بیست و دومین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات
The 22th National Conference on Computer Science and Engineering and Information Technology
April 2024 – فروردین ۱۴۰۳

بررسی تست نفوذ به روش‌های کلاسیک و ارائه مفهوم تست نفوذ بی‌رحمانه (BPT)

محمد سعید محمدزاده چالکی[۱]، امیر روحانی[۲] حمیدرضا نورصالحی [۳]

[۱] کارشناسی ارشد مدیریت فناوری اطلاعات، کسب‌وکار الکترونیک، دانشگاه علم و صنعت ایران

[۲] کارشناسی ارشد مدیریت فناوری اطلاعات، مدیریت سیستم‌های اطلاعاتی، دانشگاه آزاد واحد بناب

[۳] کارشناسی ارشد مهندسی فناوری اطلاعات، تجارت الکترونیک، دانشگاه شیراز

چکیده

پیاده‌سازی کامل کنترل‌های امنیتی یکی از گام‌های اصلی در برقراری امنیت در سازمان است. این کار مستلزم صرف منابع بسیاری است که در اغلب موارد در کوتاه مدت امکان‌پذیر نیست. از طرفی مدیران سازمان تمایل دارند تا ضمن آگاهی از وضعیت امنیتی سازمان خود در تمام ابعاد و نقاط قوت و ضعف سازمان، از اثربخشی منابع تخصیص یافته برای پیاده‌سازی کنترل‌های امنیتی و میزان تأثیر آن در ارتقای سطح امنیتی و همچنین اولویت‌های بعدی تخصیص منابع مطلع شوند. این مقاله، پس از بیان ضرورت، هدف، سؤالات و ادبیات تحقیق، یک رویکرد و نگرش فازی به منظور سنجش میزان و سطح پیاده‌سازی کنترل‌های امنیتی را بیان کرده و پس از بررسی روش های متداول ارزیابی امنیتی (تست نفوذ کلاسیک) مدل جدیدی برای ارزیابی سطح امنیت سازمان با نام تست نفوذ بی‌رحمانه (Brute Persistence Test) ارائه می‌دهد. قابلیت به‌کارگیری در تمامی سازمان‌ها صرف نظر از نوع، اندازه و ماهیت آن، سازگاری با استانداردهای بین‌المللی متداول و مرتبط در این حوزه، ارائه‌ی گزارش مدیریتی امنیتی برای مدیران ارشد، قابلیت به‌کارگیری به‌عنوان سیستم تصمیم یار مدیران، ارائه‌ی وضعیت شفاف و دقیق سازمان در همه ابعاد فناوری اطلاعات و تعیین نقاط قوت و ضعف امنیتی آینده نگرانه سازمان از مشخصه‌ها و کاربردهای مدل پیشنهادی است.

واژگان کلیدی: تست نفوذ بی‌رحمانه، Brute Persistence Test (BPT)، ارزیابی امنیتی، هک قانونمند

The 22th National Conference
18/04/2024-(Mazandaran)
Elmavaran Danesh Group
R.S. Institute
Article Code: NCCIT -117010

Indexing Accepted Articles in Civilica

مقدمه

امنیت اطلاعات یکی از جنبه های مهم در هر سازمان است. امنیت شبکه‌های رایانه ای 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 مجموعه‌ای 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، پیاده‌سازی و حفظ مجموعه ای منسجم از سیاست‌ها، فرآیندها و سیستم‌ها را برای مدیریت ریسک‌ها جهت ارزیابی اطلاعاتشان انجام دهد. در نتیجه سطح قابل قبولی از مخاطرات امنیت اطلاعات را تضمین می‌کند. امنیت اطلاعات، حفاظت از اطلاعات می باشد که موارد CIA[2] را تضمین می کند. اخیرا مساله امنیت به دلیل ازدیاد برنامه‌های کاربردی و تجاری برای استفاده در اینترنت اهمیت دو چندان 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 پیوسته 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 دارد. اما 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 بیان برخی از مهمترین نقاط ضعف تست نفوذ کلاسیک و معرفی تست نفوذ بی‌رحمانه (BPT) برای رفع این مشکلات شده است. در ادامه این نوشته، به معرفی مفهوم کلی تست امنیت پرداخته ایم. در بخش بعدی تکنیک های تست امنیت و مقایسه‌ای بین این تکنیک ها ارائه شده است. در بخش پایانی مهمترین مشکلات تست نفوذ سنتی (کلاسیک) و همچنین جدیدترین راهکارهای موجود به همراه شرح مفهوم تست نفوذ بی‌رحمانه (BPT) بیان گردیده است.

