بررسی مشکلات و جدیدترین رویکردهای تست نفوذ با هدف بهبود روش های کنونی

حسن علی پور[1]، طاهره نیری فرد[2]

[1] دانشجوی دانشگاه علمی کاربردی جهاد دانشگاهی ، همدان
Alipour_13@yahoo.com

[2] کارشناس ارشد نرم افزار، مدرس دانشگاه علمی کاربردی جهاد دانشگاهی ، همدان
Tahere.nayerifard@gmail.com

چکیده

در حال حاضر نقاط ضعف و آسیب پذیری های سیستم های تجاری در حال رشد است و این نقاط روز به روز بیشتر و بیشتر می شود. اخلاگران می توانند به راحتی با استفاده از نقاط ضعف و آسیب پذیری سیستم ها، از مشکلات آن ها بهره برداری و سوء استفاده کنند. به منظور شناسایی مشکلات سیستم ها، تست نفوذ وب به طور گسترده ای برای ارزیابی آسیب پذیری برنامه های کاربردی و تحت وب به کار می رود. اما تست نفوذ سنتی، مشکلات، نواقص و کاستی هایی دارد که ممکن است مانع از رسیدن به یک ارزیابی امنیتی کامل شود. در این مقاله، با مطالعه آخرین پژوهش های انجام شده در حوزه تست نفوذ، سعی در بررسی و تمرکز بر ایرادات روش‌های تست نفوذ فعلی و معرفی راهکارهای عملی ارائه شده در جهان در سال های اخیر با هدف رفع این مشکلات داشته ایم.

کلمات کلیدی

امنیت اطلاعات، تست امنیت، تست نفوذ، آسیب پذیری، وب سرویس.

۱- مقدمه

امنیت اطلاعات یکی از جنبه های مهم در هر سازمان است. امنیت شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری، موضوع جدیدی در حوزه فناوری اطلاعات و ارتباطات نیست، اما دغدغه تازه‌ای برای کاربران این حوزه به شمار می‌آید. امروزه همگام با پیشرفت فناوری‌های ارتباطی و گسترش شبکه‌های رایانه‌ای، امنیت فضای تبادل اطلاعات به یکی از دغدغه‌های اصلی مدیران، کارشناسان، دانش‌پژوهان و کاربران حوزه فناوری اطلاعات و ارتباطات تبدیل شده است. سیستم مدیریت امنیت اطلاعات مجموعه ای از سیاست های مربوط به مدیریت امنیت اطلاعات یا ریسک های مرتبط با فناوری اطلاعات است. اصل حاکم در سیستم مدیریت امنیت اطلاعات[1] این است که یک سازمان باید طراحی، پیاده سازی و حفظ مجموعه ای منسجم از سیاست ها، فرآیندها و سیستم ها را برای مدیریت ریسک ها جهت ارزیابی اطلاعاتشان انجام دهد. در نتیجه سطح قابل قبولی از خطر امنیت اطلاعات را تضمین می‌کند، امنیت اطلاعات، حفاظت از اطلاعات می باشد که موارد CIA را تضمین می کند. اخیرا مساله امنیت به دلیل ازدیاد برنامه‌های کاربردی و تجاری برای استفاده روی اینترنت اهمیت مازادی یافته است. تست امنیت سیستم ها، فرآیندی است که توسط یک تیم واجد شرایط ارزیاب، نرم‌افزار یا برنامه‌های کاربردی را به منظور شناسایی فرصت‌ها جهت بهبود درکنترل امنیت و اعتبارسنجی داده‌ها ارزیابی می‌کند و سازمان‌ها مداوماً به دنبال راه‌هایی برای کاهش سطح ریسک و پایین آوردن احتمال نقص‌ها می‌باشند.

یکی از روش های هدفمند و شاخص در ارزیابی امنیتی سیستم ها، انجام تست نفوذ بر روی هدف مورد نظر است، به طوری که از دید یک نفوذگر و خرابکار به سیستم نگاه کرده و سعی در پیدا کردن حفره های امنیتی آن است. امام تست نفوذ نیز مانند روش های ارزیابی دیگر، مشکلات و کاستی هایی دارد که ممکن است باعث عدم دستیابی به نتایج دلخواه و ارزیابی امنیتی

کامل یک سیستم شود. بدین منظور در مطالعه ای بر جدیدترین پژوهش ها در زمینه تست نفوذ و ارائه روش های بهینه، در این نوشته تلاش بر معرفی برخی از مهمترین نقاط ضعف تست نفوذ و معرفی روش های موجود برای رفع این مشکلات شده است. در ادامه این نوشته، در بخش دوم، به معرفی مفهوم کلی تست امنیت پرداخته ایم. در بخش سوم تکنیک های تست امنیت و مقایسه ای بین این تکنیک ها ارائه شده است. در بخش چهارم مهمترین مشکلات تست نفوذ سنتی و همچنین جدیدترین راهکارهای موجود بیان گردیده است.

