مدل و ایجاد یک شبیه‌ساز توزیع‌شده حملات سایبری می‌توان با استفاده از رویکرد شبیه‌سازی، مدیران شبکه را در ارزیابی امنیتی شبکه‌های خود یاری کرده و نیز آنها را تمرین‌دهی کرد.

تشکر و قدردانی

این مقاله با حمایت مالی مؤسسه تحقیقات ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) انجام شده است. بدین وسیله از این مؤسسه تشکر و قدردانی می‌شود.

مراجع

[1] M. Kuhl, J. Kistner, K.Costantini and M.Sudit, " *Cyber attack modeling and simulation for network security analysis*", Proc. of the 39th conference on Winter simulation,vol. 1, NJ, USA, 15-Dec, pp. 1180-1188, 2007.

[2] V. Saini, Q. Duan and V.Paruchuri, "*Threat Modeling using Attack Trees*",Journal of Computing Science in Colleges,*vol. 23, Issue.4*, pp. 124–131, 2008

[3] L.Wang, T.Islam, T.Long, A.Singhal and S.Jajodia, " *An Attack Graph-Based Probabilistic Security Metric*", Proc. of the 22nd conference on Data and Application Security,vol. 5094, London, UK, 13-Jul, pp. 283-296, 2008.

[4] J. Almasizadeh and M. Abdollahi Azgomi, "*Intrusion Process Modeling for Security Quantification*", Proc. of the 4th International Conference on Availability, Reliability and Security (ARES'09), March 16-19, Fukuoka Institute of Technology (FIT), Fukuoka, Japan, IEEE CS Press, 2009, pp. 114-121

[5] S.Zhou, Z. Qin, F.Zhang, X. Zhang, W.Chen and J. Liu, "*Coloured Petri net based Attack Modeling*", Proc. of the 9th International Conference on Rough Sets,Data Mining and Granular Computing,vol. 2639, Chongqing, China, 26-May, pp. 583 2003.

[6] R.Wu , W. Li and H.Huang , "*An Attack Modeling based on hierarchical coloured petri nets,*"Proc. of the International conference on computer and electrical engineering.ICCEE,vol. 1, Phuket, Thailand, 20-Dec, pp. 918-921, 2008.

[7] L. Flagg, G. Streeter, K.Costantini and A.Potter, " *Bringing knowledge to network defense*,"Proc. of the 2007 Spring Simulation Multi Conference,vol. 3, San Diego, USA, 25-March, pp. 370-377, 2007.

[8] *Open Source Vulnerability Database*, May 2011. http://www.osvdb.org

[9] "*NetSim: A Distributed Network Simulation to Support Cyber Exercises*", presented at Huntsville Simulation Conference – McGraw Hill, 2004

[10] *CVSS Complete Documentatiom*, version 2 ,May 2011, http://www.first.org/cvss.

[11] *CPN Tool Home page*, April 2011, http://www.cpntool.org.

[12] T.Karagiannis,M.Molle,M.Faloutsos,"Long-range dependence ten years of Internet traffic modeling" IEEE Internet computing, vol.8, Issue.5, September 27 ,pp.57-64, 2004.

زیرنویس‌ها

[1] Vulnerability
[2] Exploit
[3] Self similarity
[4] Poisson-Pareto Burst Process