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[3]، منتقل[4] یا نگهداری[5] می‌کند، به منظور جلوگیری از نفوذ به سیستم توسط هکرها، ضروری است. امنیت سیستم، نظامی است که خصوصیات امنیتی را در

[1] Information Security Management System (ISMS)
[2] Confidentiality, Integrity, Availability
[3] Process
[4] Transfer
[5] Store

مراحـل طراحـی، آزمـایش، پیاده‌سازی و بکارگیری مورد خطاب قرار می دهد، یعنی در دوره زمـانی تولیـد یا چرخه حیات گسترش سیستم و شامل فعالیت های امنیتی زیادی مانند مدل کردن تهدید، مدیریت خطر و تست های امنیتی است. به سبب پیچیـدگی روز افزون برنامه های کاربردی وب، روش سنتی تست امنیتی عملکرد، کـه فقـط مکانیزم امنیت سیستم را تست و اعتبـار سـنجی مـی کنـد در نمایـان کـردن نقص‌های امنیتی پنهان دیگر ناکارآمد شده است. بـه طـورکلی دلایـل تسـت امنیت سنتی عبارتند از:

- امنیت اطلاعات و دسترسی

تست امنیت به یافتن نقاط ضعفی کمک مـی کنـد کـه باعـث از دسـت دادن اطلاعات مهم یا اجازه نفوذ به سیستم‌ها می‌شود.

- ثبات سیستم

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

- یکپارچگی سیستم

اگر در مراحل اولیه چرخه توسعه حیـات باشـیم، تسـت امنیـت ایـن امکـان 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.

تکنیک های تست امنیت

با رشد نگرانی هایی در مورد امنیت سیستم ها، پژوهش در زمینه تست امنیـت پیشرفت داشته است که منجر به ارائه روش‌های مختلـف تسـت امنیـت شـده است. در این بخش دیدی سطح بالا از تکنیک هـای مختلـف تسـت نمـایش داده می شود که می‌توانند در زمانی که یک برنامه تست ساخته می شـود بـه کار گرفته شوند. این بخش متدولوژی مشخصی برای ایـن تکنیـک هـا ارائـه نمی‌دهد.[1]

بازبینی و بازرسی دستی

بازرسی های دستی بررسی های انسان محور هستند که بـه طـور معمـول امنیت مفاهیمی از قبیل افراد، سیاست ها و فرایند هـا را تسـت مـی کنـد امـا می‌تواند بازرسی تصمیمات فن آوری مانند طراحی‌های معماری را هم شـامل شود. این تست ها معمولا به

وسیله تحلیل اسناد و مدارک یا انجام مصاحبه بـا 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 تـرین و مؤثرترین تکنیک های موجود باشند. بازبینی و بازرسی دستی یکـی از معـدود روش های تست برای خود فرآیندهای SDLC[6] است و برای تضـمین اینکـه سیاست ها و مهارت های مناسب در محل تنظـیم شـده و وجـود دارنـد. ایـن تکنیک زمانی می تواند استفاده شود که افراد فرآیند امنیـت را درک کننـد و از سیاست مطلع باشند و برای طراحی یک برنامه کـاربردی امـن، مهـارت هـای مناسبی داشته باشند. فعالیـت هـای دیگـر شـامل بـازبینی دسـتی مسـتندات، سیاست های کدنویسی امن، نیازمندی های امنیتی و طراحی های مربـوط بـه معماری باید به وسیله بازرسی دستی به انجام برسند.