۲- تست امنیت

انجام تست امنیتی برای ارزیابی مخاطرات امنیتی، مبتنی بر دانش آزمونگر بوده و تهیه یک رویه دقیق برای انجام آزمون در این حوزه غیر ممکن است. تست امنیت برای هر سیستمی که داده‌های محرمانه را پردازش می‌کند، به منظور جلوگیری از نفوذ به سیستم توسط هکرها، ضروری است. امنیت سیستم نظامی است که خصوصیات امنیتی را در مراحل طراحی، آزمایش، پیاده‌سازی و بکارگیری مورد خطاب قرار می دهد، یعنی در دوره زمانی تولید یا چرخه حیات گسترش سیستم و شامل فعالیت های امنیتی زیادی مانند مدل کردن تهدید، مدیریت خطر و تست های امنیتی است. به سبب پیچیدگی روز افزون برنامه های کاربردی وب، روش سنتی تست امنیتی عملکرد، که فقط مکانیزم امنیت سیستم را تست و اعتبار سنجی می کند در نمایان کردن نقص‌های امنیتی پنهان دیگر ناکارامد شده است. به طورکلی دلایل تست امنیت عبارتند از:

- امنیت اطلاعات ودسترسی

تست امنیت به یافتن نقاط ضعفی کمک می کند که باعث از دست دادن اطلاعات مهم یا اجازه نفوذ به سیستم‌ها می‌شود.

- ثبات سیستم

تست امنیت به بهبود سیستم کمک می کند و درنهایت باعث می شود تا آن سیستم مدت زمان بیشتری کار کند.

- یکپارچگی سیستم

اگر در مراحل اولیه چرخه توسعه حیات باشیم، تست امنیت این امکان را می‌دهد تا معایب احتمالی را در طراحی و پیاده‌سازی سیستم از بین ببریم.

- بازده اقتصادی

جلوگیری ازمشکلات احتمالی بسیار ارزان تر است نسبت به تلاش برای حل و فصل و عواقب آن.

۳- تکنیک های تست امنیت

با رشد نگرانی هایی در مورد امنیت سیستم ها، پژوهش در زمینه تست امنیت پیشرفت داشته است که منجر به ارائه روش‌های مختلف تست امنیت شده است. در این بخش دیدی سطح بالا از تکنیک های مختلف تست نمایش داده می شود که می توانند در زمانی که یک برنامه تست ساخته می شود به کار گرفته شوند. این بخش متدولوژی مشخصی برای این تکنیک ها ارائه نمی دهد. [۱].

۳-۱- بازبینی و بازرسی دستی

بازرسی های دستی بررسی های انسان محور هستند که که به طور معمول امنیت مفاهیمی از قبیل افراد، سیاست ها و فرایند ها را تست می کند اما می‌تواند بازرسی تصمیمات فن آوری مانند طراحی های معماری را هم شامل شود. این تست ها معمولا به وسیله تحلیل اسناد و مدارک یا انجام مصاحبه با طراحان یا صاحبان سیستم هدایت می شوند. در حالی که مفهوم بازرسی های دستی و بررسی های توسط انسان ساده است، اما می توانند جزء قوی ترین و مؤثرترین تکنیک های موجود باشند. بازبینی و بازرسی دستی یکی از معدود روش های تست برای خود فرآیند های SDLC است و برای تضمین اینکه سیاست ها و مهارت های مناسب در محل تنظیم شده و وجود دارند. این تکنیک زمانی می تواند استفاده شود که افراد فرآیند امنیت را درک کنند و از سیاست مطلع باشند و برای طراحی یک برنامه کاربردی امن، مهارت های مناسبی داشته باشند. فعالیت های دیگر شامل بازبینی دستی مستندات، سیاست های کدنویسی امن، نیازمندی های امنیتی و طراحی های مربوط به معماری باید به وسیله بازرسی دستی به انجام برسند.

