مجله علمی ـ پژوهشی «پدافند الکترونیکی و سایبری»
سال اول، شماره ۳، پاییز ۱۳۹۲، ص ۵۱-۴۳

طراحی و ساخت پایگاه دانش سیستم خبره برای آزمون امنیت شبکه

محمدعلی جوادزاده[1*]، محمدرضا کنگاوری[2]، سید جواد فتحی[3]
۱- دانشجوی دکتری، دانشگاه علم و صنعت ایران، ۲- دانشیار، دانشگاه علم و صنعت ایران
۳- دانشجوی کارشناسی ارشد، دانشگاه امام حسین (ع)
(دریافت۲۴/ ۸۹/۰۸، پذیرش: ۹۲/۰۴/۰۹)

چکیده

مرحله تولید پایگاه دانش سیستم‌های خبره، تنگنای طراحی سیستم‌های خبره محسوب می‌شود. هزینه انجام این مرحله از ابعاد مختلف از قبیل زمان، سرمایه، نیروی انسانی، دقت و مانند آن به‌حدی است که بخش اعظم هزینه تولید سیستم خبره محسوب می‌شود. موفق‌ترین روش برای برخورد با این تنگنا، توسعه ابزارهای خاص اخذ دانش از انسان خبره است. این ابزارها که تک منظوره هستند، به انسان خبره امکان می‌دهد پایگاه دانش سیستم خبره را با هزینه مناسبی تولید نماید. هدف مقاله حاضر، شرح طراحی زبان مدل‌سازی دانش امنیت شبکه NSKMAL و اشاره‌ای به محیط گرافیکی NSKTOOL است که جهت تولید پایگاه دانش سیستم خبره تحلیل‌گر امنیت شبکه طراحی و تولید شده‌اند. انسان خبره امنیت شبکه قادر است با استفاده از محیط گرافیکی NSKTOOL دانش امنیت را فرموله و به پایگاه دانش منتقل نماید. نتیجه تعامل انسان خبره و NSKTOOL به مجموعه‌ای از دستورات زبان NSKMAL تبدیل شده که متعاقباً توسط مفسر زبان NSKMAL تفسیر و تغییرات لازم در پایگاه دانش اعمال می‌شود.

واژه‌های کلیدی: امنیت شبکه، دانش، سیستم خبره، پایگاه دانش، مدل‌سازی دانش.

۱. مقدمه

آسیب‌پذیری شبکه‌های کامپیوتری به‌عنوان زیرساخت فناوری اطلاعات، یکی از مشکلات مهم این حوزه محسوب می‌شود. بخش عمده این آسیب‌پذیری‌ها به‌علت پیکربندی‌های نادرست در نرم‌افزار و سازمان شبکه است. از این رو متخصصین شبکه، از ابزارهای امنیتی مختلفی استفاده می‌کنند تا از منابع و سرویس‌های ارزشمند در مقابل تهدیدات محافظت به‌عمل آورند. ابزارهای امنیتی به‌تنهایی نمی‌توانند دانش لازم را جهت همبستگی و چگونگی در کنار هم قراردادن این ابزارها در اختیار کاربران آنها قرار دهد. برای رسیدن به امنیت مطلوب، به‌ناچار سازمان‌ها باید از متخصصان حرفه‌ای برای هدف خود استفاده کنند (مانند Red Team). این متخصصان به داده‌های جمع‌آوری شده نظم و ترتیب داده و هر نوع حمله‌ای را تحلیل می‌کنند. به‌عنوان مثال ایشان نموداری از وضعیت آسیب‌پذیری‌های موجود در سیستم‌ها را که می‌توانند منجر به بروز حمله شوند، تهیه می‌کنند. از این رو نیاز مبرمی برای به‌دست آوردن درک عمیق از گزارش‌های امنیتی استخراج شده وجود دارد تا مشخص شود که واقعاً چه چیزی در پشت صحنه اتفاق می‌افتد. برای مثال باز بودن پورت غیرضروری روی یک ماشین خاص می‌تواند منجر به یک حمله ناشناخته شود. بنابراین باید کاوشی عمیق در مورد چگونگی انجام یک حمله انجام داد. حمله‌های امنیتی با اجرای یک یا چند اکسپلویت انجام می‌شود. اکسپلویت برنامه‌ای است که یک یا چند آسیب‌پذیری موجود در نرم‌افزار نصب شده که سبب ایجاد یک رفتار غیرمنتظره در سیستم نهایی می‌شود را آشکار می‌سازد. در گذشته، تلاش‌هایی به‌منظور توصیف مفاهیم حمله صورت گرفته که یکی از آنها توسط Templeton و Levitt انجام شده که اجزای تشکیل دهنده حمله و چگونگی وابستگی آنها به یکدیگر را مدل می‌کند [۶]. در این روش، حمله به اجزای سازنده خود تجزیه می‌شود. با این کار مطالعه نیازمندی‌های اجزای حمله و تأثیر آنها بر محیط اطراف امکان‌پذیر می‌شود. یکی از الزامات اصلی برقراری امنیت در شبکه‌های دارای داده‌های حساس، به‌کارگیری رویکرد دفاع در عمق، در طراحی و پیاده‌سازی این سیستم‌ها و شبکه‌هاست. سیستم‌های تشخیص و جلوگیری از نفوذ، از زیرسیستم‌های اصلی این رویکرد به‌شمار می‌روند. مقابله با حملات، وظیفه اصلی این زیرسیستم‌ها است. در سیستم‌های جدید، تلفیق زیرسیستم‌های تشخیص نفوذ و رویدادنگاری به‌عنوان روشی در جهت بهبود تشخیص نفوذ به‌کار رفته است. این سیستم‌ها در بهترین حالت در زمان رخ دادن حمله به صورت برخط و بلادرنگ، آن را تشخیص داده و در صورت امکان از آن جلوگیری می‌کنند. در راستای تکمیل این لایه دفاعی، بهترین روش، استفاده از دانش مهاجمان برای بررسی سیستم‌ها و شبکه‌های سازمان جهت شناخت نقاط آسیب‌پذیر و راه‌های نفوذ است. این فعالیت تحت عنوان آزمون نفوذ به صورت دوره‌ای توسط گروه‌های متخصص با هزینه‌های بسیار زیاد انجام می‌شود. به‌دلیل هزینه‌های هنگفت این فعالیت‌ها، هم از نظر مالی و هم از نظر توان تخصصی مورد استفاده، اجرای آزمون بیشتر از دوبار در سال توصیه نمی‌شود.

با رشد فناوری‌های دانش، استفاده از سیستم‌های مبتنی بر فناوری سیستم خبره می‌تواند با قرار گرفتن در شبکه، اصلی‌ترین فعالیت‌هایی که یک آزمونگر در راستای کشف آسیب‌پذیری‌ها انجام می‌دهد را به اجرا گذاشته و در پایان نتایج را به‌صورت گزارش‌هایی

*ایمیل نویسنده پاسخگو: javadzadeh@iust.ac.ir