مدلسازی تهدید

از آن جا که مدل سازی تهدید به طراحان سیستم کمک مـی کنـد تـا دربـاره تهدیدات امنیتی فکر کنند که سیسـتم/برنامـه‌هـای کاربردی آن ها ممکن اسـت با این تهیدات مواجه شوند، این تکنیک را به یک روش محبوب تبدیل کـرده. بنـابراین مـدل سـازی تهدید می تواند بـه عنـوان یـک ارزیـابی ریسـک بـرای برنامه‌های کاربردی دیده شود. در حقیقت، این روش طراحـان را قـادر بـه توسعه استراتژی های کاهش دهنده آسیب پذیری های بالقوه می سـازد و بـه آن هـا کمک می‌کند تا منابع بـه ناچـار محـدود و همچنـین توجـه خـود را بـر روی بخش‌هایی از سیستم که بیشترین نیاز به آن را دارنـد معطـوف کننـد. توصـیه می‌شود که همـه برنامه های کاربردی، یک مدل تهدید توسعه یافته و مسـتند شده داشته باشند. مدل های تهدید بایـد در اسـرع وقـت در SDLC ایجـاد شده باشند و مورد بازبینی قرار گیرند. برای توسعه یـک مـدل تهدیـد، اسـتاندارد NIST 800-30 بـرای ارزیـابی ریسـک پیشنهاد می‌شود. [2]

بازبینی کد

بازبینی کد منبع، فرآیند بررسی دستی کد منبع یک برنامه کاربردی تحت وب برای یافتن مشکلات امنیتی است. بسیاری از آسیب پذیری های امنیتی جـدی، بـه وسیله دیگر انواع تحلیل یا تست نمـی تواننـد شناسـایی شـوند. تقریبـا همـه کارشناسان امنیتی موافقند که هیچ جایگزینی برای جستجوی واقعـی در کـد وجود ندارد. همه اطلاعات برای شناسایی مشکلات امنیتی، در جایی در داخـل کد هستند. برخلاف نرم افزارهای متن بسته مانند سیستم عامـل هـا، وقتی تست برنامه‌های کاربردی وب انجام می شوند، کدهای منبع بـرای اهـداف تسـت بایـد در دسـترس باشند. سخت بودن شناسایی بسیاری از مشـکلات غیـر عمـدی امـا مهم امنیتی توسط دیگر اشکال تحلیل و تست، مانند تست نفـوذ، تحلیـل کـد منبع را تکنیک مورد انتخاب برای تست های فنی کرده اسـت. بـا کـد منبـع، آزمونگر می تواند به دقت آنچه را که در حال اتفاق افتادن است (یا قرار اسـت اتفاق بیافتند) را مشخص کند و کار حدسی تست جعبـه سـیاه را حـذف کنـد. نمونه هایی از مشکلاتی که به خصوص از طریق بازبینی‌های کـد منبـع پیـدا می شوند شامل مشکلات همروندی، منطق کسـب و کـار نـاقص، مشـکلات کنترل دسترسی ضعف های رمزنگاری هماننـد درهـای پشـتی، تروجـان هـا، بمب‌های زمانی، بمب های منطقی و دیگر فرم‌های کـد مخـرب مـی‌گـردد. همچنین تحلیل کد منبـع بـرای

[6] Software Development Life Cycle

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

تست نفوذ[۷]

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 آسیب‌پذیری‌ها در برنامه های کاربردی، وب و ... استفاده می شود. تکنیک های گوناگون برای شناسایی آسیب پذیری امنیتی در گذشته ارائه شده که شامل تست نفوذ، تحلیل استاتیک، تحلیل داینامیک و کشف آنومالی زمان اجرا است.

تست نفوذ یک تکنیک است که در آن ابزار تست بر برنامه های کاربردی از نقطه نظر هکر تنش ایجاد می کنند و تلاش می‌شود با ایجاد مقدار زیادی تعامل به آن نفوذ کند. تست نفوذ، روش معمولی است که سال‌های زیادی برای تست امنیت شبکه و نرم‌افزار ها 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 می‌کند.

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	تکنیک نسبتاً جدید، مدل های تهدید خوب به

[7] Penetration Test

	قابل انعطاف، امکان به کارگیری در آغازSDLC.	صورت خودکار به معنی نرم افزار خوب نیستند.
بازبینی کد	کامل و اثربخش صحت و درستی سریع	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 SDLCظاهر می شود. تأثیر ظاهری[8] فقط تست می شود.