۳-۲- مدل‌سازی تهدید

از آن جا که مدل سازی تهدید به طراحان سیستم کمک می کند تا درباره تهدیدات امنیتی فکر کنند که سیستم/برنامه‌های کاربردی آن ها ممکن است با این تهیدات مواجه شوند، این تکنیک را به یک روش محبوب تبدیل کرده. بنابراین مدل سازی تهدید می تواند به عنوان یک ارزیابی ریسک برای برنامه‌های کاربردی دیده شود. در حقیقت، این روش طراحان را قادر به توسعه استراتژی های کاهش دهنده آسیب پذیری های بالقوه می سازد و به آن ها کمک می‌کند تا منابع به ناچار محدود و همچنین توجه خود را بر روی بخش‌هایی از سیستم که بیشترین نیاز به آن را دارند معطوف کنند. توصیه می‌شود که همه برنامه های کاربردی، یک مدل تهدید توسعه یافته و مستند شده داشته باشند. مدل های تهدید باید در اسرع وقت در SDLC[۲] ایجاد شده باشند و مورد بازبینی قرار گیرند. برای توسعه یک مدل تهدید، استاندارد NIST 800-30 برای ارزیابی ریسک پیشنهاد می شود [2].

۳-۳- بازبینی کد

بازبینی کد منبع، فرآیند بررسی دستی کد منبع یک برنامه کاربردی تحت وب است برای مشکلات امنیتی. بسیاری از آسیب پذیری های امنیتی جدی، به وسیله دیگر انواع تحلیل یا تست نمی توانند شناسایی شوند. تقریبا همه کارشناسان امنیتی موافقتند که هیچ جایگزینی برای جستجوی واقعی در کد وجود ندارد. همه اطلاعات برای شناسایی مشکلات امنیتی، در جایی در داخل کد هستند. برخلاف نرم افزارهای شخص ثالث بسته مانند سیستم عامل ها، وقتی تست برنامه‌های کاربردی وب انجام می شوند (به خصوص اگر در خانه توسعه یافته شده باشند)، کدهای منبع برای اهداف تست باید در دسترس باشند.

بی نهایت سخت بودن شناسایی بسیاری از مشکلات غیر عمدی اما مهم امنیتی توسط دیگر اشکال تحلیل و تست، مانند تست نفوذ، تحلیل کد منبع را تکنیک مورد انتخاب برای تست های فنی کرده است. با کد منبع، آزمونگر می تواند به دقت آنچه را که در حال اتفاق افتادن است (یا قرار است

اتفاق بیافتند) را مشخص کند و کار حدسی تست جعبه سیاه را حذف کند. نمونه هایی از مشکلاتی که به خصوص از طریق بازبینی‌های کد منبع پیدا می شوند شامل مشکلات همروندی، منطق کسب و کار ناقص، مشکلات کنترل دسترسی ضعف های رمزنگاری همانند درهای پشتی، تروجان ها، بمب‌های زمانی، بمب های منطقی و دیگر فرم های کد مخرب می گردد. همچنین تحلیل کد منبع برای پیدا کردن مشکلات پیاده سازی مانند مکان‌هایی که اعتبارسنجی ورودی انجام نمی شوند، می تواند بسیار مؤثر باشد. برای داشتن یک بازبینی مؤثر کد می توان موارد ذیل را مورد توجه قرار داد:

- تعیین اهداف مشخص برای بازبینی
- تعیین محدوده زمانی برای بازبینی
- استفاده از لیست سوالات
- بازبینی تدریجی و مکرر
- بازبینی فقط با هدف امنیتی
- دانستن معماری برنامه کاربردی
- به روز کردن استانداردهای کد نویسی

۳-۴- تست نفوذ[۳]

یکی از مراحل مهم اطمینان از اینکه اطلاعات امن است داشتن یک تست نفوذ است که معلوم شود اطلاعات محفوظ است. تست نفوذ در صنعت به عنوان یک روش برای ارزیابی امنیتی برای مشخص کردن آسیب پذیری ها در برنامه های کاربردی وب استفاده می شود. تکنیک های گوناگون برای شناسایی آسیب پذیری امنیتی در گذشته ارائه شده که شامل تست نفوذ ، تحلیل استاتیک ، تحلیل دینامیک و کشف آنومالی زمان اجرا است. تست نفوذ، تکنیکی است که توسط سازندگان کاربردی وب استفاده می شود .