جدول (۱) مقایسه تکنیک های تست امنیت

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 متدولوژی‌های 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، نقص‌های آسیب‌پذیری 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.

عدم یکپارچگی در چرخه حیات توسعه

آزمایش نفوذ وب به طور گسترده ای برای ارزیابی آسیب‌پذیری نرم افزارهای کاربردی 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

[8] Front impact

کامل در داخل یک چرخه زندگی توسعه یافته نرم‌افزاری امنیتی قرار می‌گیرد. این رویکرد به طور خاص برای مشخص و اجرا کردن مجموعه‌هایی 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 می‌کند. 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 را 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 پلتفرم تست قابل فهم و پردازش باشد، تعریف کند که در نتیجه آن عملیات تست مطمئن شده و نتایج تست قابلیت اطمینان، اندازه‌گیری و ارزیابی بیشتری خواهند داشت.

فقدان دید بر روی عملکرد داخلی سرویس‌های وب

بر اساس تحقیقات انجام شده امنیت نرم‌افزارهای کاربردی 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 نمی‌تواند کشف نشده باقی مانده و از دید هکرها مخفی بماند. 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 یک دید کلی درباره 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 می‌تواند 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 برنامه‌های کاربردی را در مقابل مشکلات امنیتی تست می‌کنند، 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 آسیب‌پذیری در محیط وب خیلی ضعیف است. در [5] رویکرد جدیدی برای کشف آسیب پذیری های تزریق در سرویس‌های 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 SQLدر SOAP WS[9] ارائه شده است. 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 به صورت آسیب‌پذیری گزارش شده‌اند. نتایج به دست آمده با روش ارائه شده، بهتر از نتایج اسکنرهای تجاری از جمله HP WebInspect, IBM Rational AppScan و Acunetix Web Vulnerability

[9] Web Service

Scanner بوده است . این نشان می‌دهد روش حاضر می‌تواند رویکرد مناسب‌تری برای کشف آسیب‌پذیری باشد و جلوی استفاده از روش های گران را می گیرد.

پیچیدگی انجام تست نفوذ برای آزمون کننده

تست‌های 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. ابزارهای تست نفوذ نمی‌توانند یک هدف منسجم را تنظیم کنند، برای مثال در به دست آوردن حق ویژه‌ها - بدون بررسی ارتباط بین آسیب‌پذیری‌ها - تنها آسیب‌پذیری های بالقوه شناخته شده را به وسیله تلاش برای بهره‌برداری از آن‌ها اعتبار سنجی می کند، بنابراین آزمونگر نمی تواند تست نفوذ را به صورت یک تصویر واضح درک کند. در نتیجه 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 کننده‌های 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 آسیب‌پذیری و جمع آوری اطلاعات بطور یکجا هستند. انتخاب روش های تست نفوذ، شیوه‌های 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 شبکه‌ها 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 می‌کند. 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 امنیت و آسیب پذیری‌های سیستم‌های هدف انجام دهد، استراتژی‌های تست را به اسکریپت‌های تست واقعی انتقال دهد و کلاینت‌ها برای گسترش آن در حالت‌های 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 می‌دهد. در واقع هدف در این پژوهش برنامه نویسی و ایجاد سندی از ابزارهای خاص و تعیین روال اجرای آن‌ها در حوزه خاصی 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 پیکره‌بندی اولیه را به شدت ساده کرده و برای تست دستی اضافی، وقت آزاد ایجاد می‌کند.

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 وکشف 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 می‌کند و تکنولوژی کاملی شامل ارزیابی استراتژی‌ها، فرآیندها، طراحی و اجرا را فراهم می‌کند. 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 آسیب‌پذیری، زمان واقعی ضعیف، نتایج ناقص از ارزیابی آسیب پذیری، فرمت واحد مستند نتایج تست شده، نبود استانداردسازی و موارد دیگر وجود دارد. برای حل این مشکلات، در [9] سیستم تست نفوذ بر پایه XML در ترکیب با CVE، OVAL، Telnet، PING، SNMP 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 بهبود داده و نتایج تستی تولید کند لذا استاندارد، وحدت و تنوع بیشتری دارند. همچنین به منظور استفاده از روشی قاعده‌مند و اصولی و انجام یک تست نفوذ با رعایت تمام جوانب، در پژوهشی که در سال ۲۰۱۲ توسط [10] انجام شده 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 دیدگاه‌های مختلفی مانند قوانین، استانداردهای خاص صنعت، پیشرفت فنی و کاربردپذیری ها مورد پوشش قرار می دهد.[۱۱]

عدم کاربرد در حملات جدید مانند APT[10] ها

امروزه با افزایش چشمگیر حملات APT و رشد بی رویه‌ی رخدادهای سایبری علیه زیرساخت‌های حیاتی کشور، مشخص می‌شود که روش‌هایی که تاکنون جهت امن‌سازی و افزایش امنیت سیستم‌ها استفاده شده است کارا نبوده و سازمان‌ها همچنان در برابر نفوذگران واقعی، آسیب پذیر هستند. حال که با انجام اقدامات معمول در خصوص مقاوم‌سازی زیرساخت‌ها و سامانه‌ها، همچنان در برابر نفوذگران و متخاصمان آسیب‌پذیر هستیم چه باید کرد؟!

همواره در تعاریف تست نفوذ سنتی می‌شنویم که در این نوع تست، سامانه‌ها توسط هکرهای کلاه سفید یا خاکستری، مورد ارزیابی (حمله) قرار می‌گیرند تا پیش از نفوذگران واقعی، سازمان به ضعف‌ها و آسیب‌پذیری‌های خود آگاه شده و نسبت به رفع آن‌ها اقدام نماید. اما چرا با وجود این تست‌ها همچنان شاهد وقوع حملات شدید سایبری و نقض امنیت اطلاعات و حریم خصوصی کاربران و شهروندان می‌باشیم.

متاسفانه در تست نفوذهای سنتی، تیم ارزیاب صرفا به انجام حملات فنی و متداول (OWASP Top Attacks) بسنده کرده و در بهترین حالت، سناریوهای Business Logic را بررسی می‌نماید. در صورتی که تحقیقات اخیر ثابت کرده‌اند اکثر حملات بزرگ از نوع APT و یا به واسطه نفوذگر داخلی بوده و متخاصم طی یک فرایند زمان‌بر و طولانی و با کمک یک insider به شبکه هدف نفوذ کرده و مدت‌ها به صورت مخفی به جمع‌آوری اطلاعات (passive attack) مشغول بوده است.

معرفی مدل تست نفوذ بی‌رحمانه

کارآفرینانی که تجربه تلخ حباب دات کام [12] طی سال‌های ۱۹۹۵ تا ۲۰۰۱ میلادی در ابتدای مهاجرت از سیستم‌های سنتی به الکترونیکی را در کارنامه دارند، شباهت بسیاری میان تهدیدهای نوظهور برای کسب‌وکارهای آن دوران با انواع نفوذهای سایبری پیچیده و متنوع این روزها به سازمانهای مختلف را درک کرده‌اند. جدا از پیشرفت در مباحث تجاری و حقوقی که در حل بحران حباب دات کام تاثیر گذار بودند، اجماع در تعریف چند شاخص توسعه‌ای در صنایع الکترونیک و رایانه‌ها باعث شد تا رفتارهای تهدید آمیزی که زیر ساخت تبادل و نگهداری داده ها را به سمت نا امنی و فرار سرمایه سوق می‌داد، به عواملی قابل پیشبینی تبدیل شده و تحت کنترل قرار گیرند. در این ارتباط از قانون مور با طرح مساله "دو برابر شدن قدرت پردازش در هر سال" به عنوان مهمترین شاخص در پیشبینی روندهای فناورانه یاد می‌شود، چرا که وقتی قانون مور در کنار برآوردی که از مقدار کدنویسی هر برنامه‌نویس در سال قرار بگیرد، میزان مشخصی از تمهیدات امنیتی همچون طول کلید برای الگوریتم‌های رمزنگاری، نرخ به روز رسانی و برگزاری آزمون‌های نفوذ دوره‌ای مربوطه برای تامین اعتماد به سیستم‌های رایانه‌ای را معین می‌کند.