تست نفوذ یک تکنیک است که در آن ابزار تست بر برنامه های کاربردی از نقطه نظر هکر تنش ایجاد می کنند و تلاش می شود با ایجاد مقدار زیادی تعامل به آن نفوذ کند. تست نفوذ، روش معمولی است که سال‌های زیادی برای تست امنیت شبکه استفاده شده است. این تست معمولا به عنوان تست جعبه سیاه یا هک اخلاقی هم شناخته می شود. تست نفوذ اساساً "هنر" تست کردن برنامه کاربردی درحال اجرا از راه دور، بدون دانستن عملکردهای داخلی خود برنامه است، به منظور شناسایی آسیب پذیری های امنیتی. به طور معمول، تیم تست نفوذ به یک برنامه کاربردی مثل اینکه کاربر معمولی هستند، دسترسی خواهند داشت. آزمونگر مانند یک مهاجم عمل می‌کند و برای پیدا کردن و بهره برداری از آسیب پذیری ها تلاش می کند. هرچند ثابت شده است که تست نفوذ در مشکلات امنیتی مؤثر می باشد اما این تکنیک به طور طبیعی برای برنامه های کاربردی قابل تفسیر نیست.

۳-۵- مقایسه چهار تکنیک تست امنیت

در جدول (۱) مزایا و معایب هریک از تکنیک های تست امنیت که در قبلا بررسی شدند، بیان شده است.

جدول (۱) مقایسه تکنیک های تست امنیت

نام تکنیک	مزایا	معایب
بازبینی و بازرسی دستی	عدم نیاز به پشتیبانی فنی. قابلیت به کارگیری در موقعیت‌های مختلف. قابل انعطاف. ترویج کار گروهی. امکان به کارگیری در آغاز SDLC	زمان بر پشتیبانی از اطلاعات همیشه در دسترس نیست. نیازمند اندیشه و مهارت چشم گیر افراد برای اثر بخش بودن.
مدل سازی تهدید	داشتن دید عملی مهاجم از سیستم قابل انعطاف. امکان به کارگیری در آغاز SDLC.	تکنیک نسبتاً جدید. مدل های تهدید خوب به صورت خودکار به معنی نرم افزار خوب نیستند.
بازبینی کد	کامل و اثربخش. صحت و درستی. سریع (برای منقدان و بازرسان ماهر و کارآمد).	نیازمند توسعه دهندگان امنیتی بسیار با مهارت. ممکن است مشکلات در کتابخانه‌های کامپایل شده را نادیده بگیرد. خطاهای زمان اجرا را به آسانی نمی‌تواند شناسایی کند. کد منبعی که که واقعا توسعه یافته است ممکن است. متفاوت از چیزی باشد که در حال تجزیه وتحلیل است.
تست نفوذ	می تواند سریع باشد (در نتیجه ارزان) نیاز به مجموعه مهارت کمتری نسبت به بازبینی کد منبع دارد. کدی که واقعا افشا شده تست می کند.	بسیار دیر در SDLC ظاهر می شود تأثیر ظاهری[۴] فقط تست می شود.

۴- بررسی مشکلات موجود در انجام یک تست نفوذ کارا و راهکارهای موجود

ارزش اصلی تست نفوذ در ارائه مدل ها یا تئوری های خوب و به اثبات رسیده نیست بلکه در فراهم آوردن متدولوژی های عملی برای ارزیابی جریان های امنیتی برای جلوگیری از آسیب پذیری است. از آنجا که سیستم ها و شبکه ها در حال پیچیده تر شدن هستند، نقص های آسیب پذیری و امنیتی می تواند صدها یا هزاران بار در سطوح مختلف یک شرکت یا شبکه سازمانی بزرگ باشد. پس اجرای تست نفوذ باید به خوبی برنامه ریزی شده و یک روند جامع باشد. در این بخش به بررسی مهمترین و کلی ترین مسائل تست نفوذ پرداخته و جدیدترین مطالعات و پژوهش هایی که در این زمینه انجام و پیاده‌سازی شده اند را بیان خواهیم کرد.