اما همه چیز در عصر دیجیتالی شدن دست خوش تغییرات بنیادی شده است. با نزدیک شدن فناوری ساخت پردازنده های کلاسیک به ابعاد اتمی، اعتبار قانون مور در سال ۲۰۲۵ به پایان می‌رسد [13][14]. از سوی دیگر ظهور پردازنده های کوانتومی 1121 کیوبیتی IBM در سال ۲۰۲۳ و دست پیدا کردن به پردازش کوانتومی 4158 کیوبیتی در سال ۲۰۲۵ یک تهدید مستقیم

[10] Advanced Persistent Threat

برای الگوریتم‌های رمزنگاری عصر الکترونیکی شدن امور است [15]. مطابق پژوهش‌های رسمی، قدرت پردازشی ۱۵۰۰ کیوبیتی، اعداد اول مورد استفاده در امضاهای دیجیتال رایج را به راحتی فاکتور می‌کند [16]. در اختیار داشتن قدرت پردازش کوانتومی ۲۵۹۳ کیوبیتی برای تدارک یک Collision Attack به الگورتیم هش SHA-2 کفایت می‌کند [17] و تهدید بد تر از آن، این است که قدرت پردازشی ۴۰۰۰ کیوبیتی کنترل شبکه زنجیره بلوک بیت کوین را کمتر از چند ساعت در دست می‌گیرد و این پایان آخرین سد دفاعی باقی مانده از دوران الکترونیکی شدن سیستم‌ها است.

البته بالا رفتن قدرت پردازشی تنها تهدید برای سیستم‌های در آستانه تحول دیجیتال نیست، بلکه هوش مصنوعی با قابلیت چند ریختگی که می‌تواند به بدافزارها بدهد، آن‌ها را از دید IDS ها مخفی کرده [18] و به دلیل کمک‌های فراوانی که به یک برنامه نویس ارائه می‌دهد، موانع نفر/ساعت قابل پیش بینی گذشته را برای یک مجرم سایبری از میان برمی‌دارد و به این ترتیب IBM، در مجموعه اخطارهای امنیت سایبری که برای سال ۲۰۲۴ منتشر کرده است از کاهش زمان تولید بدافزار جدید از ۶۰ روز در سال ۲۰۲۳ به تنها ۴ روز در سال ۲۰۲۴ خبر می‌دهد [19].

ولی همه این پیشرفت ها در فناوری که متاسفانه به خوبی توسط جامعه مجرم های سایبری مورد استفاده قرار گرفته است، به اندازه اینترنت اشیاء و قدرت پردازش توزیع شده ای که ارائه میدهد موجب نگرانی نیست. باید این انتظار را داشته باشیم که از این پس با اینترنت اشیاء هر شی جاندار یا بی جانی به یک مبدا بالقوه برای وقوع حمله سایبری از نوع Active یا Passive تبدیل شود. از قدرت پردازش توزیع شده میتوان به عنوان شناسنامه دنیایی پر از المان های دیجیتالی شده نام برد و آنرا در اولویت برنامه ریزی و طراحی سناریوی دفاعی قرار داد. ما در کشور به لطف استفاده گسترده افراد از انواع فیلترشکن در تلفن های همراه کارمندان در پشت فایروال سازمان‌ها یا تجربیاتی که از حمله سایبری به سیستم پرداخت الکترونیکی جایگاه‌های سوخت داشته‌ایم، عملا نسخه شبیه‌سازی شده آسیب‌های گسترده ای که توسعه اینترنت اشیاء می‌تواند بر زیر ساخت‌های قدیمی ما وارد کند را مرور کرده‌ایم [20].

به همین دلیل عقیده داریم طراحی سیستم های امنیتی بر اساس منطق قدیمی سرویس دهی سازمان‌ها که بر پایه رفتار Client-Server توسعه یافته است، دیگر کارایی ندارد و در دوران دیجیتالی شدن و توزیع شدگی، مساله پردازش مجرمانه داده‌ها در هر نقطه ای از خارج یا داخل لایه های امنیتی کلاسیک می‌تواند تبدیل به یک مبدا برای حملات Passive شده و داده های ارزشمند سازمان ها را در دسترس افراد Unauthorized قرار دهد. بنابراین پاسخ ما برای مقابله با نسل جدید تهدیدها در قالب طراحی یک مجموعه تست نفوذ به سبک تهدید های نوظهور است به نحوی که ضمن استفاده از جدید ترین ابزارهای نفوذ به سیستم‌ها، تلاش دارد در بیشتر مواقع وقوع یک حمله را بر اساس به روز ترین مقالات علمی و گزارش ها، جدی و قطعی فرض کرده و سعی دارد بیشتر انرژی تیم امنیتی را روی طراحی راهکار مقابله متمرکز کند. بنابراین مقابله با Advanced Persistence Threat ها با چنان حجم از پیچیدگی و مخفی کاری که پیشتر به بخش هایی از آن اشاره شده است، از طریق نسخه پیشرفته تری از آزمون های نفوذ مقدور خواهد بود که نام تست نفوذ بی‌رحمانه (تست پایدار بی رحمانه - Brute Persistence Test) را برای آن برگزیده‌ایم. در BPT مفاهیمی همچون DMZ و CMZ از بین می‌روند و هر فرد یا بخش از سازمان در هر لحظه می‌تواند نقش مهاجم به خود گرفته و سازمان را مورد آزمون جدی امنیتی قرار دهد.

اهداف

- آماده سازی/ ممیزی تصادفی مطابق با ISO-27000
- آماده سازی/ ممیزی تصادفی مطابق با NIST CSF
- آماده سازی/ آنالیز تست های نفوذ کلاسیک دوره ای
- پیاده سازی/ تدارک تست نفوذ بی‌رحمانه پایدار
- پیاده سازی/ تشکیل درخت دانش برای امنیت سایبری

مراحل

۱. تعیین سطح بلوغ امنیت کلاسیک سازمان
۲. اعمال حمله فرضی APT – بر اساس لایه های منطقی (چارت سازمانی)
۳. اعمال حمله فرضی APT – بر اساس لایه های فیزیکی (موقعیت سازمانی)
۴. تفسیر حمله فرضی APT به مجموعه آزمون های BPT
۵. طراحی دفاع متناظر با احتمال وقوع هر APT به تفکیک BPT
۶. درج نتایج در درخت دانش اختصاصی سازمان
۷. تعیین سطح بلوغ امنیت دیجیتال سازمان
۸. بازگشت به مرحله ۱

مزایا

- در شرایط کاملا ایده آل با مطابقت ۱۰۰٪ هر سازمان با بهترین استانداردها - از آنجایی که شرایط استاندارد موجود در مستندات در اختیار مجرمان سایبری نیز وجود دارد - همواره این ایراد بزرگ مشاهده می‌گردد که هکرها با تمرکز منابع و زمان روی نقص های هر استاندارد، طیف وسیعی از سازمان ها را از یک مسیر و به یکباره مورد حمله قرار دهند. ولی استقرار دفتر BPT در یک سازمان و هدایت آن به سمت بلوغ امنیت دیجیتال باعث می‌گردد تا هر سازمان ضمن حفظ شرایط استاندارد امنیت سایبری، به لایه های دفاعی تازه ای با تفاوت‌ها و ویژگی‌هایی اختصاصی مجهز شود که شبیه هیچ سازمان دیگری نیست. در نتیجه سازمانی که تحت BPT قرار دارد، ضمن حفظ شرایط interoperate ability با پروتکل ها و روش های استاندارد، در عمق دفاعی خود دارای تفاوت هایی خواهد بود که برای مجرم سایبری ناآشنا است، که همین امر به Security Resilience نهایی کل سازمان منتهی خواهد شد.
- یافتن حفره های امنیتی از طریق باگ باتنی شرایطی لازم اما ناکافی برای بلوغ امنیت دیجیتال است. دلیل این مهم به نحوه نگرش شخص باگ-هانتر به حرفه خود بر می‌گردد و تا مادامی که طیف وسیعی از کسب و کارها از آسیب پذیری سطح پایین و یکسان رنج ببرند و ایشان بتواند با گزارش آن‌ها به سادگی کسب درآمد کند، هرگز به دنبال یاد گیری