۴-۱- عدم یکپارچگی در چرخه حیات توسعه

آزمایش نفوذ وب به طور گسترده ای برای ارزیابی آسیب پذیری کاربردهای وب به کار می رود. این کار معمولاً بعد از اینکه پیشرفت کامل شد و تقاضا به کالا تبدیل شد توسط متخصصان امنیتی خاصی انجام می شود و بنابراین تست نفوذ اصولا در داخل یک چرخه زندگی توسعه یافته نرم افزاری امنیتی قرار نمی گیرد و متأسفانه، تست نفوذ معمولاً خیلی دیر توسط متخصصان امنیتی انجام می شود.

در [3]، Bernard Stepien و همکاران، رویکرد TTCN-3 را بر اساس یک زبان سطح بالا پیشنهاد داده اند که براساس چهارچوب تست نفوذی برای

کاربردهای وب طراحی شده و یک رویکرد قابل تکرار، منظم و با ارزش را فراهم کرده که به طور کامل در داخل یک چرخه زندگی توسعه یافته نرم‌افزاری امنیتی قرار می گیرد. این رویکرد به طور خاص برای مشخص و اجرا کردن مجموعه هایی از تست در سطحی از انتزاع طراحی شده است که کنترل کاملی بر روی قطعی یا غیر قطعی بودن، زمانبندی و استفاده از مدل‌های مختلف برای اهداف تست متفاوت فراهم می کند. همچنین به منظور داشتن تست نفوذی قاعده مند و مقرون به صرفه که به طور کامل امنیت را در SDLC پوشش دهد، Pulei Xiong و همکارانش در پژوهشی [4]، متدولوژی تست نفوذ برنامه های وب را ارائه داده اند که با پشتیبانی از همکاری توسعه دهندگان و درونی کردن تست نفوذ با دیگر روش های تکمیلی تست امنیتی، باعث افزایش کیفیت تست نفوذ شده اند. در این مطالعه یک معماری تست مبتنی بر جعبه خاکستری تعریف شده که ظرفیت تست نفوذ ر افزایش داده و خودکار سازی فرآیندهای مهم در تست نفوذ را نیز ممکن می سازد. همچنین نمایشی ساخت یافته از دانش امنیت وب را که می‌تواند به وسیله برنامه های پلت فرم تست قابل فهم و پردازش باشد، تعریف کند که در نتیجه آن عملیات تست مطمئن شده و نتایج تست قابلیت اطمینان، اندازه گیری و ارزیابی بیشتری خواهند داشت.

۴-۲- فقدان دید بر روی عملکرد داخلی سرویس‌های وب

بر اساس تحقیقات انجام شده امنیت کاربردهای وب ضعیف است و بیشتر سرویس های وب اغلب با کد آسیب پذیری بکار می روند . مسئله این است که سرویس های وب آنقدر گسترده هستند که هیچ آسیب پذیری امنیتی موجودی نمی تواند کشف نشده باقی مانده و توسط هکرها کشف نشود. برای جلوگیری از آسیب پذیری ، سازندگان باید بهترین روش های کدگذاری را به کار ببرند و بررسی امنیتی کد را انجام دهند و تست های نفوذ را اجرا کنند و از تحلیل آسیب پذیری کد استفاده کنند. در عمل، تست نفوذ بر اساس اجرای کد هدف است و دید زمان اجرا از رفتار سرویس وب فراهم می کند. زمانی که سرویسی از نقطه نظر یک کاربر تست می شود، نیازی به دسترسی یا تغییر کد منبع نیست. مشکل اصلی در عمل این است که شناسایی آسیب پذیری تنها می تواند به تحلیل خروجی سرویس های وب تکیه کند. به این ترتیب، تأثیر تست نفوذ به علت فقدان دید بر روی رفتار داخلی سرویس محدود است.

آزمون کننده های تست نفوذ با ابزارهایی که برنامه های کاربردی را در مقابل مشکلات امنیتی تست می کنند، به خوبی آشنا هستند. این روش ها راه اتوماتیک برای جستجوی آسیب پذیری هستند و جلوی کار تکراری انجام صدها یا هزاران تست را برای هر نوع آسیب پذیری می گیرد. تحقیقات نشان می دهد که کارایی روش های تست نفوذ کنونی در کشف قابلیت آسیب پذیری در محیط وب خیلی ضعیف است. در]۵[رویکرد جدیدی برای کشف آسیب پذیری های تزریق در سرویس های وب بر پایه استفاده از نشانه های حمله و نظارت رابط برای افزایش دید فرآیند تست نفوذ ارائه شده است که با وجود عملکرد خوب آن، هنوز نیازی به رفتارهای داخلی وب سرویس ندارد (که اصولا هم در دسترس نیست). در این تحقیق، یک ابزار نمونه با هدف کشف آسیب پذیری SQL در[۵] SOAP WS ارائه شده. این نمونه اولیه شامل یک ماژول تولید بار حمله است که می تواند به تحلیل سرویس وب بپردازد و حمله های حاوی علامت را ایجاد کند. در حین حمله، ترافیک پایگاه داده ها کنترل می شود و علائم کشف شده بصورت آسیب پذیری گزارش شده اند. نتایج به دست آمده با روش ارائه شده، بهتر از نتایج اسکنرهای تجاری از جمله HP WebInspect, IBM Rational AppScan و Acunetix Web Vulnerability Scanner بوده است . این نشان می‌دهد روش حاضر می تواند روشی مناسب برای کشف آسیب پذیری باشد و جلوی استفاده از روش های گران را می گیرد.

۴-۳- پیچیدگی انجام تست نفوذ برای آزمون کننده

تست های نفوذ به روش سنتی، به صورت دستی توسط آزمون کننده بر اساس طرحی انجام می شدند که این فرآیند معمولا به علت پر کار و نیازمند بودن به آشنایی آزمون کننده با همه نوع ابزار تست نفوذ، پیچیده هستند. اجرای دقیق آن کار ساده ای نبوده و نیاز به زمان دارد چرا که فرآیند پیچیده ای است. ابزار تست نفوذ نمی توانند یک هدف منسجم را تنظیم کنند، برای مثال در به دست آوردن حق ویژه هاست، تنها آسیب پذیری های بالقوه شناخته شده را به وسیله تلاش برای بهره برداری از آن ها اعتبار سنجی می کند، بدون بررسی ارتباط بین آسیب پذیری ها و بنابراین آزمون کننده نمی تواند تست نفوذ را به صورت یک تصویر واضح درک کند. بنابراین استفاده از روشی واحد برای توصیف طرح آزمون که بتواند توسط کامپیوتر شناسایی شود و نیاز به توجه فراوان آزمون کننده نباشد بسیار مطلوب خواهد بود. به این ترتیب کامپیوتر می تواند برای تعویض با آزمون کننده برای انجام تست نفوذ استفاده شود.

برای حل این مشکلات، Zhiyong Dai و همکاران در [6] روشی پیشنهاد کرده اند که قبل از اینکه آزمون نفوذ انجام شود، طرح تست نفوذ که از نمونه های تست نفوذ تشکیل شده توصیف می شود تا چگونگی انجام تست نفوذ را نشان دهد. در این پژوهش، متدی به نام "زبان توصیف طرح تست نفوذ" طراحی شده که به آزمون کننده این توانایی را می دهد که طرح تست نفوذ را توصیف کند به نحوی که قابل فهم برای کامپیوتر باشد، سپس به صورت اتوماتیک تست را انجام داده و در نهایت گزارش آن را ارئه می‌کند و بدین ترتیب مشکل نیاز به توجه زیاد آزمون کننده به روند تست را حل می‌کند. تست های نفوذ کنونی وقت گیرند و روند دستی و پیچیده ای دارند که نیازمند متخصصان تست نفوذ باتجربه است تا آن را انجام دهند .در اکثر موارد ،تست کننده های نفوذ باید طبق اهداف گوناگون اکتشافات خود را بنویسند و از بین هزاران روش امنیتی آن هایی را انتخاب کنند که با شبکه ها یا محیط های سیستم گوناگون سازگارند.

تست های نفوذ اتوماتیک دارای ارزیابی نقص امنیتی ، اکتشاف آسیب پذیری و جمع آوری اطلاعات بطور یکجا هستند انتخاب روش های تست نفوذ ، شیوه های حمله و نقاط ضعف بصورت اتوماتیک کشف می شود و خطاهای دستی کاهش می یابد. همچنین یک تست عملی باید از بسیاری موقعیت های گوناگون شروع شود پس یک بکارگیری سریع نیاز است . چون شبکه ها و سرورها و کاربردها در حال پیچیده شدن هستند آسیب پذیری و نقص های ایمنی می تواند آنقدر متغیر باشد که هیچ تستی از یک نقطه ساده نتواند همه آن ها را بطور کامل پوشش دهد که بر این اساس و ویژگی ها، در[7] استراتژی طراحی پلتفرم تست نفوذی پیشنهاد شده که از مرکز کنترل و