مهارت های پیشرفته تر نفوذ نخواهد رفت و همین امر سازمان‌ها را در برخورد با نفوذگر های با سطح یا زمینه مهارتی متفاوت به شدت آسیب پذیر می‌کند. ولی قرار گرفتن یک سازمان در معرض BPT اصولا تعیین سطح یا زمینه وقوع یک حمله پیشرفته را از دوش تیم آزمون‌گر برداشته و از ابتدا فرض را بر قرار گرفتن نفوذ گر BPT در موقعیت های نامحتمل می‌گذارد. در نتیجه سطح دانش نفوذگر از دید حمله BPT همواره Transparent (بی‌اهمیت) خواهد بود و همواره سازمان را برای بدترین سناریو ها آماده می‌کند.

- تعیین انگیزه (Incentives) هکرها از تدارک حمله به سازمان‌ها همواره بخش بسیار با اهمیت در تعیین اولویت های دفاعی مهندسین امنیت است. هکرهایی که به قصد کسب شهرت در میان سایر دوستان اقدام به نفوذ به سیستم‌ها می‌کنند، با هکرهایی که انگیزه های بزرگ مالی و اخاذی را دنبال می‌کنند، در کنار هکرهای دولتی، هکتیویست‌ها و در نهایت پژوهشگرانی که صرفا برای تست یک سیستم و نگارش مقاله اقدام به اجرای حمله می‌کنند هر کدام اهداف متفاوتی را در نظر می‌گیرند که به هیچ عنوان نمیتواند توسط مهندسین امنیتی که صرفا با انگیزه درآمد ثابت ماهیانه از طریق حقوق و دستمزد – پس از کسر مالیات – اقدام به تست نفوذ کلاسیک و باگ-هانتینگ می‌کنند پوشش داده شود. بنابراین شما در اینجا هم نیاز به تدارک همان طیف وسیع انگیزه برای مهندسین امنیتی دارید تا انواع اهداف در سازمان شما مورد آزمون قرار بگیرد. همانطور که مشاهده می‌گردد، این موقعیت غیر ممکن در واقع همان شکاف امنیتی هست که همواره مورد سوء استفاده هکر ها برای نفوذ به سازمان‌ها قرار گرفته و تحت هیچ شرایطی هم قابل پوشش دادن نخواهد بود، مگر با فرض وقوع موفق یک حمله به سبکی که BPT پیشنهاد داده و به این ترتیب انگیزه انواع مجرم سایبری از تدارک حمله را در نهایت شبیه سازی می‌کند.

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 روشی نوین با نام تست نفوذ بی‌رحمانه (BPT) و جدیدترین مطالعات و راه کارهای عملی به ذکر راه حل‌های نواقص فعلی در تست نفوذ و ایجاد دیدگاهی به‌روز در سازمان ها و آزمونگران 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?con tent.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-todeploy 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, "*Designand 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

[۱۱] حسن علی پور، طاهره نیری فرد، "بررسی مشکلات تست نفوذ با هدف بهبود روش های کنونی"، کنفرانس بین‌المللی وب پژوهی، ۱۳۹۴.

[12] - *https://corporatefinanceinstitute.com/resources/career-map/sell-side/capital-markets/dotcom-bubble/*
[13] - *https://doi.org/10.1038%2F530144a*
[14] - *https://www.nytimes.com/2015/09/27/technology/smaller-faster-cheaper-over-the-future-of-computer-chips.html?&moduleDetail=section-news-2&action=click&contentCollection=Business%20Day&region=Footer&module=MoreInSection&version=WhatsNext&contentID=WhatsNext&pgtype=article&_r=0*
[15] - *https://research.ibm.com/blog/quantum-roadmap-2033*
[16] - *https://eprint.iacr.org/2020/187.pdf*
[17] - *https://arxiv.org/pdf/2202.10982.pdf*
[18] - *https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware*
[19] - *https://www.youtube.com/watch?v=6TE0LovKQa4*
[20] - *https://sites.google.com/darkcell.se/www/sparrows*