کلاینت‌های توزیع شده برای انجام تست ساده و خودکار استفاده می کند. این پلتفرم، متفاوت از مدل های تست سابق است. مرکز کنترل مدیریت شده به صورت مرکزی می تواند استراتژی های مختلف تست را تولید کرده، تحلیل خودکار از امنیتی و آسیب پذیری های سیستم‌های هدف انجام دهد، استراتژی های تست را به اسکریپت های تست واقعی انتقال دهد و کلاینت ها برای گسترش آن در حالت های توزیع شده راحت هستند. همچنین با پژوهشی که در سال ۲۰۱۳ در دانشگاه داکوتا انجام گرفته [8]، که در آن به منظور بهبود تست نفوذ برای هر دو طرف شرکت ها و تست کننده، ابزاری معرفی شده که دید عمیق‌تری در مورد روش های امنیتی فعلی و اینکه در کدام بخش ها نیاز به بهبود است می دهد. در واقع هدف در این پژوهش برنامه نویسی و ایجاد سندی از ابزارهای خاص و تعیین روال اجرای آن ها در حوزه خاصی در از تست نفوذ است که با گسترش آن می توان کل عملیات تست نفوذ را شامل شود. با استفاده از این روش، تست نفوذ خودکار برخی از جنبه های تست بعد از پیکره بندی اولیه را به شدت ساده کرده و برای تست دستی اضافی، وقت آزاد ایجاد می کند.

۴-۴- طولانی بودن چرخه تست نفوذ و عدم استاندارد سازی نتایج

با پیدایش شبکه وتکنولوژی امنیتی شبکه، تکنیک های تست نفوذ توجه زیادی به خود جلب کرده اند. تست نفوذ روندی است که مهندسان امنیتی هکرهایی شبیه سازی می کنند به منظور استفاده از تکنولوژی کشف منبع و کشف روش های حمله تا امنیت موضوعات را کشف کنند و آسیب پذیرترین بخش سیستم را پیدا کنند و نتایج تستی را ثبت کنند. تست نفوذ تهدیدهای منابع اطلاعات سازمان را تعریف کرده و هزینه امنیت IT سازمان را کاهش می دهد و ضعف ها را شناسایی کند و تکنولوژی کاملی شامل ارزیابی استراتژی ها، فرآیندها، طراحی و اجرا را فراهم می کند. اما زمانی که سیستم تست نفوذ سنتی، اطلاعات را از شبکه و تجهیزات تست شده می گیرد تأثیر کم، چرخه طولانی و کمبود مقدار اطلاعات و عدم درستی اطلاعات وجود دارد. هنگامی که آسیب پذیری ارزیابی می شود، ابزارهای نادرست ارزیابی آسیب پذیری، زمان واقعی ضعیف، نتایج ناقص از ارزیابی آسیب پذیری، فرمت واحد مستند نتایج تست شده، نبود استاندارد سازی و موارد دیگر وجود دارد.

برای حل این مشکلات، در [9] سیستم تست نفوذ بر پایه XML در ترکیب با SNMP، PING، Telnet، OVAL، CVE و تکنولوژی های دیگر برای حل اشکالات تست نفوذ سنتی پیشنهاد شده است. این سیستم می تواند بدون بررسی پیچیدگی و تفاوت اهداف تست شده، تنوع خوبی از شبکه و تجهیزات را برای تست نفوذ کسب کند. همچنین می تواند به طور مؤثر، بهره‌وری و کارایی تست را بهود داده و نتایج تستی تولید کند استاندارد، وحدت و تنوع بیشتری دارند. همچنین به منظور استفاده از روشی قاعده مند و اصولی و انجام یک تست نفوذ با رعایت تمام جوانب، در پژوهشی که در سال ۲۰۱۲ توسط انجام شده [10]، چارچوبی ارائه گردیده است که در آن تست نفوذ واحد و جامعی با تمرکز بر هر دو جنبه مشکلات فنی و غیر فنی پیشنهاد شده است. این طبقه بندی اجازه می دهد تا شناسایی و تجزیه و تحلیل آسیب‌پذیری ها توسط ۶ زیر کلاس انجام شود که مشکلات را از دیدگاه های مختلفی مانند قوانین، استانداردهای خاص صنعت، پیشرفت فنی و کاربردپذیری ها مورد پوشش قرار می دهد.

۵- نتیجه

امروزه بخش قابل توجهی از نگرانی‌های امنیتی در سازمان‌ها در حوزه امنیت شبکه و نرم افزار و به طور کلی امنیت فناوری اطلاعات و ارتباطات می‌باشد. گرچه در بعد امنیت شبکه، فعالیت‌های زیادی در داخل کشور و همچنین در خارج انجام شده است ولی دیدگاه امنیتی به تولید نرم افزار و استفاده از آن کمتر مورد توجه قرار گرفته است. این دیدگاه منجر به این واقعیت شده است که درصد بالایی از آسیب پذیری‌های فضای تبادل اطلاعات در زمینه نرم‌افزار و برنامه کاربردی باشد.به منظور نیل به ضریب قابل قبولی از امنیت در این نرم افزارها، نیازمند پیش بینی مکانیسم‌های مناسبی جهت ارزیابی امنیتی نرم‌افزارهای مورد استفاده در حوزه فناوری اطلاعات و ارتباطات هستیم. در این پژوهش سعی بر آن بود که با تمرکز بر نقش تست نفوذ در بالا بردن امنیت اطلاعات در شبکه و فضای سایبری، به معرفی نقاط ضعف آن پرداخته و همچنین با ارائه جدیدترین مطالعات و راه کارهای عملی به ذکر راه حل‌های نواقص فعلی در تست نفوذ و ایجاد دیدگاهی به روز در سازمان ها و آزمون کننده های تست نفوذ بپردازیم.

مراجع

[۱] ناصر مدیری، طاهره نیری فرد، **"مهندسی آزمون امنیت، اعتبارسنجی و تست نرم افزار"**، تهران، مهرگان قلم، ۱۳۹۳.

[2] NIST Special Publication 800-30, "*Risk Management Guide for Information Technology Systems*", National Institute of Standards and Technology, July 2002, http://www.nist.org/nist_plugins/content/content.php?content.40

[3] Bernard Stepien, Liam Peyton, Pulei Xiong, "*Using TTCN-3 as a Modeling Language for Web Penetration Testing*", IEEE International Conference onIndustrial Technology (ICIT), Athens, pp.674 – 681,2012.

[4] Pulei Xiong, Liam Peyton, SITE, University of Ottawa, "*A Model-Driven Penetration Test Framework for Web Applications*", 2010 Eighth Annual International Conference on Privacy, Security and Trust (PST), Ottawa, ON, pp.173 – 180, 2010.

[5] Nuno Antunes, Marco Vieira, "*Enhancing Penetration Testing with Attack Signatures and Interface Monitoring for the Detection of Injection Vulnerabilities in Web Services*", IEEE International Conference on Services Computing (SCC), Washington, DC, pp.104 - 111 ,2011.

[6] Zhiyong Dai, Liangshuang Lv, Xiaoyan Liang, Yang Bo, "*Network Penetration Testing Scheme Description Language*", IEEE International Conference on Computational and Information Sciences (ICCIS), Chengdu, China, pp.804 – 808,2011.

[7] Bing Duan, Yinqian Zhang, Dawu Gu, "*An Easy-to-deploy Penetration Testing Platform*", IEEE The 9th International Conference for Young Computer Scientists (ICYCS), Hunan, pp.2314 – 2318, 2008.

[8] Kevin P. Haubris, Joshua J. Pauli, "*Improving the Efficiency and Effectiveness of Penetration Test Automation*", IEEE 10th International Conference on

Information Technology: New Generations (ITNG), Las Vegas, NV, pp.387 - 391, 2013.

[9] Bin Xing , Ling Gao, Jing Zhang, Deheng Sun, "*Design and implementation of an XML-based penetration testing system*", IEEE International Symposium on Intelligence Information Processing and Trusted Computing (IPTC), Huanggang, pp.224 – 229, 2010.

[10] A. Hudic, L. Zechner, S. Islam, C. Krieg, E.R. Weippl, S. Winkler, R. Hable, "*Towards a Unified Penetration Testing Taxonomy*", ASE/IEEE International Conference on Social Computing (SocialCom) and ASE/IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT), Amsterdam, pp.811 - 812, 2012.

زیرنویس‌ها

[1] Information Security Management System (ISMS)
[2] Software (System) Development Life Cycle
[3] Penetration test
[4] Front impact
[5] Web Service